
La Direttiva (UE)
2022/2555 NIS 2
e la Cybersecurity
AIIC

La Direttiva (UE) 2022/2555 NIS 2 e la Cybersecurity

Pubblicato da AIIC
Novembre 2024

Questo documento è il risultato di un progetto congiunto coordinato da Raffaella D'Alessandro e realizzato con il contributo di (in ordine alfabetico) Elio Antonelli, Stefano Aterno, Glauco Bertocchi, Alberto Caruso De Carolis, Raffaella D'Alessandro, Lucrezia Falciai. Luisa Franchina. Marilena Hyeraci, Paola Patriarca, Giorgio Pizzi, Fabio Rosa, Tommaso Ruocco, Andrea Testi, Maria Beatrice Versaci.
Si ringraziano i soci Gianluca Cipriani, Marianna Pedrazzi e Maria Beatrice Versaci per le attività di editing finale.

Gli autori desiderano ringraziare l'Associazione Italiana Esperti in Infrastrutture Critiche (AIIC) per il suo supporto e stimolo.

La presente versione del Rapporto rappresenta lo stato dell'arte alla data di pubblicazione.

Sommario

Indice delle tabelle

Introduzione (Stefano Aterno, Paola Patriarca)

La direttiva NIS2, pubblicata nella Gazzetta Ufficiale dell'Unione Europea il 27 dicembre 2022, rappresenta un significativo ed ulteriore passo avanti nella gestione della sicurezza informatica a livello comunitario, ampliando e sostituendo il campo di applicazione della precedente direttiva NIS del 2016. Questo nuovo quadro normativo nasce dall'esigenza di rispondere alle crescenti minacce cibernetiche, in un contesto digitale in costante evoluzione e sempre più interconnesso, nel quale si assiste ad un aumento esponenziale delle infrastrutture critiche dipendenti dalla tecnologia.

A distanza di quasi venti anni dalla relazione europea firmata dall'allora Segretario generale del Consiglio dell'UE e intitolata «Garantire sicurezza in un mondo in piena evoluzione», che per la prima volta trattava esplicitamente la "sicurezza informatica" (non solo la "sicurezza") in relazione al terrorismo e alla criminalità organizzata, è chiaro che sono stati fatti notevoli passi in avanti.

In Europa è maturata la consapevolezza di dover ampliare la normativa comunitaria nell'ambito della società digitale, includendo, oltre alla regolamentazione del mercato unico digitale, anche la tutela dei diritti degli utenti a garanzia di uno spazio cibernetico "*open, safe and secure*". A tale scopo, la direttiva NIS ha rappresentato un punto di svolta, costituendo il primo insieme di regole sulla sicurezza informatica a livello europeo e delineando un framework sovranazionale nel settore della cybersecurity.

Sull'onda di questa rapida trasformazione digitale della società, intensificata dalla crisi COVID-19, nel 2020 la Commissione europea ha definito una nuova strategia per l'Unione della sicurezza, che copre il periodo 2020-2025, allo scopo di promuovere la sicurezza per tutti coloro che vivono in Europa, nel rispetto dei valori e principi europei. In risposta a queste sfide, l'UE ha definito gli strumenti e le misure da sviluppare per garantire la sicurezza negli ambienti fisici e digitali mirando a politiche di sicurezza che riflettano l'evoluzione del panorama delle minacce, costruendo una resilienza duratura e sostenibile e coinvolgendo tutti i settori della società, dalle istituzioni europee ai governi, fino al settore privato e ai cittadini. Particolare attenzione è dedicata alla cybersicurezza, con l'UE chiamata a guidare gli sforzi per una digitalizzazione sicura, promuovendo standard di cybersicurezza di livello mondiale per i servizi essenziali e le infrastrutture critiche, oltre a sviluppare e applicare nuove tecnologie.

Nel frattempo, il conflitto tra Russia e Ucraina ha dimostrato che le infrastrutture critiche posso costituire veri e propri bersagli strategici e tattici, assumendo un ruolo cruciale nella determinazione dei conflitti, che non si limitano al mondo fisico, ma che interessano in maniera sempre più rilevante anche il cyberspazio.

Allo scopo di rafforzare la resilienza cibernetica dell'Unione, quindi, la direttiva NIS2 contribuisce logicamente ad arricchire in maniera sinergica il fitto quadro normativo europeo in materia di Cyber Security e Resilience delle Infrastrutture Critiche che comprende, tra gli altri, il Digital Operational Resilience Act (DORA), il Cybersecurity Act, il General Data Protection Regulation (GDPR) e la recente Direttiva sulla Resilienza delle infrastrutture critiche (CER, Critical Entities Resilience).

È fondamentale ridurre il rischio che un'infrastruttura critica possa essere compromessa da vulnerabilità interne o derivanti dalla catena di approvvigionamento con gravi ripercussioni per la sicurezza economica e sociale dell'intera Unione. Proprio in questa direzione, la direttiva NIS2 ha ampliato l'ambito di applicazione delle nuove disposizioni, obbligando un numero maggiore di attori ed entità, anche PMI, a adottare misure avanzate di gestione del rischio cyber.

È auspicabile che la definizione di standard di sicurezza comuni a tutti coloro che operano all'interno degli Stati membri, favorisca una risposta coordinata ed efficiente alle minacce cibernetiche e il rafforzamento della cooperazione e collaborazione tra agenzie, istituzioni, Stati e privati, con l'obiettivo di raggiungere rapidamente gli obiettivi di aumentare il livello di sicurezza cibernetica in Europa e rafforzare la capacità dell'Unione di affrontare le crisi cibernetiche in modo collettivo.

Questo Rapporto si propone di analizzare in dettaglio le principali novità introdotte dalla NIS 2, valutarne l'impatto sui vari settori interessati, fornire implicazioni pratiche e suggerimenti operativi per la valutazione dei rischi, offrendo approfondimenti sul tema della gestione di cybersecurity in diverse realtà.

1 Il Decreto di recepimento della Direttiva NIS 2 in Italia e l'importanza della cybersecurity nella catena di approvvigionamento (Maria Beatrice Versaci).

Con il D.Lgs 138/2024, pubblicato in Gazzetta Ufficiale il 1° ottobre 2024, l'Italia ha recepito ufficialmente la Direttiva NIS 2, contestualizzando le disposizioni imposte dall'UE a livello nazionale.

La norma, in vigore a partire dal 16 ottobre 2024, introduce un sistema di misure di sicurezza cibernetica avanzate che mira a proteggere in modo omogeneo i settori chiave per il funzionamento del Paese e dell'Unione, come previsto dalla Direttiva.
Attraverso una strutturazione normativa specifica, il decreto impone obblighi differenziati a "soggetti essenziali" e "soggetti importanti", stabilendo requisiti rigorosi per la protezione di operatori strategici come energia, sanità, trasporti, ICT e finanza, che rappresentano pilastri dell'economia e della sicurezza nazionale e costituiscono la prima categoria, e operatori appartenenti a settori come la gestione dei rifiuti e l'industria alimentare, i quali, pur essendo meno critici, devono comunque adottare misure adeguate per mitigare rischi di natura cibernetica. Questa classificazione orienta l'allocazione efficiente delle risorse di sicurezza, permettendo di indirizzare le difese cibernetiche con un approccio proporzionato e mirato. Alle entità viene richiesto di adottare misure di gestione del rischio con l'obbligo di garantire la continuità operativa e la sicurezza della supply chain, tutto ciò attraverso la predisposizione di una strategia coordinata a livello nazionale per ottimizzare le risorse di sicurezza, adattando le misure di prevenzione e risposta agli incidenti in funzione della rilevanza del settore coinvolto, in modo da garantire che gli investimenti nella cibersicurezza siano mirati, efficienti e sostenibili.
Dal punto di vista operativo, il decreto favorisce una gestione efficace e centralizzata delle segnalazioni di rischio enfatizzando la cooperazione tra le autorità competenti attraverso protocolli di coordinamento multilaterale, con il coinvolgimento di enti nazionali quali l'Agenzia per l'Italia Digitale, il Garante per la protezione dei dati personali e lo CSIRT (Computer Security Incident Response Team) italiano, designato come nodo centrale per la gestione delle vulnerabilità e lo scambio informativo a livello nazionale e comunitario. In ambito europeo, l'Italia conferma invece la partecipazione alla rete EU-CyCLONe, contribuendo alla gestione integrata delle crisi informatiche. Inoltre, il decreto prevede la certificazione di prodotti TIC e specifiche procedure di vigilanza da parte dell'Autorità nazionale NIS, che ha il compito di monitorare e ispezionare i soggetti essenziali e importanti, imponendo sanzioni amministrative per le inadempienze accertate. Sono previste misure esecutive quali audit e scansioni di sicurezza, la pubblicazione delle violazioni e, in ultima istanza, sanzioni pecuniarie proporzionate alla criticità dell'operatore, con l'obiettivo di proteggere efficacemente le infrastrutture nazionali e allinearsi ai massimi standard di sicurezza europea.

Se la costruzione di una rete di collaborazione, nazionale ed europea, tra Istituzioni è un elemento centrale per il rafforzamento della sicurezza informatica in tutti i paesi dell'unione, tanto più lo è il riconoscere l'importanza che ricopre una seconda rete: quella delle interdipendenze tra le infrastrutture critiche di questi paesi. Interdipendenze che rappresentano un elemento di vulnerabilità e, al contempo, un'opportunità per il potenziamento della sicurezza nazionale ed europea. In questo senso, un aspetto del Decreto legislativo 138/2024 su cui porre l'accento è proprio il fatto che esso preveda un approccio alla cibersicurezza il quale considera l'intera catena di fornitura soggiacente ai settori cosiddetti ad alta criticità, riconoscendo di fatto come imprescindibile l'adozione di misure strutturali che considerino l'interconnessione sistemica delle infrastrutture essenziali. A questo proposito, già nella definizione dell'ambito di applicazione della norma, si includono all'interno di esso i soggetti identificati come "elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti" indipendentemente dalle dimensioni, come specificato nell'art.3 comma 9 punto *f* e anche nel comma 10:

10. Il presente decreto si applica, infine, indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri:

a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;

b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;

c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale;

d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

Mentre l'articolo 9 comma 3 del Decreto stabilisce che:

3. Nell'ambito della strategia nazionale per la cybersicurezza, sono previste, inoltre, le seguenti misure strategiche:

a) la sicurezza informatica *nella catena di approvvigionamento dei prodotti e dei servizi TIC* utilizzati dai soggetti per la fornitura dei loro servizi;

[…]

La sicurezza informatica dell'intera catena di fornitura è un elemento tanto più rilevante in un contesto in cui la crescente digitalizzazione ha permesso di stabilire, oltre alle già presenti interconnessioni di tipo funzionale, altrettanti legami tra i settori critici che passano invece attraverso la rete internet. La dipendenza digitale introduce una nuova dimensione di vulnerabilità poiché, con l'incremento dell'automazione e della digitalizzazione, la maggior parte dei processi interni e intersettoriali si fonda su infrastrutture ICT condivise. Questo doppio filo che connette il network infrastrutturale essenziale per il funzionamento del Sistema Paese, si configura come uno degli asset più critici da tutelare, proprio nella misura in cui funge da punto di raccordo tra molteplici settori sensibili. Una violazione in un segmento della catena di fornitura, pertanto, può propagarsi rapidamente, incidendo non solo sui singoli settori ma generando effetti a cascata su un sistema intero.

Infatti, come si legge nel considerando 3 della Direttiva:

I sistemi informatici e di rete occupano ormai una posizione centrale nella vita di tutti i giorni, con la rapida trasformazione digitale e l'interconnessione della società, anche negli scambi transfrontalieri. Ciò ha portato a un'espansione del panorama delle minacce informatiche, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. […] Pertanto la preparazione e l'efficacia della cibersicurezza sono oggi più che mai essenziali per il corretto funzionamento del mercato interno. Inoltre, la cibersicurezza è un fattore abilitante fondamentale per molti settori critici, affinché questi possano attuare con successo la trasformazione digitale e cogliere appieno i vantaggi economici, sociali e sostenibili della digitalizzazione.

Così come enfatizzato anche nel considerando 56 in merito all'importanza di includere, all'interno delle strategie di cibersicurezza dei singoli Stati UE anche le piccole e medie imprese:

Tali attacchi della catena di approvvigionamento non solo hanno un impatto sulle piccole e medie imprese e sulle loro operazioni isolatamente, ma possono anche avere un effetto a cascata su attacchi più gravi nei confronti di soggetti di cui sono fornitori.

La propagazione degli effetti a cascata di un incidente a tutta la rete rappresenta uno dei rischi più rilevanti, come espresso chiaramente anche nel considerando 80 della Direttiva:

Affrontare i rischi derivanti dalla catena di approvvigionamento di un soggetto e dalla sua relazione con i fornitori, ad esempio i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti e gli editori di software, è particolarmente importante data la prevalenza di incidenti in cui i soggetti sono stati vittime di attacchi informatici e in cui i responsabili di atti malevoli sono stati in grado di compromettere la sicurezza dei sistemi informatici e di rete di un soggetto sfruttando le vulnerabilità che interessano prodotti e servizi di terzi. I soggetti essenziali e importanti dovrebbero pertanto valutare e tenere in considerazione la qualità e la resilienza complessive dei prodotti e dei servizi, delle misure di gestione dei rischi di cibersicurezza in essi integrate e delle pratiche di cibersicurezza dei loro fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. In particolare, i soggetti essenziali e importanti dovrebbero essere incoraggiati a integrare misure di gestione dei rischi di cibersicurezza negli accordi contrattuali con i loro fornitori e fornitori di servizi diretti. Tali soggetti potrebbero prendere in considerazione i rischi derivanti da altri livelli di fornitori e fornitori di servizi.

Il decreto legislativo italiano risponde pienamente a queste esigenze attraverso gli articoli sopra citati, in cui la tutela della supply chain è estesa in modo capillare anche ai fornitori terzi e partner digitali, spesso visti come anelli vulnerabili della catena stessa. Questa attenzione particolare riflette l'esigenza di un modello di sicurezza multi-livello, in cui ciascun operatore essenziale non agisce in isolamento

ma in una rete coordinata di protezione e prevenzione. All'interno di questa rete si inserisce anche l'Agenzia per la cybersicurezza nazionale, designata come Autorità nazionale competente NIS, la quale partecipa all'elaborazione delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche (art.18, par.4);

La sicurezza della catena di approvvigionamento è annoverata anche tra gli elementi da tenere in considerazione nel mettere in atto le misure tecniche, operative e organizzative volte a proteggere i sistemi informativi e di rete che tanto i soggetti essenziali quanto quelli importanti sono tenuti ad applicare (art 24). Nel valutare tali misure, questi considerano le vulnerabilità specifiche per ogni diretto fornitore, nonché le pratiche di sicurezza informatica che i fornitori hanno implementato, conducendo una valutazione olistica e continua delle vulnerabilità in grado di stimolare lo sviluppo di una resilienza cyber proattiva, in cui la prevenzione e la risposta agli incidenti non sono relegate a singoli eventi ma fanno parte di una strategia di risk management continuativa.

Questo modello spinge alla costruzione di una rete di sicurezza in cui ciascun nodo, indipendentemente dalle dimensioni, diventa un punto di controllo essenziale per arginare i rischi connessi alla crescente digitalizzazione e alle interdipendenze sistemiche. Tale approccio integrato consente di affrontare non solo le minacce immediatamente percepibili, ma anche di attenuare il cosiddetto rischio a cascata, che vede un singolo incidente propagarsi attraverso l'intero ecosistema di servizi interdipendenti. La valutazione continua delle vulnerabilità e la valorizzazione della resilienza di ogni operatore, dal grande fornitore ai piccoli subfornitori digitali, sostengono una strategia di cybersecurity che mira non tanto a isolare gli attori della rete quanto a connetterli in un sistema di difesa diffusa e dinamica, dove la sinergia è la chiave per il mantenimento della stabilità. In quest'ottica, il decreto rafforza non solo il profilo tecnico della sicurezza ma incoraggia lo sviluppo di una cultura del rischio condivisa.

2 Panoramica dell'evoluzione normativa europea applicabile ai settori critici (Alberto Caruso de Carolis).

2.1 La resilienza informatica

L'Unione europea ha lavorato su vari fronti per promuovere la resilienza informatica, prevedendo nel tempo, norme per la salvaguardia delle comunicazioni e dei dati al fine di mantenere la società e l'economia *online* sicure.

Qui di seguito una elencazione dei provvedimenti adottati:

a) Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, del 7.2.2013[1].

b) Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004 (GU L 165, del 18.6.2013, pagg. 41-58)[2].

c) Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pagg. 8-14)[3].

d) Decisione 2013/488/UE del Consiglio, del 23 settembre 2013, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 274 del 15.10.2013, pagg. 1-50)4.

e) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pagg. 73-114)[5].

f) Documento di lavoro dei servizi della Commissione — Valutazione della strategia dell'unione del 2013 per la sicurezza delle reti e dei sistemi informativi, del 13.9.2017[6].

g) Comunicazione congiunta al Parlamento europeo e al Consiglio - Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, del 13.9.2017[7]].

h) Comunicazione della Commissione al Parlamento europeo e al Consiglio "Sfruttare al meglio le reti e i sistemi informativi — verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", del 4.10.2017[8].

[1] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A52013JC0001.
[2] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32013R0526.
[3] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32013L0040.
[4] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A02013D0488-20140426.
[5] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A02014R0910-20140917.
[6] https://commission.europa.eu/about-european-commission/service-standards-and-principles/ethics-and-good-administration/good-administration_en.
[7] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A52017JC0450.
[8] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A52017DC0476.

i) Raccomandazione (UE) 2017/1584 del 13 settembre 2017 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239, del 19.9.2017, pagg. 36-58)[9].

j) Decisione di esecuzione (UE) 2017/179 del 1° febbraio 2017 che stabilisce le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione, a norma dell'articolo 11, paragrafo 5, della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 28 del 2.2.2017, pagg. 73-77)[10].

k) Regolamento di esecuzione (UE) 2018/151, del 30 gennaio 2018, recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente (GU L 26 del 31.1.2018, pagg. 48-51)[11].

2.2 La Direttiva NIS (Network and Information Security)

La Direttiva NIS si applica ai settori e alle infrastrutture critiche, con lo scopo di migliorare le difese delle infrastrutture critiche degli Stati europei. Essa, sul cui testo finale fu trovato un accordo tra la fine del 2015 e l'inizio del 2016, ha rappresentato un punto di svolta rilevante. Recepita in Italia nel maggio del 2018, ha introdotto per certi settori l'adozione obbligatoria di misure di sicurezza informatica e sanzioni per i soggetti inadempienti.

Sono state rese altresì obbligatorie le notifiche degli incidenti cyber, anche per costituire prime raccolte di dati, opportunamente anonimizzati, da analizzare approfonditamente al fine di conoscere meglio la tipologia degli incidenti/attacchi e fornire elementi utili ai decisori politici per la loro gestione, non solo a livello nazionale ma anche transfrontaliero, e quindi europeo.

Nel dicembre 2020 la Commissione europea e l'European External Action Service (EEAS) hanno presentato una nuova strategia dell'UE in materia di cibersicurezza. L'obiettivo di questa strategia è rafforzare la resilienza dell'Europa alle minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili e affidabili. La nuova strategia contiene proposte concrete per l'impiego di strumenti normativi, di investimento e politici. Il 22 marzo 2021 il Consiglio ha adottato conclusioni sulla strategia per la cybersicurezza, sottolineando che la Cybersecurity è essenziale per costruire un'Europa resiliente, verde e digitale. I ministri dell'UE hanno fissato come obiettivo fondamentale il conseguimento dell'autonomia strategica preservando allo stesso tempo un'economia aperta. Ciò include il rafforzamento della capacità di compiere scelte autonome nel settore della cibersicurezza, con l'obiettivo di rafforzare la leadership digitale e le capacità strategiche dell'UE.

2.3 La Direttiva NIS 2: le misure per un livello comune elevato di cibersicurezza nell'Unione.

Rilevato che le minacce alla Cybersecurity sono quasi sempre transfrontaliere e che un attacco informatico alle strutture critiche di un paese può colpire l'UE nel suo complesso, si è maturata la necessità di proseguire nel solco tracciato alla direttiva NIS. I paesi dell'UE devono poter disporre di forti organismi governativi che supervisionino la cibersicurezza nel loro paese e che collaborino con le loro controparti in altri Stati membri condividendo le informazioni. Ciò è particolarmente importante per i settori critici per le nostre società. La direttiva sulla sicurezza delle reti e dei sistemi

[9] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32017H1584.
[10] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32017D0179.
[11] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018R0151

informativi (direttiva NIS), che tutti i paesi hanno recepito, garantisce la creazione e la cooperazione di tali organismi governativi. La direttiva è stata riesaminata alla fine del 2020. A seguito del processo di riesame, il 16 dicembre 2020 la Commissione ha presentato la proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (cd. direttiva NIS 2).

2.4 Il Cyber Security Act (CSA).

La nuova strategia[12] unionale per la sicurezza cibernetica trova tra i suoi pilastri principali, accanto all'ormai celebre direttiva NIS, il Regolamento (UE) n. 2019/881, altrimenti conosciuto come Cybersecurity Act (CSA)

Al fine di rafforzare la sicurezza informatica dei prodotti ICT e dei servizi digitali in Europa, la Commissione europea ha anche introdotto nel 2019 il Cyber security Act che interviene principalmente su due aspetti: il rafforzamento del mandato dell'ENISA, che viene ad assumere un ruolo primario nella identificazione degli attacchi, e la definizione del quadro europeo delle certificazioni in ambito sicurezza informatica, ovvero l'individuazione di standard – validi in tutto il territorio UE – con cui valutare se prodotti e servizi IT siano effettivamente sicuri e certificabili.

Si tratta di una cornice normativo-regolamentare europea per la certificazione della sicurezza informatica di prodotti, servizi e processi ICT.

Tale definizione di standard comuni, validi in tutti gli Stati membri, ha lo scopo di facilitare lo scambio e il commercio di tutti prodotti ICT all'interno dell'UE.

Il testo definitivo del cosiddetto Cybersecurity Act è stato pubblicato sulla Gazzetta ufficiale dell'Unione europea L 151/15 del 7 giugno scorso: la nuova legge si chiama ufficialmente Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 alla conclusione di un lungo iter approvativo iniziato nel 2017 con la presentazione del testo iniziale del Cybersecurity Act da parte della Commessione europea.

2.5 Il Regolamento Dora.

Il Digital Operational Resilience Act, o DORA, è un regolamento dell'Unione Europea (UE) che stabilisce un framework vincolante e completo riguardante la gestione del rischio delle tecnologie di informazione e comunicazione (ICT) per il settore finanziario dell'UE.

Il regolamento DORA stabilisce gli standard tecnici che le entità finanziarie e i loro fornitori critici di servizi tecnologici di terze parti devono implementare nei propri sistemi ICT entro il 17 gennaio 2025.

Il Regolamento relativo alla resilienza operativa digitale per il settore finanziario che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014". riprende il concetto di resilienza operativa già citato in precedenza in un documento emesso dal Basel *Committee on Banking Supervision: Principles for Operational Resilience*, pubblicato nella sua versione definitiva nel marzo 2021.

Il provvedimento entrerà ufficialmente in vigore il prossimo 27 giugno 2025 e, trattandosi di un Regolamento, sarà immediatamente esecutivo in tutti gli Stati membri senza necessità di interventi attuativi da parte dei legislatori nazionali.

2.6 Il Cyber Resilience Act (CRA).

Il *Cyber Resilience Act* (CRA) mira a salvaguardare i consumatori e le imprese che acquistano o utilizzano prodotti o software con un componente digitale. La legge vedrebbe caratteristiche di

[12] https://www.cybersecurity360.it/legal/strategia-ue-per-la-cyber-security-e-armonizzazione-normativa-obiettivi-e-possibili-conflitti/.

sicurezza inadeguate diventare un ricordo del passato con l'introduzione di requisiti di cibersicurezza obbligatori per i produttori e i rivenditori di tali prodotti, con questa protezione che si estende per tutto il ciclo di vita del prodotto. In esso si trova la piena attuazione del principio della cosiddetta *"security by design"*, ovvero la presa in considerazione della sicurezza informatica fin dagli stadi iniziali della progettazione dei prodotti ICT. Infatti, il sistema comune di certificazione che verrà introdotto a livello europeo dovrebbe incentivare una maggiore attenzione alla sicurezza informatica di prodotti e servizi digitali, facilitando al contempo l'accesso delle aziende produttrici ai mercati degli altri paesi europei". Il problema affrontato dal regolamento è duplice. Il primo è il livello inadeguato di sicurezza informatica inerente a molti prodotti, o gli aggiornamenti di sicurezza inadeguati di tali prodotti e software. La seconda è l'incapacità dei consumatori e delle imprese di determinare attualmente quali prodotti sono *"cybersicuri"* o di configurarli in modo da garantire che la loro sicurezza informatica sia protetta.

Il Cyber Resilience Act garantirà:

l) norme armonizzate per l'immissione sul mercato di prodotti o software dotati di una componente digitale;
m) un quadro di requisiti di cibersicurezza che disciplinano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti, con obblighi da rispettare in ogni fase della catena del valore;
n) l'obbligo di fornire il dovere di diligenza per l'intero ciclo di vita di tali prodotti.

Con l'entrata in vigore del regolamento, i software e i prodotti connessi a Internet recano la marcatura CE per indicare che sono conformi alle nuove norme. Richiedendo ai produttori e ai rivenditori di dare priorità alla sicurezza informatica, i clienti e le imprese avrebbero il potere di fare scelte meglio informate, fiduciosi delle credenziali di sicurezza informatica dei prodotti con marchio CE.

Il regolamento è stato annunciato nella strategia dell'UE per la cibersicurezza del 2020 e integra altre normative in questo settore, in particolare il quadro NIS2.

Si applicherà a tutti i prodotti collegati direttamente o indirettamente a un altro dispositivo o rete, ad eccezione di esclusioni specifiche quali software o servizi open source già disciplinati dalle norme esistenti, come nel caso dei dispositivi medici, dell'aviazione e delle automobili.

2.7 Il Cyber Solidarity Act.

La Commissione ha proposto un regolamento relativo all'atto dell'UE sulla *cybersolidarietà* per rafforzare la solidarietà dell'UE e le azioni coordinate per individuare, preparare e rispondere efficacemente alle crescenti minacce e incidenti di cibersicurezza. Il *Cyber Solidarity Act*[13], finanziato con 1,1 miliardi di euro, di cui circa due terzi provenienti dal bilancio dell'UE, introduce:

o) un *European Cybersecurity Alert System,* un network europeo di Cyber Hubs nazionali e transfrontalieri. I *Cyber Hub* sono entità in grado di rilevare, aggregare e analizzare dati e informazioni rilevanti per le minacce e gli incidenti informatici sfruttando strumenti all'avanguardia, come l'AI. Agendo nell'ambito del sistema europeo di allerta per la cybersicurezza, saranno in grado di fornire segnalazioni tempestive a livello transfrontaliero.
p) un meccanismo di revisione degli incidenti di sicurezza informatica per rafforzare la preparazione testando le entità che operano in settori critici, tra cui l'assistenza sanitaria, i trasporti, l'energia e altri, per individuare potenziali vulnerabilità e altre azioni di preparazione, come corsi di formazione ed esercitazioni. L'ENISA dovrebbe presentare una relazione che includa gli insegnamenti tratti e le raccomandazioni.

[13] https://digital-strategy.ec.europa.eu/en/library/eu-cyber-solidarity-act-factsheet.

q) su richiesta della Commissione o di EU-CyCLONe, l'ENISA dovrebbe riesaminare e valutare uno specifico incidente di cybersicurezza significativo o su larga scala. Si dovrebbe costituire gradualmente una riserva dell'UE per la cibersicurezza con servizi di risposta agli incidenti da parte di fornitori affidabili pronti a intervenire, su richiesta di uno Stato membro, delle istituzioni, degli organi e delle agenzie dell'UE o di paesi terzi associati al *Digital Europe Programme*, in caso di incidenti di cibersicurezza significativi e su larga scala Fornire sostegno finanziario per l'assistenza tecnica reciproca tra le autorità nazionali degli Stati membri.

r) fornirà sostegno finanziario per l'assistenza tecnica reciproca tra le autorità nazionali.

2.8 La Cyber Defence[14].

Il 10 novembre 2022 la Commissione e l'alto rappresentante hanno presentato una comunicazione congiunta su una politica dell'UE in materia di *cyber defence* per affrontare il deterioramento del contesto di sicurezza a seguito del conflitto in Ucraina e rafforzare la capacità dell'UE di proteggere i suoi cittadini e le sue infrastrutture. La politica dell'UE in materia di *cyber defence* si basa su quattro pilastri che coprono un'ampia gamma di iniziative che aiuteranno l'UE e gli Stati membri a essere in grado di individuare, scoraggiare e difendersi meglio dagli attacchi informatici:

1. agire insieme per rafforzare la *cyber defence* dell'UE,

2. proteggere l'ecosistema della difesa,

3. investire nelle capacità di difesa informatica,

4. collaborare per affrontare le sfide comuni.

La nuova politica prevede investimenti in capacità di *cyber defence* a tutto spettro e rafforzerà il coordinamento e la cooperazione tra le comunità informatiche militari e civili dell'UE. Rafforzerà la cooperazione con il settore privato e una gestione efficiente delle crisi informatiche all'interno dell'Unione. La nuova politica contribuirà inoltre a ridurre le nostre dipendenze strategiche nelle tecnologie informatiche critiche e a rafforzare la base industriale tecnologica di difesa europea (EDTIB). Stimolerà la formazione, attraendo e trattenendo i talenti informatici. L'UE coopera nel settore della difesa nel cyberspazio attraverso le attività della Commissione europea, del Servizio europeo per l'azione esterna, dell'Agenzia europea per la difesa, dell'ENISA e dell'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol).

[14] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

3 Aspetti generali della Direttiva NIS2 (Raffaella D'Alessandro).

3.1 Generalità.

La Direttiva NIS2, pubblicata nella Gazzetta Ufficiale dell'Unione Europea il 27 dicembre 2022 ed entrata in vigore il 16 gennaio 2023, esprime l'obiettivo di raggiungere un livello comune elevato di cybersicurezza tra gli Stati Membri, migliorando la capacità di garantire uniformità ed efficacia nell'applicazione, e quindi di garantire un'effettiva protezione per la vita sociale ed economica dell'Unione. La normativa impone, in particolare, obblighi di cybersicurezza stringenti in capo a un'ampia platea di organizzazioni operanti in settori ritenuti critici per il funzionamento della società europea.

La Direttiva NIS 2 ha aggiornato la precedente versione mantenendo il medesimo obiettivo – ossia garantire un livello comune elevato di sicurezza cibernetica all'interno dei confini dell'Unione europea – e rafforzando alcuni obblighi a carico degli Stati membri e di coloro che saranno soggetti al suo ambito di applicazione.

I principali elementi di novità possono essere sintetizzati nei seguenti punti:

1. riorganizzazione del sistema istituzionale di gestione delle tematiche relative alla sicurezza cibernetica;
2. rafforzamento delle misure per la gestione dei rischi per la sicurezza cibernetica e razionalizzazione delle misure;
3. estensione dei concetti di gestione del rischio e di valutazione delle vulnerabilità a tutta la supply chain;
4. misure di gestione dei rischi di cybersecurity e responsabilità dell'organo di gestione;
5. razionalizzazione degli obblighi di notifica;
6. information sharing.

La Direttiva NIS2 sostituirà quindi la precedente Direttiva NIS, che abrogherà, a decorrere dal 18 ottobre 2024, con l'obiettivo di affrontare un panorama di minacce mutato radicalmente e ovviare, al tempo stesso, alle problematiche che hanno impedito alla Direttiva NIS di ottenere i risultati sperati.

La Direttiva è entrata in vigore il 17 gennaio 2023, ma gli Stati membri avranno l'obbligo di adottare e pubblicare gli atti normativi per recepirla entro e non oltre il 17 ottobre 2024 (Art,41).

Il presente studio intende fornire indicazioni di natura generale riguardo la Direttiva NIS2 e indicazioni puntuali per supportare l'adozione delle Misure di Sicurezza previste.

4 Ambito di applicazione (Marilena Hyeraci e Lucrezia Falciai).

4.1 Ambito di applicazione: a cosa e a quali soggetti si applica.

4.1.1 Ampliamento dell'ambito di applicazione.

La Commissione europea ha riconosciuto[15] che la Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS) ha contribuito a migliorare le capacità di cybersecurity degli Stati membri attraverso l'obbligo di adottare strategie nazionali in materia e nominare autorità competenti. Inoltre, il testo normativo punta a rafforzare la cooperazione tra gli Stati e a migliorare la resilienza di soggetti pubblici e privati che operavano nei sette settori identificati come essenziali (energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali) e in tre servizi digitali (mercati online, motori di ricerca online e servizi di cloud computing). Dunque, dall'entrata in vigore della Direttiva NIS sono stati compiuti significativi progressi in materia di sicurezza cibernetica.

Considerati da una parte i passi in avanti fatti con la Direttiva NIS e dall'altra parte quelli ancora necessari per migliorare ulteriormente le capacità di resilienza e di risposta agli incidenti dei soggetti considerati critici il testo è stato aggiornato, circa 6 anni dopo la pubblicazione.

Infatti, sebbene gli obiettivi conseguiti attraverso l'implementazione della Direttiva NIS siano stati numerosi, la Commissione europea ha identificato anche alcuni limiti, in larga parte legati al mutamento e all'ampliamento del panorama delle minacce. Più nello specifico, tra le principali problematiche riscontrate vi sono il basso livello di resilienza cibernetica delle imprese e le differenze di applicazione riscontrate tra i diversi Stati membri, nonché tra i vari settori soggetti all'ambito di applicazione della normativa. Inoltre, un'ulteriore criticità era rappresentata dal basso livello di consapevolezza comune e, di conseguenza, dall'assenza di una risposta collettiva.

A tal fine, la Direttiva NIS 2 ha ampliato l'ambito di applicazione della sua precedente versione includendo nuovi settori anche alla luce del loro grado di digitalizzazione e interconnessione. La Direttiva NIS 2 ha espressamente ricompreso nel suo ambito di applicazione anche le pubbliche amministrazioni e, in particolare, quelle centrali e quelle regionali.

Inoltre, nell'ampliare il novero dei soggetti interessati, ha valutato anche quanto essi fossero essenziali per l'economia e la società, introducendo delle soglie di grandezza poiché, secondo il legislatore, tale criterio contribuirebbe ad eliminare le differenze di applicazione tra gli Stati e a garantire la certezza del diritto. Ciò implica che tutte le grandi e medie imprese che operano nei settori identificati negli allegati I (settori ad alta criticità) e II (settori critici) saranno soggette alla Direttiva NIS 2. La norma lascia altresì un margine di discrezionalità agli Stati membri sulla possibilità di identificare imprese più piccole che abbiano comunque un elevato profilo di rischio e che, quindi, debbano essere soggette all'applicazione della nuova Direttiva.

Nello strutturare il framework di soggetti destinatari delle disposizioni della Direttiva NIS 2, il legislatore elimina la distinzione tra operatori di servizi essenziali e fornitori di servizi digitali presente nella precedente versione, poiché essa si è rivelata obsoleta. Ai fini della nuova normativa, le imprese saranno classificate sulla base della loro importanza e divise in due categorie: i soggetti essenziali e i soggetti importanti. A ciascuna di queste categorie si applicherà un regime di esecuzione e di vigilanza differente per garantire un corretto bilanciamento tra i requisiti e gli obblighi basati sui rischi e gli oneri amministrativi della vigilanza.

15 Cfr. Commissione Europea, Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, Bruxelles 16 dicembre 2020.

In aggiunta a quanto sopra delineato, la normativa ha rafforzato e ottimizzato i requisiti di sicurezza e di notifica per le società imponendo, in linea di continuità con le principali normative in materia di cybersecurity, un approccio basato sulla gestione del rischio. Ciò ha comportato una più precisa regolamentazione dei processi di notifica degli incidenti, del contenuto della comunicazione e delle tempistiche.

4.1.2 Criteri di identificazione dei soggetti a cui si applica.

Alla luce di quanto sopra, è possibile scendere nel merito dei criteri indicati dalla normativa per identificare i soggetti a cui essa si applica.

Il primo attiene al settore di operatività. Gli allegati I e II alla Direttiva NIS 2 identificano rispettivamente i settori considerati ad alta criticità, come, ad esempio, quello dell'energia e dei trasporti, e quelli critici, come quello della gestione dei rifiuti o della fabbricazione. Saranno soggetti all'ambito di applicazione della normativa in analisi anzitutto i soggetti che operano in tali settori.

Agli operatori così identificati, dovrà poi essere applicato il secondo criterio della soglia di dimensione. Dovranno osservare le disposizioni della Direttiva NIS 2 i soggetti pubblici e privati che operano nei settori ad alta criticità e critici e che siano almeno medie imprese. Per mera completezza si ricorda che le medie imprese sono quelle che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR.

Un elemento utile sulla quale si sofferma il testo della Direttiva NIS 2 e che, invece, non era stato affrontato nella sua precedente versione è quello delle società collegate o "partner". A tal proposito la norma prevede che gli Stati membri possano tenere conto del grado di dipendenza dalle imprese partner o collegate in termini di sistemi informatici e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce al fine di valutare se esso possa essere realmente considerato una media impresa. Dunque, gli Stati membri possono anche decidere di tenere in considerazione solo i dati della singola impresa e non quelli dell'intero gruppo.

Tuttavia, il criterio della soglia di dimensione ha alcune eccezioni. Anzitutto, il considerando 7 prevede che gli Stati membri siano tenuti ad includere nell'ambito di applicazione della Direttiva NIS 2 anche piccole o micro imprese che abbiano un ruolo chiave per la società, l'economia o particolari settori.

Inoltre, un ulteriore elemento che potrà essere tenuto in considerazione per derogare al criterio della soglia di dimensione è la rilevanza delle attività prestate. Nello specifico, potranno essere tenuti ad osservare le disposizioni della Direttiva NIS 2 indipendentemente dalla propria dimensione anche quei soggetti che operano nei settori ad alta criticità e critici qualora:

- I servizi siano forniti da:
    - fornitori di reti di comunicazione elettroniche pubbliche o servizi di comunicazione elettronica accessibili al pubblico;
    - prestatori di servizi di fiducia;
    - registri dei nomi a dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio.
    - tutti quei soggetti che siano gli unici fornitori nello stato membro di servizi essenziali per il mantenimento di attività sociali o economiche fondamentali;
    - una perturbazione del servizio possa avere un impatto significativo sulla sicurezza pubblica, sull'incolumità pubblica o sulla salute pubblica;
    - una perturbazione del servizio possa comportare un rischio sistemico significativo nei settori in cui potrebbe avere un impatto transfrontaliero;

- il soggetto sia critico alla luce della sua particolare importanza a livello nazionale regionale per uno specifico settore o servizio;
- sia un ente della pubblica amministrazione centrale o regionale. in tale ultimo caso lo stato membro dovrà effettuare una valutazione del rischio volta a verificare che una perturbazione dei servizi erogati potrebbe avere un impatto significativo su attività sociali o economiche critiche. l'assoggettamento delle pubbliche amministrazioni locali e degli istituti di istruzione che svolgano attività di ricerca critiche è invece rimessa alla discrezionalità degli stati membri;
- il soggetto fornisca servizi di registrazione dei nomi a dominio.

- Come anticipato nella sezione precedente, la Direttiva NIS 2 effettua una ulteriore distinzione tra i soggetti essenziali e quelli importanti in funzione della loro rilevanza per il settore, della dimensione e del tipo di servizi che erogano. Rientrano tra i primi:
  - tutti coloro che operano in settori ad alta criticità e che superano le soglie previste per le medie imprese;
  - i prestatori di servizi fiduciari qualificati, i registri di nomi di dominio di primo livello e i prestatori di servizi di DNS ("Domain Name System");
  - fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerino medie imprese;
  - le pubbliche amministrazioni centrali;
  - tutti i soggetti che operano in settori ad alta criticità o critici che siano stati identificati come essenziali dallo Stato membro, ad esempio, in quanto unici fornitori di un determinato servizio;
  - i soggetti considerati critici ai sensi della Direttiva (UE) 2022/2557 (cosiddetta "Direttiva RCE" sulla resilienza dei soggetti critici);
  - tutti gli operatori che erano stati qualificati come operatori di servizi essenziali della precedente versione della Direttiva NIS.

I soggetti importanti, invece, vengono identificati in via residuale: rientrano in tale categoria coloro che operano nei settori ad alta criticità o critici che non rientrino nel novero di quelli "essenziali".

I soggetti qualificati come essenziali o critici e i fornitori di servizi di registrazione di nomi a dominio dovranno essere identificati dagli Stati membri entro il 17 aprile 2025 e potranno essere chiamati a fornire alcuni dettagli come, ad esempio, la denominazione e i recapiti e ad indicare i paesi in cui erogano i servivi rilevanti ai fini della normativa.

4.2 Ambito di non applicazione.

4.2.1 I soggetti espressamente esclusi.

Sebbene la Direttiva NIS 2 abbia ampliato l'ambito di applicazione a settori ulteriori rispetto alle previsioni della Direttiva NIS, vi sono comunque entità che risultano espressamente escluse.

Anzitutto, coerentemente con il diritto dell'Unione europea, la Direttiva NIS 2 fa salve le competenze degli Stati membri in materia di mantenimento della sicurezza pubblica, difesa e sicurezza nazionale.

Pertanto, tra i soggetti che non saranno assoggettati alle sue disposizioni figurano le entità pubbliche che svolgono attività nei settori della sicurezza nazionale (come, ad esempio, le agenzie di

intelligence, della pubblica sicurezza o della difesa, del contrasto, ivi incluse la prevenzione, le indagini, l'accertamento e il perseguimento di crimini). La normativa riconosce anche che vi sono delle "zone grigie" in cui il confine tra servizi essenziali o importanti e attività collegate alla sicurezza nazionale è labile. Un esempio su tutti è quello della produzione dell'energia elettrica da centrali nucleari: in tal caso, è rimessa agli Stati Membri la possibilità di esercitare la propria responsabilità per salvaguardare la sicurezza nazionale.

Il testo normativo specifica peraltro che gli enti della pubblica amministrazione le cui attività sono solo marginalmente connesse a tali settori non dovrebbero essere esclusi.

In maniera analoga, gli Stati membri possono anche decidere di esonerare dall'applicazione delle disposizioni in materia di misure di sicurezza e di segnalazioni anche gli enti privati che operino nei summenzionati settori, ma solo limitatamente ai servizi erogati e alle attività svolte in tali contesti. Qualora tali soggetti privati eroghino esclusivamente attività o servizi di tale tipo, essi potranno altresì essere esclusi dall'elenco dei soggetti essenziali o importanti e dall'elenco dei fornitori di servizi DNS, di registro dei nomi a dominio di primo livello, di registrazione dei nomi a dominio, di cloud computing di data center, di reti di distribuzione dei contenuti, di servizi gestiti, di servizi di sicurezza gestiti, di mercati online, di motori di ricerca online e di piattaforme di servizi di social network. Invece, non sono soggetti a tale esenzione coloro che agiscono in qualità di prestatori di servizi fiduciari.

In aggiunta a quanto sopra, saranno esclusi dall'ambito di applicazione della Direttiva NIS 2 anche i soggetti che gli Stati membri hanno espressamente esentato dall'applicazione delle disposizioni del Regolamento (UE) 2554/2022 relativo alla resilienza operativa digitale per il settore finanziario (cd. Regolamento DORA). In particolare, a livello nazionale potrà essere esclusa la Cassa depositi e prestiti.

4.2.2 Gli atti giuridici settoriali dell'unione.

Un'ulteriore forma di esenzione è prevista in caso di atti giuridici settoriali dell'Unione europea. Infatti, qualora un'entità qualificata come essenziale o importante sia già soggetta ad obblighi normativi che impongano l'adozione di misure di gestione dei rischi di cybersecurity o di notifica degli incidenti significativi, non troveranno applicazione le corrispondenti disposizioni della Direttiva NIS 2. Ciò a condizione che gli obblighi imposti dall'atto settoriale siano almeno equivalenti a quelli previsti dal testo in esame.

Affinché tale equivalenza sia presente:

- gli effetti delle misure di gestione dei rischi di cybersecurity devono essere almeno equivalenti a quelli che si otterrebbero implementando le misure previste dalla Direttiva NIS 2;
- l'atto giuridico settoriale deve prevedere l'accesso immediato e diretto alle notifiche da parte dei CSIRT, delle autorità competenti o dei punti di contatto unici;
- gli obblighi di notifica devono avere un effetto che sia almeno equivalente a quelli previsti dalla Direttiva NIS 2.
- Il concetto di armonizzazione minima (come sotto chiarito)

In linea generale, laddove una materia sia regolamentata attraverso una Direttiva, il diritto dell'Unione europea prevede due forme di armonizzazione: minima o massima.

La prima comporta che il testo legislativo stabilisca gli standard normativi minimi, spesso riconoscendo il fatto che i sistemi giudiziari in alcuni Stati membri ne abbiano già fissati di più elevati, o comunque la loro facoltà di introdurre disposizioni più stringenti. La seconda, invece, prevede che gli Stati membri debbano introdurre norme con gli standard minimi e massimi stabiliti nel testo europeo, lasciando, quindi, un minor margine di discrezionalità.

Nel caso della Direttiva NIS 2 il legislatore ha optato per la prima alternativa. Infatti, essa fa salvo il diritto degli Stati membri di adottare o mantenere disposizioni che garantiscano un livello più elevato di sicurezza cibernetica, purché ciò sia coerente con gli obblighi stabiliti dal diritto dell'Unione. A livello nazionale, un esempio di normativa maggiormente stringente è rappresentato, ad esempio, da quella sul perimetro di sicurezza nazionale cibernetica.

4.3 I settori di applicazione.

Come anticipato nei precedenti paragrafi, la Direttiva NIS 2 ha ampliato notevolmente il novero di soggetti a cui si applica.

Le ragioni di tale estensione possono essere ricondotte, tra le altre, a due motivazioni principali: la prima può essere rappresentata dall'intenzione di richiedere requisiti in materia di sicurezza cibernetica ad un numero sempre crescente di attori, andando così ad incrementare il livello di cybersecurity generale.

La seconda motivazione può essere riscontrata nell'esperienza della diffusione del Covid-19 nel 2020 che ha spinto verso una maggiore dipendenza dai sistemi informatici, facendo emergere le criticità di settori che in un primo momento erano stati tralasciati, come, ad esempio, quello della filiera alimentare (cfr. paragrafo 4.5 della tabella di seguito riportata).

Tra i settori "ad alta criticità" vi figurano tutti quelli classicamente collegati alle infrastrutture critiche; quelli "critici", invece, sono quelli in cui è possibile apprezzare una maggiore discrezionalità degli Stati membri, che potranno valutare quali imprese ricomprendevi anche analizzando le peculiarità nazionali e le strategie in materia di cybersecurity.

Per ciascuno di essi nelle tabelle successive sono riassunti i sottosettori e i tipi di soggetti rilevanti. Laddove è indicato "N/A" la normativa non suddivide il settore in sottosettori.

Settori ad alta criticità

ENERGIA

Sottosettore	Tipo di soggetto
Energia elettrica	**Imprese elettriche,** cioè ogni persona fisica o giuridica, esclusi tuttavia i clienti finali, che svolge almeno una delle funzioni seguenti: generazione, trasmissione, distribuzione, aggregazione, gestione della domanda, stoccaggio, fornitura o acquisto di energia elettrica, che è responsabile per i compiti commerciali, tecnici e/o di manutenzione legati a queste funzioni – che esercitano attività di fornitura, intesa come la vendita, compresa la rivendita, di energia elettrica ai clienti.
	Gestori del sistema di distribuzione, cioè qualsiasi persona fisica o giuridica responsabile della gestione, della manutenzione e, se necessario, dello sviluppo del sistema di distribuzione in una data zona e, se del caso, delle relative interconnessioni con altri sistemi, e di assicurare la capacità a lungo termine del sistema di soddisfare richieste ragionevoli di distribuzione di energia elettrica.
	Gestori del sistema di trasmissione, cioè qualsiasi persona fisica o giuridica responsabile della gestione, della manutenzione e, se necessario, dello sviluppo del sistema di trasmissione in una data zona e, se del caso, delle relative interconnessioni con altri sistemi,

	e di assicurare la capacità a lungo termine del sistema di soddisfare richieste ragionevoli di trasmissione di energia elettrica.
	Produttori, cioè la persona fisica o giuridica che produce energia elettrica.
	Gestori del mercato elettrico designato, cioè il gestore del mercato designato dall'autorità competente per svolgere mansioni relative al coupling unico del giorno prima o al coupling unico infragiornaliero.
	Partecipanti al mercato dell'energia elettrica, cioè la persona fisica o giuridica che produce, acquista o vende servizi connessi all'elettricità, alla gestione della domanda o allo stoccaggio, compresa la trasmissione di ordini di compravendita, su uno o più mercati dell'energia elettrica, tra cui i mercati dell'energia di bilanciamento – che forniscono servizi di aggregazione (una funzione svolta da una persona fisica o giuridica che combina più carichi di clienti o l'energia elettrica generata, per la vendita, l'acquisto o la vendita all'asta in qualsiasi mercato dell'energia elettrica), gestione della domanda (la variazione del carico dell'energia elettrica per i clienti finali rispetto ai modelli di consumo normali o attuali in risposta a segnali del mercato, anche in risposta a prezzi dell'energia elettrica variabili nel tempo o incentivi finanziari, oppure in risposta all'accettazione dell'offerta del cliente finale, di vendere la riduzione o l'aumento della domanda a un determinato prezzo sui mercati organizzati individualmente o per aggregazione), stoccaggio di energia (nel sistema elettrico, il differimento dell'utilizzo finale dell'energia elettrica a un momento successivo alla sua generazione, o la conversione di energia elettrica in una forma di energia che può essere stoccata, lo stoccaggio di tale energia e la sua successiva riconversione in energia elettrica o l'uso sotto forma di un altro vettore energetico).
	Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità.
Teleriscaldamento e teleraffrescamento	**Gestori di teleriscaldamento o teleraffrescamento**, cioè la distribuzione di energia termica in forma di vapore, acqua calda o liquidi refrigerati, da fonti centrali o decentrate di produzione verso una pluralità di edifici o siti tramite una rete, per il riscaldamento o il raffrescamento di spazi o di processi di lavorazione.
Petrolio	**Gestori di oleodotti**.
	Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio.
	Organismi centrali di stoccaggio, cioè l'organo o il servizio al quale possono essere conferiti poteri per operare ai fini

	dell'acquisizione, del mantenimento o della vendita di scorte di petrolio, comprese le scorte di sicurezza e le scorte specifiche.
Gas	**Imprese fornitrici**, cioè ogni persona fisica o giuridica che svolge funzioni di fornitura.
	Gestori del sistema di distribuzione, cioè qualsiasi persona fisica o giuridica che svolge la funzione di distribuzione ed è responsabile della gestione, della manutenzione e, se necessario, dello sviluppo del sistema di distribuzione in una data zona ed, eventualmente, delle relative interconnessioni con altri sistemi, e di assicurare la capacità a lungo termine del sistema di soddisfare richieste ragionevoli di distribuzione di gas.
	Gestori del sistema di trasporto, qualsiasi persona fisica o giuridica che svolge la funzione di trasporto ed è responsabile della gestione, della manutenzione e, se necessario, dello sviluppo del sistema di trasporto in una data zona ed, eventualmente, delle relative interconnessioni con altri sistemi, e di assicurare la capacità a lungo termine del sistema di soddisfare richieste ragionevoli di trasporto di gas.
	Gestori dell'impianto di stoccaggio, cioè qualsiasi persona fisica o giuridica che svolge la funzione di stoccaggio ed è responsabile della gestione di un impianto di stoccaggio
	Gestori del sistema GNL, cioè qualsiasi persona fisica o giuridica responsabile della liquefazione del gas naturale o dell'importazione, o dello scarico, e della rigassificazione di GNL e responsabile della gestione di un impianto GNL.
	Imprese di gas naturale, cioè ogni persona fisica o giuridica, ad esclusione dei clienti finali, che svolge almeno una delle funzioni seguenti: produzione, trasporto, distribuzione, fornitura, acquisto o stoccaggio di gas naturale, compreso il GNL, e che è responsabile per i compiti commerciali, tecnici e/o di manutenzione legati a queste funzioni.
	Gestori di impianti di raffinazione e trattamento di gas naturale.
Idrogeno	**Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno.**

Tabella 1- Tipi di soggetti giuridici nel settore energetico

TRASPORTI

Sottosettore	Tipo di soggetto

Trasporto aereo	**Vettori aerei,** cioè imprese di trasporto aereo titolare di una licenza di esercizio valida o documento equivalente – utilizzati a fini commerciali.
	Gestori aeroportuali, cioè il soggetto al quale le disposizioni legislative, regolamentari o contrattuali nazionali affidano, insieme ad altre attività o in via esclusiva, il compito di amministrare e di gestire le infrastrutture aeroportuali o della rete aeroportuale e di coordinare e di controllare le attività dei vari operatori presenti negli aeroporti o nella rete aeroportuale interessati.
	Aeroporti, cioè qualsiasi terreno appositamente predisposto per l'atterraggio, il decollo e le manovre di aeromobili, inclusi gli impianti annessi che esso può comportare per le esigenze del traffico e per il servizio degli aeromobili, nonché gli impianti necessari per fornire assistenza ai servizi aerei commerciali, compresi gli aeroporti centrali.
	Soggetti che gestiscono impianti annessi situati in aeroporti.
	Operatori attivi nel controllo e nella gestione del traffico aereo, cioè un servizio fornito al fine di: a) prevenire collisioni: — tra aeromobili, e — nell'area di manovra tra aeromobili e ostacoli; e b) accelerare il flusso di traffico aereo e mantenerlo ordinato.
Trasporto ferroviario	**Gestori dell'infrastruttura**, cioè qualsiasi organismo o impresa responsabili dell'esercizio, della manutenzione e del rinnovo dell'infrastruttura ferroviaria di una rete nonché della partecipazione al suo sviluppo come stabilito dallo Stato membro nell'ambito della sua politica generale sullo sviluppo e sul finanziamento dell'infrastruttura.
	Imprese ferroviarie, cioè qualsiasi impresa pubblica o privata titolare di una licenza ai sensi della presente direttiva e la cui attività principale consiste nella prestazione di servizi per il trasporto di merci e/o di persone per ferrovia e che garantisce obbligatoriamente la trazione; sono comprese anche le imprese che forniscono solo la trazione.
	Operatori degli impianti di servizio, cioè un'entità pubblica o privata responsabile della gestione di uno o più impianti di servizio o della prestazione di uno o più servizi alle imprese ferroviarie.
Trasporto per le vie d'acqua	**Compagnie di navigazione per il trasporto per vie d'acqua interne**, marittimo e costiero di passeggeri e merci escluse le singole navi gestite da tale compagnia.
	Organi di gestione dei porti (intesi come una specifica area terrestre e marittima con confini definiti dallo Stato membro in cui il porto è situato, comprendente impianti e attrezzature intesi ad agevolare le operazioni commerciali di trasporto marittimo), compresi gli impianti portuali – cioè un luogo in cui avviene l'interfaccia nave/

	porto; comprende aree quali le zone di ancoraggio, di ormeggio e di accosto dal mare, secondo i casi - e soggetti che gestiscono opere e attrezzature all'interno di porti.
	Gestori di servizi di assistenza al traffico marittimo (VTS), cioè il servizio finalizzato a migliorare la sicurezza e l'efficienza del traffico marittimo e a tutelare l'ambiente, in grado di interagire con il traffico e di rispondere alle condizioni di traffico che si verificano nell'area coperta dal VTS.
Trasporto su strada	**Autorità stradali**, cioè qualsiasi autorità pubblica responsabile della pianificazione, del controllo o della gestione delle strade che rientrano nella sua competenza territoriale - responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono soltanto una parte non essenziale della loro attività generale.
	Gestori di sistemi di trasporto intelligenti, cioè sistemi in cui sono applicate tecnologie dell'informazione e della comunicazione, nel settore del trasporto stradale, infrastrutture, veicoli e utenti compresi, e nella gestione del traffico e della mobilità nonché per interfacce con altri modi di trasporto.

Tabella 2 - Tipi di soggetti giuridici nel settore dei trasporti

BANCARIO

Sottosettore	Tipo di soggetto
N/A	**Enti creditizi**, cioè un'impresa che svolge una delle attività seguenti: a) raccogliere depositi o altri fondi rimborsabili dal pubblico e concedere crediti per proprio conto; b) svolgere una qualsiasi delle attività di cui all'allegato I, sezione A, punti 3) e 6), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio (1) se ricorre una delle condizioni seguenti ma l'impresa non è un negoziatore per conto proprio di merci e di quote di emissioni, un organismo di investimento collettivo o un'impresa di assicurazione: i) il valore totale delle attività consolidate dell'impresa è pari o superiore a 30 miliardi di EUR; ii) il valore totale delle attività dell'impresa è inferiore a 30 miliardi di EUR e l'impresa fa parte di un gruppo in cui il valore totale delle attività consolidate di tutte le imprese di tale gruppo che individualmente detengono attività totali inferiori a 30 miliardi di EUR e svolgono una qualsiasi delle attività di cui all'allegato I, sezione A, punti 3) e 6), della direttiva 2014/65/UE è pari o superiore a 30 miliardi di EUR; oppure iii) il valore totale delle attività dell'impresa è inferiore a 30 miliardi di EUR e l'impresa fa parte di un gruppo in cui il valore totale delle attività consolidate di tutte le imprese del gruppo che svolgono una qualsiasi delle attività di cui all'allegato I, sezione A, punti 3) e 6), della direttiva 2014/65/UE è pari o superiore a 30 miliardi di EUR, ove l'autorità

	di vigilanza su base consolidata - in consultazione con il collegio delle autorità di vigilanza - decida in tal senso per far fronte ai potenziali rischi di elusione e ai potenziali rischi per la stabilità finanziaria dell'Unione. Ai fini della lettera b), punti ii) e iii), se l'impresa fa parte di un gruppo di un paese terzo, le attività totali di ciascuna succursale del gruppo di un paese terzo autorizzata nell'Unione sono incluse nel valore totale combinato delle attività di tutte le imprese del gruppo.

