AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2021	N. 8/ 2021	Settembre 2021

Il rafforzamento dell'architettura nazionale di sicurezza cibernetica: il Perimetro e l'Agenzia

Perimetro di Sicurezza Nazionale Cibernetica

L'Italia ha recentemente rafforzato l'architettura nazionale di sicurezza cibernetica sia attraverso promulgazione dei decreti attuativi del Perimetro di Sicurezza Nazionale Cibernetica sia mediante la creazione dell'Agenzia per la Cybersicurezza Nazionale continuando il proprio percorso di crescita digitale.

Il Perimetro prevede sia obblighi legali volti al rispetto di stringenti misure di sicurezza e alla notifica degli incidenti, sia specifiche disposizioni in materia di forniture di determinati beni, sistemi e servizi ICT destinati a essere impiegati su reti, sistemi informativi e per l'espletamento dei servizi informatici utilizzati dai soggetti inclusi nel Perimetro stesso per l'esercizio della funzione/servizio essenziale per la sicurezza nazionale. A completamento di tale provvedimento, è previsto che siano promulgati una serie di decreti attuativi, quattro DPCM e un DPR, quattro dei quali già pubblicati.

Il primo, il DPCM n. 131 del 30 luglio 2020, dettaglia le specifiche e gli ambiti di attività dei soggetti inclusi nel Perimetro di sicurezza cibernetica nonché le modalità di elaborazione, aggiornamento e trasmissione degli elenchi dei beni ICT. La definizione di tali elementi si configura come passaggio fondamentale per la concreta realizzazione del Perimetro al fine di instaurare una serie di presidi di sicurezza funzionali a garantire un'efficace protezione cibernetica di tutto il sistema paese. (https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg)

Il secondo decreto, il DPR n. 54 del 5 febbraio 2021, definisce le procedure e i termini per le valutazioni svolte da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei Centri di Valutazione del Ministero degli Affari Interni e della Difesa su prodotti in fase di acquisizione da parte dei soggetti inclusi nel Perimetro. (https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg)

Il terzo decreto, il DPCM n. 81 del 14 aprile 2021, disciplina nel dettaglio le procedure di notifica che devono seguire i soggetti inclusi nel Perimetro in caso di incidenti impattanti su beni ICT, definendone una tassonomia per livelli di gravità, oltre che un elenco delle misure di sicurezza, basate su quanto previsto dal Framework Nazionale per la Cybersecurity e la Data Protection, che i soggetti stessi dovranno implementare per ciascun bene ICT di propria pertinenza. (https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg)

Il quarto decreto, il DPCM 15 giugno 2021, individua le categorie in relazione alle quali i soggetti inclusi nel Perimetro che intendano procedere, anche per il tramite delle centrali di committenza alle quali sono tenuti a fare ricorso, all'affidamento di forniture di beni, sistemi e servizi ICT, destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, effettuano la comunicazione al CVCN o ai Centri di Valutazione.
https://www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg)

L'ultimo DPCM, non ancora promulgato, definirà le regole di accreditamento per quanto riguarda i laboratori accreditati di prova che potranno effettuare screening di tecnologie.

In sintesi, è possibile affermare che il Perimetro di Sicurezza Nazionale Cibernetica è finalizzato a garantire nel tempo un approccio integrato e univoco dello Stato contro le minacce cibernetiche e a migliorare la capacità di resilienza di tutto il sistema paese.

Agenzia per la Cybersicurezza Nazionale

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

L'Agenzia per la Cybersicurezza Nazionale, istituita con D.L. 14 giugno 2021, n. 82 (https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg), sarà diretta da Roberto Baldoni, sarà l'Autorità nazionale per la cybersicurezza per la coordinazione tra i soggetti pubblici coinvolti in materia di cyber security a livello nazionale e promuoverà la realizzazione di azioni comuni orientate alla sicurezza e alla resilienza cyber per la digitalizzazione di tutto il sistema paese. In linea con i modelli francese e tedesco, la nuova agenzia si porrà al di fuori delle agenzie di intelligence, sottraendo così strutture quali il Computer Security Incident Response Team (CSIRT) italiano o il Nucleo di Sicurezza Cibernetica dal controllo esclusivo del DIS. Nonostante ciò, la nomina di Baldoni, già vicedirettore del DIS con delega alla cybersecurity, è emblematica della continuità necessaria per garantire la sicurezza di un settore di rilevanza strategica. Tale continuità permetterà anche di coordinare al meglio gli sforzi delle autorità competenti NIS nazionali nel porre in sicurezza e contrastare gli attacchi alle Infrastrutture Critiche.
Tra i compiti in materia di cyber security nazionale attribuiti alla nuova Agenzia rientrano tutti quelli precedentemente assegnati alla presidenza del Consiglio, al Ministero dello Sviluppo Economico, al DIS e all'Agenzia per l'Italia Digitale così come le competenze in materia di Perimetro di Sicurezza Nazionale Cibernetica. Tra essi rientreranno quindi l'elaborazione della Strategia nazionale di cybersicurezza e il supporto alle attività del Nucleo per la cybersicurezza, rappresentando inoltre l'Autorità nazionale competente e il punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi. Essendo anche Autorità nazionale di certificazione della cyber security, l'Agenzia accentrerà tutte le attività di certificazione finora esercitate dal Ministero dello Sviluppo Economico da parte dei competenti organi, quali il CVCN. In aggiunta, l'Agenzia si occuperà della prevenzione, del monitoraggio, del rilevamento, dell'analisi, delle risposte e della gestione di incidenti di sicurezza informatica e gli attacchi cyber. Infine, ma non meno importante, la nuova struttura sarà promotrice del coinvolgimento del sistema universitario e della ricerca, nonché del sistema produttivo nazionale, nel campo della cyber security e pertanto avrà il compito di promuovere la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della sicurezza informatica, anche attraverso l'assegnazione di borse di studio, di dottorato e di assegni di ricerca, favorendo l'attivazione di percorsi formativi universitari.
In ultima analisi, quindi, la definizione del Perimetro di Sicurezza Nazionale Cibernetica e la creazione dell'Agenzia per la Cybersicurezza Nazionale rappresentano senz'altro ottime iniziative funzionali al rafforzamento dell'architettura nazionale di sicurezza cibernetica. Nei mesi a venire, la promulgazione del restante decreto attuativo del Perimetro e l'entrata a regime dell'Agenzia rappresenteranno un ulteriore miglioramento della sicurezza cyber, in linea con quanto previsto anche dalle iniziative europee.

Luisa Franchina – Presidente AIIC
È stata Direttore Generale del Segretariato per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri) Ha pubblicato molti articoli e libri sulla safety e la protezione delle Infrastrutture Critiche

Matteo Taraborelli Laureato in Relazioni Internazionali e specializzato negli studi di sicurezza e difesa. Per la tesi di laurea magistrale ha svolto un periodo di ricerca presso i National Security Archive di Washington, D.C. E' Senior Consultant presso la società Hermes Bay

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

ATTIVITA' DELL'ASSOCIAZIONE

Rinnovo associativo per l'anno 2021

Si ricorda a tutti i soci che il 31 dicembre 2020 è scaduto il periodo associativo. Invitiamo tutti i soci a rinnovare per tempo l'associazione versando il relativo contributo, ormai inalterato da anni.
La quota per il rinnovo individuale è di euro 40 e può essere versata con bonifico sul c/c presso Banca Intesa Business, Coordinate bancarie IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando "rinnovo socio ordinario nome e cognome anno 2021".

Per i nuovi iscritti l'importo da pagare è di € 60,00. Le quote e le modalità di rinnovo per i soci collettivi – così come le indicazioni per chi vuole iscriversi come nuovo socio - sono contenute nel sito AIIC *http://www.infrastrutturecritiche.it /*

Ricordiamo che la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2021. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione, versando in più il relativo contributo per le spese di segreteria.

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da inserire, per esempio, in newsletter o nel sito AIIC.
In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIIC: in tal caso – però – la partecipazione di AIIC ad un evento deve essere decisa dal Consiglio Direttivo, pertanto siete pregati di contattare il CD con ragionevole anticipo, alla mail segreteria@infrastrutturecritiche.it
In caso non fosse possibile la partecipazione a nome AIIC, vi invitiamo ad indicare, nel profilo professionale, la vostra appartenenza ad AIIC.

AIIC ha sottoscritto convenzioni di collaborazione con altre Associazioni. In particolare con:

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi ed autonomi accordi.

- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).
- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza
- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo) è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

NUOVO SITO WEB AIIC

E' finalmente attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Nel corso dei prossimi mesi provvederemo ad arricchirlo sempre di più e ad illustrarvi le nuove funzionalità.
Vi terremo informati! Nel frattempo, vi invitiamo a navigare…

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

NUOVI GRUPPI DI LAVORO AIIC

Il Consiglio Direttivo di AIIC, nella riunione del 4 giugno 2021, ha approvato la costituzione di un nuovo Gruppo di Lavoro sulla "Disciplina normativa della criticità", mentre prosegue la possibilità di aderire al GdL sulla "Protezione degli spazi pubblici". I termini di adesione son scaduti e i Gruppi di Lavoro hanno già avviato le proprie attività

Gruppo di lavoro
"ICE, ICN, OSE, OSF... La disciplina normativa della criticità"
Coordinatore Luisa Franchina

Il panorama normativo europeo e italiano sulla disciplina della protezione delle Infrastrutture Critiche è divenuto complesso.
Il GdL vuole analizzare le norme in vigore e in itinere con una pubblicazione veloce, sintetica e precisa che supporti il lettore a:

1. comprendere a colpo d'occhio quanto delineato
2. valutare le implicazioni di compliance sulla propria azienda
3. identificare opportunità
4. interpretare le direttrici di ulteriori futuri sviluppi normativi

Gruppo di Lavoro
"Principi e Tecnologie per la Protezione di Spazi Pubblici"
Coordinatore Sandro Bologna

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Il Consiglio Direttivo di AIIC ha approvato la costituzione di un nuovo Gruppo di Lavoro su "Principi e Tecnologie per la Protezione di Spazi Pubblici (stazioni ferroviarie, sale aeroportuali, imbarchi portuali, stadi per concerti, ……..).

La rivoluzione digitale ha aperto la possibilità di raccogliere e recuperare immense quantità di dati in tempo reale. Lo sfruttamento delle soluzioni tecnologiche offre numerose opportunità per migliorare la protezione degli spazi pubblici. Applicati e analizzati correttamente, i dati derivati dai dispositivi IoT (Internet of Things) possono fornire informazioni per il rilevamento precoce delle minacce di molteplici scenari (terrorismo, criminalità, disastri naturali, pandemie). La disponibilità di strumenti per raccogliere informazioni più complesse, complete e rapide può aiutare a prendere decisioni più informate e più tempestive. Le applicazioni mobili e le piattaforme di social media possono fungere da forum per coinvolgere i cittadini nella protezione degli spazi pubblici. Migliori canali di comunicazione e sistemi integrati consentono un migliore coordinamento e collaborazione tra le diverse autorità. Queste ampie opportunità sono accompagnate da sfide altrettanto pesanti, che devono essere affrontate dal gruppo di lavoro.

Durata prevista un anno dal kick off meeting.

NEWS E AVVENIMENTI

IRAN'S TRAIN SIGNAGE ATTACK HIGHLIGHTS IT/OT PITFALLS A cyber attack on Friday impaired railway signage throughout Iran. The attack changed rail terminal signage to say that most or all trains had been delayed or cancelled and urged customers to call the phone number of the office of the Ayatollah Ali Khamenei for further information. Iranian news services initially reported "unprecedented chaos" at rails stations, but later withdrew that report. A subsequent post stated that the attack caused no problems whatsoever.This attack mirrors comments made in an Industrial Security podcast six months ago. In that episode, Shannon Ramsaywak pointed out how important signage was to rails systems performance and even to rails systems safety. Shannon also explained how senior decision-makers often did not realize how exposed their signage systems were to sabotage.While details on the Iranian attack are scarce, signage systems are often much more exposed to cyber attacks than are rails signaling and dispatch systems. After all, most rails systems all over the world post their latest schedule updates to their website and sometimes even to cell phone apps, both of which are Internet-accessible. In all such systems, there must be a communications path that connects the Internet to sources of locomotive location data. Modern rail systems do not permit such connectivity through mere firewalls. Instead, they push location and schedule data from rail control systems out to the Internet through Unidirectional Security Gateways. The gateways are not physically able to send any attack information from the Internet back into the switching systems. The risk of online, Internet-based attacks vanishes entirely when Unidirectional Gateways are the only connection between control-critical and Internet-exposed business systems.More generally though, the attack in Iran reminds us of the importance of correctly classifying our IT and OT systems. A table-top exercise I recommend to all OT security practitioners is to look at what happens when all IT-connected computers are utterly compromised. In this worst-case scenario, can physical OT operations continue? *(Continua)*
https://waterfall-security.com/irans-train-signage-highlight-it-ot-pitfalls/?utm_campaign=Newsletters%20Campaigns&utm_medium=email&_hsmi=140359074&_hsenc=p2ANq