Tabella 3 - Tipi di soggetti giuridici nel settore bancario

INFRASTRUTTURE DEI MERCATI FINANZIARI

Sottosettore	Tipo di soggetto
N/A	**Gestori delle sedi di negoziazione**, cioè un mercato regolamentato, un sistema multilaterale di negoziazione o un sistema organizzato di negoziazione.
	Controparti centrali, cioè una persona giuridica che si interpone tra le controparti di contratti negoziati su uno o più mercati finanziari agendo come acquirente nei confronti di ciascun venditore e come venditore nei confronti di ciascun acquirente.

Tabella 4 - Tipi di soggetti giuridici nel settore infrastrutture dei mercati finanziari

SETTORE SANITARIO

Sottosettore	Tipo di soggetto
N/A	**Prestatori di assistenza sanitaria**, cioè una qualsiasi persona fisica o giuridica o qualsiasi altra entità che presti legalmente assistenza sanitaria nel territorio di uno Stato membro.
	Laboratori di riferimento dell'UE, cioè quelli designati dalla Commissione mediante atti di esecuzione.
	Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali, cioè a) ogni sostanza o associazione di sostanze presentata come avente proprietà curative o profilattiche delle malattie umane; o b) ogni sostanza o associazione di sostanze che possa essere utilizzata sull'uomo o somministrata all'uomo allo scopo di ripristinare, correggere o modificare funzioni fisiologiche, esercitando un'azione farmacologica, immunologica o metabolica, ovvero di stabilire una diagnosi medica.
	Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di base.

	Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica.

Tabella 5 - Tipi di soggetti giuridici nel settore sanitario

ACQUA POTABILE

Sottosettore	Tipo di soggetto
N/A	**Fornitori e distributori di acque destinate al consumo umano**, cioè tutte le acque trattate o non trattate, destinate a uso potabile, culinario o per la preparazione di cibi o per altri usi domestici in locali sia pubblici sia privati, a prescindere dalla loro origine, siano esse fornite tramite una rete di distribuzione, fornite mediante cisterne o in bottiglie o contenitori, comprese le acque di sorgente. Sono esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano.

Tabella 6 - Tipi di soggetti giuridici nel settore acqua potabile

ACQUE REFLUE

Sottosettore	Tipo di soggetto
N/A	**Imprese che raccolgono**, smaltiscono o trattano acque reflue urbane (acque reflue domestiche o il miscuglio di acque reflue domestiche, acque reflue industriali e/o acque meteoriche di dilavamento), domestiche (acque reflue provenienti da insediamenti di tipo residenziale e da servizi e derivanti prevalentemente dal metabolismo umano e da attività domestiche) o industriali (qualsiasi tipo di acque reflue scaricate da edifici in cui si svolgono attività commerciali o industriali, diverse dalle acque reflue domestiche e dalle acque meteoriche di dilavamento). Sono escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale.

Tabella 7 - Tipi di soggetti giuridici nel settore acque reflue

INFRASTRUTTURE DIGITALI

Sottosettore	Tipo di soggetto
N/A	**Fornitori di punti di interscambio internet.**
	Fornitori di servizi DNS, esclusi gli operatori dei server dei nomi radice.

	Registri dei nomi di dominio di primo livello (TLD).
	Fornitori di servizi di cloud computing.
	Fornitori di servizi di data center.
	Fornitori di reti di distribuzione dei contenuti (content delivery network).
	Fornitori di servizi fiduciari.
	Fornitori di reti pubbliche di comunicazione.
	Fornitori di servizi di comunicazione elettronica accessibili al pubblico.

Tabella 8 - Tipi di soggetti giuridici nel settore infrastrutture digitali

GESTIONE DEI SERVIZI TIC B2B

Sottosettore	Tipo di soggetto
N/A	**Fornitori di servizi gestiti.**
	Fornitori di servizi di sicurezza gestiti.

Tabella 9 - Tipi di soggetti giuridici nel settore gestione dei servizi tic b2b

PUBBLICA AMMINISTRAZIONE

Sottosettore	Tipo di soggetto
N/A	**Enti della pubblica amministrazione delle amministrazioni centrali quali definiti da uno Stato membro conformemente al diritto nazionale.**
	Enti della pubblica amministrazione a livello regionale quali definiti da uno Stato membro conformemente al diritto nazionale.

Tabella 10 -Tipi di soggetti giuridici nel settore Pubblica Amministrazione

SPAZIO

Sottosettore	Tipo di soggetto
N/A	**Operatori di infrastrutture terrestri possedute**, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi

	spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica.

Tabella 11 - Tipi di soggetti giuridici nel settore Spazio

Settori Critici

SERVIZI POSTALI E DI CORRIERE

Sottosettore	Tipo di soggetto
N/A	**Fornitori di servizi postali**, cioè l'impresa che fornisce uno o più servizi postali, tra cui i fornitori di servizi di corriere.

Tabella 12 - Tipi di soggetti giuridici nel settore Servizi Postali e di Corriere

GESTIONE DEI RIFIUTI

Sottosettore	Tipo di soggetto
N/A	**Imprese che si occupano della gestione dei rifiuti**, cioè della raccolta, del trasporto, del recupero (compresa la cernita), e dello smaltimento dei rifiuti, compresi la supervisione di tali operazioni e gli interventi successivi alla chiusura dei siti di smaltimento nonché le operazioni effettuate in qualità di commercianti o intermediari. Sono escluse quelle per cui la gestione dei rifiuti non è la principale attività economica.

Tabella 13 - Tipi di soggetti giuridici nel settore Gestione dei rifiuti

FABBRICAZIONE, PRODUZIONE E DISTRIBUZIONE DI SOSTANZE CHIMICHE

Sottosettore	Tipo di soggetto
N/A	**Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele e imprese che si occupano della produzione di articoli da sostanze o miscele.**

Tabella 14 - Tipi di soggetti giuridici nel settore Fabbricazione, produzione e distribuzione di sostanze chimiche

PRODUZIONE, TRASFORMAZIONE E DISTRIBUZIONE DI ALIMENTI

Sottosettore	Tipo di soggetto
N/A	**Imprese alimentari** – cioè ogni soggetto pubblico o privato, con o senza fini di lucro, che svolge una qualsiasi delle attività connesse ad una delle fasi di produzione, trasformazione e distribuzione degli alimenti – che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione.

Tabella 15 - Tipi di soggetti giuridici nel settore Produzione, trasformazione e distribuzione di alimenti

FABBRICAZIONE

Sottosettore	Tipo di soggetto
Fabbricazione di dispositivi medico-diagnostici in vitro	**Soggetti che fabbricano dispositivi medici**, cioè qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: — diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie, — diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità, — studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico, — fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi.
	Soggetti che fabbricano dispositivi medicodiagnostici in vitro, cioè qualsiasi dispositivo medico composto da un reagente, un prodotto reattivo, un calibratore, un materiale di controllo, un kit, uno strumento, un apparecchio, una parte di attrezzatura, un software o un sistema, utilizzato da solo o in combinazione, destinato dal fabbricante a essere impiegato in vitro per l'esame di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, unicamente o principalmente al fine di fornire una o più delle seguenti informazioni: a) su un processo o uno stato fisiologico o patologico; b) su una disabilità fisica o intellettiva congenita; c) sulla predisposizione a una condizione clinica o a una malattia; d) per determinare la sicurezza e la compatibilità con potenziali soggetti riceventi; e) per prevedere la risposta o le reazioni a un trattamento; f) per definire o monitorare le misure terapeutiche. Anche i contenitori dei campioni sono considerati dispositivi medico-diagnostici in vitro.
Fabbricazione di computer e prodotti di elettronica e ottica	**Imprese che producono computer e prodotti di elettronica** come, ad esempio, produzione di computer e prodotti elettronici e ottici, produzione di periferiche.
Fabbricazione di apparecchiature elettriche	**Imprese che producono, ad esempio, motori elettrici, generatori e trasformatori.**
Fabbricazione di macchinari e	**Imprese che producono, ad esempio, pompe e compressori.**

apparecchiature n.c.a	
Fabbricazione di autoveicoli, rimorchi e semirimorchi	**Imprese che producono veicoli, le relative parti e accessori e le componenti elettriche ed elettroniche.**
Fabbricazione di altri mezzi di trasporto	**Imprese che producono imbarcazioni, strutture flottanti e moto.**

Tabella 16 - Tipi di soggetti giuridici nel settore Fabbricazione

FORNITORI DI SERVIZI DIGITALI

Sottosettore	Tipo di soggetto
N/A	**Fornitori di mercati online.**
	Fornitori di motori di ricerca online.
	Fornitori di piattaforme di servizi di social network.

Tabella 17 - Tipi di soggetti giuridici nel settore Fornitori di servizi digitali

RICERCA

Sottosettore	Tipo di soggetto
N/A	Organizzazioni di ricerca.

Tabella 18 - Tipi di soggetti giuridici nel settore Ricerca

5 Le previsioni della normativa (Marilena Hyeraci e Lucrezia Falciai).

Come la Direttiva NIS, la Direttiva NIS 2 si pone l'obiettivo di garantire un livello comune elevato di sicurezza cibernetica all'interno dei confini dell'Unione europea. Il raggiungimento di tale proposito favorirebbe il funzionamento del mercato interno sia attraverso la definizione di norme chiare e generalmente applicabili, che con l'armonizzazione di quelle relative alla gestione del rischio di cibersicurezza e alla segnalazione di incidenti[16].

La Commissione europea ha riconosciuto che l'implementazione della Direttiva NIS da parte degli Stati membri ha dato luogo a disparità nel settore della sicurezza cibernetica. Dette differenze ostacolano il buon funzionamento del mercato interno perché, ad esempio, i soggetti all'interno dell'UE impegnati in attività transfrontaliere si trovano a dover fronteggiare obblighi normativi diversi, con possibili sovrapposizioni, e/o una diversa applicazione a scapito dell'esercizio della libertà di stabilimento e libera prestazione di servizi. Norme diverse hanno anche un impatto negativo sulle condizioni della concorrenza nel mercato interno quando si tratta di soggetti che operano nel medesimo settore, sebbene in Stati membri diversi.

Anche al fine di porre rimedio a tali disparità, in sede di implementazione, la Direttiva NIS 2 rafforza alcuni obblighi a carico degli Stati membri, nonché, in ultima istanza, delle imprese che saranno soggette all'ambito di applicazione della normativa in esame.

Nello specifico, i principali elementi di novità possono essere sintetizzati nei seguenti punti:

- riorganizzazione del sistema istituzionale di gestione delle tematiche relative alla sicurezza cibernetica (cfr. paragrafo A);
- rafforzamento delle misure per la gestione dei rischi per la sicurezza cibernetica e razionalizzazione delle misure (cfr. paragrafo B);
- estensione dei concetti di gestione del rischio e di valutazione delle vulnerabilità a tutta la supply chain (cfr. paragrafo C);
- responsabilità dell'organo di gestione (cfr. paragrafo D);
- razionalizzazione degli obblighi di notifica (cfr. paragrafo E);
- information sharing (cfr. paragrafo F).

Si fornisce di seguito un'analisi di maggiore dettaglio dei punti sopra elencati.

5.1 Sistema istituzionale di gestione delle tematiche relative alla sicurezza cibernetica

In continuità con il precedente regime normativo, la Direttiva NIS 2 stabilisce il dovere per gli Stati membri di adottare strategie nazionali in materia di cybersecurity e di dotarsi di un sistema istituzionale di gestione delle tematiche relative alla sicurezza cibernetica mediante la designazione o la creazione di autorità nazionali competenti, punti di contatto unici in materia di sicurezza e team di risposta agli incidenti.

A tal riguardo, un elemento di novità è rappresentato dall'obbligo di individuare, oltre alle istituzioni menzionate, anche un'autorità di gestione delle crisi informatiche, da intendersi come incidenti e crisi di cibersicurezza su vasta scala. Inoltre, per far fronte a tali eventi, gli Stati membri sono tenuti ad

[16] Cfr. Commissione Europea, Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, Bruxelles 16 dicembre 2020.

adottare un piano nazionale di risposta alle crisi informatiche in cui sono stabiliti gli obiettivi e le modalità di gestione delle stesse.

5.2 Rafforzamento delle misure per la gestione dei rischi per la sicurezza cibernetica e razionalizzazione delle misure

La Direttiva NIS 2 rafforza le misure per la gestione dei rischi per la sicurezza cibernetica e gli obblighi di segnalazione per i soggetti che rientrano nei settori "ad alta criticità" o "critici" e per coloro che siano stati qualificati come critici ai sensi della Direttiva (UE) 2022/2557 (cd. Direttiva RCE).

Sebbene sia necessario aspettare il recepimento nell'ordinamento nazionale della Direttiva NIS 2 da parte del legislatore italiano per avere un quadro più completo delle misure di sicurezza, già dall'analisi del testo europeo emerge come un elemento cardine della normativa sia rappresentato da una razionalizzazione delle misure di sicurezza che i soggetti interessati dalla normativa devono applicare. Queste saranno non più solo tecniche, ma anche operative e organizzative.

Tali misure devono essere anzitutto adeguate e proporzionate per consentire di gestire i rischi per la sicurezza cibernetica e prevenire e/o ridurre gli impatti per i destinatari dei servizi derivanti da interruzioni o malfunzionamenti degli stessi. La valutazione deve tenere in considerazione le dimensioni del soggetto, il suo grado di esposizione ai rischi, la probabilità che si verifichino e la loro gravità, intesa anche in termini di impatto economico e sociale.

Pertanto, stando alla formulazione potrebbe non essere più possibile un approccio "*one size fits all*". Al contrario, le misure di sicurezza dovranno tenere in considerazione la realtà specifica del soggetto che le implementerà.

Il testo della Direttiva NIS 2 identifica alcune macroaree che dovranno essere coperte, quali:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

La Direttiva NIS 2 contempla misure non siano solo (i) di natura tecnica, come ad esempio l'uso della crittografia o di soluzioni di autenticazione a più fattori, ma anche (ii) organizzativa, come la predisposizione di politiche di analisi dei rischi e di sicurezza dei sistemi informatici o di strategie e

procedure per valutare l'efficacia delle misure per la gestione dei rischi, o (iii) operativa come la continuità operativa.

La Direttiva NIS 2 delinea un approccio olistico alla sicurezza cibernetica, vista non più solo nella sua dimensione tecnica informatica, ma anche nella sua dimensione organizzativa, ivi inclusa quella legale, e operativa. Inoltre, la Direttiva NIS 2 conferma l'importanza dell'avere un approccio basato sul rischio.

Ulteriore elemento di novità è che la Commissione europea dovrà stabilire, mediante atti di esecuzione, i requisiti tecnici e metodologici relativi alle misure di sicurezza. Questi potranno interessare sia soggetti specifici (come, ad esempio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di mercati online e prestatori di servizi fiduciari online, che i soggetti essenziali e importanti).

5.3 Estensione dei concetti di gestione del rischio e di valutazione delle vulnerabilità alla supply chain

Una delle novità più rilevanti che allinea la Direttiva NIS 2 alle più recenti normative in materia di cybersecurity è rappresentata dalla previsione di un obbligo di garantire la sicurezza della catena di approvvigionamento.

Tale misura di sicurezza sembrerebbe prevedere che i soggetti importanti ed essenziali debbano garantire non solo la sicurezza dei propri sistemi informatici, ma anche assicurarsi che i loro fornitori non costituiscano l'anello debole della catena.

A tal fine, coerentemente con l'approccio basato sul rischio di cui si è detto in precedenza, i soggetti importanti ed essenziali dovranno valutare quali misure di sicurezza implementare tenendo in considerazione le vulnerabilità specifiche di ogni fornitore diretto, della qualità complessiva dei prodotti e delle pratiche di cybersecurity implementate, ivi incluse le procedure di sviluppo sicuro.

Verosimilmente, tale obbligo si tradurrà in un dovere di analizzare in maniera approfondita l'approccio alla sicurezza cibernetica dei fornitori, valutando se esso soddisfi i requisiti della normativa o meno.

I soggetti importanti ed essenziali dovranno tenere in considerazione anche il risultato delle valutazioni coordinate dei rischi per la sicurezza della catena di approvvigionamento. Queste ultime sono analisi svolte dalla Commissione europea e dall'ENISA[17] in relazione a specifiche catene di approvvigionamento critiche di servizi TIC (ossia quelli relativi alle tecnologie dell'informazione e della comunicazione), sistemi TIC o prodotti TIC. Le valutazioni svolte in merito dalla Commissione europea e dall'ENISA dovranno prendere in considerazione i rischi tecnici, ma, laddove ritenuto opportuno, potranno altresì analizzare profili differenti[18].

5.4 Responsabilità dell'organo di gestione nella gestione del rischio di cybersecurity

Una delle novità più rilevanti introdotte dalla Direttiva NIS 2 è rappresentata dall'obbligo per l'organo di gestione di approvare le misure di gestione dei rischi di cibersicurezza, nonché a sovrintendere all'applicazione della normativa ("Gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi all'articolo 21, sovraintendano alla sua attuazione e possano essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo").

17 L'Agenzia dell'Unione europea per la cibersicurezza, l'agenzia dell'Unione europea che si occupa di cibersicurezza.

18 Cfr., Articolo 22 della Direttiva (UE) 2022/2555 (Direttiva NIS 2).

Tale disposizione sancisce un'innovazione cruciale in quanto richiede espressamente per la prima volta il diretto coinvolgimento del management delle società nell'adozione di un framework di cybersecurity e nella definizione dell'approccio strategico. Tale coinvolgimento non potrà limitarsi ad essere solamente formale ma, al contrario, dovrà essere effettivo. Infatti, sebbene sia necessario attendere di capire come concretamente il legislatore nazionale declinerà tale disposizione, è possibile che essa i traduca in una responsabilità degli amministratori.

A rafforzare tale concezione dell'organo di gestione quale parte attiva del processo di adozione delle misure di gestione del rischio cibernetico, vi sono gli obblighi di formazione periodici ("Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione"). Questi ultimi devono essere letti quali strumenti per incrementare la consapevolezza dei membri del board e supportarli nel processo decisionale affinché siano in grado di comprendere le implicazioni pratiche delle decisioni prese.

5.5 Razionalizzazione degli obblighi di notifica

In linea di continuità con il precedente regime normativo, la Direttiva NIS 2 prevede l'obbligo di notifica degli incidenti significativi. Questi ultimi sono quegli eventi che (i) compromettono la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi e (ii) hanno un impatto significativo sulla fornitura dei servizi:

a) causando o essendo in grado di causare una grave perturbazione operativa degli stessi o perdite finanziarie;

b) ripercuotendosi o essendo in grado di ripercuotersi su altre persone fisiche o giuridiche, causando perdite materiali o immateriali considerevoli.

Inoltre, mentre la precedente versione il testo europeo si limitava a stabilire che gli incidenti dovessero essere notificati "senza indebito ritardo"[19], la Direttiva NIS 2 definisce un processo di notifica introducendo diversi step. Nello specifico, il soggetto notificante dovrà trasmettere al CSIRT:

a) un preallarme senza indebito ritardo e comunque entro 24 ore da quando è venuto a conoscenza dell'incidente significativo. Se opportuno, la comunicazione deve specificare se l'evento è il risultato di un atto illegittimo o meno e se può avere un impatto transfrontaliero;

b) una notifica senza indebito ritardo e comunque entro 72 ore da quando è venuto a conoscenza dell'incidente significativo. Tale notifica deve aggiornare le informazioni di cui al punto precedente e includere una valutazione iniziale dell'incidente, comprensiva della sua gravità e dell'impatto, nonché degli indicatori di compromissione, ove disponibili;

c) una relazione intermedia, su richiesta del CSIRT;

d) una relazione finale entro un mese dalla trasmissione della notifica di cui al punto b. che comprenda:
   i. una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;
   ii. il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;
   iii. le misure di attenuazione adottate e in corso;
   iv. se opportuno, l'impatto transfrontaliero dell'incidente.

Nel caso in cui, al momento della relazione finale l'incidente sia ancora in corso, dovrà essere fornita una relazione sui progressi e una finale entro un mese dalla gestione dell'incidente.

19 Anche l'implementazione nazionale della Direttiva 1148/2016 prevedeva diversi step di notifica con tempistiche analoghe a quelle stabilite dalla Direttiva NIS 2. Tuttavia, si è trattato di una declinazione del legislatore nazionale e può non aver trovato un equivalente in altri ordinamenti europei.

La Commissione potrà dettagliare ulteriormente il tipo di informazioni che dovranno essere fornite, il formato e la procedura di comunicazione attraverso l'adozione di specifici atti di esecuzione.

A seguito dell'avvio del processo di notifica da parte dei soggetti essenziali o importanti, il CSIRT dovrà fornire un riscontro iniziale entro 24 ore dall'invio del preallarme e, su richiesta del soggetto notificante, orientamenti o una consulenza operativa sulle misure di attenuazione.

Inoltre, il CSIRT o le autorità competenti potranno altresì informare il pubblico dell'incidente laddove la sua conoscenza sia di interesse pubblico ovvero ciò sia necessario per esigenze di sensibilizzazione o per affrontarlo. In aggiunta, nelle more del recepimento della normativa nell'ordinamento nazionale, potrà essere altresì previsto un obbligo per i soggetti notificanti di informare senza indebito ritardo i destinatari dei propri servizi che sono potenzialmente interessati da una minaccia informatica significativa della stessa e delle misure o azioni correttive in grado di mitigarla.

5.6 Information Sharing

La Direttiva NIS 2 conferma la necessità di rafforzare il quadro di condivisione delle informazioni sulla cibersicurezza ribadendo l'istituzione di un gruppo di cooperazione per sostenere e agevolare la cooperazione strategica e lo scambio di informazioni. Inoltre, ha introdotto la possibilità per tutti i soggetti, sia quelli che rientrano nell'ambito di applicazione della normativa, che quelli esclusi, di concludere accordi per lo scambio di informazioni su base volontaria al fine di:

a) prevenire o rilevare gli incidenti, di agevolare le procedure di recovery e limitare gli impatti;

b) incrementare il livello di cybersecurity, anche grazie alla sensibilizzazione.

Infine, nell'ottica di armonizzare l'applicazione della normativa, la Direttiva NIS 2 prevede obblighi di vigilanza ed esecuzione per gli Stati Membri. A tal proposito, sono stati notevolmente ampliati i poteri delle autorità competenti che, a differenza di quanto previsto dal precedente regime normativo, possono anche disporre ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati, effettuare audit sulla sicurezza, periodici e mirati, e richiedere l'accesso a dati, documenti e altre informazioni.

Come precisato nei paragrafi precedenti, per avere maggiori dettagli sul contenuto della normativa sarà necessario attendere il recepimento nell'ordinamento nazionale. Tuttavia, di seguito sono riportati alcuni precedenti.

I. Rafforzamento delle misure per la gestione dei rischi per la sicurezza cibernetica e razionalizzazione delle misure.

Sia la Direttiva 1148/2016 (cd. Direttiva NIS) che il decreto-legge 105/2019 (cd. Perimetro di Sicurezza Nazionale Cibernetica) prevedono l'introduzione di un framework di misure di sicurezza tratte dal *"Framework Nazionale per la Cybersecurity e la Data Protection"*.

II. Estensione dei concetti di gestione del rischio e di valutazione delle vulnerabilità alla supply chain.

Anche la gestione del rischio derivante dalle terze parti non costituisce una novità. Infatti, in maniera parzialmente simile, sia il Regolamento (UE) 2016/679 (cd. GDPR), che il Perimetro di Sicurezza Nazionale Cibernetica, che il Regolamento 2022/2554 (cd. Regolamento DORA), prevedono obblighi prevedono un'attenta valutazione dei fornitori e delle garanzie da essi prestate.

III. Misure di gestione dei rischi di cybersecurity e responsabilità dell'organo di gestione.

In maniera simile a quanto stabilito dalla Direttiva NIS 2, il Regolamento DORA introduce una responsabilità dell'organo di gestione. In parte, una responsabilità è stata prevista anche dal Perimetro di Sicurezza Nazionale Cibernetica, che ha introdotto, inter alia, delle fattispecie di responsabilità amministrativa dell'ente derivante da reato.

IV. Razionalizzazione degli obblighi di notifica.

L’obbligo di notifica degli incidenti è comune a numerose normative in materia di protezione dei dati personali e cybersecurity, come, ad esempio, il GDPR, la Direttiva NIS, il Perimetro di Sicurezza Nazionale Cibernetica e il Regolamento DORA.

6 Sanzioni (Raffaella D'Alessandro)

La Direttiva prevede diverse sanzioni in funzione del fatto che un operatore sia qualificato come essenziale o come importante.

Nel merito i soggetti essenziali saranno sottoposti a sanzioni pecuniarie amministrative pari a un massimo di Euro 10.000.000 o a un massimo del 2% del totale del fatturato mondiale annuo per l'esercizio precedente, se tale importo è superiore. Per i soggetti importanti, invece, potranno essere comminate sanzioni pari a un massimo di Euro 7.000.000 o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente, se tale importo è superiore.

7 Ruoli e autorità nella NIS2 (Raffaella D'Alessandro).

La Direttiva NIS2 (Network and Information Systems Directive 2) prevede diverse autorità con compiti specifici per garantire l'attuazione efficace della medesima. Ecco le principali autorità previste dalla Direttiva NIS2 e i loro compiti:

7.1 Autorità Nazionale Competente (ANC)

Compiti:

- **Coordinamento:** Coordinare la risposta nazionale agli incidenti di sicurezza informatica e la cooperazione internazionale.
- **Supervisione:** Sorvegliare e garantire il rispetto delle disposizioni della direttiva da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali.
- **Linee guida:** Fornire orientamenti e linee guida per l'implementazione delle misure di sicurezza.

7.2 Punto di Contatto Unico (SPOC)

Compiti:

- **Comunicazione:** Funzionare come punto centrale per le comunicazioni con le altre autorità competenti nazionali e con le istituzioni dell'UE.
- **Coordinamento transfrontaliero:** Facilitare la cooperazione transfrontaliera e lo scambio di informazioni tra Stati membri.

7.3 CSIRT (Computer Security Incident Response Team)

Compiti:

- **Gestione degli incidenti:** Monitorare, rilevare, analizzare e rispondere agli incidenti di sicurezza informatica.
- **Supporto e assistenza:** Fornire supporto tecnico e consulenza agli operatori di servizi essenziali e ai fornitori di servizi digitali.
- **Collaborazione:** Collaborare con altri CSIRT nazionali ed europei per la condivisione di informazioni e le migliori pratiche.

7.4 Gruppo di cooperazione

Compiti:

- **Strategia e politica:** Promuovere la cooperazione strategica e lo scambio di informazioni tra Stati membri.
- **Linee guida:** Sviluppare linee guida e raccomandazioni per migliorare la sicurezza informatica a livello europeo.
- **Valutazione:** Valutare periodicamente lo stato della sicurezza delle reti e dei sistemi informativi nell'UE.

7.5 Rete dei CSIRT

Compiti:

- **Collaborazione operativa:** Rafforzare la cooperazione operativa tra i CSIRT degli Stati membri.
- **Scambio di informazioni:** Facilitare lo scambio di informazioni sulle minacce e sugli incidenti di sicurezza informatica.
- **Supporto reciproco:** Fornire supporto reciproco in caso di incidenti di sicurezza transfrontalieri.

7.6 Organismi di Certificazione

Compiti:

- **Certificazione di sicurezza**: Emissione di certificazioni di sicurezza per i prodotti, servizi e processi legati alla sicurezza informatica.
- **Standardizzazione:** Garantire che le certificazioni rispettino gli standard europei e internazionali.

Queste autorità collaborano strettamente per creare un ambiente sicuro e resiliente contro le minacce informatiche in tutta l'Unione Europea, migliorando la capacità di risposta e prevenzione degli incidenti di sicurezza informatica.

8 Le misure strategiche che devono essere adottate dagli stati membri (Raffaella D'Alessandro).

La Direttiva NIS2 richiede agli Stati Membri dell'Unione Europea di adottare una serie di misure strategiche per migliorare la sicurezza delle reti e dei sistemi informativi. Queste misure sono finalizzate a creare un ambiente più sicuro e resiliente contro le minacce informatiche. Di seguito le principali misure strategiche che devono essere adottate.

8.1 Strategia Nazionale di Sicurezza delle Reti e dei Sistemi Informativi

Contenuti principali:

- **Obiettivi:** Definire gli obiettivi e le priorità nazionali in materia di sicurezza informatica.
- **Ruoli e responsabilità:** Stabilire chiaramente i ruoli e le responsabilità delle autorità pubbliche e delle organizzazioni private coinvolte nella sicurezza informatica.
- **Risorse:** Allocare le risorse necessarie per attuare la strategia, incluse risorse finanziarie e umane.
- **Piani di emergenza:** Prevedere piani di risposta e gestione delle emergenze per affrontare incidenti di sicurezza informatica di grande impatto.

8.2 Quadro normativo e istituzionale

Componenti principali:

- **Autorità competenti:** Designare le autorità nazionali competenti, i punti di contatto unici e i CSIRT.
- **Normative e regolamenti:** Adottare normative e regolamenti che impongano misure di sicurezza adeguate agli operatori di servizi essenziali e ai fornitori di servizi digitali.
- **Meccanismi di vigilanza:** Stabilire meccanismi di vigilanza e sanzioni per garantire il rispetto delle norme.

8.3 Misure tecniche e organizzative

Elementi chiave:

- **Gestione dei rischi:** Richiedere agli operatori di servizi essenziali e ai fornitori di servizi digitali di adottare misure adeguate di gestione dei rischi per la sicurezza delle loro reti e sistemi informativi.
- **Incident response:** Implementare procedure efficaci per la gestione degli incidenti di sicurezza informatica, inclusa la notifica degli incidenti alle autorità competenti.
- **Resilienza:** Promuovere l'adozione di misure che migliorino la resilienza dei sistemi informativi, come la ridondanza e il ripristino rapido.

8.4 Cooperazione e condivisione delle informazioni

Aspetti principali:

- **Collaborazione:** Favorire la collaborazione tra le autorità competenti, i CSIRT e le organizzazioni private a livello nazionale e internazionale.

- **Condivisione delle informazioni:** Creare meccanismi per la condivisione tempestiva e sicura delle informazioni sulle minacce e sugli incidenti di sicurezza informatica.
- **Partenariati pubblico-privato:** Promuovere partenariati tra il settore pubblico e privato per migliorare la condivisione delle conoscenze e delle risorse.

8.5 Sensibilizzazione e formazione

Azioni principali:

- **Campagne di sensibilizzazione:** Avviare campagne di sensibilizzazione per aumentare la consapevolezza sulla sicurezza informatica tra le imprese, i cittadini e le istituzioni.
- **Formazione e sviluppo delle competenze:** Promuovere programmi di formazione e sviluppo delle competenze per gli operatori di servizi essenziali e i fornitori di servizi digitali, nonché per le autorità pubbliche.

8.6 Ricerca e sviluppo

Iniziative principali:

- **Innovazione:** Sostenere la ricerca e lo sviluppo di nuove tecnologie e soluzioni per la sicurezza informatica.
- **Collaborazione scientifica:** Promuovere la collaborazione tra istituzioni accademiche, centri di ricerca e industria per sviluppare soluzioni innovative.

8.7 Valutazione e revisione

Processi principali:

- **Monitoraggio e valutazione:** Stabilire processi per il monitoraggio continuo e la valutazione delle politiche e delle misure di sicurezza informatica.
- **Revisione periodica:** Effettuare revisioni periodiche della strategia nazionale e delle misure adottate per garantirne l'efficacia e l'adeguatezza rispetto all'evoluzione delle minacce informatiche.

Queste misure strategiche sono fondamentali per creare un quadro coerente e integrato a livello nazionale e europeo, migliorando la capacità complessiva di prevenzione, rilevamento e risposta agli incidenti di sicurezza informatica.

9 NIS2: Le nuove misure di Sicurezza per i soggetti impattati (Tommaso Ruocco).

La NIS2, ovvero la Direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, è stata revisionata e rafforzata per affrontare le sfide emergenti nel campo della cibersicurezza. La revisione, nota come NIS2, è stata adottata per garantire un elevato livello di responsabilità nelle misure di gestione dei rischi di cibersicurezza da parte dei soggetti essenziali e importanti. La normativa mira a migliorare la sicurezza delle reti e dei sistemi informativi nell'Unione Europea, promuovendo una governance efficace e la collaborazione tra gli Stati membri e gli attori interessati.

9.1 Responsabilizzazione vertici considerando anche gli aspetti organizzativi

La responsabilizzazione dei vertici è un aspetto chiave della NIS2, come indicato nell'Articolo 20, che richiede agli organi di gestione dei soggetti essenziali e importanti di approvare le misure di gestione dei rischi di cibersicurezza e sovraintendere alla loro attuazione. Questo implica che i vertici devono assumere un ruolo attivo nella definizione e nell'attuazione di politiche di cibersicurezza. Inoltre, l'Articolo 32 sottolinea la necessità che le persone fisiche responsabili dei soggetti essenziali garantiscano il rispetto della direttiva, evidenziando il ruolo cruciale dei vertici nella vigilanza e nell'esecuzione delle misure di sicurezza.

Le misure di sicurezza da adottare dai soggetti impattati, come indicato nell'Articolo 32, includono la responsabilità delle persone fisiche coinvolte nella gestione dei soggetti essenziali. Queste persone devono garantire il rispetto della NIS2 e possono essere ritenute responsabili in caso di inadempienza dei loro doveri. Inoltre, l'Articolo 20 sottolinea la necessità di formazione per i membri dell'organo di gestione, evidenziando che devono acquisire conoscenze e competenze sufficienti per individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza. Ciò implica l'implementazione di programmi formativi mirati per garantire un elevato livello di consapevolezza e preparazione del personale chiave.

In conclusione, la NIS2 pone una forte enfasi sulla responsabilità dei vertici nell'attuazione di misure di cibersicurezza, richiedendo governance attiva, formazione adeguata e vigilanza accurata per garantire la sicurezza delle reti e dei sistemi informativi nell'Unione Europea.

9.2 gestione degli incidenti e obbligo di segnalazione (C101, Art 23)

La NIS2 affronta la gestione degli incidenti e l'obbligo di segnalazione, stabilendo un approccio in più fasi per trovare un equilibrio tra la segnalazione rapida e quella approfondita. La direttiva si concentra sulla segnalazione di incidenti significativi che possono causare gravi perturbazioni operative o perdite finanziarie, coinvolgendo soggetti essenziali e importanti. L'Articolo 23 dettaglia gli obblighi di segnalazione, richiedendo ai soggetti interessati di notificare senza indebito ritardo eventuali incidenti significativi alle autorità competenti, con considerazioni sull'impatto transfrontaliero.

La NIS2 stabilisce chiaramente che la segnalazione degli incidenti dovrebbe comprendere una valutazione iniziale che consideri la gravità delle perturbazioni operative, l'importanza dei servizi interessati e la natura della minaccia informatica. La valutazione dovrebbe tener conto di indicatori come la misura in cui il funzionamento del servizio è interessato, la durata dell'incidente e il numero di destinatari dei servizi coinvolti. L'obbligo di segnalazione è esteso anche ai destinatari dei servizi potenzialmente coinvolti, promuovendo la trasparenza e la collaborazione.

La NIS2 impone misure di sicurezza chiave attraverso l'Articolo 23, richiedendo ai soggetti essenziali e importanti di notificare senza indebito ritardo gli incidenti significativi. In caso di minaccia

informatica significativa, i soggetti interessati devono comunicare misure o azioni correttive che i destinatari dei loro servizi possono adottare. Questa disposizione mira a garantire una risposta tempestiva e collaborativa per mitigare gli impatti degli incidenti. La direttiva enfatizza inoltre che la notifica non espone il soggetto che la effettua a una maggiore responsabilità, ma mira a favorire la condivisione di informazioni utili per migliorare la resilienza informatica nel tempo.

9.3 continuità operativa e gestione delle crisi

La NIS2 si occupa della continuità operativa e della gestione delle crisi per affrontare incidenti e minacce di cibersicurezza su vasta scala. La normativa mira a stabilire un quadro operativo e organizzativo efficace per la gestione delle crisi a livello dell'Unione Europea. Le sezioni citate (C68, C71, C74) delineano l'importanza della cooperazione tra gli Stati membri, le reti di CSIRT, e l'istituzione di EU-CyCLONe come intermediario tra il livello tecnico e politico durante incidenti e crisi.

La NIS2 fornisce linee guida specifiche nei seguenti punti:

- **Cooperazione e Quadro di Risposta:** Gli Stati membri sono invitati a contribuire all'istituzione del quadro di risposta alle crisi di cibersicurezza dell'UE attraverso reti di cooperazione esistenti, come EU-CyCLONe e la rete di CSIRT (C68).
- **Ruolo di EU-CyCLONe:** EU-CyCLONe deve agire come intermediario tra il livello tecnico e politico durante le crisi, sfruttando i risultati della rete di CSIRT e fornendo analisi d'impatto (C71).
- **Cooperazione con Paesi Terzi:** Gli Stati membri possono cooperare con paesi terzi, scambiando informazioni relative a minacce, incidenti, vulnerabilità e svolgendo attività di gestione delle crisi (C74).

La NIS2 richiede che gli Stati membri stabiliscano quadri nazionali di gestione delle crisi informatiche (Articolo 9), garantendo che le autorità di gestione delle crisi informatiche abbiano risorse adeguate. I piani nazionali di risposta devono includere obiettivi, procedure di gestione delle crisi informatiche, misure di preparazione, e coinvolgere portatori di interessi del settore pubblico e privato (Articolo 9). Inoltre, l'Articolo 21 richiede che i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate per gestire i rischi, inclusi aspetti come la gestione degli incidenti, la continuità operativa, e la sicurezza della catena di approvvigionamento. La valutazione delle misure deve essere proporzionata ai rischi, tenendo conto della dimensione del soggetto e della probabilità e gravità degli incidenti. La Commissione adotta atti di esecuzione per specificare requisiti tecnici e metodologici delle misure di sicurezza (Articolo 21).

9.4 sicurezza della catena di approvvigionamento

La sicurezza della catena di approvvigionamento è un aspetto critico della cibersicurezza che si occupa di proteggere i sistemi informatici e di rete da minacce e vulnerabilità legate alla fornitura di prodotti e servizi. La normativa NIS2, nelle sezioni citate (C44, C54, C56, C59, C85, C90, Articolo 7, Articolo 21), delinea le misure necessarie per affrontare le sfide specifiche associate alla catena di approvvigionamento.

Linee guida specifiche della NIS2:

- **Monitoraggio della Catena di Approvvigionamento:** I CSIRT (Computer Security Incident Response Team) devono avere la capacità di monitorare le risorse connesse a internet dei soggetti essenziali o importanti per identificare rischi organizzativi legati alle compromissioni della catena di approvvigionamento (C44).

- **Affrontare gli Attacchi Ransomware:** Gli Stati membri devono sviluppare politiche per affrontare l'aumento degli attacchi ransomware, tenendo conto di modelli di attacco, modelli criminali commerciali e aumentare la consapevolezza e le risorse delle piccole e medie imprese (C54, C56).
- **Supporto alle Piccole e Medie Imprese:** Le strategie nazionali per la cibersicurezza devono affrontare le esigenze specifiche delle piccole e medie imprese, fornendo linee guida, assistenza e servizi come la configurazione dei siti internet (C56).

Misure di Sicurezza per i Soggetti Impattati:

- **Valutazione dei Fornitori:** I soggetti essenziali e importanti devono valutare la qualità e la resilienza dei prodotti e servizi, integrando misure di gestione dei rischi nei contratti con i fornitori e fornitori di servizi diretti (C85).
- **Valutazioni Coordinate dei Rischi:** Il gruppo di cooperazione, insieme alla Commissione e all'ENISA, dovrebbe effettuare valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche, individuando misure, piani di attenuazione e migliori pratiche (C90).
- **Integrazione nella Strategia Nazionale:** Le strategie nazionali per la cibersicurezza devono includere misure strategiche riguardanti la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati dai soggetti (Articolo 7).
- **Misure Multirischio:** Le misure di gestione dei rischi di cibersicurezza devono includere la sicurezza della catena di approvvigionamento, compresi gli aspetti relativi ai rapporti con i fornitori (Articolo 21).

La NIS2 mira a garantire una gestione sicura e resiliente delle catene di approvvigionamento, coinvolgendo soggetti di diversa dimensione e importanza, con particolare attenzione alle sfide delle piccole e medie imprese.

9.5 sicurezza acquisizione, sviluppo e manutenzione dei sistemi informatici di rete, compresa la divulgazione delle vulnerabilità

La direttiva (UE) 2016/1148 mira a sviluppare le capacità di cibersicurezza nell'Unione Europea, mitigando le minacce ai sistemi informatici e di rete utilizzati per fornire servizi essenziali in settori chiave. Gli obblighi riguardano i fornitori di servizi postali, le infrastrutture digitali, i data center, gli organismi di ricerca, i fornitori di servizi di comunicazione interpersonale e altri soggetti essenziali e importanti. La cibersicurezza è cruciale per il corretto funzionamento del mercato interno e la protezione da incidenti e minacce informatiche.

L'Articolo 21 della direttiva NIS 2 dettaglia le misure richieste per affrontare la sicurezza durante l'acquisizione, lo sviluppo e la manutenzione dei sistemi informatici e di rete. I soggetti essenziali e importanti sono obbligati ad adottare misure tecniche, operative e organizzative adeguate e proporzionate. Queste misure devono garantire un livello di sicurezza adeguato ai rischi esistenti, tenendo conto delle conoscenze più aggiornate, delle norme europee e internazionali pertinenti e dei costi di attuazione.

In particolare, l'Articolo 21 (c2 lett. e) specifica che le misure devono includere la "sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità". Questo sottolinea l'importanza di integrare la sicurezza in tutte le fasi del ciclo di vita dei sistemi, dalla progettazione all'implementazione e alla manutenzione continua.

Per quanto riguarda la gestione delle vulnerabilità, il testo enfatizza che i soggetti che sviluppano o gestiscono sistemi informatici e di rete dovrebbero stabilire procedure per gestire le vulnerabilità non appena scoperte. Inoltre, si evidenzia l'importanza della divulgazione coordinata delle vulnerabilità, indicando che i fabbricanti o fornitori di prodotti TIC dovrebbero mettere in atto procedure per ricevere informazioni sulla vulnerabilità da terzi. A questo proposito, vengono richiamate le norme internazionali ISO/IEC 30111 e ISO/IEC 29147, che forniscono orientamenti sulla gestione e divulgazione delle vulnerabilità.

Il testo mette in risalto che la divulgazione coordinata delle vulnerabilità è un processo strutturato che coinvolge il coordinamento tra chi segnala le vulnerabilità e i fabbricanti o fornitori, garantendo che le informazioni dettagliate non siano divulgate a terzi prima che il problema sia risolto. Questa pratica contribuisce a ridurre il rischio e a garantire una rapida identificazione e correzione delle vulnerabilità, mitigando gli impatti negativi sugli utenti, sull'economia e sulla società in generale.

I soggetti essenziali e importanti dovrebbero stabilire procedure per gestire le vulnerabilità nei sistemi informatici e di rete non appena scoperte. Dovrebbero anche mettere in atto procedure per ricevere informazioni sulla vulnerabilità da terzi, conformandosi alle norme internazionali ISO/IEC 30111 e ISO/IEC 29147. La divulgazione coordinata delle vulnerabilità è essenziale, e i soggetti dovrebbero rafforzare il coordinamento tra coloro che segnalano le vulnerabilità e i fornitori di prodotti o servizi TIC. La gestione dei rischi di cibersicurezza deve essere basata su un approccio multirischio, affrontando sia le minacce informatiche che gli eventi fisici, come furti o incendi, e dovrebbe includere misure per la sicurezza fisica e dell'ambiente, comprese le risorse umane.

Inoltre, l'Articolo 25 incoraggia l'uso di norme tecniche europee e internazionali per garantire un'attuazione convergente degli obblighi di sicurezza. La cooperazione transfrontaliera tra Stati membri è fondamentale, come sottolineato dall'Articolo 37, per affrontare la natura interconnessa delle minacce e garantire assistenza reciproca tra le autorità competenti.

La direttiva riconosce che gli incidenti e le crisi di cybersicurezza richiedono una risposta coordinata su vasta scala a livello dell'Unione, evidenziando l'importanza della cybersicurezza per la protezione dei cittadini, delle imprese e delle istituzioni. La responsabilità principale per la sicurezza dei sistemi informatici e di rete è assegnata a soggetti essenziali e importanti, e si promuove lo sviluppo di una cultura della gestione dei rischi per affrontare le minacce in modo proattivo.

9.6 Procedure (test e audit) per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza

La Direttiva NIS 2 riconosce l'importanza cruciale dei fornitori di servizi di sicurezza gestiti, come quelli impegnati nella risposta agli incidenti, nei test di penetrazione, negli audit di sicurezza e nella consulenza, nell'assistere i soggetti nei settori essenziali e importanti. Tuttavia, nota anche che tali fornitori sono a loro volta suscettibili di attacchi informatici, rappresentando un rischio particolare a causa della loro stretta integrazione nelle attività dei soggetti.

L'attenzione è posta sui soggetti essenziali e importanti, i quali dovrebbero esercitare una maggiore diligenza nella selezione di un fornitore di servizi di sicurezza gestiti. Inoltre, le autorità competenti, nel perseguire i loro compiti di vigilanza, possono beneficiare dei servizi di cybersecurity, tra cui audit sulla sicurezza, test di penetrazione e risposta agli incidenti.

Il testo sottolinea che l'esecuzione dei compiti di vigilanza da parte delle autorità competenti non dovrebbe ostacolare inutilmente le attività commerciali del soggetto interessato, e le metodologie di vigilanza dovrebbero seguire un approccio basato sui rischi. Ciò implica la classificazione dei soggetti essenziali in categorie di rischio, con misure di vigilanza raccomandate specifiche per ciascuna categoria. La NIS 2 promuove un approccio dinamico e proporzionato per garantire la sicurezza cibernetica, con un'attenzione particolare ai

fornitori di servizi di sicurezza gestiti e alle modalità di vigilanza da parte delle autorità competenti. Inoltre, si evidenzia l'importanza di ridurre al minimo l'impatto sulle attività commerciali durante l'esercizio dei compiti di vigilanza, comprese ispezioni in loco, audit sulla sicurezza e scansioni di sicurezza.

L'articolo 32 della NIS 2 stabilisce chiaramente che gli Stati membri devono garantire che le misure di vigilanza siano efficaci, proporzionate e dissuasive, considerando le circostanze di ciascun caso. Inoltre, le autorità competenti hanno il potere di sottoporre i soggetti importanti a varie misure, tra cui ispezioni in loco, audit sulla sicurezza periodici e mirati, nonché richieste di dati che dimostrino l'attuazione delle politiche di cibersicurezza.

Questo approccio basato sui rischi è evidenziato anche dall'uso di metodologie di vigilanza che possono essere valutate e riesaminate periodicamente. Inoltre, si enfatizza che i poteri di vigilanza dovrebbero essere esercitati in conformità con i quadri legislativi e istituzionali nazionali, assicurando al contempo che le misure siano proporzionate e mirate. In sintesi, il punto 1 della NIS 2 fornisce un quadro chiaro e dettagliato delle considerazioni e delle misure relative alla valutazione dell'efficacia delle misure di gestione dei rischi di cybersicurezza.

- **Articolo 32 - Misure di vigilanza e di esecuzione relative a soggetti essenziali:** Le misure di vigilanza e di esecuzione devono essere efficaci, proporzionate e dissuasive, adattandosi alle circostanze di ciascun caso. Le autorità competenti hanno il potere di sottoporre i soggetti importanti a diverse attività, tra cui ispezioni in loco, vigilanza a distanza, audit sulla sicurezza periodici e mirati.
- **Audit sulla Sicurezza Mirati:** Gli audit sulla sicurezza mirati sono un elemento chiave (Articolo 32, paragrafo 2, lettera b). Questi audit sono basati su valutazione del rischio, che possono essere condotte dall'autorità competente o dal soggetto sottoposto all'audit. I risultati di tali audit devono essere resi disponibili all'autorità competente. È importante notare che i costi associati a questi audit, se svolti da un organismo indipendente, sono generalmente a carico del soggetto sottoposto all'audit, a meno che l'autorità competente decida diversamente in circostanze debitamente giustificate.
- **Valutazione del Rischio:** La valutazione del rischio è il fondamento per la conduzione di audit sulla sicurezza mirati. Le metodologie di vigilanza dovrebbero seguire un approccio basato sui rischi, classificando i soggetti essenziali in categorie di rischio. Ciò include criteri per la frequenza e il tipo di ispezioni, audit sulla sicurezza e scansioni di sicurezza. Tali metodologie devono essere valutate e riesaminate periodicamente, garantendo la conformità alle esigenze di risorse e il mantenimento della rilevanza in un contesto in rapida evoluzione.
- **Rispetto degli Obblighi e Sanzioni:** Gli Stati membri devono garantire che le misure di esecuzione siano rispettate dai soggetti importanti. In caso di mancato rispetto, le autorità competenti possono adottare misure, compresa l'imposizione di sanzioni amministrative pecuniarie (Articolo 32, paragrafo 5, lettera i). Le sanzioni devono essere proporzionate alla gravità della violazione, con considerazione di vari fattori, tra cui la durata della violazione, eventuali precedenti, e l'impatto causato.

In breve, la NIS 2 stabilisce chiaramente che l'efficacia delle misure di gestione del rischio di cybersicurezza deve essere valutata attraverso audit mirati basati su valutazione del rischio, con particolare attenzione al rispetto degli obblighi da parte dei soggetti importanti. La valutazione del rischio è al centro di questo approccio, garantendo una risposta proporzionata e mirata alle minacce cibernetiche.

Collaborazione con Fornitori Affidabili:

I soggetti importanti dovrebbero stabilire collaborazioni strette con fornitori di servizi di sicurezza gestiti affidabili e di comprovata competenza. La NIS 2 sottolinea il ruolo chiave di tali fornitori, come quelli specializzati in risposta agli incidenti, test di penetrazione e audit di sicurezza. La

selezione di un fornitore affidabile è essenziale per garantire la sicurezza delle attività e mitigare i rischi associati agli attacchi informatici, considerando che essi stessi possono diventare bersagli a causa della loro stretta integrazione nelle attività dei soggetti.

Audit Periodici e Mirati:
La normativa raccomanda che i soggetti importanti siano sottoposti a audit sulla sicurezza periodici e mirati. Questi audit dovrebbero essere condotti da organizzazioni indipendenti qualificate o da autorità competenti. Gli audit sulla sicurezza mirati sono specificamente basati su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto all'audit. I risultati di tali audit dovrebbero essere resi disponibili all'autorità competente. Questa pratica consente una valutazione approfondita delle vulnerabilità e delle misure di sicurezza implementate, garantendo un monitoraggio regolare dell'efficacia delle strategie di cybersicurezza adottate.

Implementazione Rapida delle Raccomandazioni:
In seguito a un audit sulla sicurezza, i soggetti importanti dovrebbero essere pronti ad attuare rapidamente le raccomandazioni fornite. Questo passo è essenziale per garantire che le vulnerabilità identificate siano affrontate in modo tempestivo e che le misure correttive siano implementate per ridurre al minimo il rischio di incidenti di cybersicurezza. L'adeguata e tempestiva attuazione delle raccomandazioni contribuisce a mantenere un livello elevato di sicurezza cibernetica.

Trasparenza e Informazione:
La NIS 2 sottolinea l'importanza della trasparenza. I soggetti importanti dovrebbero informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività sulla natura delle minacce informatiche significative e sulle misure protettive o correttive che possono adottare in risposta a tali minacce. Questo approccio proattivo non solo promuove la consapevolezza sulla sicurezza cibernetica, ma consente anche alle parti interessate di prendere misure preventive o correttive adeguate in risposta alle minacce identificate.

In sintesi, la NIS 2 impone una serie di misure di sicurezza chiave, tra cui la collaborazione con fornitori affidabili, audit periodici e mirati, implementazione rapida delle raccomandazioni e trasparenza nelle comunicazioni. L'adozione di tali misure è fondamentale per affrontare le sfide sempre crescenti nel panorama della cybersicurezza e per garantire la resilienza delle infrastrutture critiche e dei servizi digitali.

9.7 Uso della crittografia e della cifratura

La NIS 2, nel suo articolo 21 dedicato alle "Misure di gestione dei rischi di cibersicurezza", affronta dettagliatamente l'importanza di adottare un approccio multirischio per proteggere sistemi informatici e reti da incidenti. Nel contesto della valutazione dell'efficacia delle misure di gestione dei rischi di cibersicurezza, la normativa sottolinea l'essenzialità di diversi elementi.

In primo luogo, la NIS 2 evidenzia la necessità di politiche di analisi dei rischi e di sicurezza dei sistemi informatici (punto a). Questo implica un processo strutturato per identificare, valutare e mitigare i rischi di cibersicurezza. Inoltre, si fa riferimento alla gestione degli incidenti (punto b), sottolineando l'importanza di avere procedure chiare e tempestive per affrontare e risolvere eventuali incidenti di sicurezza.

La normativa estende la sua copertura alla continuità operativa (punto c), includendo la gestione del backup e il ripristino in caso di disastro, oltre alla gestione delle crisi. La sicurezza della catena di approvvigionamento (punto d) è anch'essa considerata, con un focus sugli aspetti relativi ai rapporti tra i soggetti e i loro fornitori. Inoltre, sono menzionate la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete (punto e), con un'enfasi sulla gestione delle vulnerabilità.

Un punto chiave, rilevante per la valutazione dell'efficacia, è la sezione f che menziona "strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza." Questa disposizione sottolinea l'importanza di sviluppare approcci sistematici per valutare quanto efficacemente le misure di cibersicurezza affrontino i rischi identificati. Questo potrebbe includere test regolari, audit e valutazioni delle politiche adottate.

In conclusione, la NIS 2 offre un quadro dettagliato e orientato alla pratica per la valutazione dell'efficacia delle misure di gestione dei rischi di cibersicurezza, con un'enfasi particolare sulla necessità di approcci multirischio e procedure di valutazione strutturate.

La NIS 2, nell'articolo 21 relativo alle "Misure di gestione dei rischi di cibersicurezza", non fornisce direttamente linee guida specifiche per la valutazione dell'efficacia delle misure di gestione dei rischi. Tuttavia, definisce chiaramente gli elementi fondamentali che dovrebbero essere considerati in questo contesto:

I. **Politiche di analisi dei rischi e di sicurezza dei sistemi informatici:** Le organizzazioni dovrebbero sviluppare politiche ben definite per analizzare i rischi connessi alla sicurezza dei sistemi informatici. Questo coinvolge l'identificazione, la valutazione e la gestione dei rischi cibernetici.
II. **Gestione degli incidenti:** La normativa sottolinea l'importanza di avere procedure robuste per gestire gli incidenti di sicurezza informatica. Questo include non solo la risposta agli eventi in corso ma anche l'apprendimento dagli incidenti passati per migliorare la preparazione futura.
III. **Continuità operativa:** Le organizzazioni devono garantire la continuità delle operazioni, compresa la gestione dei backup e il ripristino in caso di disastro. Questo assicura che possano continuare a funzionare anche in seguito a eventi avversi.
IV. **Sicurezza della catena di approvvigionamento:** È essenziale proteggere la catena di approvvigionamento, considerando gli aspetti relativi alla sicurezza nei rapporti tra le organizzazioni e i loro fornitori o fornitori di servizi.
V. **Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete:** Questo implica l'implementazione di misure di sicurezza durante l'intero ciclo di vita dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità.
VI. **Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza:** La valutazione periodica dell'efficacia delle misure adottate è fondamentale. La normativa non specifica le modalità precise di questa valutazione, ma sottolinea l'importanza di avere strategie e procedure ben definite.
VII. **Pratiche di igiene informatica di base e formazione in materia di cibersicurezza:** Le organizzazioni dovrebbero promuovere pratiche di igiene informatica tra il personale e fornire formazione in materia di cibersicurezza per aumentare la consapevolezza e ridurre i rischi legati alle azioni umane.
VIII. **Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura:** La NIS 2 sottolinea l'importanza di avere politiche e procedure chiare sull'uso della crittografia, rispettando contemporaneamente il diritto dell'Unione in materia di protezione dei dati.
IX. **Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi:** Questo implica adottare misure di sicurezza per gestire le risorse umane, controllare l'accesso ai sistemi e gestire in modo adeguato gli asset digitali.

La NIS 2 suggerisce una serie di misure di sicurezza fondamentali per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza:

I. **Implementazione di procedure di test e audit regolari:** I soggetti interessati dovrebbero sviluppare e attuare procedure regolari di test e audit, utilizzando un approccio multirischio. Queste attività dovrebbero valutare diversi aspetti, inclusi ma non limitati a politiche di analisi

dei rischi, gestione degli incidenti, continuità operativa, sicurezza della catena di approvvigionamento e altri elementi chiave menzionati nell'articolo 21 della NIS 2.

II. **Adozione di strategie e procedure specifiche:** I soggetti dovrebbero sviluppare strategie e procedure specifiche per valutare l'efficacia delle misure di gestione dei rischi. Queste potrebbero includere parametri di valutazione chiave, metodologie di test e criteri di audit. L'approccio dovrebbe essere personalizzato per adattarsi alle particolarità dell'organizzazione, garantendo al contempo una copertura completa dei rischi di cibersicurezza.