tz-8JsmDxbY6cQDBvO7vc_wCVwZfsVlGhoGxcTs9cXvGa5oHv6YNA92HwWxAz0r8RH-5fpyESG4GW9bPjnSxQB34fcdhpaiiFSW1A9BmTb14yGSyqQe8&utm_content=140359074&utm_source=hs_email

WATERFALLSECURITY *12 JUL 2021*

L'Industrial Internet of Things apre la strada alla trasformazione industriale del futuro - Industria di produzione, logistica e l'intera catena di approvvigionamento e smaltimento, in cui la maggior parte dei decision maker riconosce il ruolo dell'IIoT quale abilitatore della trasformazione digitale.
Il processo di trasformazione digitale del mondo industriale verso il concetto di Industria 4.0 non deve essere percepito come un salto nel vuoto legato necessariamente all'intera sostituzione dei macchinari in uso. Al contrario, infatti, i risultati di digitalizzazione migliori e più sostenibili nel tempo possono essere raggiunti con una politica di piccoli passi e delineata da un percorso graduale.
Il concetto di Industria 4.0 fa leva su una produzione in grado di adattarsi in modo agile e dinamico ad uno scenario in continuo cambiamento e di evolversi rapidamente per rispondere alle mutevoli esigenze. Per cavalcare questa tendenza, grandi volumi di dati devono essere continuamente raccolti sia all'interno sia tra i singoli macchinari e successivamente comunicati all'intero ecosistema per essere valutati nei vari livelli di tecnologie operative (OT) e tecnologie dell'informazione e della comunicazione (ICT).
Le opportunità legate alla capacità di raccogliere e valutare quantità sempre maggiori di dati riguardano la digitalizzazione di tutti i processi aziendali e produttivi, la creazione di valore industriale, le operazioni di funzionamento e manutenzione degli impianti per una maggiore efficienza e affidabilità, oltre che lo sviluppo di modelli di business completamente nuovi. I dati rappresentano il primo step per attuare una trasformazione digitale in modo agile e automatizzato: un processo che richiede, tuttavia, un collegamento in rete di tutte le macchine e degli impianti, nonché di sensori e attuatori aggiuntivi estesi a tutte le sedi di un'azienda. Un metodo espresso sotto il concetto di Industrial Internet of Things (IIoT).
Indice degli argomenti
Valutazione della situazione attuale
Adattare le tecnologie in uso
Creare modularità e indipendenza
Reti per il trasporto dei dati
Integrare o bypassare i sistemi esistenti?
Tutto da un'unica fonte
(continua)
https://www.internet4things.it/edge-computing/iot/lindustrial-internet-of-things-apre-la-strada-alla-trasformazione-industriale-del-futuro/
Internet4things *- Thomas Kruse, 23 Luglio 2021*

Attacco alla Regione Lazio: cosa impariamo dagli errori commessi - La Regione Lazio non è, e non sarà, la sola a patire un attacco informatico come quello che ha bloccato il sistema di prenotazioni vaccini: riflettere su quanto accaduto può quindi servire a individuare i punti cardine per una reale sicurezza in azienda (pubblica o privata che sia) e non commettere gli stessi errori
Per molti addetti ai lavori quello che è accaduto alla Regione Lazio è, al contempo, imbarazzante e comprensibile.