III. **Considerazione dei principi di protezione dei dati:** Nell'attuare test e audit, i soggetti dovrebbero rispettare i principi di protezione dei dati sanciti dal regolamento (UE) 2016/679. Ciò include l'accuratezza, la minimizzazione dei dati, l'equità e la trasparenza, nonché la sicurezza dei dati, come indicato nella più recente crittografia. Le misure di protezione dei dati dovrebbero essere integrate fin dalla progettazione e configurate per essere predefinite.

IV. **Formazione del personale:** Implementare pratiche di igiene informatica di base e fornire formazione continua in materia di cibersicurezza. Il personale dovrebbe essere consapevole delle minacce attuali, delle migliori pratiche di sicurezza e delle procedure aziendali per affrontare incidenti.

In conclusione, per garantire un'efficace valutazione delle misure di gestione dei rischi di cibersicurezza, i soggetti interessati dovrebbero adottare un approccio completo e personalizzato, integrando procedure di test e audit regolari, strategie specifiche, rispetto dei principi di protezione dei dati e formazione del personale.

10 La valutazione del rischio nella Direttiva NIS2 e nella Direttiva CER (Glauco Bertocchi).

10.1 La Direttiva NIS2

L'articolo 21 della direttiva NIS2, intitolato “cybersecurity risk-management measures”, evidenzia l'importanza dell'analisi multirischio come attività centrale per poter prevenire eventuali incidenti e poter recuperare, qualora si verifichino, in tempi che siano adeguati alle esigenze di continuità dei servizi essenziali ed importanti. Agli Stati membri è affidato il compito di operare affinché i soggetti essenziale ed importanti adottino misure tecniche, operative ed organizzative, adeguate e proporzionate, per gestire i rischi alla sicurezza dei loro sistemi informatici e di reti. Naturalmente le misure, tecniche e non, devono tener conto delle conoscenze più aggiornate nonché delle norme europee ed internazionali in materia.

Le misure di sicurezza adottate devono essere proporzionali al rischio inteso come grado di esposizione, rilevanza del soggetto e probabilità che si verifichino incidenti; di questi ultimi si chiede di valutare la gravità includendo gli aspetti economici e sociali.

Il paragrafo due dell'articolo 21 elenca almeno 10 elementi che devono essere presenti nelle misure di sicurezza adottate. Tali elementi sono considerati essenziali; ovviamente i soggetti potranno e probabilmente dovranno, estendere tali misure con altre che consentano di soddisfare l’approccio “all hazards” richiesto per proteggere la rete e i sistemi informativi, compreso l’ambito fisico in cui questi risiedono.

Il paragrafo tre dello stesso articolo affida agli Stati membri la valutazione delle misure di cui al paragrafo precedente e in particolare di quelle relative alla sicurezza della catena di approvvigionamento, comprendendo gli aspetti relativi alla sicurezza dei rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi. Nella valutazione gli Stati membri includeranno anche le valutazioni coordinate dei rischi per la catena di approvvigionamento effettuate dal gruppo di cooperazione in collaborazione con la Commissione ed ENISA, come previsto dall'articolo 22 comma uno.

In accordo al successivo paragrafo 4 gli Stati membri devono operare affinché un soggetto, che non sia conforme alle misure indicate nel paragrafo due, adotti tutte le misure correttive necessarie, appropriate e proporzionate.

Il paragrafo 5, ultimo dell’art. 21, indica che la Commissione adotta, entro il 17 ottobre 24, atti di esecuzione che stabiliscono i requisiti tecnici e metodologici delle misure per quanto riguarda i fornitori di particolari servizi quali: registro dei nomi di dominio di primo livello , cloud computing e altro. La Commissione può anche adottare requisiti specifici per riguardo per soggetti importanti ed essenziali diversi da quelli indicati nel il primo paragrafo; la Commissione segue, per quanto applicabili, le norme europee e internazionali e coopera con il gruppo di cooperazione e con ENISA.

Ai fini della comprensione dell’importanza della gestione del rischio nella direttiva NIS2 è significativo evidenziare che nei considerando iniziali si trovano diverse indicazioni e approfondimenti relativi alla tipologia di rischi che devono essere considerati, a quale tipo di approccio dovrebbe essere preferito, nonché varie considerazioni riguardo la proporzionalità e l'adeguatezza e, infine, la gestione della catena di approvvigionamento. I considerando che riguardano l’analisi del rischio e gli aspetti correlati sono: 78, 79, 80, 81, 82, 83, 84, 85, 86, 88, 90, 91,92, 96, 97, 101.

L'impianto previsto da questa direttiva è fondamentalmente basato sulla cooperazione tra diversi soggetti, istituzionali e privati, con la finalità di adottare misure di sicurezza coordinate e di scambiare continuamente informazioni relativamente alle minacce e a tutti quei fattori che possono modificare la valutazione del rischio. L’obiettivo è quello di attuare un ecosistema sicuro.

10.2 La Direttiva CER

La direttiva CER rappresenta, per quanto concerne l'analisi del rischio un complemento alla NIS2 in quanto estende ad altri settori i requisiti già presenti in quest'ultima. L'art 1 comma 2 della CER indica la necessità che le 2 direttive siano implementate in modo coordinato al fine .3.3) di evitare la creazione di duplicazioni o sovrastrutture.

Viene introdotto e definito il concetto di resilienza (art. 1 c.3 e art.3 p.3) come pure il capitolo III della direttiva è dedicato alla resilenza delle Entità Critiche e in particolare l'articolo 13 è dedicato alle misure di resilenza delle Entità Critiche. La resilienza è di rilevante importanza per l'analisi del rischio poiché quest'ultima deve adeguatamente considerare e valutare anche i rischi connessi alle entità fisiche, organizzative, di personale e cyber che sono preposte ad aumentare la resilienza delle Entità Critiche. Ad esempio, poiché sono previsti degli specifici controlli per il personale che opera nei settori critici, si dovrà anche valutare il rischio (probabilità ed impatto) derivante dalla non corretta applicazione o svolgimento dei controlli prescritti.

La definizione di rischio e della sua valutazione è indicata all'art3 p.7 mentre l'art 5 indica la valutazione del rischio da parte degli stati membri con particolare attenzione all'interdipendenza settoriale (c.2 p.2) e allo scambio di informazioni tra Stati (c.4.). La valutazione del rischio da parte delle Entità Critiche è indicata nell'art 12 dove il c.2 specifica esplicitamente i rischi naturale e causati dall'uomo.

I criteri per la valutazione degli impatti sono indicati all'art.7 relativamente ai "significant disruptive effect".

La direttiva CER è, come la NIS2, basata su uno scambio continuo di informazione cui contribuisco diverse strutture di supporto a livello europeo. In particolare l'art4 (c.2 p.g)indica il coordinamento per lo scambio di informazioni sulle minacce cyber e non cyber ed anche sugli incidenti. Lo scambio di informazioni tra stati è anche indicato nell'art.5 c. 4.

Il capitolo V della direttiva è dedicato alla cooperazione e al reporting, in particolare l'art 19. Istituisce un "Critical Entities Resilience Group" presieduto da un rappresentante della Commissione EU che ha anche (c.3 p.c) il compito di facilitare lo scambio di best practices per l'identificazione delle Entità Critiche con riguardo alle relazioni transfrontaliere e le dipendenze tra settori e anche riguardo ai rischi e agli incidenti.

Nello stesso capitolo V l'art.20 Indica il supporto che la Commissione EU fornirà agli stati membri e alle Entità Critiche per rispettare gli obblighi imposti dalla direttiva CER.

È utile evidenziare che anche lo scambio di informazioni, il coordinamento e il supporto estendono l'ambito dell'analisi del rischio che deve includere anche queste attività e le strutture organizzative che le realizzano.

Agli articoli prima indicati è necessario aggiungere tutte le considerazioni iniziali che rappresentano un'utile specificazione delle finalità e degli obiettivi della direttiva. La direttiva CER ha 45 considerando e molti di essi riguardano in modo diverso il rischio, la sua identificazione e valutazione; essi sono identificati con i numeri 2,3,5,6,7, 8,9,13,15, 20, 21(esclude i servizi delle financial entities dal campo di applicazione dellaCER), 24, 27,28,29,30,31.

È opportuno notare che entrambi le direttive, CER e NIS2, hanno lo stesso approccio all'individuazione e alla valutazione del rischio, prevedono inoltre le stesse tipologie di rischio, e strutturano in modo equivalente il coordinamento a livello europeo e gli obblighi per gli stati.

Tra le direttive, almeno per quanto riguarda gli ambiti prima indicati, esiste una tale convergenza che è specificamente previsto un coordinamento applicativo. La principale differenza è rappresentata dai due diversi elenchi di infrastrutture

10.3 Stato dell'Arte dell'analisi del rischio

Lo standard ISO 31000

Quanto segue è un'estrema sintesi dell'argomento sul quale esiste amplissima letteratura. Tra i vari possibili approcci e gli standard disponibili abbiamo ritenuto più idoneo, in quanto fornisce principi e linee guida generali, utilizzare lo standard ISO 31000:2018 "Risk management -- Principles and guidelines".20. Per ragioni di completezza tra i principali standard è opportuno indicare anche gli statunitensi NIST SP800-30R121 e NIST SP800-39 22 , quest'ultimo dedicato alla sicurezza delle informazioni

Questo standard ISO descrive il processo di Risk Management (Gestione del Rischio) con l'intento di armonizzare i criteri di analisi e gestione del rischio. Da esso o nello stesso periodo sono state sviluppate, ad esempio dal NIST (National Institute for Standard and Technology), diverse metodologie che, pur con alcune differenziazioni, seguono lo stesso schema di principio.

È importante evidenziare che i principali organismi di standardizzazione e di normazione europei e statunitensi hanno prodotti molti documenti che affrontano la gestione del rischio in tutte le sue articolazioni per i più svariati settori (ICT, Apparati Industriali, Medicina, Aerospace, ecc) I documenti di tipo settoriale si basano sugli schemi generali ISO o NIST citati in precedenza

È necessario anche considerare lo standard ISO/IEC 31010:2019 Risk management — Risk assessment techniques 23 che complementa lo standard ISO 31000.

Il *Risk Management* è il processo di identificazione e valutazione dei rischi per tenerli sotto controllo, ossia ad un livello accettabile nei confronti dell'entità (azienda, organizzazione, beni materiali e/o immateriali, persone, ecc.) da proteggere.

Lo standard ISO 31000 è volto a definire:

a) Il processo di Risk Management
b) come vengono identificati, analizzati e trattati i rischi
c) Il Framework di gestione del rischio
d) la struttura generale e il funzionamento della gestione del rischio in tutta la organizzazione, simile al ciclo Plan/Do/Check/Act (PDCA)
e) Un insieme di principi che guidano le attività di gestione del rischio

La figura seguente, tratta dallo standard ISO 31000:2018, descrive l'articolazione interna e le relazioni tra queste componenti.

[20] ISO 31000:2018 *Risk management -- Principles and guidelines*
https://www.iso.org/standard/65694.html
[21] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
[22] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
[23] ISO/IEC 31010:2019 *Risk management — Risk assessment techniques*
https://www.iso.org/standard/72140.html

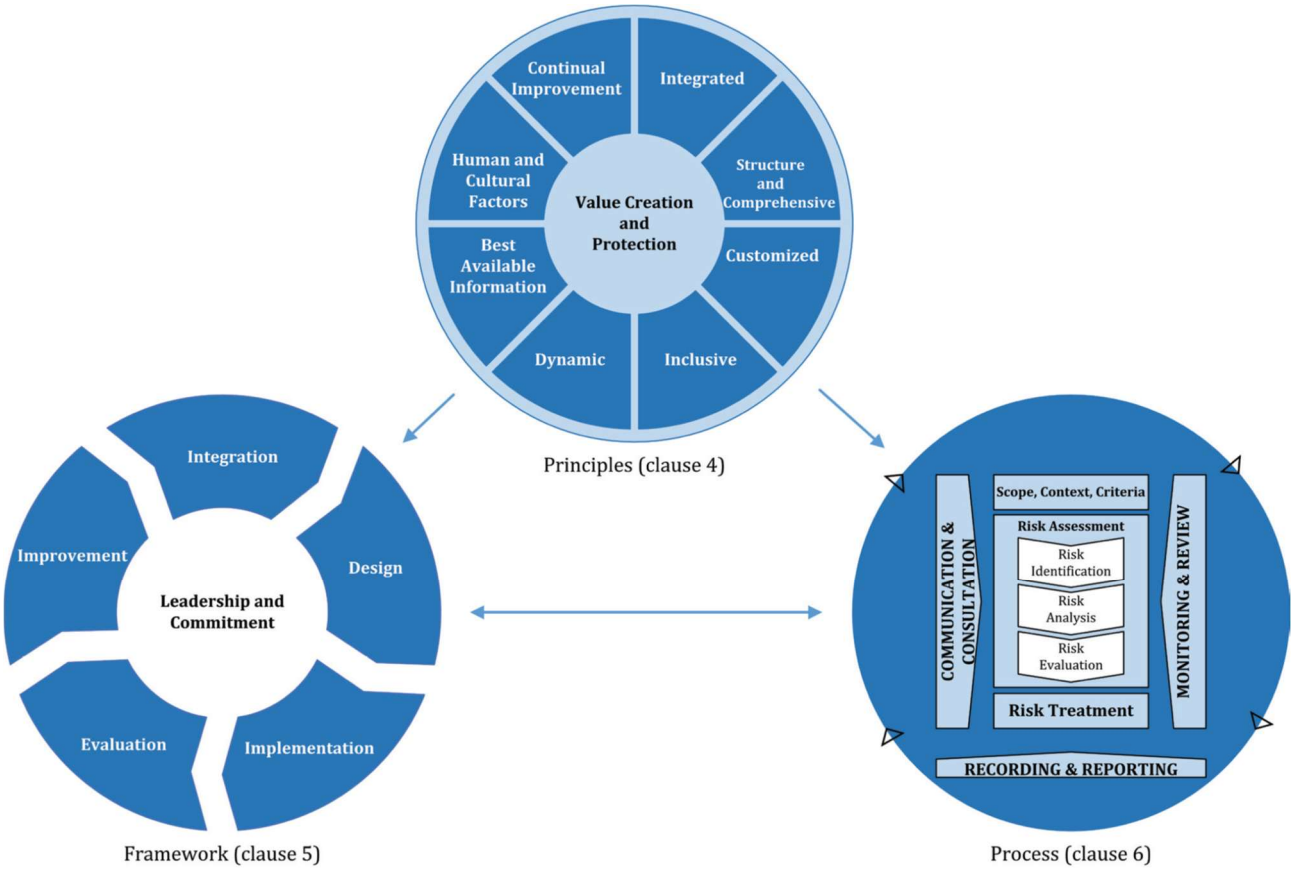


Tabella 19 - Schema delle articolazioni interne delle componenti dello standard ISO 31000:2018

Lo standard riporta uno specifico capitolo (Clause 4) dedicato ai principi che devono ispirare la costruzione di un sistema per la gestione del rischio.

Questi principi sono quelli che determinano la cornice organizzativa (framework) e il processo di gestione del rischio. Rappresentano i requisiti che devono essere soddisfatti per ottenere una gestione del rischio che sia la migliore possibile per l'organizzazione. Sono formulati in modo da essere applicabili a qualsiasi tipologia di settore di attività e in modo indipendente dalla struttura organizzativa.

Nello standard è anche indicata la cornice organizzativa (Clause 5) che governa l'instaurazione del processo di Risk Management. Ne delinea la struttura generale evidenziano la necessità dell'impegno, sostanziale e non formale, della Leadership dell'organizzazione e delinea il funzionamento della gestione del rischio in tutta la organizzazione con un ciclo simile al ben noto Plan/Do/Check/Act (PDCA)

Il processo di Gestione del Rischio (Clause 6) si compone sinteticamente di quattro fasi:

I. descrizione degli obiettivi
II. identificazione e valutazione del rischio
III. trattamento del rischio (risk treatment)
IV. verifica (monitoring)

10.4 La convergenza ICT OT IoT

Prima dell'introduzione massiva delle tecnologie ICT l'analisi del rischio in ambito OT (Operational Technology), ossia gli impianti e l'automazione in generale, aveva un approccio essenzialmente prescrittivo, ossia di conformità a norme di legge e/o regolamenti, che corrispondeva alla necessità

di assicurare un livello minimo di sicurezza a settori di attività che altrimenti sarebbero stati possibile fonte di incidenti in misura non accettabile.

L'introduzione delle reti digitali (Internet) e la diffusione dei sistemi ICT a tutti i livelli ha modificato radicalmente le opportunità di gestione degli impianti e delle aziende. Contemporaneamente ha aumentato la velocità di diffusione delle minacce e degli attacchi, modificando il concetto stesso di sicurezza specie per i gestori degli impianti che utilizzano sistemi di origine ICT nell'ambito della OT, ossia i sistemi di controllo e supervisione degli impianti. Gli attacchi informatici sempre più frequenti ai sistemi di controllo delle Infrastrutture, Critiche e non Critiche, hanno portato all'attuale convergenza della Cybersecurity OT e ICT e alla loro integrazione nel prossimo futuro come due aspetti della Cybersecurity.

10.5 ISA/IEC 62443 Standards

Molte Entità Critiche come pure gli Operatori di Servizi Essenziali, nel nostro caso useremo indifferentemente le tipologie previste dalle direttive NIS2 e CER, sono composte in parte o prevalentemente, da impianti (ad esempio la produzione dell'energia) che hanno frequentemente un elevato grado di automazione, ossia componenti OT e IoT per le quali gli aspetti di analisi del rischio devono essere condotti sia in ambito cybersecurity che per quanto concerne la safety.

Di particolare rilievo è in quest'ambito la serie di standard ISA/IEC 62443 che ha come scopo la sicurezza degli IACS (Industrial Automation and Control Systems). La serie di standard la cui pubblicazione non è ancora completata, ha il supporto delle Nazioni Unite[24] ed è basata anche sulla guida NIST per i sistemi industriali di controllo[25] Un sistema IACS è definito come: un insieme di personale, hardware, software e politiche coinvolte nel funzionamento del processo industriale e che possono influenzare o influenzare il suo funzionamento sicuro, protetto e affidabile. Si noti che uno IACS non comprende solo la tecnologia che compone un sistema di controllo, ma anche le persone e i processi lavorativi necessari per garantire la sicurezza, l'integrità, l'affidabilità e la protezione del sistema di controllo. Senza personale sufficientemente addestrato, tecnologie e contromisure adeguate al rischio e processi di lavoro lungo tutto il ciclo di vita della sicurezza, un sistema IACS potrebbe essere più vulnerabile agli attacchi informatici. Poiché i sistemi IACS sono sistemi cyber-fisici, l'impatto di un attacco informatico potrebbe essere grave.

Le conseguenze di un attacco informatico a un sistema IACS includono, ma non sono limitate a:

- Pericolo per la sicurezza o la salute del pubblico o dei dipendenti
- Danno all'ambiente
- Danno alle apparecchiature sotto controllo
- Perdita dell'integrità del prodotto
- Perdita della fiducia del pubblico o della reputazione dell'azienda
- Violazione di requisiti legali o normativi
- Perdita di informazioni proprietarie o riservate
- Perdita finanziaria
- Impatto sulla sicurezza dell'entità, locale, statale o nazionale.

Le prime quattro conseguenze dell'elenco sopra riportato sono uniche per i sistemi Cyber -fisici e non sono tipicamente presenti nei sistemi IT tradizionali. È proprio questa differenza a determinare la necessità di approcci diversi alla sicurezza dei sistemi fisico-cyber e a indurre le organizzazioni di

[24] United Nations Commission fo Integrate ISA/ IEC 62443 Into Cybersecurity Regulatory Framework, ISA InTech Magazine, Jan-Feb, 2019

[25] NIST SP 800-82 Revision 2, Guide To Industrial Control Systems (Ics) Security

sviluppo degli standard a identificare la necessità di standard unici per i sistemi IACS. Altre caratteristiche dei sistemi IACS che non sono tipiche dei sistemi IT sono:

- Modalità di guasto più prevedibili
- Criticità temporale e determinismo più stretti
- Disponibilità più elevata
- Gestione più rigorosa delle modifiche
- Periodi di tempo più lunghi tra una manutenzione e l'altra
- Durata di vita dei componenti significativamente più lunga
- Sicurezza, integrità, disponibilità e riservatezza (SIAC) invece di CIA(Confidenzialità, Integrità, Disponibilità)

La serie di standard ISA/ICE 62443 include anche uno specifico documento riguardante l'analisi del rischio[26].

Gli standard e le linee guida per la sicurezza dell'ambito OT e la sua "convergenza", con le differenziazioni prima indicate, con il mondo ICT non esauriscono l'evoluzione determinata dalle tecnologie digitali che con il diffondersi capillare della connettività, sinteticamente definibile come Internet, ha visto l'apparire dell'"Internet delle Cose" (IoT).

10.6 Il mondo IoT

I dispositivi IoT sono una realtà che interessa, ovviamente con modalità diverse, tutte le Entità oggetto delle direttive NIS2 e CER. Non è questa la sede per analizzare l'uso degli Iot e degli IIoT (la versione industriale degli IoT) nell'ambito delle Entità ma ci si limiterà a indicare i principali standard o best practice di riferimento. L'architettura di riferimento degli IoT è lo standard ISO/IEC 30141[27] .

Sull'argomento ci sono diverse pubblicazioni diverse ENISA[28] e NIST[29] che definiscono vari aspetti della security di questi dispositivi.

Per comprendere come la convergenza dei vari ambiti ICT, OT e IoT sia un'esigenza "culturale" è utile citare che la versione attuale (R5) del principale documento NIST sulla cybersecurity (NIST SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations)[30] è stato formulato per includere tutte le tipologie possibili di piattaforme computazionali , inclusi gli IoT.

10.7 L'evoluzione dell'analisi del rischio per soddisfare i requisiti delle direttive.

La direttiva NIS2 ha uno speciale focus sulla cybersecurity e sui rischi dell'ambito cyber che si allarga anche altre tipologie di rischi derivanti le cause più disparate che possono avere un effetto concreto

---

[26] ISA-62443-3-2-2020 – Security for Industrial Automation and Control Systems, Part 3-2: Security Risk Assessment for System Design

[27] ISO/IEC 30141:2018 Internet of Things (IoT) Reference Architecture

[28] ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures (2017-11)
ENISA Convergence iot e cloud (2018-09)
ENISA Iot security gap (2018-12)
ENISA Good Practices for Security of Internet of Things in the context of Smart Manufacturing (2018-11)
ENISA Iot SDLC (2019-11)
ENISA Guidelines for securing the internet of things. Secure supply chain for IoT (2020-11)

[29] NIST SP 800-183 Network of Things
NIST IR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
NISTIR 8259 (Recommendations for IoT Device Manufacturers: Foundational Activities (May 29, 2020)

[30] NIST SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations

sulle Entità da proteggere. Analoga considerazione sono valide anche per le Entità oggetto della direttiva CER.

Si dovrà quindi estendere l'ambito di applicazione dell'analisi del rischio in modo da considerare tutte le tipologie indicate dalle direttive, ovviamente tenendo conto della tipologia delle Entità nell'applicazione concreta.

Si osservi anche che quanto richiesto dalle direttive va oltre la conformità a singole norme e implica la valutazione "continua" dei rischi e delle interdipendenze.

Inoltre, l'analisi del rischio dovrebbe avere come obiettivo non solo la sicurezza intesa come protezione o la business continuity, ma piuttosto il miglioramento della resilienza delle organizzazioni ciò comporta l'estensione del campo di applicazione alle strutture interconnesse e/o interdipendenti.

Le considerazioni precedenti comportano un'evoluzione dell'analisi del rischio di cui si cercherà di individuare i principali requisiti e alcuni possibili approcci.

Tra i fattori emergenti di rischio di cui sono evidenti i possibili effetti c'è sicuramente il cambiamento climatico che richiederà soluzioni che consentano sia di proteggere le Entità per un periodo che includa la loro vita operativa e, conseguentemente da evoluzioni climatiche di lungo periodo, sia da eventi locali di sempre maggiore entità che potrebbero danneggiare seriamente le Entità o quantomeno ridurre la loro capacità di assicurare il servizio richiesto.[31]

Un altro fattore di rischio emergente, peraltro ancora in via di definizione, è rappresentato dall'utilizzo delle varie forme di intelligenza artificiale (AI) da parte delle Entità. L'utilizzo della AI è sicuramente di interesse in vari ambiti delle attività delle organizzazioni oggetto delle direttive NIS2 e CER, ad esempio nella gestione del contatto con la clientela come pure nella diagnosi di guasti e nell'addestramento del personale. I relativi rischi non sono di semplice identificazione e valutazione e siamo nella fase iniziale sia dell'utilizzo della AI che dell'assesment dei relativi rischi.[32]

Un altro fattore di rischio di particolare rilievo per le Entità interessate dalle due direttive è la sicurezza della supply-chain e i conseguenti rischi che essa comporta per la resilienza di servizi essenziali. Le due direttive dedicano una particolare attenzione a questo fattore di rischio di difficile valutazione e talvolta sottovalutato in ragione delle difficoltà di definizione e apprezzamento. Ad esempio, l'art.22 della NIS2 prevede l'intervento di specifiche entità a livello comunitario (gruppo di coordinamento, la commissione e l'Enisa) per la valutazione e il coordinamento della sicurezza di supply chains critiche.

Alcune evoluzioni nell'analisi del rischio sono già in atto, come ad esempio per il rischio cyber, per i quale sarebbe opportuna l'adozione di metodi di tipo quantitativo probabilistico che consentano di analizzare meglio gli effetti della complessità dello scenario di minacce cyber.

Quest'ambito merita sicuramente una particolare attenzione e potrà essere oggetto di un progressivo cambiamento di paradigma che porti alla definizione e alla diffusione di metodiche che consentano stime di probabilità e simulazioni di scenari di rischio come già accade in molti settori (assicurativo, bancario, epidemiologico, ecc.)[33]

---

[31] AIIC (2023). *Resilienza delle Infrastrutture Critiche e Cambiamenti Climatici*, https://infrastrutturecritiche.it/resilienza-delle-infrastrutture-critiche-e-cambiamenti-climatici-2/

[32] NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) 2023 https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[33] D. Vose, "Risk Analysis: a quantitative guide", 3rd ed.,John Wiley & Sons, 2009
Open Group, Technical Standard: Risk Taxonomy (C081, ISBN: 1-931624-77-1), January 2009, The Open Group.
J. Freund, J. Jones, "Measuring and managing Information Risk: a FAIR approach", Butterworth-Heinemann, 2015
D.W. Hubbard, R. Seiersen, "How to measure anything in Cybersecurity Risk", Wiley, 2016
ISACA, "GETTING STARTED WITH RISK SCENARIOS", 2022,

La necessità di adottare un'analisi dei rischi multifattoriale o multirischio comporta l'esigenza di dotarsi di strumenti complessi in grado di valutare, non solo i rischi settoriali ma anche le interazioni tra tutte le entità dell'ecosistema. La finalità è quella di operare una sintesi che consenta non solo l'individuazione dei rischi più rilevanti, ma anche la valutazione dell'efficacia delle misure complessivamente messo in atto. Con quest'ultimo termine si intende anche il contributo, positivo o negativo, che deriva dalle misure di sicurezza messe in atto anche dalle entità "connesse" a quella della quale si vuole valutare l'esposizione ai rischi.

Gli attuali sistemi IRM (Integrated Risk Management) possono costituire una risposta tecnica alle esigenze operative in quanto consentono l'integrazione in un unico sistema dei diversi tipi di rischio che un'organizzazione deve considerare. In questo ambito ci sono molti esempi di prodotti GRC (Governance, Risk, Compliance) anche se l'estensione degli ambiti dell'analisi del rischio prevista dalle normative NIS2 e soprattutto CER impone probabilmente un significativo incremento di metodi e prodotti.

L'analisi del rischio come delineata dalle due direttive è un processo complesso che richiede competenze multidisciplinari e strumenti tecnici sofisticati. Tutto ciò potrebbe non essere alla portata di tutti gli OSE e quindi si potrebbero verificare delle carenze. A tal proposito sono stati già indicati i numerosi articoli delle due direttive che istituiscono diversi strumenti di coordinamento e supporto a livello europeo, finalizzati ad affrontare la situazione attuale e le sue evoluzioni future in maniera coordinata e adeguata al rilievo delle minacce e delle risorse da proteggere. In tal senso assume un ruolo di assoluto rilievo l'ENISA. Altre realtà hanno avuto un approccio diverso alla sfida posta dall'evoluzione dei metodi di analisi e degli strumenti promuovendo un partenariato tra soggetti pubblici e privati per l'avanzamento dello stato dell'arte. Un esempio di tale metodo è il progetto Venture[34] per la riduzione del rischio cyber di tipo sistemico, che vede tra l'altro la partecipazione del National Risk Management Center (NRMC), del Department of Homeland Security (DHS).

Anche dal punto di vista organizzativo le direttive pongono delle sfide derivanti dalla complessità delle interazioni previste che dovrà essere esaminata anche dal punto di vista dell'analisi del rischio. Infatti, problematiche derivanti da carenze organizzative o di comunicazione tra i vari soggetti previsti potrebbero comportare degli incidenti o dei ritardi, con conseguenti impatti dal punto di vista dei servizi in termini sociali ed economici.

In base alle considerazioni precedenti si possono sintetizzare le caratteristiche della gestione del rischio secondo le direttive. Deve avere uno "scope" o perimetro di applicazione che deve includere tutti le attività fondamentali per il funzionamento dell'entità; inoltre deve essere multifattoriale o multirischio e includere tutte le tipologie di rischi che possono impedire o alterare in modo significativo le finalità dell'attività dell'entità. A queste caratteristiche "basilari" dovremo aggiungere un monitoraggio e aggiornamento "continuo" dei fattori di rischio al fine di migliorare le capacità di prevenzione, detezione e reazione. Le capacità di monitoraggio e aggiornamento "continuo" dovrebbero quindi estendersi a tutti quelle interdipendenze, a partire dalla supply chain ma non solo, che possono influire, positivamente o negativamente, sulle capacità dell'entità critica. Inoltre, la valutazione degli impatti di natura sociale ed economica implica l'esigenza di una valutazione maggiormente quantitativa dei rischi. Infine, la direttiva impone una serie di coordinamenti e di comunicazioni sia a livello di singoli stati che con le autorità europee che comportano l'analisi del rischio derivante da tali attività.

Si tratta nel complesso di una significativa evoluzione dello stato dell'arte dell'analisi dei rischi che richiederà sia sviluppo tecnologico che ricerca applicata.

L'imminente entrata in vigore della direttiva avverrà quindi in una situazione di parziale "inadeguatezza" degli strumenti disponibili. Questa "carenza" potrà forse consentire una migliore

ISACA, "Risk Scenarios Toolkit", 2022

[34] https://www.cisa.gov/systemic-cyber-risk-reduction

definizione e sperimentazione dell'efficacia dell'attuazione della direttiva in una fase iniziale; sicuramente rappresenterà un impulso al lavoro di ricerca e sviluppo necessario per l'introduzione di sistemi innovativi.

11 La gestione degli incidenti di cybersecurity e cyber resilience (Elio Antonelli).

11.1 Specificità della gestione degli incidenti di cybersecurity

L'impianto tecnologico che la NIS2 prevede nelle sue direttive è dettato dall'articolo 21. Le misure ivi previste, si potrebbero definire come "i 10 comandamenti della NIS2" visto che, numericamente, tante sono le raccomandazioni nell'articolo previste:

I. La sicurezza dell'acquisizione, dello sviluppo e della manutenzione delle reti e dei sistemi informativi, compreso il trattamento e la divulgazione delle vulnerabilità;

II. Utilizzo di metodi di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali di sicurezza e dei sistemi di comunicazione correlati al grado di riservatezza e dell'urgenza, secondo i propri bisogni;

III. Elaborazione di Politiche e Procedure per valutare l'efficacia delle misure di gestione dei rischi in materia di cybersecurity;

IV. Implementazione di pratiche di base in materia di cyber-hygene e di awareness (p.es. Clean & Clear Desktop policy, uso responsabile dei dispositivi informatici, ecc.), per una sempre maggiore formazione del personale alla cybersecurity;

V. Politiche e Procedure relative all'utilizzo della crittografia e, dove applicabile, della cifratura;

VI. Politiche relative all'analisi dei rischi e alla sicurezza dei sistemi informativi

VII. Una gestione degli incidenti efficiente e organizzata, anche in termini di ruoli e responsabilità;

VIII. La continuità H24 delle attività, per esempio la gestione dei backup e la riprese delle attività, e la gestione degli stati di crisi;

IX. La sicurezza della catena di approvvigionamento, ivi compresi gli aspetti legati alla sicurezza concernente le relazioni tra ciascuna entità e suoi fornitori che prestano dei servizi diretti;

X. La sicurezza delle risorse umane e delle pratiche di access e asset management.

È proprio per seguire questi 10 comandamenti che l'industria dell'hardware incaricata di fornire ad esempio i dispositivi OT si rifanno ormai sempre più allo standard ISA/IEC 62443, norma che prevede ipso-facto la compliance totale con quanto in essi "comandato".

11.1.1 Organizzazione, analisi dei rischi e processi

L'articolo 6, parte del Capo I Disposizioni Generali, definisce gli accadimenti perturbanti la normale continuità operativa che possono impattare l'organizzazione sia a livello di blocco delle attività che di solo rilevamento durante la fase di vigilanza e monitoraggio.

- Quasi incidente: un evento potenzialmente lesivo dei principi di C.I.A. ma che è stato evitato con successo (rilevandolo dai sistemi di Lesson Learned messi in campo nell'organizzazione);
- Incidente: un evento che compromette di fatto i principi di C.I.A.;

- Incidente cyber di vasta scala: quando il livello di perturbazione travalica la capacità di efficacia della response di uno Stato e coinvolge almeno due membri dei 24 attualmente previsti;
- Gestione degli incidenti: il processo volto alla definizione, analisi, rilevazione, risposta di ogni evento perturbante l'organizzazione;
- Minaccia: una condizione che può essere sfruttata da agenti malevoli per perpetrare delle azioni malevoli su un'organizzazione. Si distingue in "significativa" la minaccia informatica che effettivamente, non potenzialmente, ha la facoltà di poter essere sfruttata per causare danni considerevoli;
- Vulnerabilità: un parametro che, rispetto agli standard di sicurezza prevalenti, non sono compliant, mostrando difetti o bug nel contesto della particolare minaccia incombente sull'organizzazione;
- Cloud: un servizio che consente l'esternalizzazione di infrastruttura, sistemi o servizi, condividendolo tra il CSP e l'organizzazione;
- Data Center: presenza di infrastruttura, sistemi o servizi on-premise all'organizzazione

Sebbene le entità che forniscono servizi ITC a organizzazioni che svolgono attività di tipo financial siano esentate dal monitoraggio delle direttive, perché già soggette a meccanismi di vigilanza vigenti per entità di tale tipo, le direttive NIS2 consigliano di tenere bene conto nelle attività di vigilanza di quanto tracciato nel processo di Risk Assessment degli aspetti finanziari, estendendo il caso parimenti ai fornitori terzi.
Relativamente poi a quanto già successo nell'ambito finanziario di un effetto a catena nelle crisi sistemiche, la NIS2 raccomanda la convergenza delle contromisure ITC messe in campo per la riduzione del rischio informatico derivante da simili eventi. Anche nella revisione e nell'adozione di aggiornamenti e riesami delle attività inerenti all'analisi del rischio financial si pone l'attenzione sulla necessità di agevolare affinché vi sia un'omogeneità a livello di comunicazione scambio informativo con le autorità di settore interessate, nonché di cooperazione con le strutture finanziarie europee (la banca centrale privata europea BCE, in primis). Anzi, si sollecita alla edificazione di una rete di sorveglianza comune e ad una Due Diligence comune da indirizzare verso i fornitori terzi di servizi ITC critici. Insomma, particolare attenzione, e questo perché i fatti dei primi del secolo attuale lo hanno dimostrato, le pratiche di Risk Assessment sono particolarmente importanti per il ruolo che nella CSF 2.0 viene assegnato alla Governance nella sequenza temporale, prima, durante e dopo l'accadimento di un incidente. Rilevante, quindi, diventa anche che le autorità di sorveglianza si facciano external auditor nei confronti delle terze parti, effettuando visite direttamente nei locali e effettuare audit al fine di raccogliere proof di presenza di monitoraggio e evidenze di compliance a quanto richiesto dalle normative vigenti. Per le attività di questo tipo, quindi, le direttive sollecitano la nomina di un referente unico della persona giuridica con il quale l'autorità di sorveglianza può effettuare le attività di coordinamento. Attività che, ovviamente includono anche la notifica delle minacce, gli obblighi di segnalazione.
Su quest'ultimo punto in particolare si sofferma l'articolo 23.
La struttura centrale nazionale CSIRT, come noto, è il centro stella del processo di comunicazione degli incidenti significativi che hanno impatto sulla continuità operativa dei servizi. La comunicazione degli incidenti al CSIRT permetterà di valutare impatti transfrontalieri, avendo la struttura una visione più ampia rispetto a un singolo Stato. La comunicazione riguarda le minacce rilevate, le contromisure e le azioni correttive messe in campo. La notifica dell'incidente significativo al CSIRT deve avvenire senza ritardo, entro 24 ore dall'allerta che scatta quando un evento classificabile come incidente venga rilevato, ed entro 72 ore ogni azione presa, l'entità di rilevanza dell'incidente, l'impatto sull'asset, comunicando eventuali indicatori di compromissione. Solo per i

CSP la notifica è obbliga entro le 24 oreIl CSIRT, peraltro, avrà l'autorità di richiedere autonomamente aggiornamenti rispetto ai tempi di massima prescritti, incluso una relazione dettagliata su tutti i parametri di identificazione dell'incidente. Anzi quest'ultima dovrà in ogni caso far parte di una relazione finale entro un mese dalla conclusione del processo di gestione dell'incidente.
Se poi l'incidente ha caratteristiche che imputano alla criminalità organizzata la responsabilità degli accadimenti, allora il CSIRT stesso potrebbe fornire ausilio nelle attività di controreazione o orientamenti significativi sulla segnalazione. Il CSIRT stesso, poi, ha come struttura superiore, punto di contatto, l'ENISA, con il quale può condividere il complesso di informazioni ricevute. Quest'ultimo, dunque, riceve le informazioni, se l'incidente ha caratteristiche transfrontaliere, dal CSIRT, o dall'autorità o dal punto di contatto unico. Anzi, questi ultimi ogni 3 mesi devono relazionare riportando le casistiche di incidenti verificatisi, le nuove minacce rilevate, gli incidenti notificati.

Quindi, è importante ribadire che per quanto riguarda le disposizioni dell'impianto previste nella NIS2 per il PSNC viene sancito l'obbligo di notifica, entro 72 ore, degli eventi che si sono scatenati in un'organizzazione, classificabili come incidenti. Pena atti sanzionatori. Un incidente è un'anomalia che mette a rischio la salvaguardia dei principi di Confidenciality, Integrity, Availability (C.I.A.) e crea un danno di business all'organizzazione.
Un'organizzazione ben strutturata ha effettuato nel proprio Sistema di Gestione, una Business Impact Analysis in cui è descritta la lista delle applicazioni/servizi critici, specificando RTO e RPO, oltre alla descrizione del contesto. Le pratiche di Asset Management, poi, elencano le risorse, la loro localizzazione, al di là degli aspetti infrastrutturali.
Solitamente, in tema di Incident Mangement le organizzazioni si riferiscono a quello che accade nella propria infrastruttura, CED, o sede remota. Ma il dispositivo della NIS2 prevede invero anche quegli incidenti "aventi impatto su reti, sistemi informativi e servizi informatici di propria pertinenza". Quindi un incidente è qualunque cosa che anche potenzialmente crei instabilità nel regime permanente dell'operatività dei servizi forniti, causando danni tecnologici e di business, ma financo sulla ripercussione eventuale che può riflettersi sulle persone fisiche.

Di fatto in tal senso il dispositivo procede parallelamente a quanto riferito alla Supply Chain, ossia alla catena di approvvigionamento e fornitura, che va inteso come territorio entro il quale verificare la traslazione della Sicurezza Informatica. L'estensione del perimetro informatico va quindi oltre i propri confini, laddove vi siano parcheggiati dati, o sistemi di pertinenza dell'organizzazione; non più ci si deve riferire esclusivamente gli incidenti che impattano su beni ICT direttamente inclusi ed impiegati nel PSNC, bensì anche a quelli relativi a sistemi informativi, reti e servizi informatici che risultano "esternalizzati", in un'area comunque di pertinenza dei soggetti inclusi nell'applicazione della normativa di riferimento. Si parla quindi sostanzialmente dei Cloud Service Provider, attraverso l'accensione di contratti IaaS, SaaS o PaaS. Questi vanno coinvolti negli obblighi di notifica.

Uno stretto collegamento in termini di Risk Assessment al fine di disciplinare puntualmente la gestione delle terze parti tramite l'emanazione di apposite linee guida sulla conduzione delle attività di valutazione dei rischi sui fornitori.
Trattasi, in buona sostanza, di una metodologia che nasce dalla considerazione per la quale l'oggetto di una fornitura non può assicurare, di per sé, una "protezione assoluta" contro qualsivoglia violazione intenzionale o accidentale. Diventa necessario, di conseguenza, affidarsi ad una metodologia che assicuri un livello sufficientemente elevato delle misure di protezione medesime, in modo da rendere accettabili i rischi associati alle violazioni. Sotto tale punto di vista, è evidente il legame di ratio tra la metodologia in esame con l'introduzione del nuovo obbligo di notifica, oltre alla considerazione che lo svolgimento di siffatta attività di assessment dovrà necessariamente precedere la notifica medesima.

Risulta chiaro che viene richiesto delle organizzazioni coinvolte un incremento notevole dell'effort, con particolare riferimento alla necessità di estendere l'attività di risk assessment ad asset in precedenza non presi in considerazione.
Si propone in tal senso l'applicazione della metodologia di analisi del rischio "Threat, Vulnerabiilty, Risk Analysis" (c.d. TVRA) definita da ETSI (European Telecommunication Standards Institute) nel documento "Technical Specification ETSI TS 102 165-1 v. 5.2.3 (2017-10)", secondo una procedura che si scompone in due fasi:

- Fase 1 (in carico all'organizzazione): predisposizione di un documento di analisi del rischio;
- Fase 2 (in carico all'autorità): applicazione della restante parte della metodologia ETSI – TVRA, con le opportune modificazioni utili a consentire l'individuazione del livello di severità dei test.

Lo scopo della metodologia in analisi è, dunque, quello di definire il livello di protezione richiesto all'oggetto della fornitura a fronte di violazioni intenzionali, nonché la definizione del livello di severità dei test che le funzioni di sicurezza dell'oggetto della fornitura devono essere in grado di superare, successivamente ad un processo di minimizzazione del rischio secondo le logiche della ETSI -TVRA. La metodologia prevede altresì le opportune integrazioni per l'estensione del suo perimetro alle ipotesi di violazioni accidentali, non direttamente trattati nella ETSI – TVRA.
Eventi come gli attacchi alle infrastrutture critiche, sia nel conflitto russo-ucraino, che da parte di servizi segreti in quella definita la Guerra Cyber, ma anche i blackout alle centrali elettriche, i casi di avvelenamento dei serbatoi di captazione delle acque da distribuire alla popolazione attraverso l'effrazione della catena tecnologica di telecontrollo SCADA, hanno in tal senso costituito la base per affrontare una revisione notevole di tutto l'impianto.
Le misure da seguire nel paragrafo 1 della NIS sono fondamentalmente aa approccio "zero trust" e a tutto rischio".
Ma cosa prevedere per la sicurezza dei servizi informatici in chiave di prevention e detection?
La direttiva innanzitutto considera la gestione delle reti informatiche di sicurezza compito di personale interno ai soggetti essenziali o con compiti di project management in caso di eventuali esternalizzazioni della sicurezza informatica. A seguire poi si citano i seguenti elementi attuativi:

- L'esecuzione di penetration test, al fine di rilevare lo sfruttamento di vulnerabilità nell'infrastruttura e nelle applicazioni costituenti il perimetro dell'organizzazione;
- L'esecuzione di audit di sicurezza (interni, e estesi ai soggetti esterni contrattualizzati dall'organizzazione);
- Organizzazione di consulenza sulle tematiche strettamente inerenti le tematiche di Incident Management, al fine di avere personale che segua con una continuità la conoscenza di quello che avviene su scala planetaria e la riporti all'organizzazione a livello di prevention;
- Effettuazione della classificazione della criticità della catena di approvvigionamento, in modo da individuare entry point attraverso i quali aspettarsi dei tentativi di exploit, includendo la catalogazione dei sistemi tecnologici, dei fattori tecnici e non tecnici cui essi sono soggetti, di allocazione delle risorse, sia in termini di skill posseduto dal personale che della numerosità rispetto all'effort richiesto. Anzi su quest'ultimo aspetto dovrebbero essere indirizzate le pratiche per una stima realistica di ricorso alle esternalizzazioni dei servizi;
- Condivisione con i soggetti esterni contrattualizzati dell'analisi del rischio, anzi, coinvolgimento dei soggetti terzi durante tutto il ciclo di vita di un, dalla definizione, passando per la progettazione e lo sviluppo, per poi proseguire agli User Acceptance Test, e al rilascio in esercizio e concludendo il ciclo con la gestione della manutezione.

11.1.2 Aspetti tecnologici della gestione degli incidenti

L'impianto dell'art. 21 descrive alcuni aspetti tecnologico, senza fare esplicitamente riferimento, ovviamente, a prodotti o tool da utilizzare per la gestione degli incidenti, quanto per le contromisure da mettere in campo a livello di controlli. Si tratta di 10 sotto-categorie, elencaye da A a J. In linea di massima, per il caso del contesto in esame, l'Incident Management, può citarsi quanto di seguito elencato:

- Elaborazione di Politiche e Procedure
- Piani di intervento in casi di incidenti
- Catena decisionale di intervento immediato in caso di incidenti e linea di reporting
- Risposta adeguata e commisurata all'incidente
- Collezione delle evidenze
- Reporting di eventi accaduti
- Logging di attività verso tecnologie SIEM
- Uso della Treat Intelligence
- Uso della Artificial Intelligence
- Pratiche di backup
- Monitoraggio delle sedi remote attraverso tecnologie IOT
- Reporting verso il Senior management degli eventi classificati come incidenti
- Sicurezza della rete attraverso misure di segregation, o al lievllo di network subnetting o per la presenza di firewall multilivello agenti sia a livello di Circuit level che di Application gateway
- Uso della crittografia come misura per la protezione delle riservatezza delle informazioni;
- Uso della cifratura come misura per la protezione dell'integrità dei dati;
- Attività di documentazione e reporting;
- Attività di classificazione degli eventi;
- Attività di definizione della tipologia di incidenti specifici individuabili nell'organizzazione;
- Sistemi preposti all'individuazione di flagranza di exploiting (telecamere, sonde, sensori, allarmi sonori di ingressi indebiti ai tornelli, alarmi di abbattimento incendi, allarmi su eventi "strani" intorno all'area fisica dell'organizzazione, monitoraggio dei sistemi esternalizzati);

Ogni sistema tecnologico durante la permanenza dell'incidente (Detect nel CFS) deve essere adeguato e ordinatamente mappato nell'organizzazione.

Parimenti la fase post-incidente (Respond e Recover) deve prevedere strumenti adeguati che ottimizzino le attività ivi previste.

Il quadro di sorveglianza, se in gestione a terze parti, deve essere classificato dunque adeguatamente rispetto al rischio esistente. Di conseguenza, in tal caso, anche il fornitore del sistema deve essere classificato come critico. Le misure tecnologiche che esso prevede di mettere in campo devono essere documentate e presentare a loro volta un'analisi dei rischi derivanti dal loro utilizzo, o dal mancato

utilizzo o guasto. Anche riguardo alla loro classificazione come soggetti critici, i fornitori così definiti devono avere una contrattualizzazione pertinente. Prima di finalizzare i contratti i fornitori dovrebbero condividere l'impatto previsto, le raccomandazioni su questioni inerenti i rischi e i rimedi previsti. Qualora alcune raccomandazioni non possano essere eseguite, i fornitori dovrebbero documentare preventivamente e motivata. Le motivazioni addotte devono essere adeguatamente approvate dall'organizzazione.

Non si può non citare l'uso dell'Intelligenza Artificiale. Nel panorama attuale la sicurezza dei modelli di Machine Learning (ML) ha assunto una rilevanza cruciale. Sentiamo spessouna valanga di nuove terminologie come "Adversarial Machine Learning", "Adversarial Attacks", "Adversarial Examples" e "Adversarial Robustness", termini che stanno diventando pilastri nella discussione relativa alla protezione dei sistemi di apprendimento automatico da potenziali minacce incombenti su un'organizzazione.

Non trascurando l'aspetto Privacy di tali tecnologie, l'uso nel campo delle attività di Prevenzione e di Detect è quindi un aspetto che sempre più le tecnologie di questo settore includono come metodo.

11.2 Cyber Resilience.

La NIS 2 descrive nell'articolo 1 i soggetti ai quali va applicata, secondo il criterio nel settore merceologico di riferimento e indistintamente per tutte le imprese, pubbliche o private rientranti nelle medie imprese[35]. Poi viene fatta una differenziazione tra settori ad alta criticità e settori importanti. Tuttavia, la dimensione dell'impresa è più flessibile, non costituisce un vincolo nella definizione, nel senso che va posta più l'attenzione sui servizi erogati e l'importanza che nello Stato membro il servizio esposto svolge.

Le considerazioni che seguono verranno divise nei due settori specifici cui le NIS 2 fanno riferimento: operatori finanziari e servizi critici.

11.2.1 Operatori di servizi finanziari

La NIS 2 nell'affrontare la resilienza, parte dalla constatazione che questo aspetto, a fronte del sempre maggiore utilizzo della digitalizzazione nei servizi finanziari e nell'interconnessione dei sistemi sempre più crescente, necessita di una marcia in più per adeguarsi ai cambiamenti tecnologici rapidi e quindi nel conseguente aumento della capacità di attacco da parte di agenti malevoli.

Benché nei processi di Risk Management di settore uno stadio più avanzato di adeguamento si è manifestato negli ultimi anni, ancora non si può dire di aver ridotto il rischio residuo a livelli adeguati alla velocità di crescita dei nuovi rischi gravanti la stabilità e le prestazioni dei servizi informatici. Con la NIS 2 si intende porre ancora più attenzione a questo aspetto, soprattutto per quanto riguarda la fase di Response e Recovery a seguito di incidenti informatici con violazioni del principio di disponibilità. L'obiettivo è quello di armonizzare nella UE il processo di analisi del rischio operativo nella fase di Incident Management al fine di arrivare ad una maggiore protezione dei servizi, con menzione particolare ai soggetti critici per arrivare ad una riduzione dei tempi a seguito di caduta dei sistemi ITC. Soprattutto nel campo dei test di ripristino a seguito di Disaster Recovery la carenza di analisi nel rischio di servizi soggetti ad outourcing è stata sempre posta in minor rilievo in tutta l'Unione, e in modo non uniforme da Stato a Stato. La NIS 2 si propone di ottimizzare la segnalazione degli incidenti informatici a livello europeo, in modo da ottimizzare il principio di Lesson Learned, "imparare dalle lezione" ossia risolvere i problemi vedendo se nei trascorsi vi sia lo stesso caso e in tal modo velocizzare le pratiche di recupero, e quindi facilitare la mitigation degli impatti avversi su di un asset e permettere alle autorità di vigilanza di venire a conoscenza in maniera più tempestiva della tipologia degli incidenti cyber che più colpiscono i sistemi informatici.

[35] Una media impresa è quella che non supera i 250 dipendenti, e rientra nel fatturato ano di 50 mln di euro e un bilancio annuo non superiore ai 43 mln di euro.

Per quanto riguarda la resilienza delle infrastrutture, affinché il termine non rimanga una pura citazione dotta senza alcuna sostanza pratica, la NIS 2 cita esplicitamente i test di resilienza operativa digitale, ovvero delle vere e proprie prove di funzionamento, senza freni. l'esperienza insegna, infatti, che spesso i Penetration Test (PT) vengono fatti in condizioni non proprio di simulazione completa di attacco, ma ponendo una serie di vincoli, a salvaguardia dei servizi di business erogati. Nel campo dell'ingegneria meccanica i crash test delle autovetture rappresentano una buona similitudine: provare l'impatto ad alta velocità contro un ostacolo per verificane la risposta in termini di assorbimento dell'urto. Ebbene i test di resilienza digitale dovrebbero essere la stessa cosa: dei test in condizioni estreme, in cui si simulano delle condizioni di crash e si valutano le condizioni di risalita dei sistemi a seguito del ripristino dei servizi.

La NIS 2 menziona come elemento cardine che finora ha costituito un freno ai test di resilienza digitali attraverso PT i notevoli costi che tali pratiche comportano. Molto spesso, per abbassare i costi, sono stati trascurati elementi connessi al rischio inerente allo sfruttamento di minacce nel campo della comunicazione elettronica, come i servizi connessi alla rete telefonica commutata (PSTN, Public Switched Telephone Network), i servizi di rete terrestre, o quelli più tradizionali (POTS, Plain Old Telephone Service) o ancora trascurando i sistemi legacy, non trascurando le attività di verifica di internal audit in questi ambiti.

[I test di PT avanzati basati su minacce sono previsti attualmente previsti solo per entità finanziarie rilevanti, elemento questo che contribuisce ad abbattere i costi, ma dovrebbero essere considerati su tutti i soggetti critici, al fine di valutare preventivamente la possibilità da parte di agenti malevoli di sfruttare le minacce incombenti sulla specifica realtà, individuate dall'analisi del rischio. Ma vanno considerati come obbligatori. I test di PT di tipo TLPT saranno più rilevanti nelle grandi organizzazioni finanziarie e del settore bancario e creditizio, meno in settori come agenzie di rating o società di gestione patrimoniale].

Nella valutazione dei test di resilienza la NIS 2 assume come considerazione preliminare non la sola considerazione dei costi relativi agli strumenti informatici utilizzati per garantire la resilienza dei sistemi ITC, ma prevedere anche quelli connessi all'allocazione delle risorse umane, includendo all'unisono i costi delle pratiche di awareness e di cyber-higiene che devono essere messe in campo rigorosamente e che devono rientrare nell'analisi del rischio, anche sul piano dell'assicurazione di un adeguato investimento finanziario che ne garantisca la regolarità su base annuale.

Va considerato anche il monitoraggio dei sistemi ITC nel caso di contrattualizzazione a terze parti, individuando dei requisiti minimi cui i soggetti esterni devono sottostare, specie quelli operanti nel settore finanziario, sia a livello contrattuale che di specifiche contromisure in essi messe in campo; elementi questi ultimi di garanzia per la stabilità, la funzionalità, la disponibilità, l'integrità dei dati a seguito del ripristino conseguente a caduta dei sistemi. Questo è ancora più necessario per i soggetti che hanno infrastrutture ITC presso terzi per fornire servizi di pagamento; lo sfruttamento delle minacce informatiche su tale settore, infatti, registra un notevole incremento digli attacchi subiti, costituendo un veicolo di minaccia alla stabilità del mercato comune e della stabilità finanziaria dell'Unione.

Ma come si raggiunge l'obiettivo in maniera armonizzata in quadro dell'Unione in cui esistono profonde differenze di specificità degli Stati membro?

Nel capo II, sezione II del regolamento[36] NIS 2 sono presenti ben 10 articoli (dal 6 al 16) che dettagliano la gestione del rischio informatico, e va tenuto in particolare conto gli art. 11 "Risposta e Ripristino", 12 "Politiche di backup e metodi di ripristino e recupero", 13 "Apprendimento e d evoluzione" e 14 "Comunicazione". I test di resilienza operativa digitale per soggetti che erogano

[36] Si ricorda che un regolamento è un atto legislativo immediatamente applicabile in tutta l'Unione, quindi di portata generale, e obbligatorio.

servizi finanziari, convergono la NIS 2 con il regolamento DORA[37], il framework europeo per la gestione del rischio delle tecnologie di informazione e comunicazione (ITC) per il settore finanziario e per il loro fornitori critici.

Nel capo III il regolamento si occupa più specificatamente del processo di *Incident Management* esponendo 7 articoli inerenti (dal 17 al 23) la classificazione in base alla criticità, la gestione di quelli particolarmente gravi e la risposta effettuata per il ristabilimento delle condizioni di regime. In tutto il processo viene citato ENISA[38] (*European Network and Information Security Agency*), la BCE (Banca Centrale Europea) e l'AEV (Autorità Europea di Vigilanza) come le agenzie con la quale consultarsi per l'armonizzazione del processo di condivisione delle informazioni. I cardini esposti nel capo si applicano agli incidenti operativi o relativi alla sicurezza dei pagamenti ovvero ai gravi incidenti operativi o relativi alla sicurezza dei pagamenti allorché riguardano enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica.

Più operativamente, il capo IV del regolamento NIS 2 esamina il contenuto dei test di resilienza operativa digitale esponendoli in 4 articoli (24-27), con riferimento a soggetti diversi dalle microimprese[39].

Per quanto concerne entità critiche fornitori che affidano i propri servizi ITC a terze parti con un adeguato contratto di fornitura, il capo V, sezione II, contempla le azioni che devono essere messe in pratica per un'effettiva gestione dell'esternalizzazione, mentre il capo VI espone le regole di condivisione nell'Unione delle informazioni a seguito delle crisi e di circolazione delle analisi delle minacce informatiche, compreso i metodi per abbassarne il rischio inerente al valore residuo, che, come precedentemente posto come principio base, è l'humus sul quale è possibile costruire un'adeguata risposta agli incidenti in termini di ripresa delle attività, e quindi, parallelamente, garantire la resilienza dei sistemi.

Passando alle direttive inerenti la resilienza dei sistemi ITC, invece, nella NIS 2 lo Stato italiano è chiamato a recepire, entro il 17 ottobre 2024, quanto descritto nei paragrafi del capo IV, art. 21, ossia ad integrare in ottemperanza alla legislazione italiana quanto descritto nel comma c). Quindi entro tale data dovrà essere definita una disposizione nazionale che preveda come realizzare nel nostro paese gli obiettivi descritti nel paragrafo 2 comma c), riguardanti la continuità operativa e il ripristino dei backup a seguito di crisi, ivi compresa la gestione di questa fase. Queste misure sono da riguardarsi come valutazione dei rischi dei sistemi informatici, delle reti e del loro ambiente fisico.

Per i soggetti critici certificati IOS/IEC 27001 probabilmente i controlli di questa categoria di area di sicurezza informatica sono già operativi, trovando applicazione nelle contromisure descritte negli annex (40) 5.9-30, 8.13-16. Per quanto riguarda i servizi in Cloud, invece, la ISO/IEC 27017 non specifica granché circa le verifiche da effettuare sull'infrastruttura esternalizzata su CSP (*Cloud Service Provider*), pertanto questo tema sarà obiettivo delle direttive relative alla gestione della Supply Chain.

Ma, per tutti gli altri soggetti non certificati ISO/IEC 27001 l'implementazione dei controlli previsti dagli obiettivi previsti nelle direttive in maniera di continuità operativa sarà un compito più oneroso, partendo da zero.

[37] Regolamento per il mantenimento della resilienza nella cybersicurezza nel settore esplicito per i servizi finanziari nell'UE.

[38] L'Agenzia dell'Unione europea per la cibersicurezza è una delle agenzie dell'Unione europea e si occupa di cibersicurezza. Ha sede ad Atene, con un secondo ufficio a Candia, sull'isola di Creta (Grecia).

[39] Una microimpresa è classificata come ente che occupa meno di 10 persone, ha un fatturato annuo e un bilancio annuale non superiore ai 2 mln di euro.

[40] Si fa riferimento qui alle contromisure descritte nella ISO/IEC 27001:2022.

11.2.2 Soggetti Critici e servizi essenziali

I soggetti critici sono quegli operatori che forniscono servizi essenziali, ossia di vitale importanza per la società (energia, trasporti, ecc.), per le attività economiche, per la salute e la sicurezza pubbliche e dell'ambiente. Se poi vengono forniti servizi essenziali al pubblico ipso facto anche l'infrastruttura che li implementa è classificata come critici.

Vi sono poi alcuni soggetti critici che rivestono particolare rilevanza europea; l'articolo 17 in tal senso, li definisce come quelli che forniscono servizi essenziali in almeno 6 Stati[41].

L'articolo 1 delle direttive NIS 2 definisce la resilienza di tali entità in maniera similare a quanto sopra già descritto: la capacità di prevenire, attenuare, assorbire un incidente e, inoltre di resistere, adattarsi, rispondere e ripristinare le capacità operative a regime permanente.

Per quanto riguarda lo scambio delle informazioni all'interno dell'Unione nel caso di incidenti, fermo restando la stessa rilevanza descritta per i soggetti finanziari, va tenuto conto però della tutela degli interessi commerciali, per cui la condivisione delle informazioni deve essere limitata solo alle informazioni effettivamente ritenute pertinenti.

Nel capo II "Quadri nazionali per la resilienza dei soggetti critici" l'articolo 4 descrive la strategia da recepire nel nostro Stato. Ben 8 lettere espongono i principi minimi che una tale strategia deve contenere: priorità, ruoli e responsabilità, la metodologia di analisi de rischio, il quadro di coordinamento tra le autorità competenti incaricate di condividere le informazioni sugli incidenti. Va effettuato un aggiornamento di tale strategia ogni 4 anni, a partire dalla prima adozione e da parte dello Stato.

Per quanto riguarda la valutazione del rischio l'articolo 5, oltre a ribadire l'effettuazione di un'analisi adeguata al rischio inerente (p.es. facendo riferimento all'elenco delle minacce della ISO/IEC 27005) aggiunge delle novità facendo riferimento alle minacce di emergenza sanitaria, e quelle ibride o antagoniste, rimarcando i reati di terrorismo.

Le tempistiche di censimento dei soggetti critici divisi per settori e sottosettori[42] deve essere ultimato da parte degli Stati membro entro il 17 luglio 2026, effettuando un aggiornamento ogni 4 anni a partire da tale data, riportando eventuali nuovi soggetti critici o declassificando alcuni già censiti come tali (articolo 6).

Nello stesso articolo, la lettera include nella valutazione del rischio gli effetti negativi che un incidente può ripercuotersi nell'asset. Il successivo articolo 7 ritiene come determinanti come effetti negativi:

- Il numero di utenti impattati;
- Le interdipendenze su altri settori dipendenti dai servizi essenziali impattati;
- L'area geografica interessata dall'incidente, comprese eventualmente quelle transfrontaliere su cui si ripercuote;
- L'importanza del soggetto nel mantenere un livello essenziale con gli strumenti delle ridondanze in campo per assicurarne la continuità.

Questi dati vanno indicati riportando le relative soglie di rilevanza, e vanno aggiornandoli sempre ogni 4 anni.

[41] Per questi settori critici l'articolo 18 prevede "missioni di consulenza" per valutare le misure di resilienza e protezione predisposte

[42] I settori cui si fa riferimento sono: energia, trasporti, bancario, acque potabili, acque reflue, produzione, trasformazione e distribuzione di alimenti, salute, spazio, infrastrutture dei mercati finanziari e infrastrutture digitali, enti della pubblica amministrazione

Il gruppo al quale fare riferimento per gli aggiornamenti è stabilito nell'articolo 19[43]. Si tratta di un gruppo unico appositamente istituito per la resilienza dei soggetti critici, costituente altrettanto punto di riferimento e di scambio di informazioni con gli altri Stati membro, e di un punto di contatto unico per il coordinamento e il collegamento tra i diversi Stati. L'articolo 9, paragrafo 3, stabilisce che entro il termine del 17 luglio 2028, e successivamente ogni due anni, i punti di contatto unici devono redigere una relazione di sintesi in merito alle notifiche ricevute, la natura egli incidenti notificati, e le azioni intraprese per il contenimento delle avversità riscontate. Ogni Stato deve provvedere a che il punto di contatto unico disponga di poteri e di risorse finanziarie, umane per svolgere efficacemente i compiti assegnati. La segnalazione degli incidenti è generale, comprendendo anche quelle categorie non propriamente informatiche ma che hanno una potenziale ripercussione nell'asset dei soggetti critici. L'elenco dei contatti unici è reso pubblico da parte della Commissione.

I soggetti critici non sono lasciati soli nel decidere i materiali, le metodologie di orientamento, gli strumenti da mettere in campo per l'esecuzione dei test di resilienza, ma possono ricevere materiale formativo adeguato e addirittura, laddove vi siano necessari e giustificati motivi, ricevere degli aiuti finanziari da parte degli Stati membri (articolo 10). Anche per la condivisione delle informazioni inerenti dati classificati come sensibili e personali ogni Stato è chiamato ad agevolare tali scambi in modo protetto.

L'articolo 11 rilancia l'opportunità di una cooperazione tra Stati per quanto riguarda ogni qualvolta sia ritenuta necessaria una consultazione per rafforzare la resilienza dei soggetti critici, anche nel caso ciò sia rivolto ad un abbattimento degli oneri amministrativi a loro carico.

Il capo III, comprende 5 articoli (dal 12 al 16) per quanto riguarda la resilienza dei soggetti critici. In questi articoli, oltre a ribadire che i principi di Risk Analysis debbano tenere conto di tutte le minacce inerenti i soggetti critici, sia quelle di natura naturale che umana, a cui si è fatto riferimento in più parti nella presente trattazione, si pone ancora di più l'attenzione sull'interdipendenza tra servizi essenziali forniti o dai quali si dipende, non ultimi eventuali sconfinamenti ad altri Stati membri e paesi terzi.

Ma quali misure di resilienza vanno messe in campo nei soggetti critici?

L'articolo 13, in particolare, nel primo comma, individua come misure necessarie le seguenti:

- Prevenire l'evitarsi degli incidenti, anche adottando misure di mitigation del rischio relativamente a catastrofi naturali e agli effetti dei cambiamenti climatici;
- Proteggere fisicamente i propri siti e infrastrutture critiche ricorrendo a barriere, recinzioni, sorveglianza del perimetro fisico, dispositivi di controllo accessi e rilevamento intrusioni;
- Elaborare procedure e protocolli di gestione delle crisi;
- Prevedere pratiche di allerta per la gestione delle crisi;
- Agevolare la ripresa della continuità operativa a seguito di incidenti prevedendo a implementare ridondanze infrastrutturali (linee di disaster recovery);
- Prevedere l'organizzazione del personale in modo da disporre di categorie di soggetti appositamente istruiti e formati per svolgono funzioni critiche, prevedendo parimenti ad adeguata loro formazione e controllo dei requisiti di qualifica richiesti per svolgere tali funzioni;

[43] Nell'articolo 19 viene specificato come composto il gruppo per la resilienza dei soggetti critici ed i compiti per essi previsti.

- Mettere in sicurezza il personale intero restringendo l'accesso ai siti infrastrutturali critici, e istruendo in procedure l'accesso per chi ne deve essere autorizzato;
- Mettere in atto un piano di awareness per la responsabilizzazione e formazione del personale, istituendo corsi di formazione e svolgendo esercitazioni pratiche;
- Catalogare i soggetti terzi con i quali contrattualizzati dei servizi di manutenzione o approvvigionamento in modo da individuare quelli che svolgono funzione critiche.

Tutti i soggetti critici devo redigere piani di resilienza. Ogni soggetto critico deve individuare un soggetto unico a cui fare riferimento come punto di contatto.

La Commissione, inoltre, è chiamata ad adottare atti di esecuzione e linee guida non vincolanti per definire le necessarie specifiche tecniche e metodologiche relative all'applicazione delle misure necessarie sopra menzionate.

Specificatamente per il personale che segnatamente è implicato nel processo di resilienza soggetto critico, l'articolo 14 prevede dei vincoli di assunzione, come l'assicurazione che non vi siano precedenti penali rispetto a quello specifico ruolo, attingendo informazioni presso il sistema europeo di informazione sui casellari giudiziari.

In materia di vigilanza i soggetti individuati come critici sono passibili di ispezioni da parte di autorità appositamente competenti ed istituite dagli Stati membro con appositi poteri e mezzi. Inoltre, articolo 22, ogni Stato membro stabilisce le sanzioni, applicate proporzionatamente e di natura dissuasiva, applicabili nel caso di inadempienza alle direttive recepite e sancite come norma nazionale.

12 Supply Chain (Elio Antonelli).

Per inquadrare la tematica relativa al controllo della supply chain vanno fatte delle distinzioni nella catena di approvvigionamento (e in tal senso ci rifaremo a quanto indiato nel NIST SP 800-161).

La catena di fornitura, o approvvigionamento, può essere costituita dai seguenti attori:

- System integrators. Si tratta di fornitori che sono incaricati di seguire il ciclo di vita del software (SDLC, Software Delivery Life Cycle), apportando evolutive, correttive e provvedendo alla manutenzione adeguativa. Spesso questi fornitori sono una catena, giacché non è detto che chi si assicura una gara sia poi quello direttamente incaricato di avere occuparsi delle applicazioni. Deve essere fatto obbligo al fornitore capofila di assicurarsi che i subappaltatori siano controllati e verificati rispetto ai requisiti dell'organizzazione
- Fornitori (Suppliers). Le organizzazioni devono valutare se l'entità dei requisiti di Cybersecurity della catena di fornitura imposta ai fornitori, la volontà di questi ultimi o la loro capacità di consentire la visibilità sul ciclo di sviluppo o produzione dei loro prodotti influenzi il costo. Questo solitamente succede quando le organizzazioni richiedono maggiore livello di trasparenza ai fornitori. I fornitori possono correre il rischio che i clienti acquirenti dei loro prodotti richiedano un supplemento, o una serie multipla, o diversi requisiti di cybersecurity della catena di fornitura.
- Cloud Service Provider (External Providers of Information System Services). Le organizzazioni, uoi per ragioni di ottimizzazione industriale, vuoi per riduzione dei costi, si avvalgono dei CSP per gestire l'infrastruttura e rete (IaaS), o ospitare delle piattaforme informatiche (PaaS), o implementare delle applicazioni sviluppate e integrarle nella propria struttura fornendola in seguito all'organizzazione come servizio. Questa esternalizzazione spesso è vista come la panacea, nel senso che ci si libera dalle incombenze di gestire i controlli operativi delegandoli al Cloud Provider.

Il problema è che l'organizzazione perde la visibilità e la gestione diretta delle funzioni esternalizzate, considerando del tutto trusted ogni pratica del CSP, senza effettuazione di verifiche o, ancora peggio, senza stabilire in procedure operative gli obblighi cui il CSP è tenuto ad ottemperare (report periodici, controlli backup, test di resilienza, test delle performance, procedure di Patch Management, processi di Vulnerability Management, la gestione degli incidenti, ruoli e le responsabilità chiari, ecc.). Pertanto, per dirla tutta, forse la transizione dall'on-premise al cloud scarica l'organizzazione di alcuni oneri, operativi e finanziari, ma ne appesantisce quello organizzativo richiedendo un maggior rigore nella definizione dei requisiti della Supply Chain (SCRM, Supply Chain Risk Management) nell'area dell'ITC, dichiararli nelle gare d'appalto e successivamente monitorare i servizi forniti del CSP e valutarli per la conformità ai requisiti dichiarati.

Altrettanto le logiche di Access Management spesso vanno a non diventare più trasparenti, mentre invece bisogna imporre dei controlli di entitlement review, ovvero di monitorare la lista degli utenti che accedono ai servizi (altrettanto l'eventuale personale del CSP), modalità di accesso, profilo.

Altrettanto l'uso della crittografia per la garanzia della confidenzialità sui dati speciali e particolari, e hashing per la garanzia di integrità sono elementi che spesso si lasciano aperti e non si risolvono a livello di requisiti, in termini di algoritmi da utilizzare, lunghezza delle chiavi, gestione della custodia delle chiavi. Va precisato che, indipendentemente da chi esegue i servizi, l'organizzazione rimane responsabile del rischio per i sistemi e i dati dell'organizzazione che può derivare dall'utilizzo di questi servizi.

Va divisa la trattazione distinguendo tra quelle organizzazioni che sono certificate, o seguono, le norme della famiglia ISO/IEC 27000, con particolare riferimento alla UNI CEI ISO 27001, 27005 e

27017, dalle altre che sono state impattate dalla NIS1 e, in ultima distinzione, da quelle organizzazioni che magari o non hanno proprio un Sistema di gestione della Sicurezza oppure soltanto applicano alcune contromisure nel campo del rapporto con i fornitori, magari perché lo richiedono norme non propriamente Cyber (p.e. la ISO 37001).

Per le organizzazioni certificate ISO/IEC 27001, il controllo del fornitore viene generalmente messo in atto basandosi sugli obietti di controllo previsti dalle contromisure esposte negli annex 5.19 - 5.21, 6.6.

Sostanzialmente si tratta di controlli che riguardano il ciclo di vita del prodotto nei termini di contrattualizzazione, appurando la presenza di clausole di sicurezza nell'accordo con i fornitori, di redazione di accordi di riservatezza e nella ricezione, per quegli appalti avvenuti attraverso gara, di "documentazione di sistema" (antimafia, antiriciclaggio, ecc.). La filosofia principale che ha finora accompagnato la vita delle organizzazioni nei confronti della catena di fornitura è stato il rispetto del GDPR e un rimando alle raccomandazioni del Garante della Privacy. Ma nella norma ISO, certamente un baluardo nel campo della definizione dei controlli e nell'implementazione delle contromisure, un aspetto poco dettagliato (44) è appunto il concetto di "perimetro". Più esplicitamente si potrebbe dire che il perimetro è una linea netta perfettamente definita e delimitata, e che si delega al RUP e al RUF la gestione della definizione del particolare progetto in essere. Si badi bene, a livello teorico "estendere un perimetro" comporterebbe anche rivedere i Ruoli e le Responsabilità, in quanto l'ambito di intervento non sarebbe unicamente limitato al proprio spazio fisico, ma altrettanto assumere ciò che di proprio è confinato all'esterno come non delegabile al fornitore. Quindi, a rigor di logica, la superficie esposta si estende fin dentro l'organizzazione coinvolta come supplier.

Nella NIS 2 si estende invece a CSIRT il compito di identificare, comprendere e gestire i rischi organizzativi generali del soggetto con riguardo alle compromissioni della catena di approvvigionamento individuate di recente o le vulnerabilità critiche, magari predisponendo delle interfacce grafiche che semplifichino e velocizzino la messa in opera delle azioni di mitigazione.

Per i soggetti che sono stati impattati dalla NIS1 il controllo sul fornitore costituiva un "di cui", poco in evidenza rispetto ad altre contromisure da mettere in campo, come la difesa perimetrale, le misure di prevenzione e difesa, il monitoraggio delle attività. Ma spesso ci si limitava al reporting di quello che l'ufficio amministrativo stabiliva come criterio di scelta, la valutazione degli economics. Molte volte, è questa la realtà che è stata riscontrata, non vi erano nemmeno clausole di Sicurezza Cyber, piuttosto richiami al GDPR.

E comunque spesso l'applicazione della NIS1 si è rivelata inefficace, avvicinandosi più a un mero task documentale calato dall'alto; la percezione è stata quella di un episodio, tra i tanti richiesti, seccante e burocratico frettolosamente da chiudere più per "levarsi il pensiero", consegnando della documentazione ad un Ministero, senza ricevere peraltro alcun feedback e compilando delle form la cui interpretazione spesso non era chiara nemmeno agli addetti ministeriali di riferimento.

Fermo restando che la Commissione, l'ENISA, gli Stati devono proporre degli standard internazionali e migliori prassi industriali nella gestione della catena di approvvigionamento, al fine di potenziarne la sicurezza, ma basilare è rivedere la gestione del rischio sulla catena di fornitura portando in conto gli strumenti di difesa e prevenzione che i fornitori hanno attuato per proteggersi dai malware, fonte in gran parte veicolo di incidente. I soggetti essenziali dovrebbero essere incoraggiati a inserire nelle proprie check-list la valutazione della presenza negli accordi contrattuali con i loro fornitori e fornitori di servizi diretti di misure di gestione del rischio. E va considerato il fatto che i fornitori dovrebbero prendere in considerazione a loro volta i sub-fornitori nella valutazione del rischio.

Per quanto riguarda i prodotti acquistati vanno portati in conto tra le vulnerabilità anche quelle non tecniche, come l'indebita interferenza di paesi terzi che non documentano eventuali presenze di

[44] Nella ISO/IEC 27001:2022 i controlli di sicurezza sul perimetro sono trattati nel capitolo 7 e negli attributi 5.19-5.23

backdoor, valutando anche potenziali turbative o possibilità di turbative nell'approvvigionamento dovute a lock-down o shutdown della manutenzione. Durante la fase di pandemia che ha colpito globalmente il pianeta, si è avuto contezza del livello di rischio che la catena di approvvigionamento risente in caso di interruzione di una fornitura, o di impossibilità di manutenzione diretta da parte di personale specialistico. Ecco perché la NIS 2 pone particolarmente in evidenza di valutare all'unisono il grado di dipendenza del soggetto essenziale dai propri fornitori.

La direttiva (UE) 2022/2555 (direttiva NIS2) impone agli Stati membri di garantire che gli enti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza delle reti e dei sistemi informativi che tali enti utilizzano nella fornitura dei loro servizi. La sicurezza informatica della catena di approvvigionamento è considerata parte integrante delle misure di gestione del rischio di sicurezza informatica ai sensi dell'articolo 21, paragrafo 2, della direttiva NIS2.

ENISA ha condotto dei sondaggi su alcune importanti realtà, dal quale sono emerse le seguenti problematiche cybersecurity sulla supply chain:

- L'86% solo implementa politiche per le strutture informatiche ICT e OT;
- Il 47% stanzia un budget per la cybersecurity sulla supply chain della catena ICT/OT;
- Il 76% non allocato personale cybersecurity sulla supply chain, senza Ruoli e Responsabilità dedicati;
- Il 61% richiede una certificazione dei prodotti forniti
- Il 37% dimostra una due diligence o una valutazione del rischio;
- Il 51% ha una politica di Patch Management rigida; il 13,5% non ha visibilità sul 50% delle patch applicate alle proprie risorse informatiche;
- Il 46% applica le patch critiche entro meno di 6 mesi; l'altro 46% entro 6 mesi.
- Come si vede non è un buon quadro.
- ENISA individua 5 aree di intervento per attuare delle misure migliorative:
- Un approccio strategico sulla supply chain stabilito a libello di Senior Management;
- Attuare una gestione del rischio apposita per la catena di fornitura;
- Politiche meno lasche nel rapporto con i fornitori, non facendosi dominare da questi;
- Politiche e procedure di Vulnerability Assessment sulla catena di fornitura;
- Imporre dei certificati di qualità nella fornitura dei prodotti acquistati;
- Contrattualizzare con fornitori possibilmente con certificazione di qualità.

Inoltre, esiste una certa confusione tra ICT, catena delle tecnologie informatiche e OT, tecnologie operative, spesso tendendo a separare i due aspetti, se non del tutto a eliminare il controllo IT sulla supply chain OT relegandola al solo fornitore esterno, nel quale riporre fiducia cieca e non attuando forme di controllo e monitoraggio.

Eppure viene stimato che è tra il 39% e il 63% della percentuale di organizzazioni colpite per vie traverse da incidenti informatici partiti da terze parti con le quali è attivo un contratto di manutenzione. Nel 2021, poi, la compromissione della supply chain è stato il secondo vettore più in voga di diffusione dei malware da parte di agenti malevoli, passando da meno l'1% del 2020 al 17% nel 2021 di exploiting di vulnerabilità, con conseguente propagazione dell'infezione dell'infrastruttura.

In questo quadro abbastanza desolante la NIS 2 si propone di intervenire migliorando la gestione della supply chain attraverso queste misure:

- Eliminare la divisione tra operatori essenziali e fornitori di servizi digitali;
- Estendere la copertura di applicabilità a più ampi contest merceologici, mediante l'inserimento di nuove categorie (entità essenziali e entità importanti);

- Correlare in modo più approfondito la gestione della supply chain e la gestione del fornitore nell'analisi del rischio;
- Introdurre misure di Incident Management più adeguate e versatili, specie nella gestione delle crisi e nell'attuazione delle risposte e pratiche di ripristino, parlando non solo di resistenza ma altrettanto di resilienza, quindi identificando i singoli punti di guasto e altre dipendenze essenziali;
- Gestione delle vulnerabilità ed esecuzione dei test di sicurezza sulle specifiche di sicurezza in modo più chirurgico, mappando, nelle produzioni software, le dipendenze dalle criticità fino al livello di pacchetti, librerie e moduli;
- Uso della Threat Intelligence per scovare le zero days vulnerabilities insite a livello hardware;
- Sensibilizzare maggiormente il Senior Management su ogni aspetto riguardante la catena di approvvigionamento, per la conformità con le misure individuate dall'anali del rischio;
- Maggiore effort nello stanziamento di budget e FTE appropriato;
- Tenere conto delle vulnerabilità specifiche di ogni fornitore, compresi i sub-fornitori, e valutare le loro pratiche di sicurezza in campo per il contenimento dei rischi informatici, il rispetto di principi di progettazione sicura dei prodotti, il livello di garanzia di confidenzialità del personale di terza parte eventualmente coinvolto nel ciclo di produzione. Sempre su questo campo identificare le dipendenze importanti dei propri clienti (cioè le parti esterne che dipendono dalla fornitura della funzione, compresi i partner operativi) e di qui eseguire una correlazione con la catena di approvvigionamento.

12.1 Tecniche per la fornitura e il servizio acquisito

Un'organizzazione tesse con i propri fornitori dei rapporti contrattuali. In essi possono entrare a far parte misure organizzative, di processo e tecniche per la fornitura e il servizio acquisito. Tuttavia questa gamma di misure è limitata al potere di approvvigionamento di un'organizzazione e alle capacità della terza parte di poter gestire tali misure, cosa che, in una realtà come quella italiana, in cui il tessuto della piccola e media impresa o delle imprese artigiane è abbastanza ampia e ha dei rischi di ricaduta sociale abbastanza inquietanti a livello di welfare. Il controllo complessivo di un fornitore è impossibile da realizzare, giacché ad oggi non esistono diritti legali di audit né di richiesta documentazione sull'intera catena dei sub-fornitori di un fornitore; tuttavia una serie di criteri minimi di condotta possono essere applicati.

12.2 Un modello di approccio analitico

Vista l'ampiezza delle organizzazioni coinvolte, che investono i vasti settori dei servizi essenziali e critici previsti dalla NIS2, si vuole qui di seguito modellare una strategia appropriata di azione per un'ottima implementazione dei principi della cybersecurity estendendo il proprio perimetro all'intera catena di fornitura e una efficace definizione dei confini cui estendere i controlli di Sicurezza, è adottando il metodo dell'ingegneria dei Sistemi: elaborare un modello astratto, una black-box, con alcuni unici elementi misurabili e osservabili:

- un input, inteso come insieme di prodotti, merci, risorse umane, che generano un traffico dalle terze parti verso l'organizzazione,
- un output, ovvero la movimentazione dei prodotti (dati) in uscita dall'organizzazione e da considerare ancora "propri", il luogo di stazionamento;

- uno stato, inteso come complesso dei parametri che devono essere rispettati per non compromettere la stabilità del modello di sistema.

12.3 Esempi

Volendo essere più specifici, in linea generale gli input di un tale modello di sistema possono essere individuati nei seguenti esempi:

- Prodotti in ingresso (farmaci, alimenti, componenti hardware, software, etc.);
- Prodotti o servizi acquistati (software, hardware, sistemi di Intrusion Detection Systems o IPS, SOC, etc.);
- Risorse esterne come servizi di consulenza.

Riguardo agli output invece, sempre a titolo di esempio:

- I propri dati particolari parcheggiati in organizzazioni esterne che offrono servizi web (p.es. legal, financial, etc.);
- I dati verso un Cloud (siano essi implementati nei paradigmi IaaS, PaaS, SaaS);
- Il personale in outsourcing in altre realtà.

Lo stato che determina la stabilità di tale modello di sistema è sicuramente il parametro che permette di definire pienamente fino a dove si estende il proprio perimetro, l'insieme delle verifiche necessarie per mantenere il modello stabile, i controlli implementati, le business unit che devono partecipare all'implementazioni delle norme, i rischi associati ad ogni input e output.

Ancora non si ha una visione completa dei limiti sui quali ci si può spingere, in particolare nel non interferire con il cosiddetto perimetro di Privacy; è un lavoro in fieri da parte della commissione governativa incaricata del recepimento delle direttive (che appunto, non essendo regolamenti non costituiscono norme che Stati membro devono ipso-facto applicare, bensì da calare nel proprio ambito locale). Un lavoro che entro l'anno renderà più chiaro l'implementazione italiana delle misure di sicurezza "fattibili" sui fornitori e sui prodotti, ma che sicuramente non imporrà modelli organizzativi limitanti.

Facendo l'esempio tipica di un'organizzazione che ha il proprio CED nel Cloud, secondo il paradigma IaaS, ad oggi la verifica della cybersecurity è demandata ad un controllo documentale inerente il contratto, presenza in esso di clausole di sicurezza, lo stabilimento di ruoli e responsabilità; è pratico rimandare alle politiche esistenti stilate dalla terza parte. Se il CSP è una delle grandi major, tutta la documentazione è disponibile online, quindi compilata in un'ottica general-purpose, valida per ogni cliente. Di certo non è customizzabile: va presa nella sua interezza e portata come evidenza negli audit, anche se poco aderente alle specifiche policy di sicurezza redatte localmente. Così un audit completo di terza parte da attuare su fornitori come Microsoft, Amazon, Oracle, ecc. non può essere pienamente definito, giacché a meno che non si abbia maggiore conoscenza specifica di molti aspetti non citati (p. es. la localizzazione precisa dei propri dati). Un altro esempio sulla difficoltà di avere una sintesi complessiva è le evidenze da acquisire sul livello di network segregation, specie nella presenza di sistemi multi-tenant: relativamente al proprio ambito in cloud, si vorrebbe ottenere risposte adeguate in termini di impenetrabilità da parte di altri clienti, di blindatura delle risorse hardware e della limitazione delle politiche di accesso, limitato al solo personale. Un esempio ancora più calzante è sulle tecnologie di difesa del proprio perimetro informatico; potrebbe verificarsi il caso che loro manutenzione e controllo sia delegata a fornitori di Stati non nazionali, o impegnati in conflitti, sui quali niente possono le normative nazionali né tantomeno delle europee. Come garantire il rispetto dei principi base di Confidenzialità, Integrità e Disponibilità, i principi della cybersecurity in modo ottimo, dunque?

Ora estendere la catena del controllo alla supply chain vorrebbe dire in sostanza andare in profondità nell'audit delle attività svolte dalle terze parti (gli input del sistema astratto precedentemente

descritto). Addirittura spingendosi nekl controllo anche su un eventuale “albero di terze parti” ovvero sulla catena di subappalto. È quello che, per esempio, prevede la CER, le cui norme nel campo della supply chain della NIS 2 sono certamente una maggiore evoluzione verso modello ottimo.

In conclusione, se di conclusione si può trattare visto che invece siamo proprio all’inizio di un processo che sicuramente richiederà un transitorio prima di stabilizzarsi in un regime permanente, si vuole porre l’attenzione sulla circostanza che la NIS 2, relativamente al controllo dei propri fornitori e alla verifica della Sicurezza estesa “all’esterno”, avrà un valore elevato se tutte le organizzazioni approvvigionamento ai nuovi canoni filosofici e al salto di qualità che viene richiesto.

A tal riguardo si trova utile inserire una sorta di compendio di buone pratiche, con dei principi generali che possono essere di ispirazione per un’individuazione più completa del set di contromisure da attuare per una gestione della supply chain, da utilizzare in sede di internal audit, di self-assesment, di monitoraggio.

GESTIONE DEI FORNITORI NELLA SUPPLY CHAIN	
MISURA DI CONTROLLO	**ALTRE NORME**
Processo di gestione dei fornitori e dei fornitori di servizi che descriva tutto il ciclo di vita che includa almeno le procedure di selezione e qualificazione dei fornitori e dei fornitori di servizi.	**ISO 27002:2022 5.19**
Classifica ed etichettatura delle risorse e delle informazioni condivise o accessibili ai fornitori e ai fornitori di servizi. Definizione delle procedure per l'accesso e la gestione degli asset classificati.	**ISO 27002:2022 5.19, 5.20**
Stipula degli obblighi dei fornitori e dei prestatori di servizi per la protezione delle risorse informative dell'organizzazione e l'accesso alle risorse e alle risorse informative.	**ISO 27002:2022 5.19, 5.20**
Integrazione nella gestione degli incidenti delle responsabilità, degli obblighi di notifica e delle procedure.	**ISO 27002:2022 5.19, 5.20**
Organizzazione della formazione e sensibilizzazione per le organizzazioni e il personale dei fornitori o dei prestatori di servizi sulle regole di ingaggio e di comportamento in base al livello di accesso ai beni e alle risorse informative dell'organizzazione.	**ISO 27002:2022 5.19**
Definizione delle procedure per la condivisione delle informazioni.	**ISO 27002:2022 5.20**
Considerazione dei requisiti normativi e legali cogenti.	**ISO 27002:2022 5.20**
Stabilire le condizioni e autorizzazioni per l'accesso ai beni e al patrimonio informativo.	**ISO 27002:2022 5.20**

Stipula delle regole per il subappalto e i potenziali requisiti a cascata.	**ISO 27002:2022 5.20, 5.21**
Definizione di un contatto per la sicurezza da parte dell'organizzazione e del fornitore/fornitore di servizi.	**ISO 27002:2022 5.20**
Scansione di sicurezza del personale per l'accesso alle risorse critiche o alle risorse informative.	**ISO 27002:2022 5.20**
Il diritto di revisione deve essere concordato contrattualmente.	**ISO 27002:2022 5.20**
Definizione dei requisiti di sicurezza per i prodotti e i servizi ICT/OT acquisiti.	**ISO 27002:2022 5.21**
Implementazione di pratiche per verificare che i controlli di sicurezza siano inclusi nei prodotti o servizi forniti.	**ISO 27002:2022 5.21**
Stabilire le forme di garanzia che devono essere comprovate dai fornitori e i fornitori di servizi sull'assenza di consapevoli funzioni nascoste o backdoor nei prodotti.	**ISO 27002:2022 5.21**
Esistenza di procedure per la gestione di prodotti, componenti e strumenti usati a fine vita.	**ISO 27002:2022 5.21**
Monitoraggio delle prestazioni del servizio per verificare l'aderenza ai requisiti di cybersecurity previsti dagli accordi; ciò include la gestione di incidenti, vulnerabilità, patch, requisiti di sicurezza, ecc.	**ISO 27002:2022 5.19, 5.22**
Se applicabile, verifica che i piani di disaster recovery del fornitore o del fornitore di servizi soddisfino i livelli di continuità del servizio concordati.	**ISO 27002:2022 5.22**
Messa in atto di un processo per gestione delle modifiche agli accordi con i fornitori, ad esempio le modifiche agli strumenti, alle tecnologie, ecc.	**ISO 27002:2022 5.22**
Redazione di un processo per la gestione delle modifiche agli accordi di servizio, ad esempio le modifiche agli strumenti, alle tecnologie, ecc.	**ISO 27002:2022 5.22**

Tabella 20 - Gestione dei fornitori nella Supply Chain

GESTIONE DELLE VULNERABILITA' RETI ITC & OT

Redazione e mantenimento di un inventario dei beni che includa le informazioni rilevanti per le patch.	**ISO 27002:2022 5.9**
Utilizzazione delle risorse informative per identificare le vulnerabilità tecniche rilevanti.	**ISO 27002:2022 8.8**
Valutazione dei rischi di vulnerabilità per il proprio ambiente operativo e disposizione di una politica di manutenzione documentata e implementata.	**ISO 27002:2022 8.8**
Documentazione e ricezione delle patch solo da fonti legittime e catalogate.	**ISO 27002:2022 8.8**
Predisposizione di ambiente di Quality per il test delle patch prima da eseguire prima del passaggio in produzione	**ISO 27002:2022 8.8**
Valutazione di misure alternative nel caso in cui le patch non siano disponibili o applicabili.	**ISO 27002:2022 8.8**
Considerazione nel processo di distribuzione delle patch anche delle procedure di rollback, per esempio per un efficace processo di backup e di ripristino.	**ISO 27002:2022 8.31**

Tabella 21 - Gestione delle vulnerabilità delle reti ITC & OT

GESTIONE DELLE VULNERABILITA' IN PRODOTTI	
Deve essere implementato un processo per la ricezione e il monitoraggio fino alla chiusura delle vulnerabilità di sicurezza segnalate da fonti interne ed esterne che includono componenti di terze parti utilizzati.	**ISA 62443-4-1:2018 DM. 1**
Deve essere implementato un processo per analizzare i rischi di vulnerabilità nel contesto dell'uso previsto e dell'ambiente operativo documentato (se applicabile) utilizzando un sistema di punteggio di vulnerabilità (ad esempio, il sistema comune di punteggio di vulnerabilità).	**ISA 62443-4-1:2018 DM. 2, DM.3**
Deve esistere una politica di manutenzione che definisca il trattamento delle vulnerabilità identificate a seconda del rischio.	**ISA 62443-4-1:2018 DM. 4, SUM-5**
Deve essere implementato un processo per informare gli utenti del prodotto sulle vulnerabilità.	**ISA 62443-4-1:2018 DM. 5, SUM-2**
Deve essere implementato un processo per verificare che una patch affronti la rispettiva	**ISA 62443-4-1:2018 DM. 2, SUM.1**

vulnerabilità e che la patch non sia in contrasto con altri vincoli operativi, di sicurezza o legali.	
Verificare la compatibilità con i componenti di terze parti non integrati.	**ISA 62443-4-1:2018 DM. 2, SUM.3**
Deve essere implementato un processo di consegna delle patch che verifichi l'autenticità e l'integrità di una patch.	**ISA 62443-4-1:2018 DM. 2, SUM.4**
Agli utenti del prodotto deve essere fornita una documentazione relativa alle patch che includa istruzioni per l'installazione e informazioni sulle vulnerabilità chiuse	**ISA 62443-4-1:2018 DM. 2, SUM.2**

Tabella 22 - Gestione delle vulnerabilità in prodotti

GESTIONE DELLE VULNERABILITA' NEL MONDO OT	
Il personale integratore di sistemi OT deve avere le capacità di gestire le vulnerabilità che possono interessare il rispettivo sistema, comprese le relative politiche e procedure.	**ISA 62443-4-1:2019 SP.03.03**
Deve esistere una documentazione che descriva come vengono qualificate le patch.	**ISA 62443-4-1:2019 SP.11.01**
Deve esistere una procedura per documentare lo stato e l'applicabilità delle patch a un sistema.	**ISA 62443-4-1:2019 SP.11.02**
Il personale integratore di sistemi OT deve essere in grado di fornire e installare patch per il rispettivo sistema.	**ISA 62443-4-1:2019 SP.11.03, ISA 62443-4-1 SP.11.04** **ISA 62443-4-1:2019 SP.11.06 RE1**
Il personale integratore di sistemi OT deve essere in grado di garantire che il livello di perfomance venga mantenuto anche dopo l'applicazione delle patch.	
Prevedere i principi di Privacy e Security-by-Design nell'ambito dei dispositivi connessi ai sensori OT (p.es. videosorveglianza, automazione, robotica, wearable, smartphone, ecc.).	

Tabella 23 - Gestione delle vulnerabilità nel mondo OT

GESTIONE DEL FORNITORE	
L'infrastruttura utilizzata per la progettazione, lo sviluppo, la produzione e la consegna di prodotti e	**ISO 27001:2022 A.5.1-5..2, A.5.9-5.14, A.5.26A.8.1, A.6.3, A.6.5, A.8.7-8.8, A.8.20-8.23, A.8.25**

componenti va gestita dai controlli della norma ISO/IEC 27001:2022.	
Deve essere implementato un processo generale di sviluppo/manutenzione/supporto del prodotto che sia coerente con i processi di sviluppo del prodotto comunemente accettati.	**ISA 62443-4-1:2018 SM-1**
Deve essere implementato un processo di sviluppo sicuro che sia coerente con le pratiche di sicurezza comunemente accettate (Security-by-Design).	**ISA 62443-4-1:2018**
L'applicabilità o i requisiti tecnici in base alla categoria di prodotto e ai rischi devono essere considerati sulla base di standard di best practice come la ISA/IEC 62443-4-2:2019.	**ISA/IEC 62443-4-2:2019**
Le dichiarazioni di conformità devono essere accessibili agli utenti dei prodotti delle entità essenziali e importanti per ISO/IEC 27001:2022, IEC 62443-4-1:2018 e IEC 62443-4-2:2019.	**ISO/IEC 27001:2022,** **IEC 62443-4-1:2018** **IEC 62443-4-2:2019**
Gli obiettivi di qualità, come il numero di difetti o le vulnerabilità identificate dall'esterno, devono essere definiti, misurati e utilizzati come strumento per migliorare la qualità complessiva.	**ISO 9001:2015**
Gli esperti e i consulenti di CyberSecurity devono dimostrare competenza, esperienza nel campo delle attività operative loro richieste	**NISTR 8276, NIST SP 800-161r1**

Tabella 24 - Gestione del fornitore

Allegato 1: Sicurezza fisica, safety e cybersecurity: l'integrazione nel contesto metropolitano (Giorgio Pizzi)

La direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio (NIS 2) al considerato 79 evidenzia la molteplicità e la diversità delle minacce che affliggono i sistemi informatici, di rete e il loro ambiente fisico. Agli aspetti classici di protezione dei dati e di sicurezza dei sistemi IT si affiancano quelli legati ai furti, agli incendi, alle interruzioni delle comunicazioni e dell'alimentazione elettrica. Alla stessa stregua dei rischi di cibersicurezza, tra cui le azioni intenzionali e malevole, viene evidenziata la necessità di trattare guasti del sistema, errori umani e fenomeni naturali.

La molteplicità dei fattori di rischio è già riconosciuta dalle norme ISO/IEC 27000 riguardanti i sistemi di gestione della sicurezza delle informazioni. Tuttavia la direttiva NIS2 prevede un collegamento e un coordinamento con quanto previsto dalla direttiva (UE) 2022/2557 relativa alla resilienza dei soggetti critici, che si aggiunge alle misure introdotte dal considerato 89 che riguardano la sicurezza "informatica" dal punto di vista del software e della configurazione dei dispositivi, delle architetture delle reti, della gestione degli accessi e delle identità, e a tutte le misure inerenti la formazione, l'organizzazione, il principio di "zero trust" e l'utilizzo di tecnologie avanzate per la prevenzione, la rilevazione e la gestione degli incidenti.

Con queste considerazioni, le disposizioni dell'articolo 21 della direttiva NIS2, si inseriscono in un contesto più ampio che coinvolge la sicurezza fisica, la safety e la molteplicità dei rischi non necessariamente legati ad attacchi di tipo "cyber". Queste misure devono essere rese coerenti con la direttiva (UE) 2022/2557 rendendo realmente multidisciplinare l'approccio, con la necessità di collaborazione tra professionalità diverse da quelle della tecnologia dell'informazione.

Dall'approccio multirischio per la sicurezza dei sistemi informatici, che prende in considerazione i rischi che non attengono solo alla protezione dei dati, ma a tutti gli eventi che interessano i sistemi per il trattamento degli stessi, a partire dall'accesso fisico alle pertinenze, la prevenzione e la protezione dagli incendi ed inondazioni, la connessione ai sistemi di alimentazione elettrica, segue naturalmente un'ampia accezione del concetto di "sicurezza" – seppur in ambito dei sistemi IT - con il riconoscimento della sua multidisciplinarietà: basti pensare che le misure relative alla lotta al fuoco non vengono trattate da informatici, così come le misure di prevenzione dalle inondazioni attengono più propriamente all'ambito dell'ingegneria civile.

Purtroppo la lingua italiana attribuisce (almeno) due significati significati diversi al termine "sicurezza", con la necessità di dover apportare sempre delle precisazioni, distinguendo la sicurezza "fisica" (inclusa la protezione del patrimonio) e la sicurezza "informatica".

Esiste una terza accezione del termine "sicurezza" che la lingua italiana non mette in evidenza, ma che è reso in maniera ben distinta nel termine "safety" che, come vedremo nel seguito, è oggetto di un'ulteriore concatenazione con il termine "security".

Il contesto metropolitano e la smart city

Il concetto di smart city può riguardare una città metropolitana o un'area vasta e merita considerazioni sui possibili vettori di attacco specifici, sulle tecnologie impiegate e le vulnerabilità da esse derivanti, insieme ai modi in cui possono essere sfruttate, sulle conseguenze e le loro ripercussioni in un ambito più ampio (regionale o nazionale). Trasporti, generazione di energia elettrica e gestione dei servizi idrici sono le categorie fondamentali di servizi in ambito metropolitano e smart city, oltre alle infrastrutture digitali da cui tutti gli altri gestori di servizi dipendono.

L'applicazione di specifici aspetti delle direttive NIS 2 e CER e dell'integrazione tra le varie accezioni della "sicurezza" viene qui sviluppata nell'ambiente metropolitano in quanto modello in scala di una complessità dovuta all'interdipendenza di vari servizi, tra l'altro immersi in un tessuto sociale denso,

da cui derivano specifiche vulnerabilità ed in cui operano soggetti "critici", secondo la definizione della direttiva (UE) 2022/2557. D'altra parte, le città dal punto di vista politico e amministrativo sono deputate ad affrontare gli specifici problemi relativi al loro funzionamento.

Ogni soggetto critico utilizza piattaforme digitali che interconnettono il mondo fisico al mondo digitale sfruttando le potenzialità di quest'ultimo in termini di capacità di informazione e controllo. Tali piattaforme sono parte di un sistema cyberfisico ed utilizzano infrastrutture cloud a volte in comune tra loro.

La necessità di semplificare e circoscrivere il discorso ci porta ad individuare tre specifici sistemi che abitano l'ambito metropolitano: il sistema di mobilità e trasporto, inclusi i sistemi di trasporto "intelligenti", il sistema di trasmissione, distribuzione ed utilizzazione dell'energia elettrica, incluse le postazioni ed i sistemi di controllo ed infine il sistema di distribuzione idrica.

Tra tali soggetti ci sono delle dipendenze in termini di servizi. ITS (intelligent transport systems), tramvie, metropolitane, filovie, Piattaforme di integrazione dei servizi (mobility as a service), stazioni di ricarica per veicoli elettrici, sistemi per la gestione della sosta dipendono da almeno altri due, così come i gestori dei servizi idrici: le infrastrutture digitali (reti, server farm, servizi cloud) e la rete di distribuzione elettrica, in particolare gli elementi propri dei sistemi a guida vincolata quali le sottostazioni elettriche.

La direttiva NIS2 individua nell'allegato le categorie di soggetti citate e a cui si possono estendere la considerazioni che saranno sviluppate.

Nel sottosettore dell'energia elettrica:

- Imprese elettriche quali definite all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio(1)che svolgono l'attività di «fornitura» quali definite all'articolo 2, punto 12), di tale direttiva;
- Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944;
- Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944;
- Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944.
- Nel sottosettore del trasporto su strada:
- Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio.

Nel sottosettore del trasporto ferroviario:

- Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio;
- Imprese ferroviarie quali definite all'articolo 3, punto 1), della direttiva 2012/34/UE e operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva.

Nel sottosettore del trasporto pubblico:

- Operatori di servizio pubblico quali definiti all'articolo 2, lettera d), del regolamento (CE) n. 1370/2007 del Parlamento europeo e del Consiglio.

Nel settore dell'acqua potabile:

- Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1), lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio(18), esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni.

Nel settore delle acque reflue:

- Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, acque reflue domestiche o acque reflue industriali quali definite all'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio(19)escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, acque reflue domestiche e acque reflue industriali è una parte non essenziale della loro attività generale.

Sistemi complessi

Il contesto metropolitano costituisce un sistema "complesso". Nei sistemi complessi, in cui si combinano persone, processi e tecnologia, l'approccio da adottare non può essere riduzionistico, rivolto all'analisi di ogni singola parte distintamente dalle altre, ma olistico, in maniera conforme alla visione "multirischio" della direttiva NIS2.

E' necessario adottare una prospettiva larga, ed uno sguardo d'insieme che veda l'ambito urbano come un "sistema di sistemi".

Parte integrante di questo paradigma è l'individuazione di modelli che permettano di trattare globalmente il problema delle minacce cibernetiche e non solo, oltre alle conseguenze diffuse di uno o più attacchi al "sistema metropolitano".

Gli scenari che devono essere valutati necessitano di specifici modelli di interazione dinamica tra i sistemi che sono parte dell'ecosistema e di tecniche di analisi e valutazione del rischio.

Minacce ibride[45]

Tra le minacce provenienti da azioni intenzionali una specifica categoria è costituita dalle minacce "ibride" che consistono in una combinazione di azioni e attività che possono essere attuate da tipologie eterogenee di attori ciascuno dei quali può utilizzare molteplici strumenti di attacco e agire in parallelo su diversi domini o ambiti (infrastrutturale, cyber, economico, sociale,…) per colpire un obiettivo complesso di importante rilevanza, come possono essere i servizi i servizi di ambito metropolitano.

La minaccia ibrida si ripercuote su entrambe le dimensioni fisica e cyber e coinvolge anche il livello sociale mediante effetti a cascata.

L'approccio alle minacce ibride deve essere omnicomprensivo e definire quali informazioni condividere da parte degli operatori e con quale strumento (piattaforma) di analisi stabilire un ambiente di analisi.

Per la risposta alle minacce ibride è richiesto il riconoscimento di indicatori di compromissione per le varie categorie di minacce ed analisi combinate che determinino la rilevanza di tali indicatori nell'evidenziare una minaccia ibrida (o multi-dominio). Il caso più semplice prevede solo due componenti, quella cyber e quella fisica.

Il riconoscimento di un'effettiva minaccia richiede un coordinamento nella reazione.

[45] A riguardo, il progetto HybNet (https://euhybnet.eu/) tratta nello specifico le minacce ibride mentre il progetto Praetorian (https://praetorian-h2020.eu/) , sviluppa casi di studio concreti per la protezione delle infrastrutture critiche da minacce ibride proponendo un'implementazione per la valutazione del rischio, l'analisi degli effetti a cascata, la rilevazione e la risposta coordinata agli attacchi, proponendo un utile framework architetturale.

La minaccia cyber si può generare in ambito IT, ma le infrastrutture complesse hanno tipicamente una componente OT (come nel caso dei servizi metropolitani), verso la quale mediante movimenti laterali viene spostata la compromissione.

La rilevazione di attacchi fisici si può basare, in casi applicativi, su una gamma di sensori (video, audio, termici…) che siano in grado di coprire tutti i possibili effetti di un evento fisico.

Criticità degli aspetti tecnologici

L'introduzione delle tecnologie crea interconnessioni tra le aree ed i vari domini di competenza. Tuttavia la disuniformità nell'adozione delle stesse e degli standard di riferimento crea delle lacune dal punto di vista della sicurezza ed espone vulnerabilità che caratterizzano l'intero sistema. Anche con il crescente livello di automazione viene estesa la potenziale superficie di attacco, con le necessarie valutazioni legate al rischio di sovvertimento degli scenari automatizzati.[46]

Vengono inoltre alla luce modifiche agli specifici piani di emergenza già adottati, la necessità di gestire le configurazioni sistemi e dispositivi e le valutazioni sugli effetti a cascata di guasti ed attacchi.

Una peculiarità che riguarda la Operational Technology (OT) è la necessità di disporre di tecnologie specifiche per la rilevazione di attacchi, distinte da quelle impiegate in ambito IT ed un ciclo di vita prolungato rispetto a quello della tecnologia IT, con sistemi ancora in esercizio benché installati da molti anni senza che siano sottoposti ad aggiornamento in seguito ad analisi di vulnerabilità.

I sistemi di supervisione, comando e controllo utilizzati nei sottosettori citati precedentemente sono tipici esempi di sistemi cyber-fisici, caratterizzati da un'interazione fisica con l'ambiente esterno, con gli operatori umani e con la collettività.

L'integrazione tra cybersecurity e safety

Il considerato 79 della direttiva NIS2 riporta "Le misure di gestione dei rischi di cibersicurezza dovrebbero pertanto affrontare anche la sicurezza fisica e dell'ambiente dei sistemi informatici e di rete includendo misure volte a proteggere detti sistemi da guasti del sistema, errori umani, azioni malevole o fenomeni naturali, in linea con le norme europee e internazionali, come quelle di cui alla serie ISO/IEC 27000".

Guasti ed errori, insieme ad azioni malevole, sono allora cause di rischio di cybersicurezza. Questa considerazione è analoga quella che si può sviluppare nell'ambito della safety e della sua integrazione con la cybersecurity per i sistemi cyber-fisici.

Essa si basa su due osservazioni:

- i pericoli possono determinare dei guasti, che a loro volta portano a malfunzionamenti che causano comportamenti anomali del sistema e quindi determinare un rischio per la safety;
- gli errori umani possono determinare dei guasti o introdurre delle vulnerabilità (che riguardano la cybersecurity) che quando sfruttate dalle minacce causano comportamenti anomali del sistema e quindi determinare un rischio per la safety.

[46] Per una metodologia strutturata di analisi delle criticità dei servizi nell'ambito smart city si può far riferimento allo studio, datato ma valido per l'approccio, "The Future of Smart Cities: Cyber-Physical Infrastructure Risk" dell' Office of Cyber and Infrastructure Analysis of the U.S. Department of Homeland Security (DHS) - https://www.cisa.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf

Un terzo fattore di natura esterna, agendo su un sistema cyberfisico, può determinare conseguenze paragonabili a quelle degli altri due:

- le minacce che possono sfruttare le vulnerabilità dando luogo ad accessi ed azioni non autorizzate sui sistemi tecnologici (attacchi cibernetici), causandone comportamenti anomali e quindi determinare un rischio riguardante la safety.

In conclusione, in un sistema cyberfisico malfunzionamenti ed azioni intenzionali hanno quindi lo stesso effetto e questo è il motivo per cui è fondamentale l'integrazione tra safety e cybersecurity a partire dal progetto fino all'esercizio dei sistemi.

Una delle possibili tecniche di analisi integrata del rischio è costituita dal fault-attack tree.

L'analisi fault-tree è un metodo per l'analisi dei rischi e dei guasti basata sulla rappresentazione delle concatenazioni tra guasti all'interno di un sistema o un sottosistema. L'analisi attack-tree, introdotta da Bruce Schneier nel 1999 rappresenta un cyberattacco utilizzando una struttura ad albero in cui ogni nodo costituisce una fase dell'attacco. L'ulteriore combinazione con il metodo dell'event-tree analysis permette valutazioni sul rischio combinato.47

Tecnologie per la circolazione ferroviaria

Un primo dominio di applicazione riguarda il trasporto su ferro ed è adottato, a vari livelli di profondità, sui sistemi di trasporto ferroviari, metropolitani e tramviari. E' costituito dai sistemi di gestione della circolazione, dai sistemi di distanziamento, di protezione della marcia e di supervisione e telecomando della circolazione.

Questi sistemi hanno in generale una macro-architettura composta da un centro di controllo, un sistema di comunicazione con gli enti (segnali, deviatoi), distribuiti lungo la linea e nelle stazioni, un sottosistema di bordo ed un sottosistema di terra che comunicano tra loro affinché vengano trasmessi comandi e informazioni che regolano la marcia sicura (nel senso della "safety") dei veicoli.

Uno scenario che merita di essere menzionato è quello in cui un attaccante, dopo aver ottenuto un accesso al sistema di controllo violando le protezioni di "cybersecurity", ne manipola il funzionamento, provocando conseguenze sulla safety, che nel caso specifico riguardano, ad esempio, deragliamenti, collisioni, o arresti indebiti dei veicoli, interruzione delle comunicazioni con necessità di gestione manuale della circolazione e conseguenti rallentamenti.

Citiamo due casi relativi ad incidenti del tipo descritto:

Il 2 marzo del 2022 un attacco all'infrastruttura ferroviaria bielorussa, che ha causato notevoli disservizi, ha interessato il sistema di controllo centralizzato del traffico che sovrintende alla circolazione dei treni ed il loro ingresso in stazione. 48

Il 29 agosto del 2023 il sistema ferroviario della Polonia è stato oggetto di un attacco che ha comportato l'arresto contemporaneo di 20 treni, inviando il comando "radio-stop" sul canale ad esso dedicato, non protetto da crittografia ed autenticazione, utillizzando un normale trasmettitore radio.[49]

Sebbene i sistemi di controllo della marcia e di gestione della circolazione siano realizzati mediante una logica "fail-safe" sono da prendere in considerazione i possibili sovvertimenti di tale logica.

Il legame tra sicurezza IT e safety è oggi riconosciuto dalla norma CEI EN 50129 riguardante i sistemi di telecomunicazione, segnalamento ed elaborazione ed i sistemi elettronici di sicurezza per il

[47] Si rimanda a titolo di esempio al caso di studio trattato in G. Pizzi, "Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment," Transportation research procedia, vol. 45, pp. 250–257, 2020. https://doi.org/10.1016/j.trpro.2020.03.014

[48] https://www.railway-technology.com/news/belarus-hackers-attack-train-systems

[49] https://www.wired.com/story/poland-train-radio-stop-attack/

segnalamento per le applicazioni ferroviarie, tramviarie, metropolitane e filoviarie. In particolare, la necessità di gestire le minacce inerenti la sicurezza IT durante il processo di valutazione del rischio per l'impatto che esse possono avere sulla sicurezza funzionale (safety), riportando nel cosiddetto "safety case" le misure rivolte alla "security".

Oltre alla sicurezza fisica la norma citata riconosce anche l'importanza della sicurezza "fisica" (security) dei dispositivi oggetto della sua applicazione.

Intelligent transport systems

Altro caso di studio importante nel contesto metropolitano o regionale è quello degli ITS: dati acquisiti in tempo reale riguardanti la circolazione e la posizione dei veicoli sono raccolti ed utilizzati come input per un sistema di regolazione della circolazione che agisce, ad esempio, sui tempi delle semaforizzazioni o sulle informazioni ai passeggeri. Agli ITS appartengono anche le applicazioni delle Smart Roads e dei Veicoli autonomi connessi, con le varie comunicazioni tra veicoli e tra veicoli ed infrastruttura.

Anche il MaaS (mobility as a service) è una specifica applicazione degli ITS. Si tratta di un paradigma, implementato sul cloud che rende servizi via apps, basato sui dati esposti relativi ai servizi degli operatori di trasporto e mobilità e sul loro andamento, che offre funzioni prenotazione, acquisto anche a pacchetti e gestione di viaggi multimodali tipicamente in ambito urbano e metropolitano, ed anche a livello regionale e nazionale. In tale paradigma i flussi di informazioni determinano flussi di passeggeri, così che le conseguenze di un cyber-attacco sui flussi di informazione determinano criticità nei flussi dei passeggeri ed hanno un impatto sul sistema sociale.

Per un sistema di controllo del traffico l'architettura è costituita da sensori che raccolgono dati sul traffico o sul posizionamento dei veicoli, attuatori che agiscono sui semafori ed un centro di controllo computerizzato che implementa le logiche adeguate.

Un attaccante che interferisca con la logica di regolazione del traffico, o alteri i dati provenienti dai sensori o diretti agli attuatori può causare un'assoluta difformità nel traffico e criticità nella mobilità urbana e nella sicurezza.

L'impiego di piattaforme "software as a service" o comunque che centralizzano diverse aree fa si che le conseguenze di un attacco rivolto ai servizi centrali abbia conseguenze diffuse. In un contesto delineato dagli ITS sono molteplici i dispositivi che costituiscono il sistema, e ognuno di essi costituisce un punto di attacco. Se da un lato spire induttive e semafori sono i dispositivi periferici classici degli ITS, l'evoluzione ha portato gli smartphones a farne parte. L'utilizzo di reti di comunicazioni estese è un'altra fonte di importazione dei rischi nel sistema. L'approccio uniforme all'aggiornamento dei dispositivi e alla gestione del rischio è fondamentale in un contesto articolato e frastagliato come quello degli ITS per ridurre i punti di attacco e non esporre vulnerabilità isolate che costituiscono il punto debole dell'intero sistema.

Generazione di energia elettrica

I servizi elettrici hanno visto un'evoluzione recente con i sistemi di generazione distribuita che immettono in rete, insieme alle relative tecnologie che consentono l'automazione della generazione, la trasmissione, la distribuzione e la misura con la conseguente diffusione di nuovi dispositivi fisici, molti dei quali a servizio degli utenti finali. Il tutto espande notevolmente la superficie di attacco.

I dispositivi periferici costituiscono una schiera di sensori e strumenti di misura in rete. La tecnologica SCADA è largamente impiegata per il monitoraggio, la supervisione e la regolazione dell'intero sistema di generazione distribuzione, trasmissione e misura. L'intero SCADA a sua volta un sistema

potenzialmente critico in quanto un eventuale accesso non autorizzato provoca scenari di malfunzionamento disservizi e danni fisici.

I sistemi di generazione infatti dispongono di vari attuatori e dispositivi periferici (pompe, valvole, turbine, sistemi elettromeccanici…) il cui funzionamento è asservito allo SCADA (sono ben note dal caso di scuola STUXNET quali siano le conseguenze di una compromissione della logica programmabile di controllo). Tale logica si basa comunque su dati acquisiti, in tempo reale; pertanto, le compromissioni del canale di comunicazione hanno un'analogo effetto sull'intero sistema di controllo. Per sistemi di Operational Technology (OT) infatti, in cui rientrano gli SCADA e i sistemi di controllo industriale (ICS), gli attacchi da prendere in considerazione non sono solo gli ormai tipici ransomware che caratterizzano gli attacchi IT, ma i false data injection, gli attacchi side-channel, gli attacchi elettromagnetici ai sensori, gli attacchi man in the middle sulle reti di controllo industriale.

Così come esistono vulnerabilità dei PLC, esistono anche strumenti che sono in grado di sfruttarle e d'altra parte di proteggerle. Una problematica è costituita dall'obsolescenza tecnologica delle logiche programmabili che, benché funzionanti, non offrono protezione dalle vulnerabilità dovute ad una loro obsoleta concezione. Sistemi che prima erano isolati, inoltre, sono ora interconnessi, esponendo le loro vunerabilità sulle reti ed estendendo la superficie di attacco. In ogni caso la sostituzione delle tecnologie specifiche è onerosa e richiede un progetto di revamping dell'intero impianto OT/ICS. Il virtual patching può essere una soluzione attuabile dal punto di vista tecnico-economico.

L'IT può essere usata come veicolo per accedere all'OT, soprattutto quando vengono utilizzati servizi IT ampiamente diffusi che costituiscono una dorsale informativa/elaborativa per molti sistemi e producono effetti diffusi in conseguenza di un attacco.

La sicurezza della catena di approvvigionamento è altrettanto importante in quanto vulnerabilità o backdoors possono offrire numerose possibilità di attacco distribuito.

La strategia di protezione è quella di elevare in modo uniforme la sicurezza dei sistemi di generazione (distribuiti), implementare logiche di gestione e misure organizzative adeguate a valutare i rischi di nuove possibilità di cyber attacco, si pensi alle possibil variazioni di un attacco simil-Stuxnet (Triton, Industroyer…).

Uno scenario interessante riguarda un attacco mirato e coordinato a sistemi di generazione dell'energia, anche gestiti da diversi soggetti, con l'effetto potenziale di interrompere il servizio di erogazione o di creare danni. Particolarmente rilevante è quanto verificatosi in Danimarca, dove una vulnerabilità sistematica esposta da diversi gestori di servizi elettrici è stata sfruttata in maniera estesa, benché l'attacco sia stato poi rilevato in tempi utili da non produrre effetti sulla parte di controllo o fisica.[50]

E' il caso di citare anche i vettori di attacco che caratterizzano una sottostazione elettrica a servizio di un sistema di trasporto, ovvero quel sistema che fornisce energia per la trazione elettrica alimentando una "linea di contatto". I componenti obiettivo dell'attacco sono gli interruttori, tipicamente telecomandati, e di cui l'attacco può provocare un intervento intempestivo, un'apertura indebita, con conseguenze gravi e diffuse sulla regolarità del servizio di trasporto.

Trattamento delle acque

I sistemi di trattamento delle acque costituiscono un altro servizio essenziale o critico in ambito metropolitano, con la particolarità che le loro funzioni riguardano il trattamento di una sostanza fisica mediante molteplici sistemi e componenti interconnessi costituiti da pompe, valvole,condotte di distribuzione, sistemi di drenaggio, sistemi di ventilazione.

[50] https://www.securityweek.com/22-energy-firms-hacked-in-largest-coordinated-attack-on-denmarks-critical-infrastructure/

Anche in questo caso la tecnologia SCADA consente, da un lato, una gestione omogenea ed automatizzata degli impianti e dall'altra espone la propria superficie di attacco cibernetico.

Il trattamento delle acque è effettuato anche mediante agenti biologici e ciò estende la portata e gli effetti di eventuali attacchi. Non è in gioco soltanto la sicurezza fisica e la sicurezza funzionale ma c'è anche una ricaduta sulla salute pubblica. Basti pensare a arresti indebiti di pompe che trattano sostanze chimiche. Allo stesso modo attacchi di tipo spoofing, false data injection o man in the middle possono nascondere un attacco di più ampia scala in corso ed impedire l'intervento delle azioni di protezione. Altro aspetto da tenere in considerazione nella valutazione di un attacco cyberfisico ad un sistema di trattamento acque sono le possibii dispersioni di sostanze che contaminano o allagano aree pubbliche e private.

Possibili attacchi "alla Stuxnet" possono riguardare il danneggiamento di pompe portate a funzionare in assenza di sostanze con il danneggiamento o la distruzione conseguente.

Nei sistemi di trattamento delle acque ci sono anche quelli che smaltiscono le acque piovane e i disservizi fisici dovuti ad attacchi OT sono facilmente immaginabili.

Interdipendenze tra soggetti critici[51]

La valutazione del rischio richiede un modello di riferimento, che un'analisi degli effetti "a cascata" delle minacce e di individuare quale infrastruttura abbia la maggior quota di nodi che in conseguenza di una minaccia provochino un disservizio (esposizione) e l'intensità delle interdipendenze tra sistemi in funzione dei parametri caratteristici (tempi di latenza, risposta, propagazione e recupero), permettendo di valutare le azioni per ridurre la vulnerabilità incrementando la robustezza, rendendo più rapido il recupero o riducendo il tempo di risposta.

Mappatura dei sistemi

L'approccio prevede innanzitutto una mappatura di tutti i sistemi operanti nell'ambito urbano (solo tre nel nostro esempio) e delle loro interconnessioni o interdipendenze in funzione dei parametri citati.

Vanno poi individuati i nodi "critici" che, nella rete fisica-cibernetica-funzionale delineata, sono quelli che permettono di soddisfare la parte più rilevante della domanda.

Tipologie di interdipendenze

La necessità di semplificare e circoscrivere il discorso ci porta ad individuare tre specifici sistemi che abitano l'ambito metropolitano: il sistema di mobilità e trasporto, il sistema di trasmissione, distribuzione ed utilizzazione dell'energia elettrica, incluse le postazioni ed i sistemi di controllo ed infine il sistema di distribuzione idrica.

Tra questi sistemi vige evidentemente un'interdipendenza multipla che è infatti di tipo funzionale (si pensi al disservizio di una sottostazione elettrica di una linea tramviaria o filoviaria), informativo o cibernetico (è il caso del degrado di una control-room o della trasmissione delle informazioni verso di essa, considerato che le metropoli sono dotate molto frequentemente di sistemi di controllo integrato dei servizi urbani), di tipo geografico o di prossimità (è il caso della rottura di una conduttura idrica che produce rivenute d'acqua nella galleria di una linea metropolitana), di tipo logico, tipologia

[51] Per la trattazione ampia e sistematica dell'argomento si rimanda al fondamentale articolo:
S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," in IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11-25, Dec. 2001, doi: 10.1109/37.969131.

che accoglie i casi che non possono essere classificati nelle altre, e quindi a legami che non sono cibernetici, di prossimità o funzionali.

Mappatura delle interdipendenze

Dopo l'individuazione delle minacce pertinenti, si individuano le possibilità di propagazione delle stesse dal nodo esposto verso i nodi della rete pià interni. Questa propagazione può avvenire o verso nodi dello stesso sistema (interdipendenza interna) o verso nodi di un altro sistema (interdipendenza esterna).

Intensità delle interdipendenze

Le interdipendenze tra infrastrutture critiche vengono classificate in 3 livelli di intensità utilizzando una matrice da/a. e utilizzando una classica mappa di colori (verde, giallo, rosso) per identificare i livelli.

Esiste un'interdipendenza reciproca tra trasporto ferroviario e trasporto urbano, e ovviamente le infrastrutture dell'energia costituiscono una dipendenza per tutte le infrastrutture critiche.

Per quantificare l'intensità e fare una caratterizzazione dell'interdipendenza vengono utilizzati i seguenti parametri[52]:

- Tempo di latenza (TL): tempo trascorso da quando il nodo è influenzato fino a quando non inizia a subire qualche effetto
- Tempo di propagazione (TP): durata del transitorio dopo il quale raggiunge il suo nuovo valore di regime;
- Tempo di risposta (TS): tempo minimo richiesto per l'istituzione di una contromisura dopo una perdita totale dell'integrità dovuta alla minaccia. Pertanto, è il tempo minimo trascorso dal momento dell'impatto prima che l'integrità funzionale del nodo possa iniziare a riprendersi.
- Tempo di recupero (TR): durata del transitorio fino al quale l'integrità funzionale del nodo viene completamente ripristinata il suo valore iniziale se influenzato da una minaccia di massimo intensità

Effetti a cascata

La metodologia citata permette un'analisi quantitativa degli effetti "a cascata" delle minacce e di individuare quale infrastruttura abbia la maggior quota di nodi che in conseguenza di una minaccia provochino un disservizio (esposizione) e l'intensità delle interdipendenze tra sistemi in funzione dei parametri caratteristici (tempi di latenza, risposta, propagazione e recupero), permettendo di valutare le azioni per ridurre la vulnerabilità incrementando la robustezza, rendendo più rapido il recupero o riducendo il tempo di risposta.[53]

---

[52] I parametri citati caratterizzano la curva di resilienza dell'infrastruttura critica. Si rimanda a
Craig Poulin, Michael B. Kane, Infrastructure resilience curves: Performance measures and summary metrics, Reliability Engineering & System Safety, Volume 216, 2021, 107926, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2021.107926.

[53] Il progetto Precinct (Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection https://www.precinct.info) ha sviluppato, attraverso dei living labs, dei casi di studio per migliorare la resilienza delle infrastrutture critiche interdipendenti in caso di attacco cyber-fisico.

La conseguenza tipica degli effetti a cascata di una o più minacce è l'interruzione del servizio. Nel caso di una minaccia agente direttamente su un nodo questo perde la propria integrità funzionale, così come nel caso in cui esso subisca gli effetti di un'interdipendenza di prossimità. Gli altri tipi di interdipendenza portano allo stesso modo all'interruzione del servizio.

La simulazione degli effetti a cascata parte dalla modellazione delle infrastrutture critiche con un grafo di interdipendenze che implementa un modello a stati finiti. Lo stato di un nodo è caratterizzato da funzionalità, disponibilità, danno e cambia in funzione di un evento trasmesso mediante una relazione con altri nodi. Questo evento ha anche valore di notifica e viene trasmesso agli altri nodi adiacenti in modo da permettere la riconfigurazione della rete.

Una rappresentazione di questo tipo consente di simulare gli effetti a cascata e di stabilire l'indice di resilienza complessivo come il rapporto tra il livello di servizio residuo rispetto a quello massimo, secondo il concetto di resilienza come capacità di continuare a fornire il servizio anche in conseguenza di un evento distruttivo.

L'esempio delle reti di trasporto

I sistemi di trasporto, per la loro struttura a rete, si prestano bene per evidenziare in maniera semplice gli effetti a cascata dovuti alla riduzione del servizio da parte di un nodo in seguito ad un attacco.

In scala, e fatte le dovute sostituzioni in merito alla natura dell'interconnessione tra nodi, questa esemplificazione si può riportare anche ai sistemi di sistemi.

Conseguenze a cascata di un attacco

Per vulnerabilità di una rete di trasporto, come quella metropolitana, intendiamo la riduzione del servizio offerto in rapporto al verificarsi di determinati eventi.

L'analisi della vulnerabilità viene condotta tramite un modello "capacità-carico" sulla base di una rappresentazione della rete basata su un grafo, in cui il nodo rappresentano le stazioni, gli archi le tratte e le successioni di archi gli itinerari.

La vulnerabilità è quindi valutata dal punto di vista del passeggero, la cui domanda in conseguenza dell'evento può risultare insoddisfatta o può essere ancora soddisfatta seppur con un livello di servizio inferiore.

Nel caso in cui, a causa di un attacco, un nodo riduca la sua capacità di servizio (ossia si congestioni) rispetto al carico, quest'ultimo, cioè il numero di passeggeri da servire in un determinato tempo, si distribuisce sui nodi adiacenti, producendo guasti "a cascata".

I passeggeri possono sperimentare in questo caso l'impossibilità di raggiungere la destinazione oppure raggiungerla ma in tempi non accettabili. Oltre al caso di mancata soddisfazione della domanda, il passeggero potrebbe anche raggiungere la destinazione in tempi accettabili ma superiori a quelli attesi.

La vulnerabilità viene calcolata come somma pesata dei passeggeri "insoddisfatti" e quelli "ancora soddisfatti" in relazione agli effetti del guasto a cascata.

La propagazione di un attacco può essere a cascata e se riguarda servizi trasversali gli effetti sono diffusi e si riferiscono a tutti i servizi che si basano sull'infrastruttura colpita. Una piattaforma per la gestione dei servizi urbani è, ade esempio, un'infrastruttura trasversale su cui le conseguenze di un attacco sono diffuse.

Gli scenari rispetto ai quali la vulnerabilità è stata valutata rispetto a guasti a cascata riguardano: l'attacco al nodo singolo, l'attacco simultaneo a gruppi di nodi, l'attacco ad un nodo specifico (il più

rilevante per grado e centralità), l'attacco ad un gruppo di nodi specifico rilevanti rispettivamente per grado e centralità.

Ciò che risulta è che ovviamente la vulnerabilità calcolata senza tenere conto degli effetti a cascata risulta fortemente sottostimata rispetto a quella calcolata tenendone conto, e che la vulnerabilità nello scenario che prevede l'attacco al gruppo di nodi col più alto indice di centralità è la più alta.

Entrambi i risultati sono intuitivi, in particolare il secondo evidenzia come il punto critico della rete sia costituito dai nodi che è necessario attraversare nel maggior numero di itinerari (considerati come i percorsi più brevi tra un'origine ed una destinazione).

L'effetto a cascata può essere interno, cioè correlato ad una singola tipologia di infrastruttura critica: ad esempio le ripercussioni di un attacco subito da una modalità di trasporto verso altre modalità di trasporto, o esterno, ad esempio quelle di un attacco alla rete di distribuzione elettrica sui sistemi di trasporto.

Gli impatti di un attacco su un fornitore di servizi digitali si possono stimare qualitativamente in funzione di parametri quali: copertura geografica, estensione degli effetti, popolazione interessata, durata.

Metodologia per l'analisi delle interconnessioni, le interdipendenze tra sistemi, assets ed infrastrutture critiche.

Una specifica applicazione delle metodologie di modellazione e analisi di impatto di attacchi trasversali o a cascata è costituita dalle CPaaS (Communication Platform-as-a-Service) introdotta dal progetto Cityscape.[54]

Le piattaforme MaaS sono un caso specifico di CPaaS. Esse offrono funzioni che soddisfano determinati casi d'uso, la cui combinazione dà luogo agli scenari oggetto di analisi.

Il modello di sistema su cui si basa l'analisi del rischio, delle minacce e delle vulnerabillità parte dall'identificazione degli asset elementari e sulla loro composizione in sistemi che ne ereditano le vulnerabilità. Tra asset ed asset e tra assets e sistemi si devono identificare le relazioni per cui una minaccia può interessare un altro asset, l'intero stesso sistema o un altro sistema. Costituiscono asset elementari i componenti hardware, i dati, il software di sistema ed applicativo, gli utenti e le reti di comunicazione. Per ogni caso d'uso si devono preliminarmente definire gli asset compositi.

Esempi rilevanti di asset compositi sono i veicoli, i sistemi AVM, i sistemi di bigliettazione, le piattaforme. Gli asset compositi contribuiscono a costruire l'architettura di altro livello, costituendone i blocchi funzionali. A livello specifico gli asset compositi sono scomposti negli asset costituenti. Il veicolo, in particolare quello autonomo, è considerato un dispositivo IoT esteso. Le tecnologie di comunicazione (LTE, 5G, NFC, Ethernet, TCP/IP; CANBus) sono a loro volta un tipo di asset elementare.

Anche un dispositivo mobile come un telefono cellulare è un asset composito. Minacce o vulnerabilità che riguardano i suoi componenti possono propagarsi e compromettere la sicurezza del sistema.

Le relazioni tra asset sono rappresentate da uno strumento detto matrice di correlazione (o di transizione) con il quale evidenziare le comunicazioni e le tecnologie che costituiscono tali relazioni. Si perviene a tale strumento a partire dall'architettura di sistema per individuare in maniera agevole i percorsi di propagazione delle minacce verso altri asset.

[54] Il progetto Cityscape, particolarmente rilevante per le applicazioni di mobilità urbana (ITS),

Questo tipo di strumento, sebbene nasca per modellare le interdipendenze di tipo cyber, può essere anche esteso a categorie non tecnologiche con relazioni che permettano la propagazione di tipo geografico, fisico, logico ecc…

La matrice di transizione può anche essere utilizzata per rappresentare le concatenazioni dei modi di propagazione delle minacce (da cyber a fisico a geografico) per implementare un'analisi interdominio.

La matrice di transizione deve essere utilizzata in funzione delle minacce prese in considerazione: non tutte le minacce si possono propagare attraverso una determinata relazione tra assets. Il trasferimento del rischio verso un'altra parte è un'opzione nella fase di valutazione e gestione del rischio stesso.

Quando per una determinata vulnerabilità non c'è un'origine della relativa minaccia che abbia la motivazione o la capacità tecnica di sfruttarla, allora non si può parlare di minaccia. Allo stesso modo, quando non c'è una vulnerabilità per cui un'origine della minaccia non abbia le necessarie capacità, tempo e risorse finanziarie, allora quest'origine di minaccia non costituisce un'effettiva minaccia.

In sostanza, l'attaccante, in funzione della sua motivazione, della sua capacità e del tempo e risorse a disposizione, attua una minaccia sfruttando una vulnerabilità.

La dipendenza tra infrastrutture o tra sistemi informativi all'interno della stessa infrastruttura implica la definizione di reti complesse di infrastrutture indipendenti. I grafi di interdipendenza rilevano informazioni sugli scenari che si verificano in caso di guasto. Evidenziano il percorso critico la cui sicurezza definisce la sicurezza dell'intero grafo e quindi dell'intero sistema complesso.

Conseguenze sulla safety

Stuxnet è un esempio di dipendenza del sistema OT dall'infrastruttura critica (modo fisico di interdipendenza) e di quello da esse dipendenti. Il processo di identificazione del rischio deve prendere in considerazione minacce di origine esterna, tra cui quelle provenienti da altre infrastrutture critiche. Allo stesso modo la valutazione dell'impatto di eventuali mancce deve prendere in considerazione che questo possa essere a sua volta l'origine di una minaccia per un'altra infrastruttura critica.

Il grafo di sequenza e trasformazione delle minacce può essere usato per un sistema informativo o per sistemi complessi di reti di infrastrutture critiche.

Un'analisi più approfondita porta a considerare che gli effetti diretti di una minaccia su un particolare nodo possano essere non solo quelli dell'interruzione del servizio ma, attraverso la perdita dell'integrità funzionale, la compromissione delle sue funzioni di tutela della safety.

Il caso riguarda i sistemi di controllo, comando e segnalamento ai quali sono affidate funzioni critiche per la safety i quali non devono subire compromissioni in caso di attacchi di tipo cyber.

È importante citare la tipicità degli attacchi che possono interessare la safety, più legati alla compromissione della logica di funzionamento dei sistemi che all'interruzione del servizio. Gli attacchi DOS o Ransomware, quindi, non assumono immediata rilevanza ai fini della safety quanto quelli di tipo fault-injection, glitch, buffer overflow o anche quelli riconducibili all'hardware, derivati dal concetto applicato nel "Row Hammer".

I sistemi di comando, controllo e segnalamento vengono progettati secondo il principio del "fail-safe", presente in ogni applicazione che riguarda la sicurezza funzionale (functional safety). La logica "fail-safe" va tuttavia preservata anche a fronte di un attacco cyber.

Casi particolarmente esplicativi per l'integrazione tra safety e security possono essere applicati ai sistemi di trasporto o ai sistemi idrici.[55]

Coordinamento e sistemi di gestione

Un sistema di gestione (SG) è un insieme di regole e procedure, definito in una norma riconosciuta a livello internazionale, che un'organizzazione o azienda può applicare allo scopo di raggiungere obiettivi definiti, quali ad esempio la capacità di dimostrare a terzi la propria affidabilità. L'obiettivo generalmente è quello di attuare strumenti che consentono all'organizzazione di tenere sotto controllo i propri processi e le proprie attività.

E' richiesto che ruoli, responsabilità e risorse sono chiari e ben definiti.

Possono esserci diversi sistemi di gestione, a seconda del settore cui si applicano. A ciascun sistema di gestione si applica una particolare norma tecnica volontaria, che definisce le regole cui il SG deve rispondere.

Essi dovrebbero assicurare che l'organizzazione può adempiere ai compiti necessari a raggiungere i suoi obiettivi (qualità, security, safety, ecc…).

Il concetto di HyperSOC per l'orchestrazione

Per HyperSOC intendiamo un Security Operation Center che possa aggregare informazioni provenienti da più SOC, possa rilevare scenari che indicano una compromissione generale delle infrastrutture critiche di un determinato ambito, supportare la reazione a questi eventi implementando le azioni opportune.

Tale concetto ha ispirato uno specifico progetto PNRR italiano, tuttavia ci riferiamo ad un'aggregazione di ambito metropolitano, dove le agenzie di servizi, i gestori delle utilities e di gestori dei servizi di trasporto e mobilità operano già con dei posti centrali di controllo che possono essere fatti evolvere in SOC.

L'HyperSOC di cui abbiamo parlato ora riguarda esclusivamente le minacce cyber. Tuttavia l'interdipendenza tra le infrastrutture critiche fa nascere l'esigenza di un coordinamento centralizzato che abiliti lo scambio di informazioni per migliorare i piani d'azione in corrispondenza di eventi a cascata, insieme alla reattività ed alla formazione necessaria per fronteggiarli, anche mediante simulazioni, rilevare conseguenze non rilevabili altrimenti senza una visione complessiva, uniformare i livelli di protezione ed i processi, far migliorare gli operatori meno strutturati, creare condizioni di fiducia.

Tecnologie quali AI, digital twins e blockchain costituiscono le basi per sistemi che rilevino le anomalie, anticipino le minacce e rilevino dinamicamente le interdipendenze tra infrastrutture critiche e gli effetti a cascata.

[55] Per un caso di studio relativo agli effetti a cascata di un cyber-attacco su un sistema di trattamento delle acquee e di distribuzione delle acque si rimanda a:
Palleti, V., Adepu, S., Mishra, V. et al. Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecur 4, 8 (2021). https://doi.org/10.1186/s42400-021-00071-z
Per i casi riguardanti i sistemi di trasporto si rimanda alle note 3, 4 e 5.

Allegato 2: Infrastrutture Critiche e Infosharing (Alberto Caruso de Carolis).

Generalità

A partire dall'11 settembre 2001 è emersa con particolare evidenza la necessità che le informazioni rilevanti ai fini della sicurezza nazionale debbano essere condivise tra tutti gli attori, pubblici e privati, che devono garantire a vario titolo la regolarità del funzionamento della società civile a fronte del crescente aumento delle minacce antropiche, frutto di turbamenti geopolitici e di dissidi sociali e storici mai sopiti.

Nella necessità quindi di mettere a fattore comune il patrimonio di informazioni, ora più che mai disponibili per qualità e quantità come non mai nella storia umana, urge adottare modelli organizzativi trasversali al settore pubblico e quello privato che consentano un allineamento informativo per poter individuare non solo i trend delle minacce, ma anche i segnali deboli che, evidenziandosi in un settore o area geografica molto diversa o distante, possano essere indicatori di una pianificazione strategica di gravi turbative, o il segnale di inizio delle stesse, al pacifico evolvere delle società contemporanea.

E' quindi questa la traccia che segue questa trattazione, dagli esempi di normative oltreoceano, che vedono l'infosharing imposto ex lege con ordini esecutivi di rango presidenziale, alle timide indicazioni dei vari organismi UE, ripresi flebilmente dalle istituzioni ed apparati della sicurezza informatica nazionale che ne evidenziano, correttamente, la necessità e la futura adozione diffusa, ma ne possono imporre l'adozione solo agli organismi della stretta cerchia degli addetti ai lavori delle amministrazioni pubbliche.

Spicca pertanto l'iniziativa del mondo delle società di gestione aeroportuale che in controtendenza nazionale, ma in linea con la mentalità internazionale di safety e security, insita nel settore dell'aviazione civile commerciale e non, di creare un ISAC nazionale del trasporto aereo cui partecipano le più importanti società di gestione aeroportuale nazionali e l'ente gestore del traffico aereo, naturale prima vedetta dei cieli nazionali ed efficiente regolatore del relativo traffico, da sempre sensibile, per sua natura . alle esigenze di tutela del dominio cyber, ma anche fisico, delle sue delicate infrastrutture di guida e supporto alla navigazione aerea.

Premessa: l'Infosharing nella Direttiva NIS2.

La Direttiva NIS2 fornisce ampia rilevanza al tema della condivisione delle informazioni ed alla riservatezza delle informazioni.

A partire dal "Considerando 9",

Dovrebbero essere prese in considerazione in tale contesto le norme dell'Unione o nazionali per la protezione delle informazioni classificate, gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo TLP[56]. Il protocollo TLP deve essere inteso come uno strumento per fornire informazioni su eventuali limitazioni per quanto riguarda l'ulteriore diffusione delle informazioni. È utilizzato in quasi tutti i team di risposta agli

[56] Lo standard TLP è utilizzato nella comunità dei teams di risposta agli incidenti di sicurezza informatica per facilitare una maggiore condivisione di informazioni sensibili. Indica, inoltre, le limitazioni alla condivisione che i destinatari devono considerare quando comunicano informazioni potenzialmente sensibili ad altri (https://sicurezza.net/news/traffic-light-protocol-aggiornato-protocollo-semaforico/#Traffic_Light_Protocol_cosa_contiene).

incidenti di sicurezza informatica (CSIRT) e in alcuni centri di analisi e condivisione delle informazioni[57].

viene introdotto tale istituto, delegandone il meccanismo di funzionamento al regolamento interno di EU-CyCLONe nel quale verrebbero specificati ulteriormente i meccanismi di funzionamento della rete, compresi i ruoli, i mezzi di cooperazione, le interazioni con altri attori pertinenti e i modelli per la condivisione delle informazioni, nonché i mezzi di comunicazione, come espressamente dichiarato nel Considerando 68:

(68) Gli Stati membri dovrebbero contribuire all'istituzione del quadro di risposta alle crisi di cibersicurezza dell'UE, di cui alla raccomandazione (UE) 2017/1584 della Commissione (15), attraverso le reti di cooperazione esistenti, in particolare la rete europea di collegamento per le crisi informatiche (EU-CyCLONe), la rete di CSIRT e il gruppo di cooperazione. EU-CyCLONe e la rete di CSIRT dovrebbero cooperare sulla base di disposizioni procedurali che specifichino i dettagli di tale cooperazione ed evitare duplicazioni dei compiti. Il regolamento interno di EU-CyCLONe dovrebbe specificare ulteriormente i meccanismi di funzionamento della rete, compresi i ruoli, i mezzi di cooperazione, le interazioni con altri attori pertinenti e i modelli per la condivisione delle informazioni, nonché i mezzi di comunicazione. Per la gestione delle crisi a livello dell'Unione, le parti pertinenti dovrebbero affidarsi ai dispositivi integrati dell'UE per la risposta politica alle crisi nel quadro della decisione di esecuzione (UE) 2018/1993 del Consiglio (16) (dispositivi IPCR). A tal fine la Commissione dovrebbe far ricorso al processo di coordinamento intersettoriale delle crisi ad alto livello del sistema ARGUS. Se la crisi implicasse un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune dovrebbe essere attivato il meccanismo di risposta alle crisi del servizio europeo per l'azione esterna.

La rilevanza strategica assegnata dalla Direttiva NIS2 all'Infosharing appare chiaramente espressa nei Considerando 119 e 120, ritenendo che la validità delle misure di rilevamento e prevenzione dipende in larga misura da una costante condivisione tra i soggetti di informazioni di intelligence relative alle minacce e alle vulnerabilità:

(119) Di fronte a minacce informatiche che si fanno sempre più complesse e sofisticate, la validità delle misure di rilevamento e prevenzione dipende in larga misura da una costante condivisione tra i soggetti di informazioni di intelligence relative alle minacce e alle vulnerabilità. La condivisione delle informazioni contribuisce a una maggiore consapevolezza delle minacce informatiche che, a sua volta, accresce la capacità dei soggetti di impedire che tali minacce si trasformino in incidenti e consente ai soggetti di arginare in maniera più efficace gli effetti degli incidenti e di riprendersi in modo più efficiente. In assenza di orientamenti a livello dell'Unione, diversi fattori, tra cui in particolare l'incertezza sulla compatibilità con le norme in materia di concorrenza e responsabilità, sembrano aver ostacolato tale condivisione delle informazioni di intelligence.

(120) È quindi opportuno che i soggetti siano incoraggiati e assistiti dagli Stati membri al fine di sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le loro capacità di prevenire e rilevare adeguatamente gli incidenti, riprendersi da essi, rispondervi o mitigarne gli impatti. È pertanto necessario consentire la creazione a livello dell'Unione di accordi volontari di condivisione delle informazioni in materia di cibersicurezza. A tal fine, gli Stati membri dovrebbero sostenere e incoraggiare attivamente anche i soggetti quali i soggetti che forniscono servizi di cibersicurezza e di ricerca, nonché i soggetti pertinenti che non

[57] Il protocollo TLP è adottato anche dalla CISA (https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage).

rientrano nell'ambito di applicazione della presente direttiva, a partecipare a tali accordi di condivisione delle informazioni in materia di cibersicurezza. Tali accordi dovrebbero essere stabiliti in conformità delle norme dell'Unione in materia di concorrenza e di protezione dei dati.

Tali orientamenti vengono pertanto traslati nel dispositivo normativo della Direttiva in argomento che ne riferisce fin dall'Art. 1,

Articolo 1 Oggetto e ambito di applicazione
La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno.
A tal fine, la presente direttiva stabilisce:

- obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT);
- misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557;
- norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza;
- obblighi in materia di vigilanza ed esecuzione per gli Stati membri.

Dedicandone poi l'intero Capo VI:

CAPO VI CONDIVISIONE DELLE INFORMAZIONI

Articolo 29. Accordi di condivisione delle informazioni sulla cibersicurezza

Gli Stati membri provvedono affinché i soggetti che rientrano nell'ambito di applicazione della presente direttiva e, se del caso, altri soggetti che non rientrano nell'ambito di applicazione della presente direttiva siano in grado di scambiarsi, su base volontaria, pertinenti informazioni sulla cibersicurezza, comprese informazioni relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di cibersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cibersicurezza per individuare le minacce informatiche, se tale condivisione di informazioni:

mira a prevenire o rilevare gli incidenti, a riprendersi dagli stessi o ad attenuarne l'impatto;

aumenta il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di attenuazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati.

- Gli Stati membri provvedono affinché lo scambio di informazioni avvenga nell'ambito di comunità di soggetti essenziali e importanti e, se opportuno, dei loro fornitori o fornitori di servizi. Tale scambio è attuato mediante accordi di

condivisione delle informazioni sulla cibersicurezza che tengono conto della natura potenzialmente sensibile delle informazioni condivise.

- Gli Stati membri facilitano la conclusione degli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 del presente articolo. Gli Stati membri possono specificare gli elementi operativi, compreso l'uso di piattaforme TIC[58] dedicate e di strumenti di automazione, i contenuti e le condizioni degli accordi di condivisione delle informazioni. Nello stabilire i dettagli relativi alla partecipazione delle autorità pubbliche a tali accordi, gli Stati membri possono imporre condizioni per le informazioni messe a disposizione dalle autorità competenti o dai CSIRT. Gli Stati membri offrono assistenza per l'applicazione di tali accordi conformemente alle loro misure strategiche di cui all'articolo 7, paragrafo 2, lettera h).
- Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino alle autorità competenti la loro partecipazione agli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 al momento della conclusione di tali accordi o, se opportuno, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo.
- L'ENISA offre assistenza per la conclusione di accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 fornendo orientamenti e provvedendo allo scambio delle migliori pratiche.

Il valore della condivisione delle informazioni.

Il tema della condivisione delle informazioni rientra ormai pienamente tra le modalità più efficaci di prevenzione e di intervento nella gestione degli incidenti cyber e non solo.

Al fine di avvalorare l'esattezza di tale affermazione occorre fare riferimento allo studio pubblicato da RAND Corp.[59], nel 2014 a firma di Brian A. Jackson, dal titolo "How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts"[60]

In tale studio vengono esaminate dettagliatamente tutte le iniziative adottate negli USA a seguito degli eventi dell'11 settembre, al fine di individuare un metodo di misurazione dell'efficacia delle tecniche di condivisione delle informazioni, sollevando importanti quesiti in merito all'attribuzione e responsabilità degli investimenti su tali progetti e sul mantenimento degli stessi.

In particolare, lo studio porta alle seguenti conclusioni:

Gli investimenti effettuati negli sforzi di condivisione delle informazioni negli anni trascorsi dall'11/9 hanno creato una chiara necessità di modi per valutare il valore delle iniziative e soppesarne costi e benefici. In aggiunta ai costi associati alla creazione di nuove condivisioni tali attività, in particolare quelle che comportano Impegni e risorse del personale: possono

[58] TIC, acronimo di "Tecnologie dell'Informazione e della Comunicazione".

[59] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest (https://www.rand.org/).

[60] https://www.rand.org/pubs/research_reports/RR380.html.

avere anche i costi di sostentamento. Al di là del confronto dei loro costi e benefici, questi programmi hanno anche sollevato domande significative su chi dovrebbe pagare i costi.

Nonostante l'importanza delle domande, la letteratura sulla valutazione della condivisione delle informazioni è piuttosto scarsa. Quella mancanza, associata ad argomenti appassionati sia a favore che contro il valore di tali sforzi, ha prodotto un dibattito politico stentato che è insufficiente a sostenere compromessi ragionati e ragionevoli tra questi programmi e altri modi per perseguire la sicurezza e altri obiettivi che sono progettati per avanzare. Parte delle difficoltà in quest'area sembrano sorgere dalla gamma di diverse iniziative che sono state raggruppate sotto il termine generale di condivisione delle informazioni, e questa relazione ha cercato di distinguere in modi ragionevoli e utili. Con un'inquadratura più chiara degli obiettivi valutabili che i programmi stanno perseguendo: trasmissione di allerta e allarme, condivisione dei dati, diffusione delle conoscenze, e condivisione delle competenze: i dati sui risultati organizzativi possono essere collegati a diversi modi di valutare il "dosaggio" dell'esposizione alla condivisione delle informazioni a diversi livelli.

In un mondo di risorse limitate a tutti i livelli di governo, effettuare questi investimenti analitici ora è importante se le decisioni future sulla conservazione, la manutenzione o l'espansione di questi sistemi deve essere basata su dati oggettivi invece di ipotesi e prove aneddotiche dei loro effetti e il loro valore.

Tali conclusioni quindi pur riconoscendo una efficacia oggettiva della condivisione delle informazioni, non consentono però di stabilire elemento oggettivi per la valutazione delle stesse ai fini degli investimenti.

È questa, infatti, la principale limitazione del diffondersi di tali pratiche anche nel nostro paese.

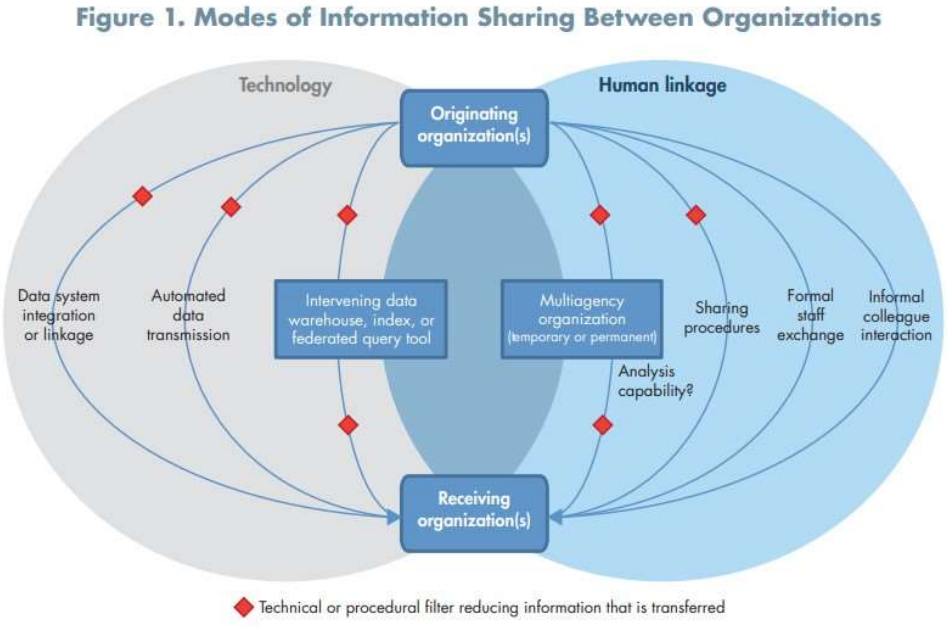


Figura 1: https://www.rand.org/pubs/research_reports/RR380.html by Brian A. Jackson.

L'approccio USA all'Infosharing.

Come indicato nella ricerca della Rand di cui al precedente paragrafo, nel sistema organizzativo della sicurezza USA, il tema della condivisione delle informazioni è affrontato nell'ambito del sistema della Sicurezza Nazionale ed è oggetto di specifica menzione della Direttiva Presidenziale Nr. 7 del 7 dicembre 2003 sulla Homeland Security.

Essa stabilisce una policy nazionale per le Agenzie e i Dipartimenti federali per identificare e dare la priorità alle infrastrutture critiche ai fini della protezione da attacchi terroristici. La direttiva definisce i termini pertinenti e fornisce 31 dichiarazioni politiche. Queste dichiarazioni politiche definiscono ciò che la direttiva copre e i ruoli che le varie agenzie federali, statali e locali svolgeranno nella sua attuazione.

In particolare, tra i compiti e le responsabilità del Segretario per la Homeland Security[61],

La missione dell'organizzazione include analisi, allarme, condivisione delle informazioni, riduzione delle vulnerabilità, mitigazione e assistenza agli sforzi nazionali di ripristino per i sistemi informativi delle infrastrutture critiche. L'organizzazione sosterrà il Dipartimento di Giustizia e altre forze dell'ordine nelle loro continue missioni per indagare e perseguire minacce e attacchi contro il cyberspazio, nella misura consentita dalla legge.

L'Executive Order no. 13691.

[61] https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7.
"Roles and Responsibilities of the Secretary.
The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The organization will support the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law.
Roles and Responsibilities of Other Departments, Agencies, and Offices
In addition to the responsibilities given the Department and Sector-Specific Agencies, there are special functions of various Federal departments and agencies and components of the Executive Office of the President related to critical infrastructure and key resources protection.
Consistent with the E-Government Act of 2002, the Chief Information Officers Council shall be the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of information resources of Federal departments and agencies.
Coordination with the Private Sector
In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms: to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."

Ma è con l'Ordine Esecutivo (Executive Order) nr. 13691 del 2015[62], che viene promossa con grande efficacia la condivisione delle informazioni. In particolare, l'Ordine Esecutivo, a firma del Presidente Barak Obama, ha lo scopo di "incoraggiare la formazione volontaria di tali organizzazioni, di stabilire meccanismi per migliorare continuamente le capacità e le funzioni di queste organizzazioni e di consentire meglio a queste organizzazioni di collaborare con il governo federale su base volontaria" e stabilisce in sintesi questi principi:

Sez. 1. Policy.

Al fine di affrontare le minacce informatiche alla salute e alla sicurezza pubblica, alla sicurezza nazionale e alla sicurezza economica degli Stati Uniti, le aziende private, le organizzazioni senza scopo di lucro, i dipartimenti esecutivi e le agenzie (agenzie) e altre entità devono essere in grado di condividere informazioni relative ai rischi e agli incidenti di sicurezza informatica e collaborare per rispondere il più vicino possibile in tempo reale. Le organizzazioni impegnate nella condivisione di informazioni relative ai rischi e agli incidenti di sicurezza informatica svolgono un ruolo inestimabile nella sicurezza informatica collettiva degli Stati Uniti. Lo scopo di questo ordine è quello di incoraggiare la formazione volontaria di tali organizzazioni, di stabilire meccanismi per migliorare continuamente le capacità e le funzioni di queste organizzazioni e di consentire meglio a queste organizzazioni di collaborare con il governo federale su base volontaria.

Tale condivisione delle informazioni deve essere condotta in modo da proteggere la privacy e le libertà civili delle persone, preservare la riservatezza aziendale, salvaguardare le informazioni condivise e proteggere la capacità del governo di rilevare, indagare, prevenire e rispondere alle minacce informatiche alla salute e alla sicurezza pubblica, alla sicurezza nazionale e alla sicurezza economica degli Stati Uniti.

Sez. 2. Organizzazioni di condivisione e analisi delle informazioni.

(a) Il Segretario per la Sicurezza Nazionale (Segretario) deve incoraggiare fortemente lo sviluppo e la formazione di organizzazioni per la condivisione e l'analisi delle informazioni (ISAO).

b) Gli ISAO possono essere organizzati sulla base di settori, sottosettori, regioni o qualsiasi altra affinità, anche in risposta a particolari minacce o vulnerabilità emergenti. I membri dell'ISAO possono provenire dal settore pubblico o privato o consistere in una combinazione di organizzazioni del settore pubblico e privato. Gli ISAO possono essere costituiti come entità a scopo di lucro o senza scopo di lucro.

c) Il National Cybersecurity and Communications Integration Center (NCCIC), istituito ai sensi della sezione 226(b) dell'Homeland Security Act del 2002 (la "Legge"), si impegna in un coordinamento continuo, collaborativo e inclusivo con gli ISAO sulla condivisione delle informazioni relative ai rischi e agli incidenti di sicurezza informatica, affrontando tali rischi e incidenti e rafforzando i sistemi di sicurezza delle informazioni coerenti con le sezioni 212 e 226 della legge. (d) Nel promuovere la formazione di ISAO, il Segretario si consulta con altri enti federali responsabili della conduzione di attività di sicurezza informatica, comprese le agenzie settoriali, le agenzie di regolamentazione indipendenti a loro discrezione e le agenzie di sicurezza nazionale e di applicazione della legge.

Sez. 3. ISAO Standards Organization.

[62] Executive Order 13691 of February 13, 2015, https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing.

(a) Il Segretario, in consultazione con altri enti federali responsabili della conduzione della sicurezza informatica e delle attività correlate, dovrà, attraverso un processo aperto e competitivo, stipulare un accordo con un'organizzazione non governativa che funga da ISAO Standards Organization (SO), che identificherà un insieme comune di standard volontari o linee guida per la creazione e il funzionamento degli ISAO ai sensi del presente ordine. Le norme perseguono l'obiettivo di creare una solida condivisione delle informazioni relative ai rischi e agli incidenti di cybersicurezza con gli ISAO e tra gli ISAO al fine di creare reti più profonde e più ampie di condivisione delle informazioni a livello nazionale e di promuovere lo sviluppo e l'adozione di meccanismi automatizzati per la condivisione delle informazioni. Gli standard riguarderanno le capacità di base che gli ISAO in base a questo ordine dovrebbero possedere ed essere in grado di dimostrare. Questi standard devono riguardare, ma non essere limitati a, accordi contrattuali, processi aziendali, procedure operative, mezzi tecnici e protezioni della privacy, come la minimizzazione, per il funzionamento ISAO e la partecipazione dei membri ISAO.

(b) Per essere selezionato, l'SO deve dimostrare la capacità di impegnarsi e lavorare in tutta la vasta comunità di organizzazioni impegnate nella condivisione di informazioni relative ai rischi e agli incidenti di cybersicurezza, compresi gli ISAO, e le associazioni e le società private impegnate nella condivisione delle informazioni a sostegno dei propri clienti.

(c) L'accordo di cui alla sezione 3, lettera a), richiede che l'agente di affidabilità si impegni in un processo di revisione e commento pubblico aperto per lo sviluppo degli standard di cui sopra, sollecitando i punti di vista delle entità esistenti impegnate nella condivisione di informazioni relative ai rischi e agli incidenti di cybersicurezza, dei proprietari e degli operatori di infrastrutture critiche, delle agenzie competenti e di altre parti interessate del settore pubblico e privato.

(d) Il Segretario sosterrà lo sviluppo di questi standard e, nell'adempimento dei requisiti stabiliti in questa sezione, si consulterà con l'Ufficio di gestione e bilancio, l'Istituto nazionale di standard e tecnologia del Dipartimento del commercio, il Dipartimento di giustizia, l'Ufficio di supervisione della sicurezza delle informazioni nell'Amministrazione nazionale degli archivi e dei registri, l'Ufficio del direttore dell'intelligence nazionale, le agenzie settoriali e altre entità federali interessate. Tutte le norme devono essere coerenti con le norme internazionali volontarie quando tali norme internazionali faranno avanzare gli obiettivi di questo ordine e devono soddisfare i requisiti del National Technology Transfer and Advancement Act del 1995 (Public Law 104-113) e della circolare OMB A-119, come riveduta.

Sez. 4. Programma di protezione delle infrastrutture critiche.

(a) Ai sensi delle sezioni 213 e 214 (h) del Critical Infrastructure Information Act del 2002, con la presente designo il NCCIC come programma di protezione delle infrastrutture critiche e gli delego l'autorità di stipulare accordi volontari con ISAO al fine di promuovere la sicurezza delle infrastrutture critiche in relazione alla sicurezza informatica.

(b) Altre entità federali responsabili della conduzione della sicurezza informatica e delle attività correlate per affrontare le minacce alla salute e alla sicurezza pubblica, alla sicurezza nazionale e alla sicurezza economica, coerentemente con gli obiettivi del presente ordine, possono partecipare alle attività nell'ambito di questi accordi.

(c) Il Segretario determinerà l'ammissibilità degli ISAO e dei loro membri per qualsiasi necessaria autorizzazione di sicurezza della struttura o del personale associata ad accordi volontari in conformità con l'Ordine Esecutivo 13549 del 18 agosto 2010 (Programmi classificati di informazione sulla sicurezza nazionale per entità statali, locali, tribali e del

settore privato) e l'Ordine esecutivo 12829 del 6 gennaio 1993 (Programma nazionale di sicurezza industriale), come modificato, anche come modificato dalla presente ordinanza.

Con tale Ordine Esecutivo viene quindi statuita formalmente la necessità dello scambio di informazioni, l'organizzazione e modalità di costituzione delle "organizzazioni per la condivisione e l'analisi delle informazioni"(ISAO), gli standard di funzionamento degli ISAO, il coordinamento degli stessi in capo al National Cybersecurity and Communications Integration Center (NCCIC) e la sua delega a stipulare accordi volontari con ISAO al fine di promuovere la sicurezza delle infrastrutture critiche in relazione alla sicurezza informatica.

In conformità con la citata Direttiva Presidenziale (EO 13691), il DHS ha stipulato un accordo di cooperazione con un'organizzazione non governativa per gli standard ISAO guidata dall'Università del Texas a San Antonio con il supporto del Logistics Management Institute (LMI) e del Retail Cyber Intelligence Sharing Center (R-CISC).

La riunione pubblica iniziale dell'ISAO Standards Organization per discutere gli standard per lo sviluppo di ISAO si è tenuta il 9 novembre 2015.

Il ruolo della CISA (Cybersecurity & Infrastructure Security Agency) e la sua visione nella condivisione delle informazioni.

La CISA è un'agenzia federale all'interno del Dipartimento della sicurezza interna (DHS) ed è stata istituita il 16 novembre 2018, quando il presidente Donald Trump ha firmato la legge sulla sicurezza informatica e la sicurezza delle infrastrutture del 2018. Secondo il sito web del CISA, la loro missione è quella di "costruire la capacità nazionale di difendersi dagli attacchi informatici" e di lavorare "con il governo federale per fornire strumenti di sicurezza informatica, servizi di risposta agli incidenti e capacità di valutazione per salvaguardare le reti.gov che supportano le operazioni essenziali dei dipartimenti e delle agenzie partner".

Come dichiarato sul proprio sito ufficiale[63],

"la partnership e la collaborazione sono il nostro fondamento e la linfa vitale di ciò che facciamo. La condivisione delle informazioni e l'azione cooperativa – sia nel settore pubblico che in quello privato – sono essenziali per il nostro obiettivo di aumentare la difesa collettiva della nazione. Il settore privato possiede e gestisce la maggior parte delle infrastrutture critiche della nostra nazione e le partnership tra i settori pubblico e privato che promuovono la fiducia e un coordinamento efficace sono essenziali per mantenere la sicurezza e la resilienza delle infrastrutture critiche. Attraverso queste partnership, facilitiamo un ambiente di squadra in cui la condivisione bidirezionale delle informazioni sulle minacce critiche, la mitigazione dei rischi e altre informazioni e risorse vitali è rapida, senza soluzione di continuità e attuabile. Questo impegno reciproco per la condivisione delle informazioni attraverso le nostre partnership di fiducia è essenziale per la protezione delle infrastrutture critiche e per promuovere la sicurezza informatica per la nazione."

[63] https://www.cisa.gov/topics/partnerships-and-collaboration.

Emerge quindi come il concetto di Information Sharing rivesta un "ruolo essenziale" per la protezione delle infrastrutture critiche. Le modalità in cui questa collaborazione si esplica sono nell'essenza stessa del ruolo della CISA. In particolare,

In qualità di coordinatore nazionale per la sicurezza e la resilienza delle infrastrutture critiche, CISA ha sviluppato e implementato numerosi programmi di condivisione delle informazioni per promuovere risorse e strumenti che aiutano i nostri partner a costruire sicurezza e resilienza. Questi programmi includono campagne di sensibilizzazione e sensibilizzazione come l'annuale Cybersecurity Awareness Month (CAM) e programmi di sensibilizzazione nazionali più ampi che offrono toolkit per i partner. Attraverso questi programmi, CISA sviluppa e condivide informazioni sostanziali con il settore privato e con i governi statali, locali, tribali e territoriali.

Riconoscendo che gli attori delle minacce alla sicurezza informatica non sono vincolati da confini geografici, CISA promuove le relazioni con i partner internazionali per promuovere la condivisione collaborativa delle informazioni, le migliori pratiche di sicurezza informatica e i modelli di partnership in tutto il mondo.

L'Infosharing nel Piano Strategico 2023-2025 della CISA

La strategia attuale della CISA è riportata nel Piano Strategico 2023-2025[64]:

Questo piano strategico comunica la sicurezza informatica e l'infrastruttura. La missione e la visione dell'Agenzia per la sicurezza (CISA) promuovono l'unità degli sforzi attraverso l'agenzia e i nostri partner, e definisce il successo per CISA come un'agenzia. Descrive le parti interessate, la politica e il contesto operativo in cui dobbiamo eseguire e presenta i cambiamenti strategici che CISA farà fare per eseguire meglio la nostra missione vitale nei prossimi tre anni. Esso si basa e si allinea al Strategic Plan for Fiscal Years 2020 – 2024 del Department of Homeland Security.

Per quanto attiene all'Information Sharing, si rinviene l'azione intrapresa nell'Obiettivo 3.4:

Per migliorare la consapevolezza situazionale sia per CISA che per i nostri stakeholder, dobbiamo migliorare le comunicazioni multidirezionali con i partner esterni, compresa la segnalazione tempestiva degli incidenti e la condivisione di minacce e vulnerabilità, requisiti di intelligence e intelligence, nonché altre informazioni e dati. Facilitare una maggiore condivisione delle informazioni richiede che continuiamo a costruire nuove strutture di collaborazione come il Joint Cyber Defense Collaborative (JCDC), che lavora a stretto contatto con SRMA e Federal Cyber Center. Stiamo anche maturando strutture esistenti come il Federal Senior Leadership Council (FSLC), le organizzazioni di condivisione e analisi delle informazioni (ISAO), i centri di condivisione e analisi delle informazioni (ISAC), gli SCC e i GCC. Questi posizioneranno meglio le parti interessate per una risposta tempestiva agli incidenti. Il miglioramento si riferisce all'accelerazione della velocità, al miglioramento

[64] https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf.

dell'accuratezza e all'efficacia della condivisione e della collaborazione delle informazioni, utilizzando al contempo le autorità della CISA per preservare la privacy, i diritti civili e le libertà civili.

La visione sull'infosharing di ENISA

Come noto, il quadro normativo dell'ENISA è il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

Il Regolamento (UE) 2019/881 prevede inoltre che l'ENISA assista la Commissione nelle funzioni di segretariato del gruppo europeo per la certificazione della cibersicurezza (ECCG) e provveda alle funzioni di segretariato del gruppo dei portatori di interessi per la certificazione della cibersicurezza (SCCG)[65].

La strategia di ENISA sull'infosharing[66] è dettagliata ai fini pratici nel testo "Information Sharing and Analysis Center (ISACs) - Cooperative models"[67], pubblicato nel 2018.

Come affermato fin dall'introduzione,

La collaborazione è un obiettivo comune di ogni strategia nazionale europea di sicurezza informatica. Collaborazione per migliorare la sicurezza informatica a tutti i diversi livelli, ovvero la condivisione delle informazioni sulle minacce, la sensibilizzazione può essere raggiunta in due strutture formali: i centri di condivisione e analisi delle informazioni (ISAC) e i partenariati pubblico-privato (PPP). Questo anno L'ENISA ha condotto uno studio sui modelli cooperativi per il partenariato pubblico-privato (PPP) e i Centri di condivisione e analisi delle informazioni (ISAC), che raccolgono informazioni sulle migliori pratiche e sugli approcci comuni.

Il suddetto report esamina dettagliatamente tutti gli aspetti sia di carattere giuridico che economico, sottesi all'utilità di realizzare ISACs, ed in particolare per quanto attiene alle infrastrutture critiche muove da questa considerazione,

L'industria è la principale forza trainante di tutti gli ISAC. In primo luogo, perché garantire un elevato livello di sicurezza e continuità delle sue attività sono l'interesse principale per il settore privato. Poiché il settore dipende sempre più dalle tecnologie IT e dal loro buon funzionamento, gli aspetti informatici sono sempre più cruciali per la sicurezza del settore. In secondo luogo, l'industria è obbligata per legge per segnalare incidenti e garantire la continuità dei servizi critici (ad es. infrastrutture critiche e regolamentazione per la gestione

[65] https://www.enisa.europa.eu/about-enisa/about/it.
[66] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.
[67] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.

delle crisi). Infine, perché il settore privato è il proprietario patrimoniale della maggior parte delle infrastrutture[68].

Per quanto attiene alla partecipazione agli ISACs degli Organismi per la sicurezza nazionale, ENISA indica un principio di sicura utilità che ricollega alla necessità che con questo documento venga anche affrontata la tematica della tutela del segreto,

Le forze dell'ordine e i servizi di intelligence rappresentano un tipo unico di entità governative, grazie alla loro missione speciale. Di solito non sono coinvolti direttamente negli ISAC, ma hanno un collegamento diretto per cooperare con loro. Il coinvolgimento non può essere raggiunto a causa della grande quantità di informazioni classificate che gestiscono che mettono a repentaglio l'equilibrio della condivisione delle informazioni in un ISAC[69].

Infatti, il documento stesso incoraggia all'utilizzo del protocollo TLP (di cui alla nota 57),

TLP è uno strumento per la condivisione di informazioni all'interno di una comunità fidata, comunemente seguito in una cooperazione pubblico-privato. Quando sono coinvolte organizzazioni pubbliche come la polizia o l'intelligence, la condivisione delle informazioni potrebbe essere influenzato da modelli di classificazione dominati dallo Stato (confidenziale, segreto, ecc.). È importante che i membri ISAC si rendano conto dell'esistenza di queste differenze quando si stabiliscono regole o termini di riferimento per la condivisione delle informazioni[70].

E tale modalità è ancor più sottolineata nella raccomandazione "Recommendation: Law enforcement and intelligence community should have a special role when engaging with ISACs", che rende quindi indispensabile tale collaborazione, e quindi le modalità di gestione dedicata della stessa anche nelle necessità di trattare informazioni classificate, ovvero di utilizzarne il contenuto per accrescere le capacità di sviluppo,

C'è una linea molto sottile quando si discute del coinvolgimento o meno delle Forze di Polizia e delle comunità di intelligence. Questo la raccomandazione spiega che, in circostanze specifiche, le Forze di Polizia e l'intelligence potrebbero essere partner di un ISAC e condividere informazioni in sessioni dedicate. Di solito l'industria fa appello alla necessità di avere un luogo di discussione che consenta la cooperazione con le forze dell'ordine e la comunità dell'intelligence. Dà loro un'opportunità nel campo della lotta contro la criminalità informatica e l'opportunità di ottenere informazioni sulle nuove minacce. C'è una convinzione generale nel settore privato che il governo abbia accesso a conoscenze speciali e la cooperazione potrebbe offrire il beneficio di raccogliere queste informazioni.

[68] 3.2.2 The role of industry and critical infrastructure operators, pag. 26.
[69] 3.2.3 Law enforcement and intelligence community involvement, pag. 27.
[70] Recommendation: ISAC participants should follow the Traffic Light Protocol (TLP) for information sharing.

In definitiva, il documento di ENISA fornisce un valido supporto per ogni aspetto che riguardi la creazione di un ISAC, fornendo indicazioni dettagliate e principi organizzativi estremamente efficaci di cui in questa trattazione si sono evidenziati in particolare i rapporti con gli enti investigativi e di intelligence.

L'approccio italiano all'infosharing.

Un efficace quadro della situazione italiana sull'argomento, ci viene offerto dall'utilissimo articolo "Prevenire ed identificare le minacce cyber, ma anche condividere tra gli operatori strategie e risultati: cos'è la Cyber Threat Information Sharing e una panoramica sul percorso verso una strategia difensiva condivisa in Italia", pubblicato sulla testata online Agenda Digitale, il 12 Set 2018 a firma di Stefania Colombo dello Studio Legale Albè e Associati.[71]

In particolare,

La Cyber Threat Information Sharing in Italia

Nel panorama italiano il percorso per addivenire all'elaborazione di una strategia difensiva condivisa è in timida ma costante evoluzione, sia nel settore pubblico che in quello privato.

Tra le principali iniziative si evidenzia l'Agenzia per l'Italia Digitale con la Computer Emergency Response Team Pubblica Amministrazione (CERT-PA), che supporta le amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica.

L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica.

CERT-PA è in grado di fornire alle amministrazioni richiedenti servizi di analisi e di indirizzo, finalizzati a supportare la definizione dei processi di gestione della sicurezza; servizi reattivi per la gestione degli allarmi di sicurezza; servizi relativi alla raccolta e l'elaborazione di dati; formazione e comunicazione per promuovere la cultura della sicurezza cibernetica.

Il CERT-PA interviene a seguito di segnalazioni provenienti da pubbliche amministrazioni, organizzazioni di sicurezza informatica italiane ed internazionali. Il CERT-PA è censito presso ENISA (European Network and Information Security Agency), l'agenzia dell'Unione Europea che supporta la creazione della rete Europea dei CERT e la loro collaborazione e dal 19 luglio 2016 ha ottenuto lo status di "Team accreditato" presso Trusted Introducer, la rete di fiducia dei CERT mondiali fondata in Europa nel 2000.

Un capitolo a parte è il CertFin (per gli attori finanziari).

Gli standard MISP e TIP

Proprio su quest'ultimo settore la comunità internazionale di Cybersecurity ha delineato un suo standard, rappresentato dalle piattaforme di Cyber Threat Intelligence MISP (Malware Information Sharing Platform) o TIP (Threat Intelligence Platform). In particolare, la MISP è usata principalmente per lo scambio delle informazioni e l'arricchimento e correlazione dei

[71] https://www.agendadigitale.eu/sicurezza/cyber-threat-intelligence-e-information-sharing-in-italia-il-quadro/.

dati esterni, mentre la TIP viene utilizzata per la condivisione di informazioni e l'analisi e investigazione di dati interni ed esterni di un'organizzazione.

In un panorama caratterizzato dalla costante evoluzione delle minacce informatiche e da una crescente proliferazione di Internet of Things (IoT), la disponibilità e la maturità delle tecnologie di supporto unita alla capacità interna degli specialisti di Threat Hunting permetteranno di migliorare ulteriormente il livello di sicurezza ed aumentare le capacità di contenimento e contrasto degli attacchi informatici.

Per far ciò, sarà fondamentale da un lato potenziare un'attività di intelligence che consenta di addentrarsi con approfondimenti specialistici all'interno del panorama della minaccia, identificando i cd. bad actors per ogni specifico settore di mercato, dall'altro sarà necessario non interrompere il processo di arricchimento e condivisione di tali informazioni, lavorando sulla costruzione di canali di interconnessione solidi e formalizzati tra i differenti comparti e agevolando l'idea di circolarità alla base degli scambi informativi tra diversi apparati nazionali e sovranazionali pubblici e privati.

Un ulteriore utile contributo ci viene offerto nell'articolo "Info-sharing, le sfide globali oltre la cyber sicurezza. Il modo in cui trattiamo le informazioni nell'era del digitale sta mutando? Scopriamo cosa significa "info-sharing" e come stia cambiando alcuni paradigmi consolidati da decenni", pubblicato il 26 maggio 2022 sulla testata online Agenda Digitale, a firma di Lorenzo Visaggio, di Cybersecurity @ Liguria Digitale.

L'articolo, che fa una attenta, disanima delle modalità in cui è disciplinato l'Infosharing in Italia, trae le seguenti conclusioni:

Seguendo il modello USA, lo CSIRT e l'ACN hanno predisposto diversi meccanismi per condividere aggiornamenti, indicatori di compromissione e best practices generali con la pubblica amministrazione ed aziende strategiche. In particolare, la recentissima strategia nazionale di cybersicurezza prevede la creazione di un ISAC ("information sharing and analysis center"), ossia un punto di raccolta e condivisione delle informazioni con altri centri affini sul territorio nazionale.

L'info-sharing in ambito cyber ha dimostrato molteplici volte le sue potenzialità, sebbene rimangano diverse problematiche non risolte completamente:

Quali informazioni condividere tra gli enti, soprattutto tra aziende;

Quali enti includere in questo sistema di condivisione;

Le modalità con cui questa pratica si sviluppa.

L'esempio di successo dell'applicazione dell'info-sharing in ambito cybersecurity spinge a pensare a quali sarebbero le sue potenzialità anche al di fuori di questo settore; ad oggi, questo termine non viene applicato a contesti esterni, se non raramente e comunque in maniera attinente all'ambito della sicurezza.

Molto utile è anche la posizione della Banca d'Italia riassunta nell'Articolo Bankitalia: "Cyber resilience e info sharing per evitare crisi sistemica a causa di un attacco cyber a sistema finanziario", a firma di Luigi Garofalo, pubblicato sul sito www.cybersecitalia.it il 9 marzo

2022[72]. L'articolo commenta nel dettaglio il paper della Banca d'Italia "Mercati, infrastrutture, sistemi di pagamento (Markets, Infrastructures, Payment Systems) Cyber resilience per la continuità di servizio del sistema finanziario", di Boris Giannetto e Antonino Fazio[73].

"Le numerose e profonde interconnessioni fisiche e logiche tra le diverse componenti del sistema finanziario travalicano i confini nazionali, estendendosi a una dimensione globale e dando luogo a una fitta rete di interdipendenze sia operative che economico-finanziarie. La crescente digitalizzazione amplifica tali relazioni" e, pertanto, "un attacco cyber su larga scala contro punti nodali del sistema finanziario può innescare una crisi sistemica a livello globale". È quanto evidenzia la Banca d'Italia nel paper.

Quindi, prosegue Bankitalia, "uno degli aspetti da rafforzare è l'information sharing, per promuovere una pronta e completa condivisione delle informazioni da parte degli operatori impattati. Al fine di predisporre difese efficaci, è ovviamente essenziale che le entità finanziarie, e in particolare gli operatori di rilevanza sistemica e i gestori di infrastrutture centrali, sviluppino una adeguata conoscenza circa la capacità degli attaccanti di aggirare i presìdi di sicurezza e di difesa, adottando anche misure proattive".

"Un ulteriore aspetto da sottolineare – scrive ancora la Banca d'Italia – è il carattere time critical del sistema finanziario: le transazioni devono concludersi il più rapidamente possibile, e comunque entro un tempo massimo predeterminato. Ciò assicura da un lato la definitività di un'operazione finanziaria e in ultima analisi la certezza e la fiducia degli operatori; al contempo, ne discende una debolezza intrinseca legata alla rapidità con cui un evento anomalo o fraudolento può contagiare l'intero sistema", si legge ancora nel paper.

La strategia adottata dall'Agenzia di Cybersicurezza Nazionale.

Come riportato nell'omonimo documento,

"Con la creazione dell'ACN si è voluto mettere a sistema l'esperienza accumulata nei precedenti cinque anni di lavoro, nel contesto del DPCM 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali", nonché di quella maturata da altri Paesi, riconoscendo autonoma dignità alla sicurezza e alla resilienza cibernetica ponendole sotto la responsabilità del Presidente del Consiglio dei ministri a fondamento del processo di digitalizzazione del Paese, attraverso un più ampio ruolo di sinergia e coordinamento con tutte le Amministrazioni competenti in materia. Si è quindi voluto definire un ulteriore pilastro, attestandolo ad un unico soggetto governativo, a completamento di quelli esistenti di prevenzione e repressione dei reati informatici (di competenza delle Forze di polizia), di difesa e sicurezza militare dello Stato nello spazio cibernetico (di spettanza del Ministero della Difesa) e di ricerca ed elaborazione informativa (di competenza degli Organismi di informazione per la sicurezza).

[72]https://www.cybersecitalia.it/bankitalia-cyber-resilience-e-info-sharing-per-evitare-crisi-sistemica-a-causa-di-un-attacco-cyber-a-sistema-finanziario/17114/

[73]https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2022-018/N.18-MISP.pdf.

A proposito di information sharing, si possono individuare nella strategia dell'ACN le seguenti iniziative:

Al di là degli attori istituzionali con competenze in materia cyber – che non si esauriscono in quelli sopra citati – la presente strategia è ispirata ad un approccio "whole-of-society", che vede coinvolti anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza. Nella presente visione strategica, infatti, quest'ultima è concepita non solamente come un indiretto beneficiario delle misure contemplate nel Piano di implementazione della strategia, ma anche come parte attiva. L'obiettivo ultimo della sicurezza cibernetica nazionale può essere raggiunto solo attraverso il contributo di tutte le componenti del tessuto sociale, nessuno escluso.

Analogamente, nell'Obiettivo risposta nr. 1 "Protezione",

La protezione degli asset strategici nazionali, attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possono abilitare una transizione digitale resiliente del Paese. Di particolare importanza è lo sviluppo di strategie e iniziative per la verifica e valutazione della sicurezza delle infrastrutture ICT, ivi inclusi gli aspetti di approvvigionamento e supply-chain a impatto nazionale.

si individua la seguente azione:

C. la conoscenza approfondita del quadro della minaccia cibernetica e il possesso di adeguati strumenti tecnici, competenze specialistiche e capacità operative, in capo agli attori a vario titolo coinvolti.

L'ulteriore rafforzamento della situational awareness mediante il monitoraggio continuo degli eventi cibernetici e la tempestiva condivisione delle connesse risultanze, secondo gli specifici ambiti di competenza, costituisce, infatti, condizione necessaria ai fini dell'incremento delle capacità nazionali di difesa,

resilienza, contrasto al crimine informatico e cyber intelligence. A tal fine, appare essenziale il costante scambio informativo pubblico-privato e pubblico-pubblico, anche mediante l'introduzione di canali di comunicazione protetti e di un sistema integrato di gestione del rischio cyber per identificare e analizzare vulnerabilità, minacce e rischi in chiave previsionale e programmatica;

Ed infine, più dettagliatamente, al nr. 2. Obiettivo "Risposta", troviamo specificamente richiamato il concetto di ISAC come elemento costituente della gestione degli incidenti e delle crisi di cybersicurezza e al punto B,

L'integrazione degli attuali servizi cyber nazionali nei seguenti ambiti:

- identificazione della minaccia realizzando un "Hyper SOC", ovvero un sistema di raccolta, correlazione e analisi di eventi di interesse da Security Operation Center

(SOC), nonché dagli Internet Service Provider (ISP) mediante apposite convenzioni, al fine di individuare precocemente eventuali "pattern" di attacco complessi che potrebbero rappresentare minacce emergenti di interesse;

- assicurare e facilitare modalità di notifica unitaria degli incidenti di sicurezza cibernetica al Computer Security Incident Response Team (CSIRT), così da rendere più efficace la capacità di risposta e allarme tempestivo;
- risposta agli incidenti realizzando una rete di CSIRT/Computer Emergency Response Team (CERT) settoriali federati con lo CSIRT Italia per la condivisione di procedure, informazioni e supporto nella risposta alle minacce emergenti e agli incidenti;
- condivisione di informazioni realizzando un Information Sharing and Analysis Center (ISAC) centrale presso l'Agenzia, integrabile con una rete di ISAC settoriali sviluppati mediante iniziative pubblico-private, che possa potenziare la diffusione e l'applicazione di informazioni a maggior valore aggiunto per l'innalzamento del livello di cyber resilience del Paese, quali ad esempio best-practice di settore, linee guida, avvisi di sicurezza e raccomandazioni;
- qualificazione di aziende in materia di incident response, in grado di fornire supporto allo CSIRT Italia nel caso in cui dovesse verificarsi una moltitudine di incidenti cyber di natura sistemica.

Figura 2 - l'integrazione degli attuali servizi cyber nazionali (https://www.acn.gov.it/ACN_Strategia.pdf).

Le modalità pratiche di attuazione di queste strategie le troviamo dettagliatamente esposte nel Piano di implementazione delle misure, descritte nel documento "Strategia Nazionale di Cybersicurezza 2022 – 2026"[74]:

Il presente piano di implementazione – che non incide sulle competenze attribuite dalla normativa vigente alle Amministrazioni – riporta, per ciascuno degli obiettivi della Strategia Nazionale di Cybersicurezza – protezione, risposta e sviluppo – le misure da porre in essere per il loro conseguimento, suddivise per aree tematiche, per ognuna delle quali è indicato il novero degli attori responsabili per la loro attuazione e tutti gli altri soggetti a vario titolo interessati – per la cui disamina si rimanda al paragrafo successivo sul quadro di governance nazionale – al netto di quelli che, direttamente o indirettamente, beneficiano degli effetti che ne derivano.

Le Amministrazioni indicate come attori responsabili, sono chiamate a porre in essere le attività necessarie a dare attuazione alle corrispondenti misure, utilizzando le risorse finanziarie a disposizione, a legislazione vigente comprese quelle del PNRR, occorrenti allo scopo.

In particolare, le azioni di interesse si trovano descritte nelle seguenti misure:

Misura #34

Creare un ISAC presso l'ACN, con il compito di coordinare la collazione e l'analisi di informazioni operazionali e strategiche a maggior valor aggiunto prodotte dai vari servizi cyber nazionali. La struttura sarà collegata alla rete europea degli ISAC contribuendo alla realizzazione dello "European CyberShield", previsto dalla Strategia di cybersecurity dell'UE.

Misura #35

Promuovere la creazione di ISAC settoriali integrati con l'ISAC dell'ACN, anche mediante iniziative pubblico-private, così da favorire il potenziamento dello scambio informativo e di best-practice a servizio delle Pubbliche Amministrazioni e dell'industria nazionale (Fig.2).

Un caso pratico di successo: l'ISAC ITAIR[75].

Il settore del trasporto aereo, da tempo aveva percepito il rischio cyber come elemento da considerare con particolare attenzione sulla base della sensibilità del settore stesso ai temi della safety e della security che tradizionalmente lo contraddistingue.

Il progetto, realizzato da Assaeroporti in qualità di project leader, ha visto la partecipazione attiva del Gruppo ENAV, di SEA Aeroporti di Milano, dell'Aeroporto Guglielmo Marconi di Bologna, di SACBO Aeroporto di Bergamo e di SAGAT Aeroporto di Torino. A Roma, il 20 ottobre 2022, si tenuto, presso il Centro di controllo d'area di ENAV, la società che gestisce il traffico aereo civile in Italia, l'evento conclusivo del Progetto in materia di cybersecurity ITAIR ISAC (Italian Airports Information Sharing Analysis Center), il Centro di condivisione e analisi delle informazioni in ambito cyber per mitigare e contrastare gli attacchi informatici.

[74] https://www.acn.gov.it/ACN_Implementazione.pdf.
[75] https://assaeroporti.com/itair-isac/.

Essere parte di una comunità di information sharing che coinvolge molteplici attori a livello nazionale e internazionale è stata la base dell'iniziativa, avviata nel 2020 grazie ai finanziamenti erogati dall'HaDEA, la European Health and Digital Executive Agency della Commissione europea, nell'ambito del Programma Connecting Europe Facility 2014-2020.

Con il progetto sono state, inoltre, gettate le basi per il primo Centro ISAC in Italia nel settore dell'aviazione civile, attraverso il quale sarà possibile raccogliere e condividere informazioni real-time personalizzate rispetto ai bisogni degli utenti, incrementare la visibilità sui rischi informatici e aumentare la conoscenza e la consapevolezza del panorama delle minacce emergenti e future. Sarà così facilitato il processo di arricchimento delle informazioni condivise nella Community e saranno migliorate le capacità di prevenzione, identificazione e mitigazione degli attacchi informatici[76].

L'approccio adottato dal sistema del settore aeroportuale e del controllo del traffico aereo appare di particolare utilità per ipotizzare uno standard di riferimento per le singole categorie di infrastrutture critiche.

Il presupposto di partenza è la connaturata digitalizzazione di processi avvenuta in un settore di per sé particolarmente orientato alla safety e alla security, secondo il principio "Duty of care, sicurezza delle informazioni e aviazione civile".

Come evidenziato nella documentazione di presentazione del progetto,

In questo quadro, l'aspettativa della collettività è quella di preservare il «valore sicurezza», come tendenziale riduzione degli incidenti, non solo riguardo alla safety, ma anche alla security.

L'evoluzione in senso digitale dell'aviazione civile pone tutti gli attori della comunità aeronautica in una posizione di doverosità: il «duty of care» non è solo un principio etico, ma anche un vincolo giuridico che, per i titolari di un dovere di garanzia, si traduce in un chiaro principio di diritto penale: Non prevenire un evento, che si ha l'obbligo giuridico di prevenire, equivale a cagionarlo (art. 40 comma 2 Cod. Pen.)

Il quadro normativo di riferimento in cui è maturato il progetto di infosharing del settore aeroportuale e del controllo del traffico aereo, trae origine prioritariamente dalla normativa aeronautica internazionale di cui alla ICAO Aviation Cybersecurity Strategy approvata dalla 40^ Sessione dell'Assemblea ICAO e pubblicata nel 2019[77],

The ICAO Aviation Cybersecurity Strategy has endorsed during the 40th Session of the ICAO Assembly and published in 2019,

[76] Dalla documentazione disponibile all'apposita sezione del sito https://assaeroporti.com/itair-isac/.

[77] Un guida completa delle previsioni di Cybersecurity nel settore del trasporto aereo è stata pubblicata dalla IATA (International Air Transport Association) ed è reperibile al link https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regulations-standards-and-guidance_3.0.pdf.

Considering the multifaceted and multidisciplinary nature of cyber security and noting that cyber-attacks may rapidly affect a wide spectrum of areas, ICAO's works aimed to deliver a common vision and define a set of global principles addressed by the Strategy. The Aviation Cybersecurity Strategy is aligned with other ICAO activities relative to cyber security and coordinated with the safety and security management provisions. The goal of the Strategy will be achieved by the series of principles, measures, and actions addressed through the following seven pillars:

- *International cooperation;*
- *Governance;*
- *Effective legislation and regulations;*
- *Cybersecurity policy;*
- *Information sharing;*
- *Incident management and emergency planning; and*
- *Capacity building, training, and cybersecurity culture*

In Q4 of 2020, the ICAO Council adopted the Cybersecurity Action Plan (CyAP) to implement the Cybersecurity Strategy. The updated version of the ICAO CyAP is expected in early 2022.

Per quanto attiene alla normativa europea, lo scambio di informazioni è già modalità consolidata nel settore del trasporto aereo e se ne trova fondamento nel riferimento al Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea.

La pratica dello scambio di informazioni tipica del settore aereo è infatti promossa tra i principi base della regolamentazione aeronautica europea che ne dà la seguente definizione fin dall'art.1:

Oggetto e finalità

- L'obiettivo principale del presente regolamento è stabilire e mantenere un livello elevato ed uniforme di sicurezza dell'aviazione civile nell'Unione.
- Il presente regolamento intende inoltre:
- (omissis) la raccolta, l'analisi e lo scambio di informazioni a sostegno di un processo decisionale basato su dati di fatto; (omissis)

e ne specifica i contorni all'Art. 72:

Articolo 72 Raccolta, scambio e analisi di informazioni

- *La Commissione, l'Agenzia e le autorità nazionali competenti si scambiano le informazioni di cui dispongono nel contesto dell'applicazione del presente regolamento e degli atti delegati e di esecuzione adottati sulla base del medesimo, che sono rilevanti per le altre parti per l'esecuzione dei loro compiti a norma del presente*

regolamento. Anche le autorità competenti degli Stati membri preposte alle inchieste su incidenti e inconvenienti nel settore dell'aviazione civile oppure all'analisi di eventi hanno il diritto di accedere a tali informazioni ai fini dell'esecuzione dei propri compiti. Le informazioni possono inoltre essere diffuse alle parti interessate a norma degli atti di esecuzione di cui al paragrafo 5.

- *Fatti salvi i regolamenti (UE) n. 996/2010 e (UE) n. 376/2014, l'Agenzia coordina a livello dell'Unione la raccolta, lo scambio e l'analisi di informazioni su questioni che rientrano nell'ambito di applicazione del presente regolamento, compresi i dati operativi di volo. A tal fine, l'Agenzia può concludere accordi riguardanti la raccolta, lo scambio e l'analisi di informazioni con persone fisiche e giuridiche soggette al presente regolamento, oppure con associazioni di tali persone. Al momento di raccogliere, scambiare e analizzare le informazioni e di concludere e attuare tali accordi, l'Agenzia limita per quanto possibile gli oneri amministrativi a carico delle persone interessate e garantisce la protezione adeguata delle informazioni, nonché di eventuali dati personali ivi contenuti, in conformità del paragrafo 6 del presente articolo, dell'articolo 73, paragrafo 1, e degli articoli 123 e 132 del presente regolamento*.

Da evidenziare fin d'ora il tema della riservatezza delle informazioni, che sempre nel medesimo art. 72 viene disciplinato come segue:

6. La Commissione, l'Agenzia e le autorità nazionali competenti nonché le persone fisiche e giuridiche e le associazioni di tali persone di cui al paragrafo 2 del presente articolo adottano, conformemente al diritto nazionale e dell'Unione, le misure necessarie per garantire l'opportuna riservatezza delle informazioni da esse ricevute ai sensi del presente articolo. Il presente paragrafo non pregiudica eventuali obblighi più rigorosi di riservatezza previsti dai regolamenti (UE) n. 996/2010[78] e (UE) n. 376/2014[79], oppure da altra legislazione dell'Unione.

Infine, da non sottovalutare, la valenza di compliance data all'iniziativa di infosharing anche ai fini del GDPR e del Modello di Organizzazione e gestione previsto dal D.Lgs. nr.231/01:

[78] Regolamento (Ue) N. 996/2010 del Parlamento Europeo e del Consiglio del 20 ottobre 2010 sulle inchieste e la prevenzione di incidenti e inconvenienti nel settore dell'aviazione civile e che abroga la direttiva 94/56/CE, "*Considerando* 22. *Il sistema di sicurezza dell'aviazione civile si basa sul feedback e sugli insegnamenti tratti da incidenti e inconvenienti, il che comporta una rigida applicazione delle regole in materia di riservatezza al fine di garantire la futura disponibilità di preziose fonti di informazione. In questo contesto le informazioni sensibili in materia di sicurezza dovrebbero essere protette in modo adeguato"*, e artt. 14 e 15. (https://www.enac.gov.it/la-normativa/normativa-internazionale/normativa-europea/regolamenti/regolamento-ue-9962010.)

[79] Regolamento (Ue) N. 376/2014 del Parlamento Europeo e del Consiglio del 3 aprile 2014 concernente la segnalazione, l'analisi e il monitoraggio di eventi nel settore dell'aviazione civile, *"Considerando 25. I soggetti interessati dovrebbero poter chiedere l'accesso a talune informazioni contenute nel repertorio centrale europeo, nel rispetto delle norme in materia di riservatezza di tali informazioni e dell'anonimato delle persone interessate*." ed art. 15 (Riservatezza e uso adeguato delle informazioni) (https://www.enac.gov.it/sites/default/files/allegati/2019-Feb/Reg_376-2014.pdf).

Compliance e duty of care: qualcosa in più della semplice conformità, ma effettiva capacità delle organizzazioni a rispondere alle minacce, indirizzando la gestione delle vulnerabilità[80].

Struttura dell'ISAC ITAIR

Come illustrato nella conferenza di presentazione dello stesso,

L'ITAIR ISAC, teso a diventare il focal point per la raccolta, la valorizzazione e la condivisione delle informazioni sulle minacce in ambito cyber, consente inoltre ai soggetti del trasporto aereo di incrementare lo scambio informativo di esperienze, conoscenze e analisi, divenendo così uno strumento utile a stabilire relazioni di cooperazione tra operatori pubblici e privati del settore, a livello nazionale ed internazionale[81].

Obiettivo del progetto era supportare la costituzione di un ISAC per il settore del trasporto aereo

- Disegno degli elementi costitutivi dell'ISAC e delle regole per il funzionamento e la partecipazione dei membri dell'ISAC
- Sviluppo di un modello e piano di sostenibilità del business a medio lungo termine
- Implementazione di un'architettura tecnologica dedicata a supporto della fornitura dei servizi di ITAIR ISAC
- Definizione di una strategia di marketing volta a diffondere le informazioni sulle attività dell'ISAC tra gli stakeholder del settore e ad attrarre potenziali membri nella community.

La Missione dell'ISAC ITAIR viene quindi riassunta nel:

- Promuovere consapevolezza del panorama delle minacce informatiche attuali ed emergenti, accrescendo la capacità degli operatori di identificarle e contrastarle e, al contempo, rafforzare la resilienza del settore del trasporto aereo.
- Si colloca nell'ambito della misura 35 della "Strategia Nazionale di Cybersicurezza 2022 – 2026" dell'ACN, inserendosi nella rete degli ISAC locali.

Nella configurazione tecnologica di ISAC ITAIR, di particolare rilievo il ruolo di ENAV S.p.A[82], la società nazionale di controllo del traffico aereo, che ospita la soluzione MISP[83] (Fig. 3).

[80] Presentazione Evento finale 20 ottobre 2022 (https://assaeroporti.com/wp-content/uploads/Evento_finale_20_ottobre_2022.zip)
[81] https://assaeroporti.com/itair-isac/.
[82] La società per azioni denominata "ENAV S.p.A." deriva dalla trasformazione dell'Ente Nazionale di Assistenza al Volo, disposta dalla Legge 21 dicembre 1996 n. 665, così come modificata dalla Legge 17 maggio 1999 n. 144 (https://www.enav.it/).
[83] https://www.misp-project.org/.

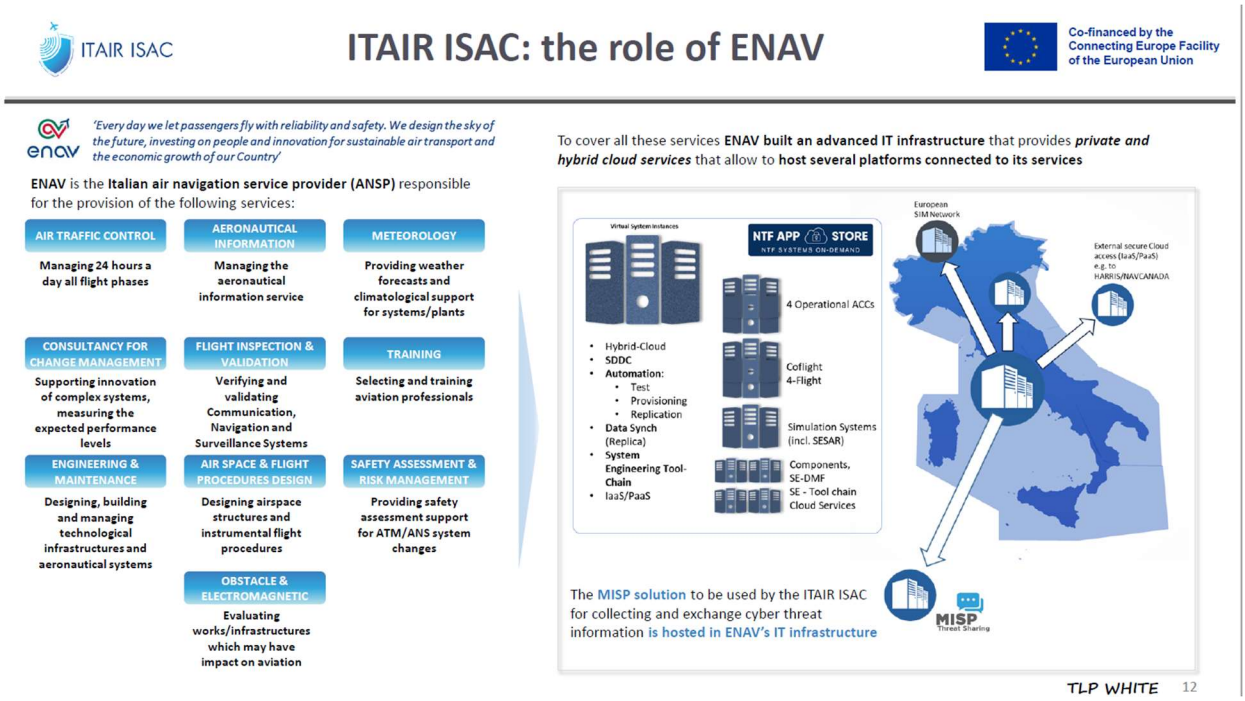


Figura 3 - ITAIR ISAC: The role of ENAV (https://assaeroporti.com/wp-content/uploads/Workshop_11_ottobre_2022.zip).

Conclusioni: un ISAC delle infrastrutture critiche come community istituzionale.

La tutela delle Infrastrutture Critiche è un valore strategico che si ottiene attraverso l'applicazione di norme già esistenti nell'ordinamento giuridico EU e nazionale (Direttive. NIS, NIS2, DORA e CER, Normativa sul "Golden Power" e sulla tutela del segreto di Stato). Essa si ottiene attraverso una efficace governance da adottare attraverso le buone pratiche di gestione aziendale (Codice di Corporate Governance delle Società Quotate84, Codici di autoregolamentazione GDPR, ecc.).

Richiede la condivisione delle informazioni tra tutti gli attori del processo di erogazione del servizio essenziale e di coloro deputati a difenderli ed a proteggere la popolazione dai possibili effetti della loro compromissione (Infosharing, ISACs, ecc.), in una cornice di sicurezza delle informazioni e delle strutture, in cui il Management si proponga come «…garanzia di fedeltà alle Istituzioni della Repubblica, alla Costituzione e ai suoi valori[85]», ed assicuri la propria gestione aziendale a vantaggio dell'azienda stessa, e a tutela della Nazione e della comunità a cui rende il servizio essenziale quale infrastruttura critica (nulla osta di sicurezza[86], collaborazione istituzionale[87], ecc.).

[84] https://www.borsaitaliana.it/comitato-corporate-governance/codice/2020.pdf.
[85] Costituzione, Articolo 54 "Tutti i cittadini hanno il dovere di essere fedeli alla Repubblica e di osservarne la Costituzione e le leggi. I cittadini cui sono affidate funzioni pubbliche hanno il dovere di adempierle con disciplina ed onore, prestando giuramento nei casi stabiliti dalla legge."
[86] Si rimanda al Capitolo "Tutela del segreto".
[87] https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/collaborazione-istituzionale.html.

Allegato 3: Infrastrutture critiche e segreto di stato (Alberto Caruso de Carolis).

Generalità

La tematica del segreto è strettamente connessa con l'interesse nazionale, di cui le infrastrutture critiche rappresentano un asset strategico fondamentale. Da tale considerazione emerge la necessità che la materia, fino ad ora appannaggio esclusivo delle pubbliche amministrazioni o delle grandi aziende di Stato (e relativi appaltatori e fornitori), per settori specifici come la Difesa e la sicurezza dello Stato, venga esplorata anche dalle nuove categorie di soggetti economici rilevanti ai fini ella sicurezza nazionale, quali ad esempio gli operatori di servizio essenziale, i fornitori di servizi digitali e finanziari (e conseguentemente i relativi addetti e consulenti), che ne potrebbero divenire, per loro natura, i prossimi destinatari.

Ciò alla luce delle sempre più turbinose vicende geopolitiche che vedono il repentino ritorno dei conflitti non più solo "asimmetrici" ma anche "convenzionali" e "ibridi", tipici di un nuovo scenario multipolare, e della "weaponizzazione" di molti strumenti economici, finanziari e mediatici, che vedono nel dominio cyber e nelle risorse energetiche (e relativi produttori e distributori), i nuovi campi di battaglia virtuali e reali, in cui l'integrità delle informazioni che le riguardano e per tale natura sensibili ai fii della sicurezza nazionale nella sua più ampia declinazione attuale, siano custodite e comunicate nella maniera appropriata e trasmesse a coloro che ne siano i legittimi destinatari.

Questa sezione traccerà un percorso logico tra le normative sovranazionali e nazionali di riferimento, quasi a guisa di guida pratica, evidenziando come gli aspetti di sicurezza nazionale cyber ne siano strettamente connessi e come la tutela del segreto ponga anche adempimenti direttamente collegati all'esercizio del "Golden Power" da parte dell'autorità governativa, detentrice appunto del potere di tutelare le informazioni.

Premessa: Infrastrutture critiche e segreto di stato

Il rapporto tra infrastrutture critiche e segreto di Stato è sempre stato molto stretto. Con D.P.C.M. del 08.04.2008, "Criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato" [88].

All'art.1, sono disciplinati

"…i criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato, nonché individua gli uffici competenti a svolgere, nei luoghi coperti da segreto di Stato, le funzioni di controllo ordinariamente svolte dalle aziende sanitarie locali e dal Corpo nazionale dei vigili del fuoco."

Il successivo art. 5, "Materie di riferimento"

"1. Ferma restando la necessità di valutare in concreto ogni singolo caso sulla base di quanto disposto dagli articoli 3 e 4 del presente regolamento, sono suscettibili di essere oggetto di segreto di Stato le informazioni, le notizie, i documenti, gli atti, le attività, i luoghi e le cose attinenti alle materie di riferimento esemplificativamente elencate in allegato.

[88] Pubblicato nella Gazz. Uff. 16 aprile 2008, n. 90, https://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=2836.

Nell'allegato al predetto DPCM, che elenca appunto "le informazioni, le notizie, i documenti, gli atti, le attività, i luoghi e le cose attinenti alle materie di riferimento", al nr.17 sono testualmente citate,

17. gli stabilimenti civili di produzione bellica e gli impianti civili per produzione di energia ed altre infrastrutture critiche;

e pertanto la trattazione delle questioni attinenti alle infrastrutture critiche, devono essere trattate con attenzione al tema del segreto di Stato e non tanto nella generica riservatezza delle informazioni aziendali come normalmente previsto e comunque di opportuna adozione da parte delle aziende, di cui alla norma ISO/IEC 27002:2022[89], circa le procedure utili ai fini di assicurare la tutela della riservatezza delle informazioni aziendali.

Infatti, una analoga considerazione può emergere facendo riferimento ad una esauriente esposizione apparsa su Analisi Difesa a firma di Giovanni Pagani, circa la protezione delle infrastrutture critiche[90],

"L'ultima annotazione riguarda la tutela delle informazioni sensibili applicate "… alle IC, nonché ai dati ed alle notizie relativi al processo d'individuazione, di designazione e di protezione delle ICE…" alle quali "… fatte salve le necessità di diffusione, anche preventiva, di notizie e di informazioni verso gli utenti ed i soggetti diversi dal proprietario e dall'operatore dell'infrastruttura, che a qualsiasi titolo prestano attività nell'IC, ai fini della salvaguardia degli stessi … è attribuita adeguata classifica di segretezza ai sensi dell'articolo 42 della legge 3 agosto 2007, n. 124, e relative disposizioni attuative". A proposito dei livelli di classifica il decreto detta infine i criteri di comportamento: "Ove venga attribuita classifica di segretezza superiore a riservato[91], l'accesso ed il trattamento delle informazioni, dei dati e delle notizie di cui al comma 1 è consentito solo al personale in possesso di adeguato nulla osta di segretezza (NOS) nazionale ed UE, ai sensi dell'articolo 9 della legge 3 agosto 2007, n. 124, relative disposizioni attuative". Il decreto, facendo riferimento al Regolamento (CE) 1049/2001, dispone infine che "nelle comunicazioni con altri Stati membri e con la Commissione europea, alle informazioni sensibili relative alle IC ed ai dati e notizie che consentono comunque l'identificazione di un'infrastruttura, sono attribuite le classifiche di segretezza UE …". (Decreto Legislativo 61/2011);"

Le norme UE sulle informazioni classificate

[89] Si richiama l'utilissimo articolo apparso sul sito di Federprivacy a firma di Monica Perego, https://www.federprivacy.org/informazione/primo-piano/tutela-della-riservatezza-delle-informazioni-aziendali-e-iso-27002-2022-le-misure-di-sicurezza-per-i-trattamenti-di-dati-personali-verbali.

[90] https://www.analisidifesa.it/2013/10/la-protezione-delle-infrastrutture-critiche/.

[91] In pratica, laddove un documento fosse contrassegnato dalla dicitura "Riservato" esso può essere gestito, visionato e custodito anche da soggetti che non hanno il nulla osta di segretezza ma deve essere custodito e conservato con il massimo rispetto delle disposizioni aziendali sulla tutela delle informazioni che, in presenza di tale corrispondenza, deve essere necessariamente adottata. Si ricorda infatti che con l'adozione della Direttiva NIS, la comunicazione agli Operatori di Servizio Essenziale fu fatta, dalle rispettive Autorità NIS ministeriali, proprio con comunicazione avente la qualifica di sicurezza "Riservato".

Le disposizioni che prevedono l'adozione del segreto nell'ambito dell'Unione Europea sono contenute in diversi provvedimenti comunitari a partire dalla Decisione 2011/292/UE del Consiglio, del 31 marzo 2011, sulle norme di sicurezza per la protezione delle informazioni classificate UE (GU L 141 del 27.5.2011, pag. 17.) che faceva seguito alla Decisione 2001/264/CE del Consiglio, del 19 marzo 2001, che adotta le norme di sicurezza del Consiglio (GU L 101 dell'11.4.2001, pag. 1).

La Decisione del Consiglio del 23 settembre 2013 sulle "norme di sicurezza per proteggere le informazioni classificate UE" (2013/488/UE) che, all'Articolo 2 (Definizione delle ICUE, delle classifiche e dei contrassegni di sicurezza), stabilisce,

1. Per «informazioni classificate UE» (ICUE) si intende qualsiasi informazione o qualsiasi materiale designati da una classifica di sicurezza UE, la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'Unione europea o di uno o più Stati membri.

2. Le ICUE sono classificate ad uno dei seguenti livelli:

a) TRÈS SECRET UE/EU TOP SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri;

b) SECRET UE/EU SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'Unione europea o di uno o più Stati membri;

d) RESTREINT UE/EU RESTRICTED: informazioni e materiali la cui divulgazione non autorizzata potrebbe essere pregiudizievole per gli interessi dell'Unione europea o di uno o più Stati membri.

3. Le ICUE recano un contrassegno di classifica di sicurezza conformemente al paragrafo 2. Esse possono recare contrassegni supplementari intesi a designare il settore di attività cui si riferiscono, identificare l'originatore, limitare la distribuzione, restringere l'uso o indicare la divulgabilità.

La Decisione in argomento dettaglia approfonditamente l'organizzazione della tutela del segreto UE e tutte le procedure per il trattamento dello stesso con numerosi allegati[92].

Con successive Decisioni del Consiglio nel 2019 vengono adottate le norme di attuazione relative alle singole classificazioni delle informazioni ricoperte da segreto UE e segnatamente:

[92] https://eur-lex.europa.eu/legal-content/it/TXT/PDF/?uri=CELEX:32013D0488&from=EN.

- Decisione (UE, Euratom) 2019/1961 della Commissione, del 17 ottobre 2019, sulle norme di attuazione per il trattamento di informazioni CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET,
- Decisione (UE, Euratom) 2019/1962 della Commissione, del 17 ottobre 2019, sulle norme di attuazione per il trattamento di informazioni RESTREINT UE/EU RESTRICTED,
- Decisione (UE, Euratom) 2019/1963 della Commissione, del 17 ottobre 2019, che stabilisce le norme di attuazione in materia di sicurezza industriale per quanto riguarda i contratti di appalto classificati[93].

Per eventuale utilità e per approfondimenti, si rimanda a quanto pubblicato sul sito del Consiglio, in cui sono riportati gli elementi della normativa vigente e gli aggiornamenti come utile prontuario per gli addetti ai lavori[94].

La posizione dell'ENISA sulla riservatezza delle informazioni.

La materia è trattata nella Decision No MB/2020/21 del Consiglio di amministrazione di ENISA del 30 novembre 2020[95].

In sostanza ENISA adotta il sistema di classificazione delle informazioni adottato dalla Commissione Europea.

La tutela del segreto nella Direttiva NIS2.

Per quanto riguarda l'identificazione degli operatori di servizi essenziali, il decreto di recepimento ripropone i criteri di cui all'Articolo 5(2) della Direttiva:

- fornitura di un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
- dipendenza di tale servizio dalla rete e dai sistemi informativi; e
- effetti negativi rilevanti sulla fornitura di tale servizio in caso di incidente informatico, rilevanza da valutarsi secondo i criteri specificati all'Articolo 6 della Direttiva (e riproposti all'Articolo 5 del decreto).

Questi sono i criteri che le autorità competenti NIS hanno seguito per identificare gli operatori di servizi essenziali per ciascun settore coperto dalla Direttiva. Nel complesso (e fino ad ora), sono 465 le società e gli enti identificati quali operatori di servizi essenziali e quindi tenuti a

[93] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L:2019:311:FULL.

[94] https://www.consilium.europa.eu/it/general-secretariat/corporate-policies/classified-information/information-assurance/.

[95] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2020_21_-on-handling-classified-information.

rispettare la normativa NIS. Tuttavia, la lista completa non è stata resa pubblica per motivi di sicurezza nazionale[96].

Il decreto attuativo ripropone i generici obblighi di sicurezza previsti dalla Direttiva NIS all'Articolo 14. In sostanza, gli operatori di servizi essenziali sono tenuti ad adottare misure tecnico-organizzative "adeguate" alla gestione dei rischi e alla prevenzione degli incidenti informatici. Il decreto specifica però che nell'adottare tali misure gli operatori sono tenuti a tenere in debita considerazione le linee guida predisposte dal Gruppo di Cooperazione, nonché le linee guida predisposte dalle autorità competenti NIS. Tali linee guida acquisiscono quindi un'importanza fondamentale ai fini di dimostrare l'adeguatezza delle misure adottate. A tale proposito, le linee guida sulla gestione dei rischi e la prevenzione, mitigazione e notifica degli incidenti adottate dalle autorità NIS nel mese di luglio 2019 assumono un ruolo di primaria importanza. Queste ultime sono state però condivise solo con i 465 operatori di servizi essenziali individuati.

La Direttiva NIS2 affronta il tema della necessità di riservatezza sulle informazioni oggetto di trattazione e di scambio tra i soggetti interessati, fin dal Considerando (9)

(9) Gli Stati membri dovrebbero essere in grado di adottare le misure necessarie a garantire la tutela degli interessi essenziali della sicurezza nazionale, a salvaguardare l'ordine pubblico e la pubblica sicurezza e a consentire la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati. A tal fine, gli Stati membri dovrebbero poter esentare soggetti specifici che svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'applicazione della legge, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati da determinati obblighi previsti dalla presente direttiva per quanto riguarda tali attività. Qualora un soggetto fornisca servizi esclusivamente a un ente della pubblica amministrazione escluso dall'ambito di applicazione della presente direttiva, gli Stati membri dovrebbero poter esentare tale soggetto da determinati obblighi stabiliti dalla presente direttiva per quanto riguarda tali servizi. Inoltre, nessuno Stato membro dovrebbe essere tenuto a fornire informazioni la cui divulgazione sia contraria agli interessi essenziali della propria pubblica sicurezza. Dovrebbero essere prese in considerazione in tale contesto le norme dell'Unione o nazionali per la protezione delle informazioni classificate, gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo TLP. Il protocollo TLP deve essere inteso come uno strumento per fornire informazioni su eventuali limitazioni per quanto riguarda l'ulteriore diffusione delle informazioni. È utilizzato in quasi tutti i team di risposta agli incidenti di sicurezza informatica (CSIRT) e in alcuni centri di analisi e condivisione delle informazioni.

e nel Considerando (118),

(118) Qualora informazioni classificate in conformità al diritto nazionale o dell'Unione siano scambiate, comunicate o altrimenti condivise a norma della presente direttiva, dovrebbero essere applicate le corrispondenti norme sulla gestione delle informazioni classificate. Inoltre, l'ENISA dovrebbe predisporre l'infrastruttura, le procedure e le norme per il trattamento delle

[96] https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/.

informazioni sensibili e classificate in conformità alle norme di sicurezza applicabili alla protezione delle informazioni classificate dell'UE.

La normativa italiana sulle informazioni classificate UE e nazionali.

Con Decreto del Presidente Del Consiglio Dei Ministri 11 aprile 2002 "Norme di sicurezza per la tutela delle informazioni UE classificate di attuazione della Decisione del Consiglio dell'Unione europea del 19 marzo 2001[97], che con articolo unico stabilisce:

1. Per gli aspetti di rilevanza interna, piena e completa attuazione è data alla Decisione 2001/264/CE del Consiglio dell'Unione europea del 19 marzo 2001, che adotta le norme di sicurezza del Consiglio, pubblicata nella Gazzetta Ufficiale delle Comunità europee n. L 101 dell'11 aprile 2001, di cui all'allegato 1.

2. L'organizzazione nazionale per la sicurezza, istituita ai fini della tutela delle informazioni classificate, è di conseguenza aggiornata secondo le disposizioni contenute nell'allegato 2.

3. L'Autorità nazionale per la sicurezza prescrive le altre disposizioni di dettaglio per l'integrale attuazione delle norme di sicurezza contenute nella predetta Decisione, nell'ambito nazionale e nel rispetto della disciplina di protezione dei dati personali, eventualmente applicabile.

Al predetto procedimento segue il Decreto del Presidente del Consiglio dei ministri 11 Aprile 2003 (anch'esso dell'11 aprile a firma del Presidente del Consiglio Berlusconi ma dell'anno successivo e pubblicato nel Supplemento ordinario alla "Gazzetta Ufficiale" n. 167 del 21 luglio 2003 - Serie generale)[98] che dettaglia accuratamente ogni aspetto della normativa nazionale sul segreto, integrata con quella dell'UE.

In questa sede può essere utile riportare i principi generali a cui si informa la normativa che ben esplicano in generale il sistema di gestione della segretezza delle informazioni e degli ambiti in cui si estende la regolamentazione:

PRINCIPI BASILARI

7. Le misure di sicurezza:

a) riguardano tutte le persone che hanno accesso alle informazioni classificate, ai supporti delle informazioni classificate, agli edifici che contengono tali informazioni e a importanti installazioni;

b) sono destinate a individuare le persone la cui posizione possa mettere a repentaglio la sicurezza di informazioni classificate e di importanti installazioni che contengono informazioni classificate e a provvedere alla loro esclusione o allontanamento;

c) impediscono alle persone non autorizzate di accedere alle informazioni classificate o alle installazioni che le contengono;

---

[97] (GU n.143 del 20-6-2002 - Suppl. Ordinario n. 130), https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario.

[98] https://www.gazzettaufficiale.it/eli/gu/2003/07/21/167/so/114/sg/pdf.

d) garantiscono che le informazioni classificate siano diffuse soltanto in base al principio della necessità di sapere che è fondamentale per tutti gli aspetti della sicurezza;

e) assicurano l'integrità (ossia la prevenzione della corruzione, dell'alterazione o della cancellazione non autorizzata) e la disponibilità (ossia l'accesso non è negato a coloro che devono e sono autorizzati ad averlo) di tutte le informazioni, siano esse classificate o non, e soprattutto delle informazioni immagazzinate, elaborate o trasmesse sotto forma elettromagnetica.

L'Autorità NIS.

Un cenno su tale autorità occorre che venga fornito in quanto l'istituto, previsto dalla prima Direttiva NIS, può essere Autorità originatrice di documentazione classificata e quindi possa imporre ai soggetti sottoposti alla sua vigilanza, l'adozione delle procedure previste per il segreto di Stato.

Come noto, con il Decreto Legislativo 18 maggio 2018, n.65, l'Italia ha dato attuazione, alla Direttiva (UE) 2016/1148, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).

Per una breve disanima sul ruolo delle Autorità NIS, si richiama il contenuto di una pubblicazione del Sistema della Sicurezza Nazionale che ne descrive efficacemente il ruolo[99]:

Le Autorità competenti NIS, quali responsabili dell'attuazione del decreto:

- vigilano sulla sua applicazione ed esercitano le relative potestà ispettive e sanzionatorie, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica. Salvo che il fatto costituisca reato, la violazione da parte di OSE e FSD degli obblighi previsti dal decreto legislativo comporta l'irrogazione di sanzioni amministrative pecuniarie fino ad un massimo di 150.000 euro; la reiterazione determina l'aumento fino al triplo della sanzione prevista;
- procedono ad identificare gli OSE entro il 9 novembre 2018 (consultando, laddove necessario, le Autorità competenti NIS degli altri Stati Membri), individuando anche le soglie in ragione delle quali un incidente è da considerarsi pregiudizievole per la sicurezza delle reti e dei sistemi informativi. Se un evento implica anche violazione di dati personali, le Autorità competenti NIS operano in stretta cooperazione con il Garante per la protezione dei dati personali. Al riguardo, sono in corso approfondimenti per propiziare un raccordo tra gli obblighi introdotti dal Decreto legislativo di recepimento della Direttiva NIS e quelli previsti dal nuovo Regolamento europeo per la protezione dei dati personali (GDPR);
- possono predisporre linee guida per la notifica degli incidenti e dettare specifiche misure di sicurezza, sentiti gli OSE.

[99] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf.

L'elenco nazionale degli OSE è istituito presso il Ministero dello sviluppo economico e viene aggiornato, almeno ogni due anni, a cura delle Autorità competenti NIS.

Il punto di contatto unico NIS assicura, a livello nazionale, il coordinamento delle questioni relative alla sicurezza delle reti e dei sistemi informativi e, a livello europeo, il raccordo necessario a garantire la cooperazione transfrontaliera delle Autorità competenti NIS italiane con quelle degli altri Stati membri, con il Gruppo di cooperazione istituito presso la Commissione europea - anche attraverso l'elaborazione di linee guida e lo scambio di informazioni e best practices - e la rete dei CSIRT UE. Rientra tra i compiti del punto di contatto unico NIS trasmettere a:

- Gruppo di cooperazione, annualmente, una relazione sulle notifiche ricevute, contenente numero e natura degli incidenti e le azioni intraprese da OSE e FSD;
- Commissione UE, ogni due anni, le informazioni per verificare l'attuazione della Direttiva NIS in Italia.

Quale punto di contatto unico NIS è stato designato il Dipartimento Informazioni per la Sicurezza (DIS), in ragione del ruolo svolto nell'architettura cyber nazionale.

Allo scopo di agevolare le Autorità competenti NIS nell'adempimento dei compiti loro affidati, verrà istituito, attraverso un apposito DPCM, un Comitato tecnico di raccordo.

Il Comitato opererà presso la Presidenza del Consiglio dei ministri, riunendo i delegati dei Ministeri-Autorità competenti NIS e i rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

A valle del recepimento della Direttiva NIS, sarà integrata di un apposito addendum la Strategia nazionale di sicurezza cibernetica, adottata dal Presidente del Consiglio dei ministri, sentito il Comitato Interministeriale per la Sicurezza della Repubblica (CISR).

La normativa nazionale in materia di tutela del segreto

La normativa in generale.

Le norme che disciplinano la materia in ambito nazionale sono le seguenti:

- Legge 3 agosto 2007, n. 124, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto".
- Decreto del Presidente del Consiglio dei ministri 11 aprile 2002, recante "Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato".

- Decreto del Presidente del Consiglio dei ministri 8 aprile 2008, recante "Criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato".
- Decreto del Presidente del Consiglio dei ministri 12 giugno 2009, n. 7, recante "Determinazione dell'ambito dei singoli livelli di segretezza, dei soggetti con potere di classifica, dei criteri d'individuazione delle materie oggetto di classifica nonché dei modi di accesso nei luoghi militari o definiti di interesse per la sicurezza della Repubblica".
- Decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 4, recante "Disciplina della firma digitale dei documenti classificati".
- Decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 5, recante "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva", così come modificato dal decreto del Presidente del Consiglio dei ministri 2 ottobre 2017.
- Decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, recante "Indirizzi per la protezione cibernetica e la sicurezza informatica nazionali".
- Articoli 255-262 del Codice penale.

Il riconoscimento delle classifiche di segretezza internazionali e dell'UE sono recepite dagli artt. 20 e 21 del DPCM 6 novembre 2015, n. 5 recante "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva":

Art. 20

Classifiche di segretezza internazionali e dell'Unione europea.

1. Le classifiche di segretezza internazionali e dell'Unione europea sono previste da trattati, convenzioni, accordi, regolamenti e decisioni comunque denominati, recepiti o a cui è data attuazione in conformità alle norme previste dall'ordinamento.

Art. 21

Qualifiche di sicurezza.

1. Le informazioni classificate appartenenti ad organizzazioni internazionali e all'Unione europea ed a programmi intergovernativi recano le qualifiche previste dai rispettivi trattati, convenzioni, accordi, regolamenti e decisioni comunque denominati e sono assoggettate al regime giuridico di rispettiva appartenenza.

Una esaustiva sintesi del sistema organizzativo nazionale in tale materia si può trarre dal sito del Sistema della Sicurezza Nazionale dalla sezione "Tutela delle informazioni"[100]:

[100] https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/tutela-delle-informazioni.html.

La legge 124/2007 detta la disciplina sul segreto di Stato, prevedendone i casi di apposizione, opposizione e conferma, come pure i casi in cui è espressamente escluso il ricorso a tale strumento.

La stessa legge contempla il ricorso a specifiche classifiche di segretezza per tutelare le informazioni e limitarne la conoscenza ai soli soggetti interessati, articolandole su quattro livelli di classifica: segretissimo, segreto, riservatissimo e riservato.

Per la tutela amministrativa del segreto di Stato e delle classifiche è istituito nell'ambito del DIS l'Ufficio centrale per la segretezza (UCSe), di cui si avvale il Presidente del Consiglio per esercitare le sue funzioni di Autorità nazionale per la sicurezza.

In tale ambito, l'UCSe è competente per il rilascio delle abilitazioni di sicurezza.

Con il DPCM 22 luglio 2011 alcune amministrazioni dello Stato sono state delegate al rilascio di abilitazioni di sicurezza nei confronti di specifiche categorie di personale dipendente.

Le abilitazioni di sicurezza agli operatori economici sono sempre rilasciate dall'UCSe.

L'UCSe è una funzione interna all'Autorità nazionale per la Sicurezza (ANS)[101]:

L'Autorità nazionale per la sicurezza (ANS) è nata a seguito di accordi in ambito NATO, in base ai quali ogni Stato membro si impegnava a istituire un'autorità responsabile della protezione delle informazioni classificate dell'Alleanza.

Oltre ad assolvere a questo compito organizzativo originario, in Italia l'Autorità nazionale per la sicurezza è responsabile anche della tutela amministrativa delle informazioni coperte da segreto di Stato e di quelle nazionali classificate.

Le funzioni di Autorità nazionale per la sicurezza spettano al Presidente del Consiglio dei ministri che le esercita attraverso l'Ufficio centrale per la segretezza (UCSe), istituito nell'ambito del DIS.

L'Ufficio centrale per la segretezza (UCSe) svolge funzioni direttive, consultive, di coordinamento e controllo in materia di tutela amministrativa del segreto di Stato e delle classifiche di segretezza.

In particolare l'UCSe:

- *cura gli adempimenti istruttori relativi all'esercizio delle funzioni del Presidente del Consiglio quale Autorità nazionale per la sicurezza, a tutela del segreto di Stato*
- *predispone le misure volte a garantire la sicurezza di quanto è coperto dalle classifiche di segretezza*
- *cura il rilascio e la revoca delle abilitazioni di sicurezza per le persone fisiche e giuridiche*
- *conserva e aggiorna l'elenco di tutti i soggetti muniti di NOS*

[101] https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/tutela-delle-informazioni/autorita-nazionale-per-la-sicurezza.html.

- *cura l'attività di negoziazione e predisposizione degli accordi di sicurezza con organizzazioni internazionali e Paesi esteri.*

Come ben sintetizzato nella specifica sezione del medesimo sito[102],

Il segreto di Stato è un vincolo posto dal Presidente del Consiglio dei ministri – mediante apposizione, opposizione, o conferma dell'opposizione – su atti, documenti, notizie, attività, cose e luoghi la cui conoscenza non autorizzata può danneggiare gravemente gli interessi fondamentali dello Stato.

Si tratta di un atto politico che può essere disposto esclusivamente dal Presidente del Consiglio dei ministri in quanto vertice del potere esecutivo.

La costruzione dell'istituto – concepito quale elemento di tenuta dell'intero sistema democratico – è volta da un lato, attraverso la previsione di limiti e garanzie, a circoscrivere e regolare l'utilizzo del segreto di Stato, dall'altro ad assicurarne l'effettività, limitando l'accesso alle notizie tutelate da questo vincolo a un numero estremamente ristretto di soggetti.

In tale quadro il legislatore ha disciplinato anche il rapporto tra segreto di Stato e processo penale, stabilendo che l'esistenza del segreto di Stato impedisce all'Autorità giudiziaria l'acquisizione e l'utilizzo, anche indiretto, delle notizie sottoposte al vincolo, fermo restando la possibilità per il giudice di ricorrere ad altri strumenti di prova, purché gli stessi non incidano sul medesimo oggetto.

Pertanto, il segreto di Stato:

- impedisce all'Autorità giudiziaria l'acquisizione e l'utilizzazione delle notizie sulle quali è apposto
- si differenzia dalle classifiche di segretezza, la cui attribuzione ha natura di atto amministrativo, che non sono opponibili all'Autorità giudiziaria
- Quanto ai limiti e alle garanzie, la legge 124/2007:
- esclude tassativamente che il segreto di Stato possa riguardare informazioni relative a fatti eversivi dell'ordine costituzionale o concernenti terrorismo, delitti di strage, associazione a delinquere di stampo mafioso, scambio elettorale di tipo politico-mafioso
- limita la durata del vincolo a 15 anni, ulteriormente prorogabili dal Presidente del Consiglio dei ministri per un periodo che non può complessivamente superare i 30 anni
- impone al Presidente del Consiglio dei ministri di comunicare i casi di conferma dell'opposizione del segreto di Stato al Comitato parlamentare per la sicurezza della Repubblica, indicandone le ragioni essenziali. Su richiesta del Presidente del COPASIR, il Presidente del Consiglio dei ministri è tenuto a esporre, in una seduta segreta, il quadro informativo idoneo a consentire l'esame nel merito della conferma dell'opposizione del segreto di Stato. Se ritiene infondata l'opposizione, il Comitato ne riferisce a ciascuna delle Camere per le conseguenti valutazioni,
- fa obbligo al Presidente del Consiglio dei ministri di motivare l'opposizione e la conferma dell'opposizione del segreto di Stato. Avverso tali atti può essere sollevato un

[102] https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/tutela-delle-informazioni/segreto-di-stato.html.

conflitto di attribuzione dinanzi alla Corte costituzionale, cui il segreto non può in alcun caso essere opposto.

- Infine, la legge 124/2007 dispone che, nel caso in cui l'opposizione del segreto di Stato determini un contrasto con l'Autorità giudiziaria, a decidere debba essere la Corte Costituzionale, organo nei cui confronti il segreto di Stato non può essere mai opposto.

La gestione delle informazioni riservate nel settore privato.

Per quanto attiene agli eventuali aspetti di competenza di infrastrutture critiche o comunque soggetti rilevanti ai fini della Direttiva NIS e NIS2 (in pratica gli Operatori di Servizio Essenziale e i Fornitori di Servizi Digitali, la norma di interesse il Decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 5, "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva", così come modificato dal decreto del Presidente del Consiglio dei ministri 2 ottobre 2017.

Tale provvedimento un vero e proprio "manuale di istruzioni" sulla gestione del segreto di stato e la tutela delle informazioni classificate e richiama specificatamente l'ambito cyber come possibile destinatario dell'adozione del regime della segretezza delle informazioni per i soggetti economici privati.

Infatti, a partire dall'art. Art. 7 "Ufficio centrale per la segretezza", esso:

f) definisce le misure di sicurezza cibernetica che devono essere adottate a protezione dei sistemi e delle infrastrutture informatiche che trattano informazioni classificate, a diffusione esclusiva o coperte da segreto di Stato; fornisce consulenza ai fini della realizzazione di reti di comunicazione telematica protette ai fini dell'attuazione del Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" in materia di sicurezza dello spazio cibernetico; promuove la realizzazione di reti di comunicazione telematica protetta con le organizzazioni di sicurezza pubbliche e private[103];

La parte che riguarda il settore delle imprese con obblighi in materia di riservatezza delle informazioni è trattata a partire dall'Art. 12 "Organizzazione di sicurezza nell'ambito degli operatori economici",

1. L'operatore economico abilitato alla trattazione delle informazioni classificate, (omissis), istituisce, previa autorizzazione dell'Organo nazionale di sicurezza o, se delegato, dell'UCSe, una propria organizzazione di sicurezza, secondo le previsioni di cui agli artt. 8, 9, 10 e 11, in relazione al livello di segretezza e alle qualifiche delle informazioni classificate che ha necessità di trattare, nonché alle proprie dimensioni o caratteristiche infrastrutturali o gestionali.

Il modello organizzativo aziendale per la gestione delle informazioni classificate.

[103] Lettera così modificata dall'art. 1, comma 8, DPCM 2 ottobre 2017, n. 3.

Esso è definito all'Art. 13 "Responsabilità della protezione e della tutela delle informazioni classificate e a diffusione esclusiva nell'ambito degli operatori economici":

- Presso ogni operatore economico abilitato alla loro trattazione, la responsabilità della protezione e della tutela delle informazioni classificate e a diffusione esclusiva, a livello centrale e periferico, fa capo al legale rappresentante in possesso di cittadinanza italiana.
- Il legale rappresentante dell'operatore economico può delegare l'esercizio dei compiti e delle funzioni per la protezione e tutela delle informazioni classificate ad un dirigente o funzionario legato da un rapporto professionale esclusivo, fatte salve specifiche esigenze organizzative e funzionali, in possesso di sola cittadinanza italiana, di abilitazione di livello adeguato ed esperto nel settore, che assume la denominazione di "Funzionario alla sicurezza".
- Presso le sedi periferiche dell'operatore economico abilitate per la trattazione di informazioni classificate il legale rappresentante di cui al comma 1 nomina un dirigente o funzionario dipendente in via esclusiva dall'operatore economico, quale "Funzionario alla sicurezza designato", in possesso di sola cittadinanza italiana e di abilitazione di livello adeguato. Il "Funzionario alla sicurezza designato" è alle dipendenze del "Funzionario alla sicurezza".
- Il legale rappresentante dell'operatore economico nomina, a livello centrale e presso ciascuna sede periferica abilitata alla trattazione di informazioni classificate, un sostituto "Funzionario alla sicurezza" e un sostituto "Funzionario alla sicurezza designato" in possesso dei requisiti indicati ai commi 2 e 3. Essi sostituiscono i titolari dell'incarico nei casi di assenza o impedimento.
- La nomina del "Funzionario alla sicurezza", del "Funzionario alla sicurezza designato" e di un sostituto di ciascuno di essi è soggetta alla preventiva approvazione dell'UCSe.

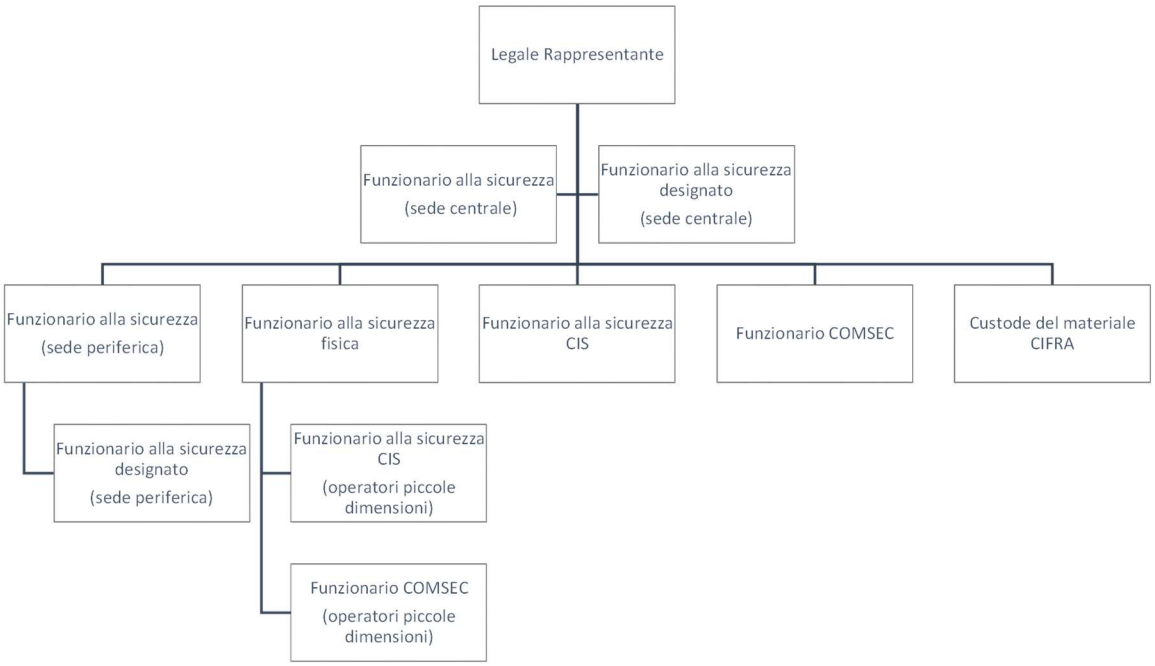


Tabella 25 - Il modello organizzativo aziendale per la gestione delle informazioni classificate (organizzazione aziendale)

Appare di tutta evidenza l'orientamento del sistema della sicurezza nazionale, che ha la responsabilità della tutela del segreto nazionale ma anche della tutela dell'apparato industriale strategico nazionale, di voler mantenere un doveroso regime di stretto controllo sullo stesso, anche attraverso questo strumento. L'imprescindibile previsione che il legale rappresentante e gli altri soggetti previsti nel modello organizzativo della tutela del segreto, siano di nazionalità italiana, ne è chiara evidenza.

Appare quindi evidentemente a ciò correlato quanto riportato nella Relazione al Parlamento 2021 dei Servizi Informazione e Sicurezza, circa le infrastrutture critiche nazionali[104]:

Con riferimento alle infrastrutture critiche nazionali, anche in ragione della ripresa del commercio internazionale che ha caratterizzato il 2021, i sedimi portuali hanno continuato ad attirare l'attenzione degli operatori di settore internazionali. In parallelo a una parziale riduzione delle proiezioni asiatiche sugli scali nazionali, che restano tuttavia rilevanti, si è registrato un forte attivismo degli operatori europei. In risposta a tale quadro – fenomenicamente positivo in quanto espressivo della capacità del nostro sistema infrastrutturale di attrarre investimenti stranieri – l'attenzione del Comparto si è focalizzata su possibili iniziative ostili provenienti da attori internazionali, che, pronti a sfruttare la propria posizione di oligopolio, ma anche lo stato di difficoltà dei player nazionali e talune debolezze strutturali del nostro sistema infrastrutturale, hanno condotto strategie di proiezione aggressive, sfociate in acquisizioni mirate di attività terminalistiche e logistiche, nonché di trasporto ferroviario e stradale.

Nel successivo art. 14, "Compiti del legale rappresentante o del Funzionario alla sicurezza dell'operatore economico", sono specificati i numerosi adempimenti:

---

104 https://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2021.html, pag.35.

1. Il legale rappresentante, o, se delegato, il Funzionario alla sicurezza dell'operatore economico:

ha l'obbligo di conoscere le disposizioni in materia di protezione e tutela delle informazioni classificate o coperte da segreto di Stato, e di farle puntualmente applicare;

a) adotta il Regolamento interno di sicurezza (RIS), che descrive le misure di sicurezza fisica, documentale, personale e industriale, predisposte per la protezione e tutela delle informazioni classificate, e lo invia all'UCSe, per la relativa approvazione, per il tramite dell'Organo centrale di sicurezza della Forza armata di riferimento;

b) segnala tempestivamente all'UCSe e all'ente appaltante o al committente ogni elemento suscettibile di valutazione ai fini di cui all'art. 37, 47 e 48, nonché eventuali casi di sospetta o accertata compromissione delle informazioni classificate;

c) dirige, coordina e controlla tutte le attività che riguardano la protezione e la tutela delle informazioni, dei documenti e dei materiali classificati o coperti da segreto di Stato, trattati nell'ambito dell'operatore economico, sia a livello centrale che periferico;

d) assicura il controllo delle lavorazioni classificate o coperte da segreto di Stato e la salvaguardia delle stesse dall'accesso di personale non in possesso di abilitazione di sicurezza di livello adeguato e, comunque, non autorizzato;

e) comunica semestralmente all'UCSe le lavorazioni classificate in corso di esecuzione secondo le modalità previste dalle direttive di attuazione;

f) comunica all'UCSe i contratti classificati di cui l'impresa è affidataria;

g) coordina i servizi di sorveglianza e controllo delle infrastrutture COMSEC e dei CIS[105];

h) cura gli adempimenti relativi al rilascio dei NOS al personale dell'operatore economico che ha necessità di trattare informazioni classificate a livello RISERVATISSIMO o superiore;

i) comunica all'UCSe ogni variazione riguardante la legale rappresentanza, i componenti del Consiglio di amministrazione, il direttore tecnico, l'Organizzazione di sicurezza e le relative preposizioni, nonché il possesso di quote di partecipazione qualificate in rapporto al capitale sociale ovvero di quote in relazione alle quali il titolare possa esercitare sull'impresa un'influenza notevole, ancorché non dominante;

i) comunica all'UCSe proposte di delibere di operazioni che comportano il trasferimento di informazioni classificate o a diffusione esclusiva, quali, tra l'altro: fusione, scissione, cessione, a qualsiasi titolo, di azienda o di ramo d'azienda, sottoscrizione di un contratto di rete, acquisizioni di partecipazioni che determinano la concentrazione del capitale sociale in capo ad un medesimo soggetto o il controllo dell'impresa attraverso l'esercizio di una influenza notevole, ancorché non dominante, ovvero distacco temporaneo di personale abilitato presso altro operatore economico o tra imprese che abbiano sottoscritto un contratto di rete;

l) istruisce il personale abilitato alla trattazione di informazioni classificate sulle disposizioni che regolano la materia;

m) comunica all'UCSe ogni evento che possa costituire minaccia alla sicurezza e alla tutela delle informazioni classificate;

m) nel caso di operatori economici di cui all'art. 11 del DPCM del 17 febbraio 2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali", comunica

[105] Vedi nota nr. 110.

al Nucleo per la sicurezza cibernetica, ai sensi dell'art.11, comma1, lett.a), dello stesso DPCM, ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti;

n) assicura la corretta osservanza delle procedure relative alle visite da parte di persone estranee all'operatore economico nei siti dove sono trattate informazioni classificate;

o) chiede l'autorizzazione prevista dalle norme vigenti e cura i relativi aspetti di sicurezza inerenti le trattative contrattuali che prevedono la cessione di informazioni classificate.

2. Per lo svolgimento dei compiti di cui al comma 1 la Scuola di formazione del Dipartimento delle informazioni per la sicurezza, d'intesa con l'Ufficio centrale per la segretezza, organizza appositi corsi in materia di protezione e tutela delle informazioni classificate, a diffusione esclusiva, o coperte da segreto di Stato. A tali corsi possono essere ammessi anche altri dirigenti o dipendenti dell'operatore economico.

Appare evidente come la materia del segreto sia strettamente legata a quella del cosiddetto "Golden power" soprattutto nella lettera delle lettere i) e i1) del sopraripportato art. 14[106].

Inoltre, la normativa in argomento mostra anche una specifica inerenza con la tematica della sicurezza informatica e degli obblighi degli operatori privati e delle infrastrutture critiche come richiamati alla lettera m1), che li evoca specificatamente con il riferimento all'art. 11 del DPCM del 17 febbraio 2017[107]. Appare opportuno evidenziare ancora una volta la spiccata contiguità tra i temi del segreto, della sicurezza informatica e delle infrastrutture critiche e la stretta collaborazione con gli apparati della sicurezza nazionale dei soggetti erogatori di servizio pubblico[108].

---

[106] Grazie al "*Golden Power*" l'esecutivo ha la facoltà di opporsi all'acquisto di determinate partecipazioni o comunque di dettare delle specifiche condizioni in merito, e può altresì apporre veti sull'adozione di particolari delibere aziendali. Nel DL. 15 marzo 2012 n. 21 è stata rivista e ridefinita la sezione dedicata ai poteri speciali del governo, esercitabili per salvaguardare gli assetti proprietari delle società operanti in settori strategici.

[107] Art. 11 del DPCM del 17 febbraio 2017 *"1. Gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, gli operatori di servizi essenziali e i fornitori di servizi digitali, di cui rispettivamente all'articolo 2, comma 1, lettere p) e q), quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici, ivi comprese quelle individuate ai sensi dell'articolo 1, comma1, lettera d), del decreto del Ministro dell'interno 9 gennaio 2008, secondo quanto previsto dalla normativa vigente, ovvero previa apposita convenzione:*

a) comunicano al Nucleo per la sicurezza cibernetica, anche per il tramite dei soggetti istituzionalmente competenti a ricevere le relative comunicazioni ai sensi dell'articolo16-bis, comma2, lettera b), del decreto legislativo n.259 del 2003, ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti;

b) adottano le best practices e le misure finalizzate all'obiettivo della sicurezza cibernetica, definite ai sensi dell'articolo 16-bis, comma 1, lettera a), del decreto legislativo n. 259 del 2003, e dell'articolo 5, comma 2, lettera d), del presente decreto;

c) forniscono informazioni agli organismi di informazione per la sicurezza e consentono ad essi l'accesso ai Security Operations Center aziendali e ad altri eventuali archivi informatici di specifico interesse ai fini della sicurezza cibernetica, di rispettiva pertinenza, nei casi previsti dalla legge n.124 del 2007, nel quadro delle vigenti procedure d'accesso coordinato definite dal DIS;

d) collaborano alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti."

[108] L'accesso da parte deli organismi per la sicurezza nazionale alle informazioni degli operatori privati di cui alla lettera c) dell'art. 11 del DPCM del 17 febbraio 2017, nonché la collaborazione richiamata alla lettera d) sono indubbiamente ricollegabili al disposto dell'art. 13 della Legge 3 agosto 2007, n. 124 "(Collaborazione richiesta a pubbliche amministrazioni e a soggetti erogatori di servizi di pubblica utilità):

Il successivo Art. 16 prosegue nella definizione dell'organigramma del modello organizzativo del segreto per gli operatori economici, prevedendo le ulteriori figure del "Funzionario alla sicurezza fisica":

Incarichi relativi a sicurezza fisica e COMSEC[109] e per la sicurezza dei CIS[110] presso gli operatori economici.

- Per l'esercizio delle sue funzioni, il Legale Rappresentante, ovvero il "Funzionario alla sicurezza" ove delegato, si avvale di un "Funzionario alla sicurezza fisica", come definito all'articolo 70.
- Fermo restando quanto stabilito dall'articolo 39, ove l'operatore economico abbia necessità di trattare informazioni classificate con sistemi CIS e COMSEC, il rappresentante legale nomina responsabili delle relative attività, denominati rispettivamente, "Funzionario alla sicurezza CIS", "Funzionario COMSEC", un "Custode del materiale CIFRA" ed i relativi sostituti, in possesso della sola cittadinanza italiana. In ragione delle dimensioni dell'operatore economico, e tenuto conto delle specifiche necessità relative alla trattazione delle informazioni classificate, gli incarichi di "Funzionario alla sicurezza CIS" e di "Funzionario COMSEC" possono essere assegnati alla stessa persona cui è conferito l'incarico di "Funzionario alla sicurezza".

1. Il DIS, l'AISE e l'AISI possono corrispondere con tutte le pubbliche amministrazioni e con i soggetti che erogano, in regime di autorizzazione, concessione o convenzione, servizi di pubblica utilità e chiedere ad essi la collaborazione, anche di ordine logistico, necessaria per l'adempimento delle loro funzioni istituzionali; a tale fine possono in particolare stipulare convenzioni con i predetti soggetti, nonché' con le università e con gli enti di ricerca.

2. Con apposito regolamento, adottato previa consultazione con le amministrazioni e i soggetti interessati, sono emanate le disposizioni necessarie ad assicurare l'accesso del DIS, dell'AISE e dell'AISI agli archivi informatici delle pubbliche amministrazioni e dei soggetti che erogano, in regime di autorizzazione, concessione o convenzione, servizi di pubblica utilità, prevedendo in ogni caso le modalità tecniche che consentano la verifica, anche successiva, dell'accesso a dati personali.

[109] DPCM 6 novembre 2015, n. 5, Art. 1, lett ii) *"COMSEC" (sicurezza delle comunicazioni), le misure di sicurezza crittografica, delle trasmissioni, fisica e del personale, finalizzate a garantire la protezione delle informazioni classificate o coperte da segreto di Stato, trattate attraverso sistemi di comunicazione, nonché ad impedirne la conoscenza da parte di soggetti non autorizzati. I materiali COMSEC comprendono i materiali crittografici in senso stretto (CIFRA) ed i materiali a controllo COMSEC (CCI– COMSEC Controlled Item), come disciplinato dall'articolo 53;*

[110] DPCM 6 novembre 2015, n. 5, Art. 1, lett ll) *"Communication and Information System" (o "CIS") è il complesso di apparati, aree ad accesso riservato, personale abilitato, hardware, software e procedure operative, finalizzato all'elaborazione, memorizzazione e trasmissione di informazioni classificate o coperte da segreto di Stato, attraverso sistemi informatici.*

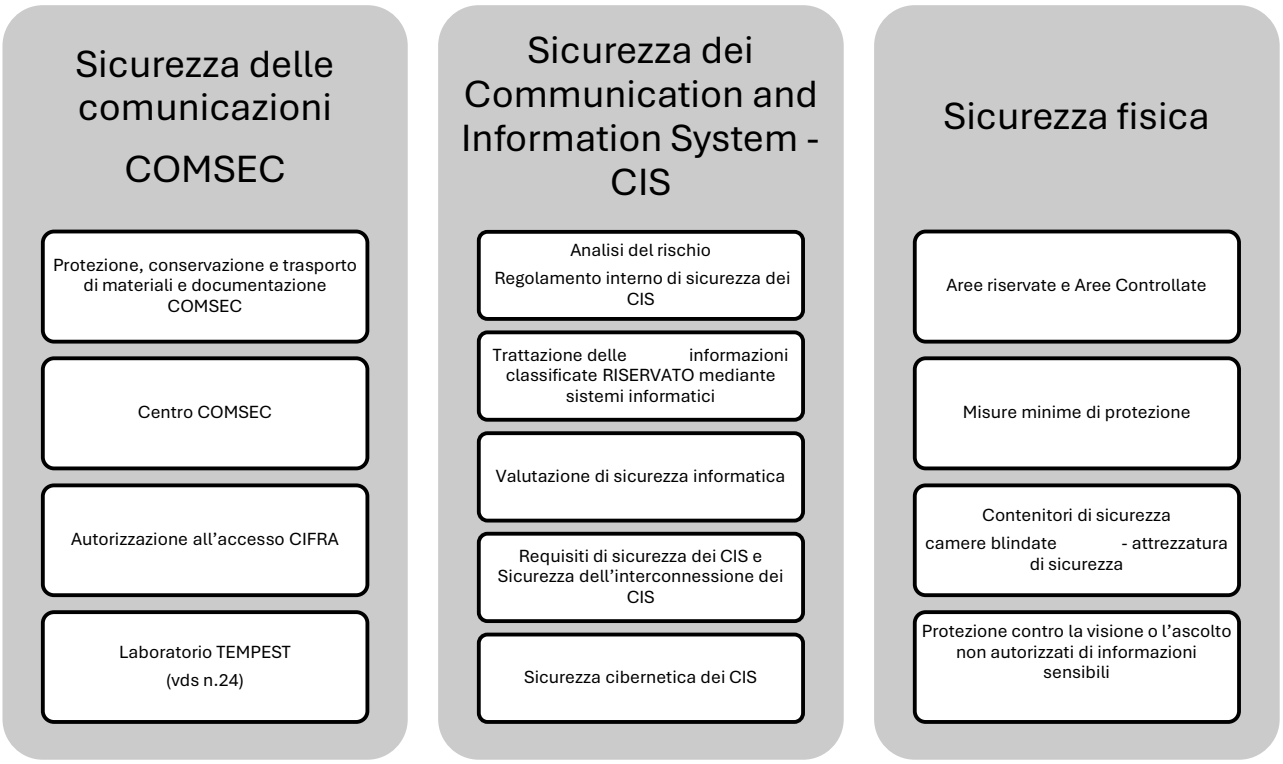


Tabella 26: Il modello organizzativo aziendale per la gestione delle informazioni classificate per le principali aree di responsabilità e compiti delle funzioni aziendali[111].

Un regime semplificato è previsto per le aziende che debbano trattare esclusivamente materiale classificato RISERVATO, in quanto la normativa in argomento, all'art. 38 consente la possibilità di prescindere dall'adozione di un modello organizzativo come sopra esposto, prevedendo solo una delega da parte del legale rappresentante a chi a la necessità di accedere a tale documentazione, previa necessaria formazione circa le responsabilità per la divulgazione delle informazioni, pur prescrivendo specifiche disposizioni circa la conservazione (area controllata) ed il divieto di trasmissione per via informatica o telematica (quindi anche via e-mail) consentendo esclusivamente la trasmissione postale tracciabile (ad esempio raccomandata R/R) ovvero l'utilizzo di corriere (vettore commerciale) o il trasporto a mano[112].

Di particolare interesse per le società che gestiscono infrastrutture critiche, l'art. 40 che istituisce il Nulla Osta di Sicurezza Industriale Strategico (NOSIS), rilasciato, a richiesta degli operatori o d'ufficio da una Amministrazione pubblica agli operatori economici la cui attività, per oggetto, tipologia o caratteristiche, assume rilevanza strategica per la protezione degli interessi politici, militari, economici, scientifici e industriali nazionali, tenuto conto appunto del contenuto del D.Lgs. 11 aprile 2011, n. 61 "Attuazione della Direttiva 2008/114/CE recante

[111] DPCM 6 novembre 2015, n. 5, Art. 1, lett. nn) *""TEMPEST", le tecnologie atte ad eliminare, o ridurre entro valori non pericolosi ai fini della sicurezza, le emissioni prodotte dalle apparecchiature elettroniche che elaborano e trattano informazioni classificate o coperte da segreto di Stato"*.

[112] Art. 38, co. 6.:*"La trasmissione di informazioni classificate RISERVATO non è consentita con sistemi elettrici o elettronici non autorizzati dall'UCSe; è consentita la trasmissione postale che consenta la tracciabilità, ovvero mediante vettori commerciali o trasporto a mano, secondo le disposizioni applicative del presente regolamento".*

l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione", che all'art. 3 prevede:

Tutela delle informazioni sensibili

1. Alle informazioni sensibili relative alle Infrastrutture Critiche, nonché ai dati ed alle notizie relativi al processo d'individuazione, di designazione e di protezione delle ICE, è attribuita adeguata classifica di segretezza ai sensi dell'articolo 42 della legge 3 agosto 2007, n. 124, e relative disposizioni attuative.

Ai fini del predetto NOSIS,

Rientrano in tale ambito, in particolare:

a) le attività volte ad assicurare la difesa e la sicurezza dello Stato;

b) le attività volte alla produzione o allo sviluppo di tecnologie suscettibili di impiego civile/militare;

c) le attività connesse alla gestione delle infrastrutture critiche anche informatiche e di interesse europeo;

d) la gestione di reti, di infrastrutture e di sistemi di ricetrasmissione ed elaborazione di segnali e/o comunicazioni;

e) la gestione di reti e infrastrutture stradali, ferroviarie, marittime ed aeree;

f) la gestione di reti e sistemi di produzione, distribuzione e stoccaggio di energia ed altre infrastrutture critiche;

g) la gestione di attività finanziarie, creditizie ed assicurative di rilevanza nazionale.

Appare opportuno sottolineare che tale autorizzazione all'accesso a informazioni classificate che, come abbiamo visto, riguardano specificatamente le infrastrutture critiche, prevede l'adozione del modello organizzativo precedentemente delineato, oltre che i noti requisiti soggettivi imprescindibili:

3. *Il NOSIS è rilasciato all'esito di accertamenti diretti ad escludere dalla conoscibilità di notizie, documenti, atti o cose classificati e a diffusione esclusiva i soggetti che non diano sicuro affidamento di scrupolosa fedeltà alle istituzioni della Repubblica, alla Costituzione e ai suoi valori, nonché di rigoroso rispetto del segreto. Per il rilascio del NOSIS si applicano le disposizioni dell'articolo 44 e dell'articolo 45, per quanto compatibili. Ai fini del rilascio del NOSIS l'operatore economico deve dotarsi di un'area riservata con le caratteristiche di cui al Capo VIII, di omologazione CIS e, ove necessario, COMSEC, nonché delle certificazioni che saranno, a regime, rilasciate ai sensi dell'art.11, comma2, del Decreto del Presidente del Consiglio dei Ministri del 17 febbraio 2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali".*

Conclusioni

La stretta inerenza geopolitica della normativa in argomento, che vede quindi il dominio cyber quale nuovo dominio di difesa nazionale, (oltre a terra, aria, mare e da ultimo spazio), è perfettamente riconoscibile nelle cause che possono portare taluno ad essere privato delle clearance di segretezza sia come persona fisica che come persona giuridica, come chiaramente esposto nell'art. 37 del DPCM 6 novembre 2015, n. 5:

- Quando nei confronti della persona interessata emergono elementi, acquisiti o verificati ai sensi dell'articolo 27, che influiscono negativamente sulla sua affidabilità in termini di scrupolosa fedeltà alle Istituzioni della Repubblica, alla Costituzione e ai suoi valori, nonché di rigoroso rispetto del segreto e delle norme finalizzate alla tutela delle informazioni, dei documenti e dei materiali classificati, l'abilitazione è negata, revocata, sospesa, ridotta di livello di segretezza, di qualifica di sicurezza e dequalificata ovvero limitata territorialmente o temporalmente, secondo quanto previsto nei commi successivi.

E nel successivo art. 47:

- per le società di capitali, quando sul conto dei titolari, diretti o indiretti, anche stranieri, di quote di partecipazione che, in rapporto al capitale sociale dell'impresa, avuto anche riguardo alle circostanze di fatto e di diritto, conferiscano la possibilità di esercitare sull'impresa stessa un'influenza notevole, ancorché non dominante, emerga taluno degli elementi indicati all'art.37.

Allegato 4: Gestione degli incidenti: aspetti tecnologici in ambito OT/IoT (A. Testi / F. Rosa)

Abstract

Aspetti tecnologici (misure tecnologiche di prevenzione, detection, log e allarmi, investigazione dell'incidente) rilevanti nella gestione degli incidenti di Cybersecurity nella NIS 2, partendo da quelle previste all'Art. 21 e dal Considerato 89 (C89):

- Stato dell'arte e best practice, standard: aspetti tecnologici in ambito OT / IOT
- Vigilanza ed esecuzione in ambito OT / IoT: le nuove linee guida NIST
- Utilizzo di applicazioni AI-based per la prevenzione, predizione e gestione degli incidenti Cyber
- Caso d'uso su adozione di un processo di security

Gestione degli incidenti secondo la Direttiva NIS 2

L'articolo 21 della normativa, "Misure di gestione dei rischi di cyber sicurezza", rappresenta un importante passo avanti nella protezione della sicurezza delle reti e dei sistemi informativi per le organizzazioni nell'Unione Europea, dato che gli obblighi di mitigazione dei rischi stabiliti in esso sono più specifici e rigorosi rispetto a quelli previsti dalla NIS originale. Tuttavia, è importante notare che la sua attuazione può essere impresa complessa e impegnativa per i soggetti obbligati: essi dovranno infatti investire risorse significative per valutare e gestire i rischi e implementare le relative misure di sicurezza predisponendosi inoltre a collaborare con le Agenzie Nazionali di Sicurezza Cibernetica (ANSC).

Richiamiamo infatti qui di seguito la lista che comprende le categorie previste dalle misure indicate come minime per attuare una corretta gestione dei rischi e una minimizzazione degli impatti degli incidenti informatici:

- analisi dei rischi e di sicurezza dei sistemi informatici;
- gestione degli incidenti;
- continuità operativa;
- sicurezza della catena di approvvigionamento (supply chain security);
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete (third party security e secure development operations – SecDevOps);
- strategie e procedure per valutare l'efficacia delle misure;
- igiene informatica di base e formazione in materia di cyber sicurezza;
- procedure relative all'uso di crittografia e cifratura;
- sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
- autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Come appare subito evidente, rendere sicura e resiliente un'organizzazione moderna, dotata di infrastrutture informatiche multi-dominio, e di una molteplicità di fornitori fortemente connessi, comporta sempre di più una visione olistica ed integrata di tutte le sue componenti, perché le debolezze di una di esse può portare alla compromissione delle altre.

Con l'estensione, ad opera della NIS 2, degli ambiti di applicazione della direttiva a tutti i soggetti Essenziali e Importanti, questo concetto diventa di importanza cruciale e, visti i settori operativi critici definiti negli allegati 1 e 2 (Energia, Trasporti, Banche, Sanità, Servizi ICT, Pubbliche Amministrazioni, Spazio solo per il primo), lo scenario sarà per la maggior parte di tipo industriale, tenendo conto che l'infrastruttura IT è una componente oramai di base per tutte le organizzazioni.

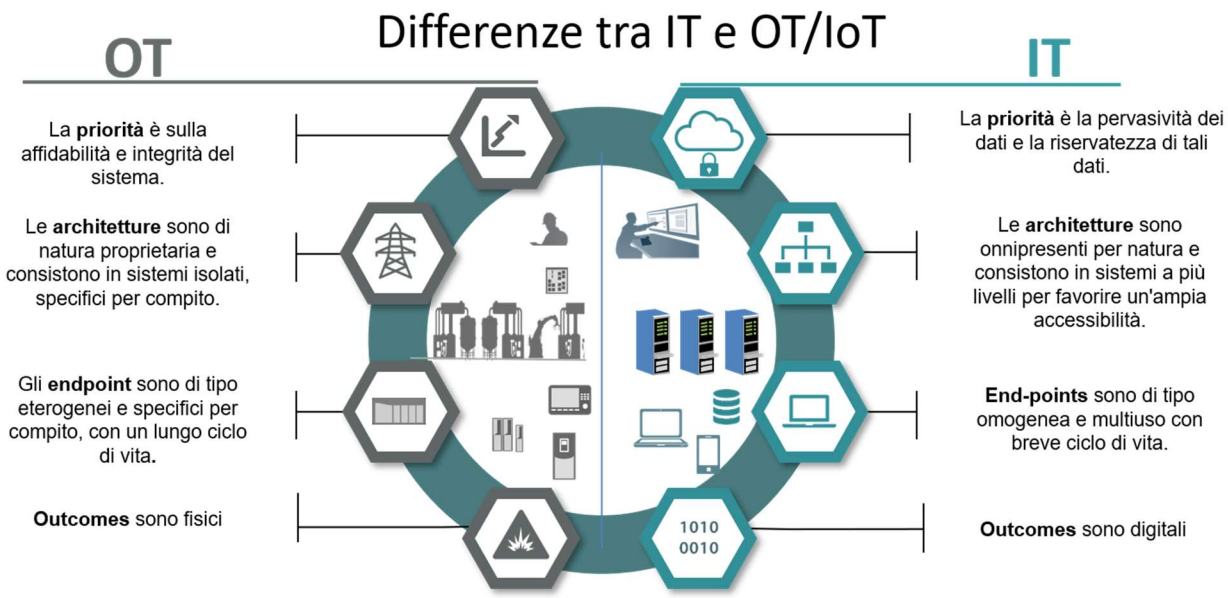
Obiettivo dei prossimi paragrafi, allora, è una disamina dei principi generali che regolano l'analisi dei rischi e la successiva gestione degli incidenti proiettate negli ambiti della Operational Technology (OT) e dell'Internet of Things (IoT e IIoT), che sono propri dei soggetti essenziali e importanti.

I concetti e le metodologie descritti, comunque, possono nella quasi totalità dei casi, essere applicati a qualsiasi organizzazione ed entità dotata di sistemi di produzione industriali, di qualsiasi dimensione.

Analisi del rischio in ambito OT

Come ampiamente provato, la valutazione del rischio informatico aiuta a determinare strutturalmente quali rischi informatici sono presenti nel vostro ambiente. Solo dopo aver identificato esplicitamente questi rischi, è possibile comprendere l'efficacia delle contromisure (esistenti). Questo a sua volta permette di ragionare su nuove contromisure, sulla loro eventuale necessità e sulla loro possibile efficacia. Inoltre, la valutazione della gravità dei rischi identificati consente di decidere e dare priorità alle contromisure e di decidere con cognizione di causa se i costi della loro implementazione sono in grado di compensare le potenziali conseguenze.

A differenza degli ambienti IT, i rischi in ambito OT non riguardano solo la riservatezza, l'integrità e la disponibilità dei dati o dei processi (RID), ma possono anche avere un impatto sull'affidabilità, le prestazioni e la sicurezza fisica delle strutture. Inoltre, i diversi tipi di sistemi di controllo industriale (ICS), come i PLC, i DCS e i sistemi SCADA, richiedono un'attenzione particolare in quanto costituiscono la spina dorsale di qualsiasi ambiente OT.



Per valutare correttamente i rischi e proporre contromisure in tali ambienti, è necessario prendere in considerazione queste differenze, analizzandole in modo dettagliato:

Focus

IT	OT
La sicurezza delle tecnologie dell'informazione (IT) ruota attorno alla salvaguardia delle risorse digitali, con particolare attenzione ai sistemi e ai dati. Si tratta di computer, server, reti, archiviazione dati e applicazioni. L'obiettivo è proteggere la riservatezza, l'integrità e la disponibilità delle informazioni digitali.	La sicurezza della tecnologia operativa (OT), invece, ha lo sguardo rivolto al regno fisico. Si occupa di salvaguardare i sistemi e i dati che gestiscono e monitorano dispositivi e processi tangibili. I sistemi di controllo industriale (ICS), i sistemi di controllo di supervisione e acquisizione dati (SCADA) e i sistemi embedded rientrano in questo ambito.

Asset Progetti

IT	OT
La sicurezza informatica protegge una serie di beni, dall'infrastruttura digitale alle applicazioni software. Si tratta di computer, server, data center, reti, servizi cloud, database e dei dati sensibili in essi contenuti.	La sicurezza OT è la protezione di macchinari, attrezzature industriali e infrastrutture critiche. Si concentra su beni quali apparecchiature di produzione, reti elettriche, sistemi di trasporto, sistemi HVAC e qualsiasi tecnologia che interagisca direttamente con l'ambiente fisico.

Panoramica delle Minacce

IT	OT
Il panorama delle minacce alla sicurezza informatica è prevalentemente digitale. Le minacce comprendono malware (virus, worm, ransomware), attacchi di phishing, attacchi denial-of-service e violazioni di dati. Queste minacce mirano al furto di dati, all'interruzione del sistema e alla compromissione delle risorse digitali.	La sicurezza OT deve affrontare un più ampio spettro di minacce: oltre a malware e attacchi digitali, esistono minacce fisiche come l'accesso non autorizzato ai siti industriali, il sabotaggio, la manomissione delle apparecchiature e le conseguenze dei disastri naturali. Spesso l'obiettivo non è solo la compromissione dei dati, ma anche danni fisici, danni ambientali o interruzioni del servizio.

Impatto di un Incidente

IT	OT
Nella sicurezza informatica, le conseguenze di una violazione si manifestano in genere con perdite finanziarie, danni alla reputazione e potenziali responsabilità legali. Le violazioni possono portare a furti di dati, furti di identità, frodi finanziarie e interruzioni di servizio.	Le ripercussioni di una violazione della sicurezza OT possono essere gravi e di vasta portata. Oltre alle ramificazioni finanziarie e ai danni alla reputazione, un attacco ai sistemi OT può causare interruzioni alle infrastrutture critiche, danni fisici alle persone e disastri ambientali. Si pensi alle interruzioni di corrente, alle interruzioni dei trasporti o persino agli incidenti negli impianti di produzione.

La comprensione di queste differenze è importante perché sottolinea le sfide uniche che le organizzazioni devono affrontare per salvaguardare la loro tecnologia operativa. Come più volte sottolineato, mentre la sicurezza IT si concentra sul dominio virtuale, la valutazione del rischio OT si confronta con il mondo fisico, tangibile e spesso insostituibile, rendendo le sue sfide e conseguenze peculiari ed eccezionalmente critiche.

La scelta della metodologia di calcolo del rischio cyber in ambito OT dipende da diversi fattori, come la complessità dei sistemi OT, le risorse disponibili e le specificità aziendali. È importante quindi utilizzare un approccio olistico che tenga conto di tutti questi fattori, al fine di ottenere una valutazione il più precisa possibile. Le principali attività da svolgere sono quindi:

- In maniera analoga alle infrastrutture IT, identificare i sistemi OT più critici per l'azienda e valutare gli impatti in caso di interruzione della loro operatività.
- Identificare le minacce e le vulnerabilità a cui sono esposti i sistemi OT.
- Valutare l'efficacia dei controlli di sicurezza in atto per mitigare il rischio.
- Valutare l'impatto potenziale di un incidente informatico in termini di interruzione del servizio, perdita di dati, danni finanziari e danni alla reputazione.

Analogamente a quanto accade per le “convenzionali” infrastrutture IT, Le metodologie di calcolo del rischio cyber in ambito OT (Operational Technology) mirano a stimare la probabilità e l'impatto di un incidente informatico sui sistemi industriali; per attuare tali stime, esistono diverse metodologie, ognuna con i suoi vantaggi e svantaggi:

Analisi Qualitativa del Rischio (RRA)

- Si basa su un'analisi qualitativa dei sistemi OT per identificare le minacce, le vulnerabilità e gli impatti potenziali.
- Non fornisce una valutazione numerica del rischio, ma è utile per ottenere una panoramica generale e per identificare le priorità di intervento.
- Esempi di metodi RRA sono STRIDE (Microsoft) o OCTAVE Allegro (Carnegie Mellon University)

Analisi Quantitativa del Rischio (QRA)

- Assegna valori numerici alle probabilità e agli impatti delle minacce per ottenere una valutazione complessiva del rischio.
- Permette di confrontare diversi rischi e di ottimizzare le risorse per la sicurezza.
- Richiede dati precisi e aggiornati, che possono essere difficili da ottenere in ambito OT.
- Esempi di metodi QRA sono FAIR (Factor Analysis of Information Risk) o LORA (Loss Event Rate Analysis)

Esistono poi alcuni standard e linee guida molto conosciuti ed importanti che forniscono metodologie per la valutazione del rischio cyber in ambito IT e ora anche OT. Tra tutte, citiamo le seguenti:

- ISO/IEC 27001
- NIST Cybersecurity Framework
- ISA/IEC 62443

La normativa ISO 27001 è uno dei capisaldi nella gestione del rischio, e fornisce un framework per la gestione e il controllo dei rischi per la sicurezza delle informazioni in qualsiasi tipo di organizzazione. Consideriamola come già conosciuta e lasciamo al lettore eventuali approfondimenti esterni.

Affrontando il comparto industriale, invece, faremo da adesso riferimento al framework NIST e alla normativa IEC 62443: mentre il primo fornisce un quadro flessibile con raccomandazioni volontarie alle organizzazioni per migliorare la loro posizione di sicurezza informatica e aiuta a identificare, proteggere, rilevare, rispondere e recuperare dagli attacchi informatici, la seconda definisce una serie di requisiti e specifiche per la sicurezza informatica dei sistemi di controllo

di automazione industriale (IACS – Industrial Automation Control System, anche abbreviati in ICS), con l'obiettivo di stabilire un livello minimo di sicurezza. Viene spesso utilizzata come standard di conformità anche per le organizzazioni che si occupano di infrastrutture critiche.

Un metodo che le infrastrutture industriali possono quindi adottare per dotarsi di processi e procedure di cyber sicurezza, è quello di seguire il NIST CSF come punto di partenza per una strategia globale, e successivamente implementare controlli e raccomandazioni specifiche della norma IEC 62443 per il proprio ambiente ICS. Analizziamo con maggiore dettaglio questi standard.

Il framework NIST

Il NIST Cybersecurity Framework (CSF) fornisce un insieme di best practice per la gestione del rischio cyber applicabile a tutte le organizzazioni del settore privato che possono valutare e migliorare la loro capacità di prevenire, rilevare e rispondere agli attacchi informatici anche in ambito OT. I concetti principali del NIST Cybersecurity Framework includono:

Core framework

Il Core Framework è un insieme di attività, risultati e indicazioni applicabili a tutti i settori delle infrastrutture critiche. Fornisce un approccio strutturato per la gestione dei rischi di cybersecurity. Esso è composto da cinque funzioni di alto livello:

- Identificare (Identify)
- Proteggere (Protect)
- Rilevare (Detect)
- Reagire (Respond)
- Recuperare (Recover)

Ogni funzione è ulteriormente suddivisa in categorie e sottocategorie che rappresentano risultati specifici di cybersecurity.

Livelli di implementazione

I livelli descrivono il grado con cui le pratiche di gestione del rischio di cybersecurity di un'organizzazione presentano le caratteristiche definite nel Framework (ad esempio, consapevolezza del rischio e delle minacce, ripetibilità e adattamento). I valori previsti sono (1-4): parziale, informato sul rischio, ripetibile, adattivo. Questi livelli guidano le organizzazioni ad allineare le loro attività di cybersecurity con i requisiti aziendali, la tolleranza al rischio e le risorse.

Framework Profile

Il meccanismo del Framework per descrivere la postura di cybersecurity attuale e desiderata di un'organizzazione, e quindi le sue opportunità di miglioramento è definito Framework Profile. I profili vengono utilizzati per comprendere, valutare, dare priorità e adattare i risultati del CSF Core (cioè Funzioni, Categorie e Sottocategorie) in base agli obiettivi dell'organizzazione, alle aspettative degli stakeholder e alle minacce.

Vengono quindi considerati due tipi di profili: un Current Profile, anche detto "as is", ossia i risultati del CSF Core che un'organizzazione sta attualmente raggiungendo (o cercando di

raggiungere) e caratterizza come o in che misura ciascun risultato viene raggiunto, e un Target Profile cioè il "to be", che comprende i risultati desiderati selezionati e resi prioritari dal Core per raggiungere i propri obiettivi di gestione del rischio di cybersecurity.

L'utilizzo dei profili può essere molto vario:

- Confronto delle pratiche di cybersecurity con gli standard e i requisiti normativi.
- Documentazione dei riferimenti informativi e delle pratiche.
- Definizione degli obiettivi di cybersecurity dell'organizzazione.
- Definizione le priorità dei risultati di cybersecurity.
- Valutazione dei progressi ottenuti verso gli obiettivi.
- Identificazione delle lacune o vulnerabilità rispetto a minacce emergenti.
- Comunicazione e presentazione delle capacità di cybersecurity verso clienti.
- Espressione dei requisiti e delle aspettative di cybersecurity verso fornitori e partner.

Come emerge chiaramente da questa breve descrizione, il NIST Cybersecurity Framework rappresenta uno strumento estremamente pratico e completo, che permette ad organizzazioni diverse di "parlare la stessa lingua" ed utilizzare gli stessi standard di riferimento in materia di sicurezza informatica.

Focalizziamoci ora sulle attività che il framework indica come parte del processo di gestione del rischio, ed analizziamo come possiamo introdurre alcune attività con riferimento specifico per il mondo industriale:

Identificazione

- Identificare gli asset critici e le loro dipendenze.
- Comprendere le minacce e le vulnerabilità specifiche dell'ambiente OT.

Protezione

- Implementare controlli di sicurezza adeguati per proteggere i sistemi da intrusioni, malware e altre minacce.
- Proteggere i dati sensibili e l'accesso ai sistemi.

Rilevamento

- Monitorare i sistemi per attività sospette e intrusioni.
- Sviluppare capacità di rilevamento di minacce specifiche per l'ambiente OT.

Risposta

- Disporre di un piano di risposta agli incidenti informatici che includa procedure specifiche per l'ambiente OT.
- Ripristinare i sistemi e i dati in modo sicuro dopo un incidente.

Recupero

- Implementare un piano di ripristino che consenta di ripristinare rapidamente i sistemi in caso di incidente.
- Testare regolarmente il piano di ripristino per garantirne l'efficacia.

Per questo ambito vanno, come detto all'inizio del capitolo, tenute di conto le seguenti considerazioni:

- L'ambiente OT è spesso caratterizzato da sistemi legacy con limitate capacità di sicurezza.
- I sistemi OT sono spesso interconnessi con i sistemi IT, creando nuove vulnerabilità.
- Le interruzioni ai sistemi OT possono avere gravi conseguenze per la sicurezza e la salute pubblica.

Per questo motivo, il NIST CSF fornisce una serie di guide e risorse specifiche per l'OT, tra cui la "Special Publication (SP) 800-82, Guide to Operational Technology (OT) Security" e la "Special Publication (SP) 800-53 Revision 4, Security Controls for Federal Information Systems and Organizations".

Lo standard IEC 62443

La serie di norme ISA/IEC 62443 definisce i requisiti e i processi per l'implementazione e la manutenzione di sistemi di automazione e controllo industriale (IACS o ICS), per garantire che essi siano sicuri da un punto di vista globale, secondo un insieme di requisiti e termini comuni che vengano utilizzati da tutti gli attori identificati nell'interazione con tali sistemi:

- Asset owner: utilizzatori e manutentori
- Service provider: utilizzatori e manutentori
- System integrator: progettisti, integratori ed installatori
- Fornitori di prodotti (Supplier): sviluppatori e produttori

Questo approccio, quindi, introduce un concetto di protezione olistica dei sistemi industriali, prevedendo la sicurezza in termini di persone, tecnologia e processi:

Per coprire tutti gli ambiti e le fasi che riguardano i sistemi industriali (progettazione, produzione, installazione, esercizio, manutenzione, ecc.), lo standard è composto da quattro

gruppi principali ai quali sono attribuiti i diversi ambiti: generale, politiche e procedure, sistema e componente come indicato nella figura che segue.

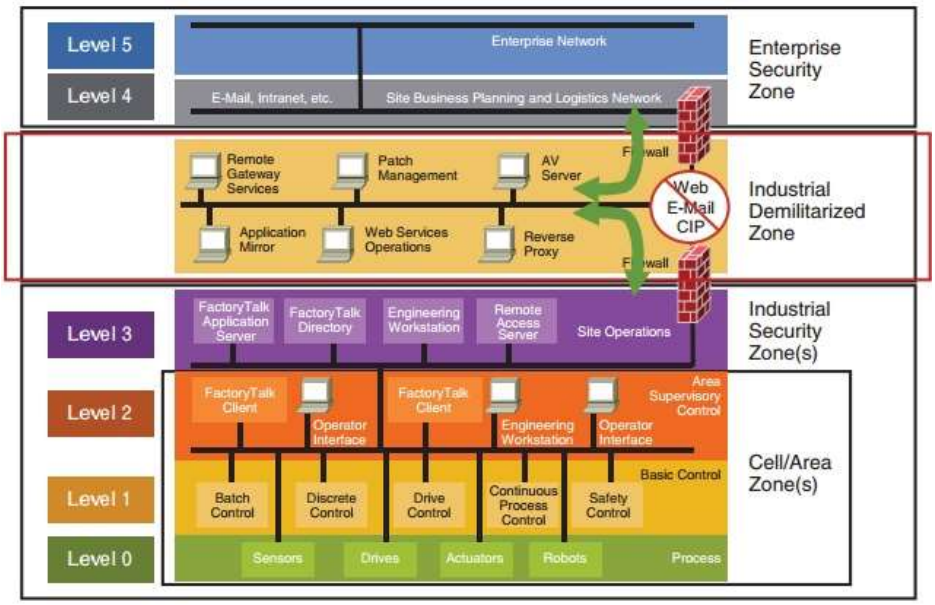
Le parti più rilevanti di ciascuno di essi sono:

- Parte 1-1: Introduce i concetti e i modelli utilizzati in tutto lo schema. Il destinatario è chiunque desideri acquisire familiarità con i concetti fondamentali che costituiscono la base di questi standard.
- Parte 2-1: La definizione di un programma di sicurezza per i sistemi di controllo descrive ciò che è necessario per definire e implementare un efficace sistema di gestione della sicurezza informatica. I destinatari sono gli end user che hanno la responsabilità della progettazione e dell'attuazione di tale programma.
- Parte 3-2: Affronta il Cyber Security Risk Assessment e la progettazione del sistema. Il risultato di questi processi è una valutazione del rischio su livelli di sicurezza, documentati nella specifica dei requisiti di cyber security. Questo standard è rivolto principalmente a end user e system integrator
- Parte 3-3: Descrive i requisiti per un IACS in base al suo livello di sicurezza. Si rivolge ai fabbricanti di componenti e sistemi, system integrator e end user.
- Parte 4-1: Descrive i requisiti del ciclo di vita dello sviluppo della sicurezza (Cyber Security Lifecycle) del fabbricante, al quale la parte 4-1 si rivolge.
- Parte 4-2: Descrive i requisiti per i componenti IACS in base al loro livello di sicurezza. I componenti IACS includono embedded devices, host devices, network devices e applicazioni software. Questa parte si rivolge ai costruttori di componenti IACS.

Lo standard definisce quindi le migliori pratiche per la cyber sicurezza e fornisce anche un metodo per valutarne i livelli di prestazioni. L'approccio alla sfida della cybersecurity è, come detto, olistico, e colma il divario tra Operational Technology e Information Technology, nonché quello tra sicurezza dei processi e sicurezza cyber. Esso stabilisce i parametri di riferimento in

tutti i settori industriali, tra cui l'automazione degli edifici, la generazione e la distribuzione di energia elettrica, i dispositivi medici, i trasporti e le industrie di processo come quelle chimiche e del petrolio e del gas; nasce quindi per proteggere l'Industria moderna, rendendo sicura ed affidabile la condivisione di dati dall'interno verso l'esterno e viceversa.

Per questo, uno dei cardini dello standard è costituito dall'utilizzo di un modello logico dei livelli in cui una moderna organizzazione industriale deve essere suddivisa, ed è il modello Purdue, un modello di riferimento per l'architettura aziendale degli anni '90, che prevede una segmentazione della rete a supporto della sicurezza degli Industrial Control System:



Il modello suddivide le operazioni di supporto industriale in tre aree principali (le cosiddette Zone):

- Zona aziendale (livelli 4 e 5): controllata dall'IT, include data center aziendali e hosting di applicazioni.
- Zona demilitarizzata industriale (IDMZ): funziona come strato di mezzo tra sistemi di produzione critici e la rete aziendale.
- Zona di sicurezza industriale (livelli 0-3): Contiene sistemi operativi critici con comunicazione frequente e a bassa latenza.

Anche se sta andando incontro ad aggiornamenti ed evoluzioni soprattutto alla luce delle nuove sfide e minacce che emergono con l'evoluzione delle tecnologie, il modello ha portato indubbiamente dei vantaggi nella gestione e nella sicurezza delle organizzazioni industriali:

- Segmentazione delle reti:
    - Il modello fornisce una struttura chiara per la segmentazione delle reti, riducendo il rischio che le minacce possano propagarsi facilmente da un livello all'altro.
- Isolamento delle funzioni critiche:

    - Esso aiuta a isolare le funzioni critiche di controllo industriale dalle reti IT, che sono più frequentemente bersagliate da attacchi informatici.
- Chiarezza organizzativa:
    - Offre una chiara divisione delle responsabilità e delle risorse, facilitando la gestione della sicurezza e la conformità normativa.

E proprio il concetto di responsabilità condivisa, uno dei principi fondanti dello standard IEC 62443 ad essere elemento essenziale della sicurezza informatica dell'automazione: tutti i soggetti coinvolti nella gestione di un'organizzazione industriale, quali i proprietari degli asset (utenti finali), i fornitori di apparati per l'automazione, gli integratori che costruiscono e manutengono le soluzioni e i loro componenti e i fornitori dei sistemi, devono concordare una linea comune per garantire sicurezza, integrità, affidabilità e protezione dei sistemi di controllo. Tutto questo significa che le persone, i processi e la tecnologia svolgono insieme un ruolo critico nella sicurezza di tali sistemi, arrivando così alla visione olistica rappresentata dalla triade presentata ad inizio paragrafo.

Da un punto di vista più pratico, le linee guida che compongono le norme riguardano le seguenti principali attività:

- Definire termini, concetti e modelli comuni che possono essere utilizzati da tutte le parti interessate responsabili della sicurezza informatica dei sistemi di controllo.
- Aiutare i responsabili degli asset a determinare il livello di sicurezza necessario per soddisfare le proprie esigenze di business e di rischio.
- Stabilire un insieme comune di requisiti e una metodologia del ciclo di vita della cybersecurity per gli sviluppatori di prodotti, compreso un meccanismo di certificazione dei prodotti e dei processi di sviluppo dei fornitori.
- Definire i processi di valutazione del rischio che sono fondamentali per proteggere i sistemi di controllo.

In questo scenario, occorre allora definire alcuni concetti vicini a quello di IACS:

- IACS Security Lifecycle: è il ciclo di vita della sicurezza, ossia l'insieme delle fasi che è necessario percorrere affinché la protezione degli IACS sia conforme con quanto stabilito dallo standard IEC. Le fasi del ciclo di vita della sicurezza di uno IACS sono:

Ogni fase è composta da alcune attività correlate:

- Asssess
- Risk Assessment
- Vulnerability Assessment
- Penetration Test
- Threat Modeling
- Security Level Allocation
- Implement
- Defence Strategy
- CSMS
- Security Level verification
- Maintain
- Auditing
- Follow up

CSMS: è il Cyber Security Management System, ossia il Sistema di Gestione della Sicurezza Informatica che rappresenta l'insieme delle pratiche e delle azioni mirate a identificare i rischi informatici e definire la strategia di contrasto. Esso è costituito da sei elementi principali:

- Avvio del programma CSMS (per fornire le informazioni necessarie a ottenere il supporto della direzione).
- Valutazione del rischio di alto livello (prioritizzazione dei rischi).
- Valutazione dettagliata del rischio (valutazione tecnica dettagliata delle vulnerabilità).
- Stabilire politiche di sicurezza, organizzazione e awareness.
- Selezionare e implementare le contromisure (riduzione del rischio).
- Manutenzione del CSMS (per garantire che esso rimanga efficace e supporti gli obiettivi dell'organizzazione).

Non è obiettivo di questo capitolo descrivere l'implementazione delle linee guida e raccomandazioni dello standard, ed è difficile semplificare un corpus di informazioni così ampio. Raccomandiamo quindi alle aziende che intendano seguirne le indicazioni di rivolgersi a partner ed esperti certificati per intraprendere il proprio viaggio nella IEC 62443.

Nel paragrafo conclusivo del capitolo verrà esaminato, come caso d'uso, un reale processo di accompagnamento alle certificazioni IEC 62443 di processo e prodotto che è possibile conseguire.

Concludiamo questo argomento osservando che anche a prescindere delle possibilità di certificazione, i proprietari di asset dovrebbero comunque considerare l'implementazione olistica dello standard IEC 62443, perché esso riunisce aspetti importanti ampiamente discussi e verificati da una comunità globale di esperti in materia.

La gestione degli incidenti

Dopo l'esame della fase di analisi del rischio, occupiamoci ora di quella altrettanto importante della gestione degli incidenti. Anche per questa materia, torniamo a considerare gli standard e le pubblicazioni del NIST come linee guida di riferimento per l'attuazione delle misure imposte dalla NIS 2, ed esaminiamo più in dettaglio la pubblicazione 800-61 che descrive ed organizza la gestione di un incidente di sicurezza informatica: essa definisce quattro fasi del ciclo di vita della risposta agli incidenti, così come mostrato in figura:

Preparazione

Consente a un'organizzazione e al suo team di risposta agli incidenti di prepararsi alla gestione degli incidenti (e, se possibile, di ridurre la probabilità che si verifichi un incidente). Le attività principali sono:

- Sviluppare policy, procedure e un piano di risposta agli incidenti
- Creare un team di risposta agli incidenti
- Identificare e acquisire gli strumenti e le attrezzature necessarie
- Fornire formazione e sensibilizzazione
- Sviluppare un piano di comunicazione
- Stabilire metriche e monitoraggio ed esercitazioni

Rilevamento e analisi

Questa fase fornisce un approccio strutturato per la gestione degli incidenti, prevedendo l'identificazione e l'analisi di potenziali incidenti di sicurezza o anomalie nei sistemi, reti o dispositivi dell'organizzazione. Le principali attività sono:

- Monitorare costantemente i sistemi, le reti e i dispositivi per potenziali incidenti di sicurezza o anomalie utilizzando vari strumenti e tecniche, come:
    - Analisi del traffico di rete

    - Analisi dei registri di sistema
    - Sistemi di rilevamento di intrusioni (IDS)
    - Sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM)
- Identificare potenziali incidenti di sicurezza o anomalie sulla base dei dati di monitoraggio, come:
    - Pattern di traffico di rete insoliti
    - Registri di sistema sospetti
    - Allarmi attivati dai sistemi IDS o SIEM

Prioritizzare gli incidenti identificati sulla base del loro impatto potenziale, severità e probabilità di causare danni all'organizzazione.

- Condurre un'analisi approfondita dell'incidente identificato per determinare la sua causa radice, portata e impatto potenziale, compresi:
    - Recensione dei registri di sistema e dei captures di traffico di rete
    - Analisi delle configurazioni e impostazioni dei sistemi
    - Interviste con i dipendenti coinvolti
    - Utilizzo di strumenti di analisi forense per analizzare il malware o altri codici malevoli
- Classificare l'incidente sulla base della sua severità, impatto e probabilità di causare danni all'organizzazione, utilizzando un sistema standardizzato (che il framework stesso fornisce).

- Segnalare l'incidente al team di risposta agli incidenti, compresi i dettagli rilevanti come:
    - Classificazione dell'incidente
    - Descrizione dell'incidente
    - Impatto potenziale
    - Causa radice
    - Portata

- Gli obiettivi principali di questa fase sono
    - Ridurre il tempo necessario per rilevare e rispondere agli incidenti
    - Migliorare efficacia ed efficienza della risposta
    - Ridurre il rischio di ulteriori eventi

Contenimento, eliminazione e ripristino

E’ il periodo fondamentale in cui il team di risposta agli incidenti cerca di contenere l'incidente e, se necessario, di ripristinare i sistemi (le risorse, i dati e/o i processi interessati). In questa fase (in cui è critica la velocità di azione) le attività sono per la maggior parte tecniche e svolte da personale specializzato sui sistemi impattati dall’incidente:

- Contenimento:
    - isolare il sistema o la rete colpiti per evitare ulteriori danni o la diffusione dell'incidente;
    - scollegare l'alimentazione o le connessioni di rete al sistema o alla rete colpiti;
    - implementare i controlli di accesso per impedire l'accesso non autorizzato al sistema o alla rete interessati;
    - monitorare il sistema o la rete colpiti per individuare ulteriori segni di compromissione.
- Eliminazione:
    - eliminare la causa principale dell'incidente, come il malware o una vulnerabilità;
    - applicare le patch alle vulnerabilità del software o del firmware;
    - riconfigurare le impostazioni di sistema o le configurazioni di rete per evitare incidenti futuri;
    - ripristino delle configurazioni di sistema o di rete a uno stato noto come buono.
- Ripristino:
    - ripristinare il sistema o la rete colpiti in uno stato noto e buono;
    - assicurarsi che il sistema o la rete siano sicuri e funzionino correttamente;
    - verificare che tutti i sistemi o le reti interessati siano completamente ripristinati e funzionino come previsto.

Gli obiettivi principali di questa fase sono

- prevenire ulteriori danni o la diffusione dell'incidente;
- garantire che l'incidente sia completamente risolto

Attività post-incidente

Questa (ultima) fase si concentra sul completamento del processo di risposta all'incidente e sulla garanzia che l'organizzazione sia preparata a rispondere ad analoghi eventi futuri. Le attività principali in questa fase sono:

- Lesson learned:
    - I team di incident response devono dare priorità all'apprendimento e al miglioramento dopo ogni incidente; ciò comporta l'organizzazione di una riunione di "lesson learned" con tutte le parti coinvolte per esaminare ciò che è accaduto, ciò che è stato fatto per intervenire e quanto ha funzionato. La riunione aiuta a chiudere l'incidente, identificare le aree di miglioramento delle misure di sicurezza, riflettere sulle nuove minacce e su eventuali miglioramenti tecnologici, e migliorare la risposta agli incidenti nel tempo.

    - Il consiglio è di organizzare questa riunione entro alcuni (pochi) giorni dalla fine dell'incidente, ed eventualmente di trattare più incidenti in un'unica riunione, se possibile. Questo può portare ad indentificare migliorie o caratteristiche generali da tenere in considerazione.

- Utilizzo dei dati relativi all'incidente.

  Le attività lessons learned devono raccogliere dati oggettivi e soggettivi su ogni incidente. Questi dati possono essere utilizzati per:

    - giustificare investimenti aggiuntivi sul team di incident response;
    - identificare le debolezze e le minacce sistemiche alla sicurezza;
    - aggiornare il processo di risk assessment e l'eventuale adozione di controlli aggiuntivi;
    - misurare la performance del team di incident response;
    - stimare l'impatto di modifiche alle funzioni di incident response sulle prestazioni del team;

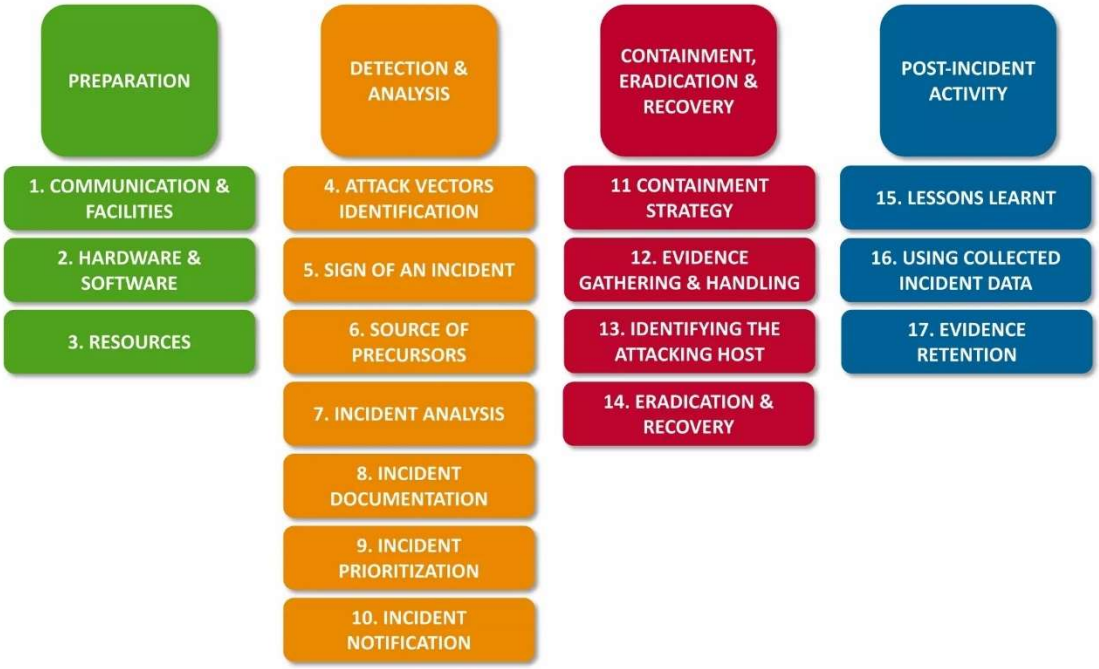
I dati archiviati verranno analizzati per fornire informazioni sulle tendenze degli incidenti, sulle prestazioni del team e sull'efficacia delle capacità di risposta agli incidenti. Una notevole importanza risiede nella scelta dei dati collezionati: essi devono essere soprattutto utilizzabili per le valutazioni. Possibili esempi di metriche utili sono:

- Numero di incidenti gestiti
- Tempo occorrente per la gestione di un incidente
- Valutazione oggettiva e soggettiva di ciascun incidente

Oltre a utilizzare le metriche per misurare le performance del team, è anche possibile verificare periodicamente i programmi di risposta agli incidenti, individuando eventuali problemi e carenze e correggendoli.

- Retention delle evidenze:
    - Le organizzazioni devono stabilire una politica per la durata della conservazione delle prove di un incidente, considerando i fattori legale (durata della causa verso l'attaccante), le regole di data retention generali (p. es. le email di tutto il personale vengono mantenute per 6 mesi, ma quelle relative ad un incidente potrebbero essere necessarie per anni) ed infine il costo degli asset (PC, dischi, ecc.) che costituiscono prova.

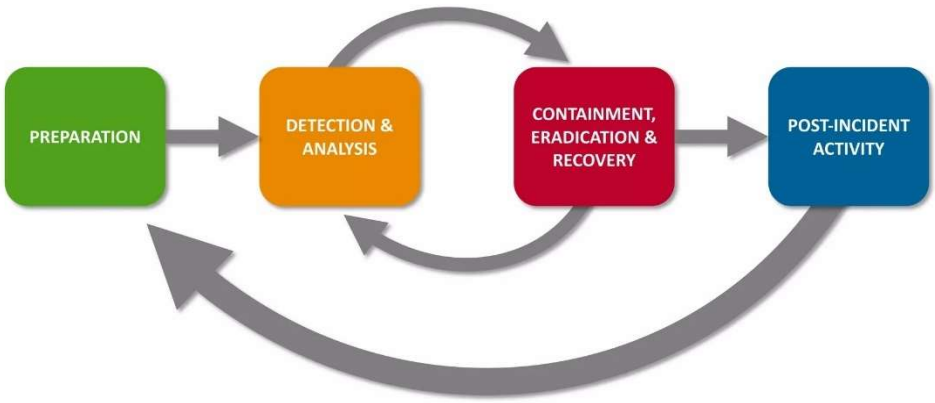
Le fasi appena presentate possono essere quindi scomposte nelle sotto-attività descritte ed eseguite in sequenza o contemporaneamente per garantire all'organizzazione (industriale o meno) di essere protetta, preparata alla risposta ed in continuo miglioramento verso le minacce cyber che la possono colpire. Le sotto-attività sono quindi riportate nella figura seguente:



Molto spesso, la pratica comune tende a limitare la gestione degli incidenti alle fasi 2 e 3. È qui, infatti, che si svolge la maggior parte delle attività "visibili". Ad esempio, raramente, capita di osservare la squadra di incident response lavorare sulla preparazione per un intervento. In effetti, però, tutte e quattro le fasi del ciclo sono ugualmente importanti.

Esiste infatti più di una correlazione tra di esse, e non sono semplicemente lineari. Secondo il NIST, infatti:

- il risultato della fase "Attività post-incidente" è un input per la fase "Preparazione";
- i risultati della fase "Contenimento, eliminazione e recupero" sono un input per la fase "Rilevamento e analisi".



È quindi molto importante smettere di pensare alla gestione degli incidenti come una semplice sequenza temporale di attività; altro esempio, il team di incident response dovrebbe avere una procedura operativa standard che correli la fase di rilevamento e analisi con i risultati della fase

di contenimento; anche se ciò può sembrare non intuitivo, (la seconda viene dopo la prima). Procedure operative analoghe dovrebbero essere previste anche per:

- dedicare tempo (dopo la chiusura di ogni incidente) all'analisi di ogni aspetto di quell'incidente, comprese le procedure utilizzate in ogni fase della risposta;
- alimentare la fase di preparazione con i risultati dell'analisi post-incidente.

Come già è apparso chiaro nello svolgimento dell'intero capitolo, le fasi della gestione degli incidenti cyber non è realmente diversa tra ambito IT e OT; ciò che differenzia questi due "mondi" sono le implicazioni che gli incidenti portano (ricordiamo che in Operational Technology abbiamo a che fare alla fine con dispositivi fisici potenzialmente dannosi anche per l'uomo o per i servizi di cui l'uomo usufruisce) e gli strumenti e piattaforme tecnologiche disponibili per garantire la sicurezza delle organizzazioni, sia come prevenzione che come risposta.

Misure tecnologiche di prevenzione e rilevamento

Analizziamo quindi come un perimetro industriale possa essere messo in sicurezza, fornendo un panorama delle soluzioni tecniche attualmente disponibili sul mercato ed elencando le principali caratteristiche di ognuna di esse.

Per prima cosa, da un punto di vista tecnologico, introduciamo le attività da considerare fondamentali per una corretta postura di sicurezza. Gli ambiti e le funzioni critici su cui un'organizzazione industriale deve porre grande attenzione sono:

- Endpoint security (per i sistemi che supportano agent)
- Segmentazione della rete (garanzia di isolamento)
- Accesso remoto sicuro (controllo delle connessioni in entrata)
- Controllo degli accessi basato su ruoli (controllo dei privilegi degli utenti remoti)
- Visibilità della rete OT (molti sistemi industriali non supportano agent)
- Centralizzazione dei servizi di security

Come già descritto in precedenza nel capitolo, i dispositivi OT/IoT/SCADA/ICS fanno spesso uso di tecnologie abbastanza datate, hanno software/firmware scritti in linguaggi proprietari o fortemente personalizzati, e sono quindi poco adatti ad ospitare agenti software quali gli EDR, antivirus, ecc. Sarà quindi molto importante sorvegliare costantemente le comunicazioni che essi scambiano con gli altri dispositivi di pari livello o superiore, in modo che sia garantita la rilevazione di anomalie nei dati che essi ricevono o producono.

Ad esempio, verificare costantemente che i comandi forniti ad una turbina di una centrale elettrica come ad un dispositivo elettromedicale siano sempre nei range operativi e non siano discordanti con quelli del normale funzionamento in quel contesto, può essere un modo molto efficace di contrastare eventuali manomissioni remote da postazioni che cerchino di interrompere o modificare l'operatività di questi dispositivi.

E’ quindi molto importante la visibilità delle comunicazioni di rete con dispositivi di network monitoring, di intrusion detection & prevention (NIDS / IPS)

Tornando quindi alle attività fondamentali della sicurezza (OT), viene qui presentata una tabella di strumenti che possono essere utilizzati per “mappare” ciascuna di esse:

Fase	Strumento
Risk Management	SIEM, Log Analyzer
Asset management	SIEM, NAC, Firewall, NIDS
Access control	Firewall, NAC, Token, IAM, Client authentication
Network Segmentation	Firewall, Switch, AP, XDR
Logging & Monitoring	SIEM, SOAR, Log Analyzer, Sandbox, Honeypot, NIDS

Nei paragrafi che seguono, analizziamo con più dettaglio le caratteristiche di alcuni degli apparati e piattaforme più importanti per un’organizzazione industriale.

Network Access Control (NAC)

Un dispositivo NAC è una soluzione hardware o software che controlla e gestisce l'accesso a una rete, garantendo che solo i dispositivi e gli utenti autorizzati possano connettersi ad essa. Essi forniscono un ambiente sicuro e controllato per l'accesso alla rete, garantendo al tempo stesso la conformità ai requisiti normativi e alle politiche organizzative.

Il NAC può anche fornire protezione agli endpoint, come software antivirus, firewall e valutazione delle vulnerabilità con criteri di applicazione della sicurezza e metodi di autenticazione del sistema.

I principali benefici dell’utilizzo di un NAC sono:

- Controllo degli utenti che accedono alla rete aziendale
- Controllo di accesso alle applicazioni e alle risorse a cui gli utenti vogliono accedere
- Consentire l’accesso di fornitori, partner e ospiti secondo necessità e privilegi.
- Segmentare i dipendenti in gruppi basati sulle loro funzioni lavorative sui ruoli.
- Proteggere dagli attacchi utilizzando sistemi e controlli che rilevino attività insolite o sospette.
- Automatizzare la risposta agli incidenti.
- Generare report e statistiche sui tentativi di accesso per tutta l'organizzazione

Firewall di nuova generazione (NGFW)

Il Firewall di Prossima Generazione (NGFW) è un tipo di firewall che fornisce funzionalità e capacità di sicurezza avanzate al di là dei firewall tradizionali. Gli NGFW sono progettati per proteggere contro minacce moderne, come malware, ransomware e minacce persistenti avanzate (APTs), utilizzando tecnologie avanzate come il controllo delle applicazioni, la prevenzione delle intrusioni e la sandboxing.

SIEM e SOAR e EDR

I sistemi SIEM di nuova generazione (Next-Gen Security Information and Event Management) rappresentano un'evoluzione nel campo della cybersecurity, incorporando tecnologie e metodologie avanzate per migliorare la rilevazione, la risposta e la gestione delle minacce alla sicurezza. Le principali caratteristiche di sistemi sono:

- Rilevamento Avanzato delle Minacce
    - Machine Learning e AI: Utilizzo di algoritmi di machine learning e intelligenza artificiale per rilevare anomalie e schemi indicativi di minacce sofisticate.
    - Analisi Comportamentale: il comportamento degli utenti e delle entità che si connettono alla rete vengono analizzate per identificare deviazioni dai modelli normali, con la possibilità di rilevare minacce interne o account compromessi.
- Elaborazione Dati Avanzata e Scalabilità
    - Architettura Big Data: Costruiti su architetture scalabili di big data che possono gestire grandi volumi di dati da varie fonti in tempo reale.
    - Integrazione con il Cloud: Supporta l'integrazione con ambienti cloud, fornendo flessibilità e scalabilità per gestire i dati attraverso infrastrutture ibride.
- Monitoraggio e Risposta in real-time
    - Analisi in Tempo Reale: Offre elaborazione dei dati e analisi in tempo reale per identificare e rispondere rapidamente alle minacce emergenti.
    - Automated Response: Incorpora l'automazione per la risposta agli incidenti, consentendo un contenimento e una mitigazione rapidi delle minacce senza intervento umano.
- Integrazione dei Dati
    - Ampia Gamma di Fonti di Dati: Capace di ingerire dati da un'ampia gamma di fonti, inclusi dispositivi di rete, endpoint, applicazioni e servizi cloud.
    - Consapevolezza Contestuale: Fornisce contesto correlando i dati da varie fonti, migliorando l'accuratezza e la rilevanza degli avvisi.
- Interfacce Intuitive e Reporting
    - Dashboard Intuitive: Presenta dashboard user-friendly che offrono visualizzazioni chiare degli eventi di sicurezza e delle metriche.
    - Report Personalizzabili: Consente la creazione di report personalizzabili che soddisfano le esigenze specifiche dei diversi stakeholder all'interno dell'organizzazione.
- Integrazione della Threat Intelligence
    - Feed di Threat Intelligence: si integra con feed esterni di threat intelligence per rimanere aggiornati sulle minacce emergenti e sulle vulnerabilità.
    - Threat Hunting: supporta la threat hunting proattiva da parte degli analisti di sicurezza, sfruttando capacità di ricerca avanzate e dati di intelligence.

- Compliance e Governance
    - Conformità Regolamentare: aiuta le organizzazioni a soddisfare i requisiti normativi e di conformità fornendo capacità complete di registrazione, audit e reporting.
    - Gestione delle Politiche: facilita la gestione e l'applicazione delle politiche di sicurezza in tutta l'organizzazione.
- Gestione degli Incidenti e Collaborazione
    - Gestione degli Incidenti: fornisce strumenti integrati per la gestione degli incidenti per tracciare, gestire e risolvere gli incidenti di sicurezza.
    - Strumenti di Collaborazione: include funzionalità di collaborazione che consentono ai team di sicurezza di comunicare e coordinare efficacemente i loro sforzi.
- Integrazione con Altri Strumenti di Sicurezza
    - Integrazione SOAR: si integra con le piattaforme di Security Orchestration, Automation, and Response (SOAR) per migliorare le capacità di risposta agli incidenti.
    - Integrazione con EDR/XDR: lavora senza problemi con soluzioni EDR per fornire visibilità e protezione complete degli endpoint.
- Analisi Avanzata e funzionalità forensi
    - Analisi Avanzata: utilizza analisi predittive e altre tecniche avanzate per anticipare potenziali incidenti di sicurezza.
    - Funzionalità di Forensics: fornisce robusti strumenti forensi per l'investigazione approfondita degli incidenti di sicurezza, aiutando a comprendere la causa principale e l'impatto.
- Opzioni di Distribuzione Flessibili
    - On-Premises, Cloud e Ibrido: offre opzioni di distribuzione flessibili, inclusi modelli on-premises, basati su cloud e ibridi, per soddisfare le diverse esigenze organizzative e infrastrutturali.
    - Servizi Gestiti: alcune soluzioni SIEM di nuova generazione forniscono servizi gestiti, offrendo gestione e monitoraggio esperti del sistema SIEM.
- User and Entity Behavior Analytics (UEBA)
    - Integrazione UEBA: si integra con strumenti UEBA per migliorare la rilevazione delle minacce interne e degli account compromessi attraverso l'analisi del comportamento.

Incorporando queste caratteristiche, i sistemi SIEM di nuova generazione forniscono un approccio più completo, efficiente ed efficace alla cybersecurity, aiutando le organizzazioni a rilevare, rispondere e gestire meglio le minacce alla sicurezza in un panorama digitale sempre più complesso.

Piattaforme di Intrusion e Anomaly Detection

Esaminiamo ora le piattaforme di intrusion detection (IDS) o di anomaly detection (AD) per le reti OT e come esse aiutino ad affrontare le sfide legate alla visibilità della situazione attraverso l'identificazione degli asset, dei flussi di traffico, delle vulnerabilità e dei rischi e aiutino nelle attività di monitoraggio continuo e di risposta agli incidenti.

Come detto, a causa della convergenza tra IT e OT, le reti OT/ICS o di controllo della produzione mancano di visibilità in termini di ciò che è connesso alla rete e di come il traffico fluisce tra gli asset. L'aumento di complessità delle industrie dovuto alle necessità di maggiore efficienza, produttività e requisiti di connettività (IIoT), ha reso il panorama ancora più complesso. Fino a pochi anni fa, esistevano poche soluzioni al problema, con capacità limitate di interpretare i protocolli industriali e di rilevare le anomalie, e con la necessità di competenze avanzate.

Dopo un primo periodo basato su strumenti dedicati a specifici vendor o con funzionalità puntuali e limitate, si è assistito a una crescita accelerata in termini di maturità di tali soluzioni, di ampliamento della copertura dei protocolli OT, di maggiore accuratezza nel rilevamento di asset, vulnerabilità e anomalie/minacce e di altre funzionalità aggiunte (ad esempio, visibilità dei dispositivi IoT, IIoT ed altri). Queste soluzioni sono ora disponibili in diverse forme, come hardware on-premise, su software o containerizzate in apparati di rete e gestite tramite portali come Software-as-a-Service (SaaS).

Esistono diversi metodi per l'analisi degli asset e del traffico di rete che possono essere utilizzati dalle soluzioni OT IDS e AD, tra cui quello passivo, attivo e mediante file di configurazione. Ognuno di questi metodi ha caratteristiche e vantaggi unici e può essere utilizzato da solo o in combinazione, a seconda degli obiettivi specifici definiti:

- Il rilevamento PASSIVO (tramite sonda) non è intrusivo, è facile da configurare ed è in tempo reale.
- Le sonde ATTIVE interrogano i dispositivi nel perimetro e sono particolarmente adatte a rilevare dettagli (p. es. sui dispositivi Windows) che non si trovano con il metodo passivo.
- L'analisi dei dispositivi presenti tramite scansione dei file di configurazione permette ricostruire un inventario degli asset e delle loro caratteristiche.
- L'utilizzo di API permette di interrogare l'infrastruttura e rilevare i dispositivi connessi.

Le soluzioni IDS possono sfruttare una combinazione di analisi statistica, apprendimento automatico e tecniche di intelligenza artificiale (AI) per migliorare le capacità di rilevamento e di allarme.

Volendo adottare una piattaforma IDS/AD per ambito industriale, esistono diversi prerequisiti importanti da considerare, i più importanti dei quali sono:

- Disporre del supporto della Direzione aziendale (assegnazione di fondi e risorse)
- Effettuare una verifica completa per i siti produttivi che devono far parte del perimetro di installazione e la loro conseguente preparazione.
- L'ambito di monitoraggio deve essere definito nel dettaglio (ad esempio, DMZ OT, linee di produzione, magazzino, gestione degli edifici, laboratori, ecc.).
- Collaborazione e coordinamento in termini di risorse identificate con obiettivi chiari di responsabilità, assegnazione, consultazione ed informazione (RACI) e la preparazione di una struttura di supporto tra i team IT/OT.

- Supporto da parte di produttori, system integrator e/o fornitori che gestiscono/operano/supportano la produzione e le strutture di rete associate.
- Gestione dei dati raccolti, della loro sicurezza e della privacy.

Da un punto di vista pratico, invece, riportiamo qui di seguito un elenco di alto livello dei criteri di valutazione e selezione delle soluzioni:

- **Funzionalità:** allineamento con le variabili ambientali specifiche dell'utente finale OT/IoT (architettura di rete, protocolli OT utilizzati e relativo supporto, elementi minori).
- **Precisione e prestazioni:** identificazione corretta degli asset, capacità di creare baseline e mappatura delle reti (flussi di traffico tra zone/conduits e anomaly detection).
- **Fonti di dati e copertura:** capacità di ricezione dati da fonti IT/OT/IoT/IIoT e copertura dei vari protocolli.
- **Metodi e tecniche:** sonde passive e attive, parsing delle configurazioni, altro.
- Scalabilità e integrazione: facilità di scalare verso l'alto/il basso e integrazione con lo stack tecnologico IT/OT esistente.
- **Allarmi, report e dashboard:** scostamenti dalle baseline, avvisi di sicurezza o operativi, reportistica di risk management, report e dashboard locali/globali personalizzabili, ecc.
- **Supporto e manutenzione:** assistenza tecnica, frequenza degli aggiornamenti, documentazione, formazione, ecc.
- **Costi e ritorno sull'investimento (ROI):** costi diretti e indiretti di hardware, licenze, abbonamenti, manutenzione annuale e servizi (ad es. implementazione, messa a punto, manutenzione per risorse esterne/interne).
- **Mappatura con standard industriali:** ISA/IEC 62443, NIST CSF, CSC20 o il framework MITRE ATT&CK.

Come possiamo vedere, queste caratteristiche sono sovrapponibili a quelle di un SIEM di nuova generazione come descritto in un paragrafo precedente. Si giunge quindi alla conclusione che le capacità fondamentali dei sistemi di monitoraggio di infrastrutture OT non si discostano tanto da quelle tradizionali dedicate al mondo IT. Esisteranno sicuramente delle specificità tecniche, che però non modificano i paradigmi di funzionamento e le best practice di cybersecurity comuni. E' per questo che alla base del processo di implementazione degli strumenti di sicurezza OT occorre che sia stato ben progettato ed eseguito il passo base di analisi e gestione del rischio, in questo caso calato nel mondo industriale.

Applicazioni AI-based

I security team odierni devono affrontare sfide sempre più difficili, hacker sofisticati, una superficie di attacco in continua espansione al pari dell'esplosione nelle quantità di dati, e una crescente complessità delle infrastrutture, che ostacolano la loro capacità di rispondere agli incidenti, di gestire l'accesso degli utenti e di rilevare e rispondere rapidamente anche alle minacce alla sicurezza dell'intelligenza artificiale.

Alcune delle maggiori aziende di cyber security forniscono oggi soluzioni basate sull'intelligenza artificiale che ottimizzano il tempo degli analisti, accelerando la detection e la mitigazione delle minacce, accelerando le risposte e proteggendo identità e dati degli utenti, mantenendo i team di cybersecurity sempre nel controllo delle operazioni.

Gli strumenti di rilevamento delle anomalie basati su IA sono progettati per identificare modelli o comportamenti insoliti nei dati che non sono conformi a policy o norme determinate. Questi strumenti utilizzano algoritmi di apprendimento automatico e modelli statistici per analizzare grandi insiemi di dati e rilevare anomalie che possono indicare potenziali minacce alla sicurezza, frodi o altri tipi di attività insolite. L'utilizzo della IA nelle applicazioni dedicate alla cyber security, porta quindi con sé una serie di vantaggi potenziali:

- **Maggiore precisione:** i sistemi basati sull'intelligenza artificiale possono analizzare grandi quantità di dati e identificare schemi e anomalie che potrebbero non essere rilevabili dagli analisti umani.
- **Maggiore velocità:** l'intelligenza artificiale è in grado di elaborare i dati molto più velocemente degli esseri umani, consentendo di rilevare e rispondere alle minacce in tempo reale.
- **Riduzione dei falsi positivi:** l'intelligenza artificiale è in grado di ridurre il numero di falsi positivi, che possono rappresentare un problema importante nei metodi tradizionali di rilevamento della cyber security.
- **Rilevamento avanzato delle minacce:** l'intelligenza artificiale può rilevare minacce che potrebbero non essere conosciute o riconosciute dai metodi di rilevamento tradizionali, come ad esempio lo sfruttamento di zero-day o email di phishing.
- **Miglioramento della risposta agli incidenti:** l'intelligenza artificiale può aiutare chi risponde agli incidenti fornendo approfondimenti e raccomandazioni in tempo reale per la risposta e la bonifica.
- **Caccia alle minacce automatizzata:** l'intelligenza artificiale può automatizzare il processo di ricerca delle minacce, consentendo ai team di sicurezza di concentrarsi su attività di livello superiore.
- **Riduzione dei costi:** l'intelligenza artificiale può ridurre i costi della cyber security automatizzando molte attività e riducendo la necessità (ma non azzerandola!) di analisti umani.

In definitiva, l'utilizzo di motori e moduli di IA nelle soluzioni di monitoraggio e anomaly detection porterà sempre più verso l'automazione di alcuni processi e attività, ma tutto dovrà sempre essere configurato, supervisionato e ottimizzato da un team composto da esseri umani, che rimarranno sempre le figure più importanti del controllo di sicurezza dell'organizzazione.

Ipotesi di realizzazione di un processo di sicurezza ed un perimetro sicuro

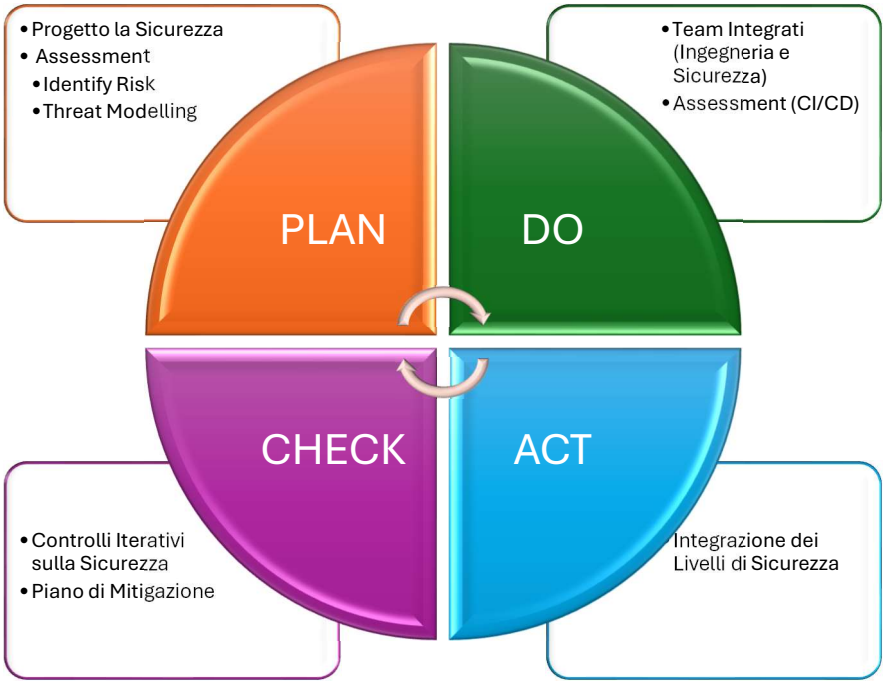
La soluzione più ottimale per fare fronte ai requisiti dettati dalla NIS 2 sia in caso di produzione che nel caso di utilizzatore, è quella di adottare uno standard specifico legato allo scope dell'azienda/industria.

Nell'ambito della produzione industriale di dispositivi OT, come già sopra descritto, la scelta è direzionata verso lo standard ISA/IEC 62443 che riesce a coprire gli aspetti di gestione del

processo di sviluppo (ISA/IEC 62443-4-1) e di gestione della produzione di apparati (ISA/IEC 62443-4-2).

Fatti questi preamboli l'ipotesi di realizzazione di processo di sicurezza ed un perimetro sicuro all'interno di una organizzazione che produce dispositivi industriali dovrà interagire con differenti reparti che si integreranno in un flusso di lavoro unico.

L'idea alla base è quella dell'impiego del classico ciclo di Deming integrato con il ciclo di vita applicato al processo di sviluppo.

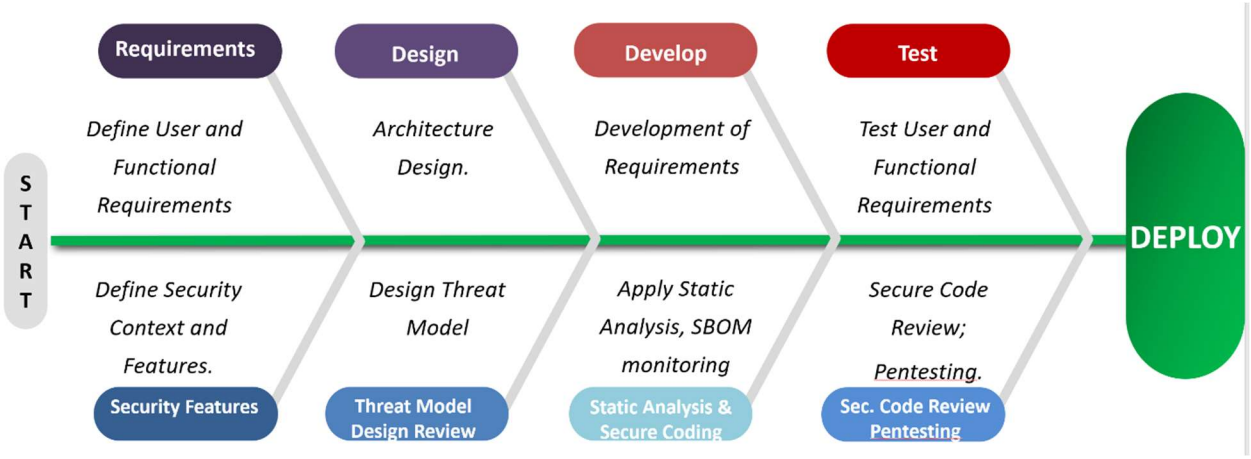


Nella fase di Pianificazione (PLAN) del prodotto si progetta già la sicurezza in termini di analisi del rischio, andando ad identificare i rischi, modellando le minacce (Threat Modelling) e conseguentemente definendo potenziali vulnerabilità. Il team di Ingegneria di Produzione/Sviluppo è integrato e opera in sinergia con il team di Ingegneria della Sicurezza in modo tale da assicurare un corretto flusso di Continuous Integration e Continuous Delivery (DO) del prodotto tanto da mantenere un'aderenza ai requisiti di sicurezza allo stato dell'arte (ACT). Il ciclo è controllato periodicamente (CHECK) attraverso review di sicurezza che concorrono all'emissione di piani di mitigazione e remediation che si applicano nuovamente al progetto di produzione/sviluppo.

Assume una certa rilevanza la fase DO in quanto è opportuno definire un workflow adeguato alle aspettative che supporti il raggiungimento dell'obiettivo.

Il concetto è l'introduzione del ciclo di vita relativo allo sviluppo sicuro o meglio il Secure Software Development LifeCycle (SSDLC) che ben si allinea al classico ciclo waterfall o al più contemporaneo ciclo agile (SecDevOps). Il SSDLC ci aiuta a ragionare in ottica di processi che impongano un reale presidio continuo della sicurezza, adottando soluzioni che affrontino efficacemente l'ambito della sicurezza delle applicazioni su ogni elemento (servizi esposti, front end, middleware, applicazioni mobili, IoT, OT) e non solo in fase di scrittura del codice.

Un esempio di quanto asserito è illustrato dal presente grafo:



Come possiamo vedere si declinano tutte le fasi di progetto in fasi duali con il corrispettivo punto di vista della sicurezza, tale approccio permette di avere sotto stretto controllo tutto il processo produttivo dall'ingegnerizzazione alla delivery mantenendo un'aderenza alle problematiche di sicurezza.

La scelta di dotarsi di un sistema di gestione secondo lo standard ISA/IEC 62443 prevede quindi due principali fasi:

- Definizione e gestione del processo di sviluppo;
- Definizione e gestione del processo di produzione.

L'adozione di un ciclo SSDLC all'interno di un processo produttivo già presente, prevede l'integrazione di cinque passi fondamentali.

- avviare campagna di VA/PT su quanto già prodotto all'interno dell'azienda/industria per avere una GAP-Analysis sullo scostamento rispetto alle potenziali vulnerabilità;
- Emissione del I Piano di remediation per permettere l'adeguamento dei prodotti già in fase di delivery il che porterebbe ad azioni di rilavorazione parziale;
- Introduzione nella fase di sviluppo/produzione di interventi di sicurezza volti ad analizzare il codice come la Secure Code Review e ad analizzare l'uso di prodotti di terze parti attraverso un controllo della Software Composition (SBOM);
- Emissione del II Piano di remediation per permettere l'adeguamento del processo di sviluppo/produzione dell'oggetto e ne avvia la fase di controllo continuo;
- Finalizzazione dell'integrazione del processo SSDLC anche nelle fasi di Progettazione con l'introduzione della definizione dei requisiti di sicurezza e la modellazione delle minacce (Threat Model).

Tale schematizzazione può supportare un'azienda/industria ad introdurre uno nuovo standard di sicurezza all'interno di un processo produttivo già in essere. Questo è molto importante perché salvaguarda anche gli investimenti già fatti, in quanto il processo parte dall'analisi su quanto già prodotto mettendolo in sicurezza e successivamente opera sul restante della catena di produzione così da ottenere un ciclo sicuro.

Sintetizzando durante l'attività di inserimento di uno standard come il ISA/IEC 62443 è opportuno costituire tre team; uno che segue il processo di elaborazione della documentazione in termini di definizione dei processi e procedure, un altro che si occupa della definizione dei livelli di sicurezza e dell'integrazione del processo di sviluppo sicuro ed infine l'ultimo che si occupa più in dettaglio della sicurezza modellando le minacce, eseguendo attività di analisi statica e dinamica del codice, analisi degli oggetti di terze parti e in ultimo vulnerbaility assessment epenetration test.

In particolare, le logiche di security by design devono diventare parte dei processi di sviluppo di prodotti e servizi a partire da quando i servizi vengono concepiti, dall'on-premise al cloud, con una sempre più stringente gestione dei processi di sourcing e delle terze parti, non solo in ottica di compliance, ma anche in ottica di tutela aziendale.

Il fenomeno degli impatti derivanti dalla sicurezza della catena di forniture è forse uno di quelli che si dimostra più difficile da intercettare dai dati degli ultimi rapporti come quello del Clusit, ma è certamente un fenomeno importante, sul quale si sta concentrando anche lo sforzo legislativo europeo e nazionale.

Tale tema diventa particolarmente rilevante nel mondo manufatturiero, o comunque ovunque siano presenti sistemi OT/IoT, spesso bersagli semplici per attacchi come i DDoS o utilizzando le connessioni utilizzate dai manutentori.

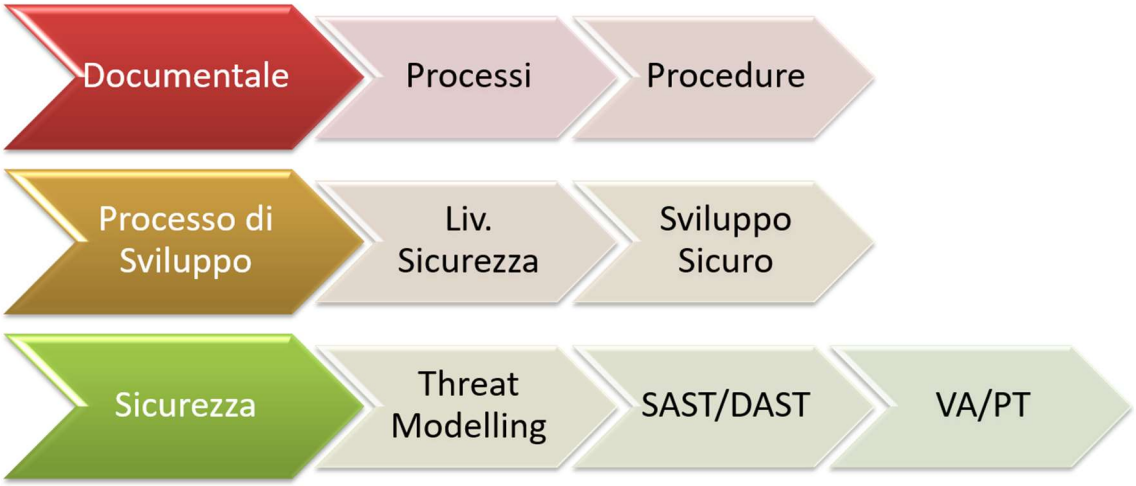
Caso d'uso: applicazione delle linee guida IEC 62443

In questo ultimo paragrafo vogliamo illustrare, quale esempio di implementazione di un processo di sicurezza, l'accompagnamento alla certificazione IEC 62443 di un dispositivo OT denominato Remote Terminal Unit (RTU):

Le caratteristiche del progetto sono:

- Obiettivo: realizzare il processo Secure-by-Design della RTU attraverso l'adozione dello standard IEC 62443
    - Componenti Dispositivo OT
    - Modulo principale: sistema dotato di microprocessore con firmware Linux embedded
    - Applicazioni installate: Web application e management application (in linguaggio HTML, Java, Javascript , C++)
- Attività del Laboratorio di Verifica e Validazione:
    - VA/PT in modalità «Black Box»
    - Analisi statica del software installato nella RTU
    - Analisi della Software Composition per la verifica di oggetti di terze parti o Open Source utilizzati all'interno delle applicazioni
    - Analisi dinamica del modulo binario per individuare potenziali vulnerabilità di flusso

Le attività svolte hanno riguardato i tre ambiti:

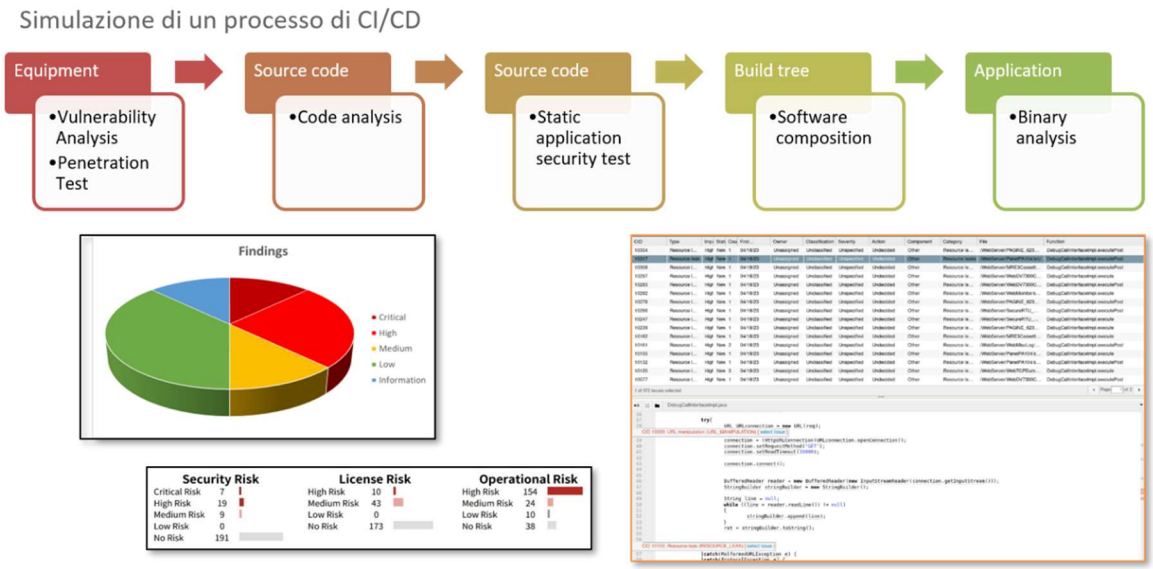


Nello specifico le attività VA/PT erano rivolte ad analizzare in dettaglio tutte le funzionalità dell'asset in esame, al fine di trovare modi non intenzionali per compromettere la riservatezza, l'integrità e/o la disponibilità dei dati. Le tecniche e le metodologie utilizzate nella fase di Penetration Test hanno coperto gli scenari più ampi possibili in modo da identificare i possibili vettori di attacco e le tecniche di intrusione a cui potevano essere esposte le applicazioni target.

La metodologia adottata per i security assessment si è basata sui seguenti standard:

- Open Web Application Security Project (OWASP)
- Open Source Security Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)

Le sfide affrontate attraverso queste attività sono state molteplici, i risultati intermedi hanno comportato alcune rilavorazioni che hanno permesso il raggiungimento del livello di sicurezza e quindi l'innalzamento della postura di sicurezza dell'RTU:



Dall'immagine è possibile intravedere il risultato di attività di analisi sul codice e di vulnerability assessment che hanno a loro volta avviato valutazioni interne e successivamente implementato aggiornamenti con lo scopo di mitigare il rischio.

Al termine del processo i risultati conseguite sono stati dunque due certificazioni:

- la certificazione IEC 62443-4-1 relativa al processo di sviluppo conforme agli standard di security for «Industrial Automation and Control System» (IACS).
- la certificazione IEC 62443-4-2 relativa alla produzione di dispositivi e apparati IACS.

Questo processo ha quindi abilitato l'azienda che lo ha intrapreso ad operare, d'ora in avanti, seguendo un processo di produzione nativamente sicuro, sottoposto a controllo periodico, ed in continuo aggiornamento.

Da un punto di vista del prodotto (la RTU), la certificazione di sicurezza permette in alcuni casi di poter fornire il dispositivo in maniera preferenziale, oppure di partecipare a forniture riservate esclusivamente ad oggetti certificati.

Concludiamo con il sottolineare che l'investimento iniziale dedicato alla certificazione deve essere comunque considerato parte di un processo di sicurezza che la Direttiva NIS 2 ha oramai reso sistemico e imprescindibile per tutte le organizzazioni tecnologiche moderne, visto il preoccupante trend che stanno seguendo le minacce cyber.

Autori

	**Elio Antonelli** Laureato in Ingegneria Nucleare all'Università degli studi "La Sapienza", ha da sempre svolto attività in ambito informatico, da programmatore a sistemista in contesti molto variegati. Si è poi specializzato nell'area Information Security dove ha lavorato in contesti internazionali. Attualmente si occupa di infrastrutture critiche come consulente Cyber Security e svolge attività di auditor ISO 27001.
	**Stefano Aterno** Nato a Roma, laureato presso l'Università La Sapienza, iscritto all'albo degli avvocati di Roma dal 1998. Avvocato Cassazionista, professore presso l'Università di Foggia, Università LUISS di Roma, Università di Roma TRE. Esperto di diritto penale dell'informatica, diritto delle nuove tecnologie e data protection Certificato: UNI 11697:2017 Data Protection Officer, certificato ISO 27001 sicurezza dei dati e delle informazioni, CIFI (Certified Information Forensics Investigator, by IISFA). Dal 1996 al 2000 ha svolto l'attività di Magistrato onorario presso il Tribunale di Roma. Svolge attività di contenzioso legale e di consulenza nella materia del diritto delle nuove tecnologie, data protection e diritto penale dell'informatica. È Responsabile della protezione dei dati (DPO) di alcune società importanti a livello nazionale e internazionale. Dal 2005 ad oggi ha pubblicato alcuni libri e numerosi articoli scientifici in tema di cybercrime, indagini informatiche, computer forensics e Data Protection. È docente in Master universitari nelle materie sopra indicate. È Socio dello Studio E- Lex dall'ottobre 2020.
	**Glauco Bertocchi** Laurea in Fisica all'Università di Roma "la Sapienza" Più di 40 anni di esperienza in ICT e nella sicurezza acquisita all'interno di università e istituzioni nazionali. Attivo nella ricerca in ambito protezione e resilienza delle Infrastrutture critiche. Coordina un gruppo sviluppo e ricerca di ISACA Roma per l'applicazione di metodi quantitativi nell'analisi dei rischi di tipo cyber e non solo. Vicepresidente del capitolo ISACA Roma, componente del CD di AIIC.

Alberto Caruso De Carolis

Ufficiale superiore in congedo della Guardia di Finanza, dal 2002 è stato dirigente d'azienda, nel settore aeroportuale, in ruoli di alta direzione, *Security*, *internal audit* e gestione rapporti e sinergie pubblico/privato, anche nel settore della Cybersecurity; docente al Master di Primo livello_"Crisis & Disaster Management" presso l'Università Cattolica del Sacro Cuore di Milano. Attualmente è partner di società di consulenza strategica.

Raffaella D'Alessandro

Laurea in Scienze Economiche. 40 anni di esperienza nell'ICT, dei quali 35 anni in Cybersecurity, con attività di progettazione architetturale e di consulenza GRC in ambito Cybersecurity, Data Protection, Standard e Digital Law Compliance. Ha lavorato in Olivetti, Arthur Andersen, Ernst & Young e IBM. Competenze di Artificial Intelligence in ambito trustworthiness (legal, ethics and robustness), legislazione AI ACT, standardizzazione dei sistemi di gestione AI e di Cybersecurity. Membro del Consiglio Direttivo di Associazione Italiana esperti in Infrastrutture Critiche, Socio Fondatore e Segretario di TOPForGrowth, Official Speaker Word Protection Forum, past member dei comitati tecnici di standardizzazione dell'ente italiano di normazione UNI – UNINFO.

Lucrezia Falciai

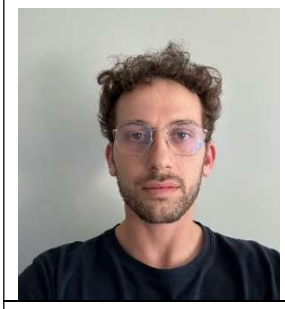
Laureata in Giurisprudenza all'Università degli Studi di Milano, attualmente lavora come avvocato presso lo Studio Legale Chiomenti. Ha maturato una solida expertise sulle normative nazionali ed europee in materia di cybersecurity, come, ad esempio, la Direttiva NIS o il Perimetro di Sicurezza Nazionale Cibernetica. Infatti, collabora nella practice area di Data Protection & Cybersecurity assistendo clienti su tutti i profili derivanti dall'applicazione delle suddette normative. Inoltre, supporta i clienti nella gestione di attacchi informatici e data breach.

È autrice di numerosi articoli e pubblicazioni su *data protection* e cybersecurity in diverse riviste scientifiche e ha partecipato, in qualità di *speaker* a numerose conferenze e seminari sui medesimi temi.

Luisa Franchina

Cofondatore di AIIC ne è attualmente Presidente. È stata Direttore Generale della Segreteria per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri 2010-2013). Ha pubblicato numerosi articoli e libri sulla sicurezza e sulla protezione delle infrastrutture critiche.

	**Marilena Hyeraci** Laureata in Giurisprudenza all'Università Cattolica del Sacro Cuore di Milano, attualmente ricopre il ruolo di Of Counsel presso lo Studio Legale Chiomenti, nel dipartimento di Privacy & Cybersecurity. Ha esperienza ventennale nella consulenza strategica in materia di protezione dei dati personali, cybersecurity e compliance generale, redazione dei sistemi di data governance, gestione dei data breach, nonché nel diritto delle nuove tecnologie. Autrice di varie pubblicazioni ed articoli, é regolarmente invitata come relatrice a convegni in Italia e all'estero. E' riconosciuta come leader del settore nelle principali guide legali nazionali ed internazionali, quali Chambers & Partners, Legal 500, Legal Community e Who's Who Legal.
	**Paola Patriarca** Laureata in Giurisprudenza presso l'Università Federico II di Napoli e iscritta all'Ordine degli Avvocati di Roma, Master in Diritto delle Nuove Tecnologie presso l'Università Alma Mater Studiorum di Bologna, attualmente frequenta il Master in Responsabile della protezione dei dati personali: Data Protection Officer e Privacy Expert presso l'Università Roma Tre. Appassionata di diritto delle nuove tecnologie, in qualità di *associate* dello Studio Legale E-Lex, presta principalmente consulenza stragiudiziale e giudiziale a soggetti pubblici e privati su questioni relative alla protezione dei dati personali e alla compliance GDPR, cybersecurity, cybercrime e intelligenza artificiale. È cultrice della materia in Diritto Digitale e Tutela dei Dati presso l'Università Luiss Guido Carli, autrice di articoli e pubblicazioni e relatrice in convegni in tema di data protection, cybercrime, indagini informatiche e computer forensics.
	**Giorgio Pizzi** Laureato in Ingegneria Elettronica, è dirigente del Ministero delle infrastrutture e dei trasporti. Attualmente si occupa di piattaforme digitali per la mobilità ed è componente di vari gruppi di lavoro e comitati in ambito ministeriale, CEN e UITP riguardanti la sicurezza dei sistemi di trasporto, la normazione tecnica funiviaria e l'integrazione tra la cybersecurity e la safety nei sistemi di trasporto.
	**Fabio Rosa** LABs Supervisor presso Digitalplatforms S.p.A. dove gestisce i laboratori di Verifica e Validazione di Sicurezza. Supporta i prori clienti nel perseguimento della certificazione di sicurezza dei prodotti nell'ambito dello schema nazionale (CommonCriteria) e per il perseguimento della certificazione ISO/IEC 62443 attraverso attività di Threat Model e VA/PT.

	**Tommaso Ruocco** Laureato in diritto internazionale presso la facoltà di giurisprudenza e in economia e politiche europee presso la London School of economics and polical science. Vanta diversi anni di esperienza nel settore dell'intelligence, della risk analysis e della sicurezza informatica con progetti nazionali ed internazionali portati avanti in questi settori.
	**Andrea Testi** Ingegnere Informatico all'Università La Sapienza (Roma), è Responsabile Tecnico dell'area Cyber & AI Operations di DigitalPlatforms, che fornisce soluzioni di Cybersecurity per sostenerne la trasformazione digitale delle aziende. E' stato Delivery Manager, Project Manager, Solution Specialist e Presales per importanti aziende italiane di Cybersecurity e di Intelligence, ambito in cui ha maturato 10 anni di esperienza, soprattutto in campo internazionale.
	**Maria Beatrice Versaci** Ha conseguito una laurea magistrale in Lingue e Civiltà Orientali (Arabo) presso l'Università La Sapienza di Roma, successivamente si è specializzata in Protezione Strategica del Sistema Paese (Cyber Intelligence, Big Data e Sicurezza delle Infrastrutture Critiche) presso la Società Italiana per l'Organizzazione Internazionale (SIOI). Attualmente analista e consulente presso Hermes Bay srl.

Supporto editoriale

	**Gianluca Cipriani** Laureato in Relazioni Internazionali all'Università degli Studi "Roma Tre" e Master in Protezione Strategica del Sistema Paese alla SIOI di Roma. Attualmente lavora come Senior Consultant presso Hermes Bay SrL su Enterprise Risk Management, Cyber Security e Cyber Governance.
	**Marianna Pedrazzi** Consulente e Project manager presso Hermes Bay srl, in cui lavora in ambito Security Awareness, Risk Managemetn e Gap analysis. Ha conseguito una laurea in Ingegneria edile e Architettura presso l'Università di Bologna nel 2022.
	**Maria Beatrice Versaci** Ha conseguito una laurea magistrale in Lingue e Civiltà Orientali (Arabo) presso l'Università La Sapienza di Roma, successivamente si è specializzata in Protezione Strategica del Sistema Paese (Cyber Intelligence, Big Data e Sicurezza delle Infrastrutture Critiche) presso la Società Italiana per l'Organizzazione Internazionale (SIOI). Attualmente analista e consulente presso Hermes Bay srl.