Di certo rimangono parecchie domande aperte che probabilmente non avranno mai risposta, o almeno non prima che le procedure investigative e legali siano concluse. Proprio mentre scrivo il TG1 annuncia che manca poco alla scadenza dell'ultimatum degli "hacker". Quanto meno inutile se i dati sono stati recuperati e la falla chiusa davvero. Anche qui non si capisce se i dati siano o meno stati immessi in rete per rivenderli o utilizzarli in altre attività criminali.
Sulla non comunicazione c'è poco da dire. Sull'uso della terminologia, invece, temo che si debba lavorare ancora molto e la neonata unità di cyber security governativa non è da meno e dovrà vedersela con un "backlog" non banale.
Leggiamo ancora termini come attacco hacker, sicurezza informatica, cyber security, incidenti di sicurezza inseriti nelle frasi come se fossero parole magiche o chiavi per attrarre l'attenzione. In effetti, l'uso improprio non solo è formalmente scorretto, ma alimenta la disinformazione e la confusione. Come pensiamo di coinvolgere le persone e crescere utilizzando termini errati?
Io ho una domanda: se foste l'AD/CEO di una organizzazione (pubblica o privata che sia), sborsereste soldi per l'ultimo modello di uno strumento costosissimo già comprato lo scorso anno perché: "necessario" per una maggiore efficienza? Ovviamente la risposta è articolata ma tendenzialmente sarebbe un "no, perché dovrei farlo avendo già investito fior di quattrini per la stessa cosa lo scorso anno?".
Questa è la percezione quando un Security Manager/CISO ecc. si presenta "cappello in mano" alle riunioni di budget con richieste del genere (permettetemi la semplificazione per rendere la scena anche a chi non è addetto ai lavori, perché sono loro che dobbiamo coinvolgere in questa lotta).
Indice degli argomenti
I fattori cardine per una reale sicurezza
Sicurezza delle informazioni, business continuity e disaster recovery
Conclusioni *(continua)*
https://www.cybersecurity360.it/nuove-minacce/attacco-alla-regione-lazio-cosa-impariamo-dagli-errori-commessi/
Cybersecurity360.it *- Fabrizio Cirilli – 16 agosto 2021*

Minacce alla sicurezza nella supply chain: ecco come contrastare gli attacchi più diffusi - ENISA, nel suo compito di fornire informazione e consapevolezza generale sulla sicurezza informatica quale agenzia dell'Unione sul tema, ha pubblicato a fine luglio scorso un rapporto dal titolo "ENISA threat landscape for supply chain attacks" che mira a mappare e studiare gli attacchi nelle catene di fornitori che sono stati scoperti da gennaio 2020 all'inizio di luglio 2021, in piena era "Covid-19" con relativa digitalizzazione forzata del mercato. Sulla base delle tendenze e dei modelli osservati, l'ente suona l'allarme: gli attacchi di questo tipo sono aumentati di numero e in sofisticazione nel corso del 2020, continuando nel 2021 (si stima che nel 2021 vi saranno quattro volte più attacchi rispetto all'anno passato). Tali attacchi sfruttano l'interconnessione e interdipendenza dei mercati globali per avere maggior penetrazione ed effetto nella accresciuta complessità e commistione, alimentando anche la "reputazione" di determinati gruppi di attaccanti che si fanno forti di certi exploit resi noti dalla stampa.
Il tema è anche di pregnante interesse sotto la lente della protezione dei dati personali: è di giugno ad es. una serie di sanzioni del Garante Privacy nel caso dell'aeroporto Marconi di Bologna ove si era scoperta una serie di malpractice anche del fornitore software dell'aeroporto. Il rischio di subire dunque non solo un danno di sicurezza ma anche una sanzione per la cattiva gestione del tema è elevato.
Trattandosi di minacce alla sicurezza di maggior complessità rispetto ad altri, l'analisi dell'ENISA è fondamentale nel cercare di allertare le aziende, i professionisti, le pubbliche amministrazioni,

suggerendo anche metodi di protezione al passo coi tempi e che coinvolgano maggiormente i fornitori stessi.
Proviamo, dunque, ad analizzarlo premettendo che il documento è un corposo volume di quasi sessanta pagine: qui ci limitiamo a indicazioni generali e a sottolineare alcune casistiche di rilievo pratico, sia per la sicurezza che per la protezione dei dati (personali e non).

Indice degli argomenti

Minacce alla sicurezza nella supply chain: i dati
Attacco alla supply chain: di cosa si tratta
Ciclo di vita della supply chain
Analisi di attacchi e incidenti della filiera
Sicurezza nella supply chain: le raccomandazioni
(continua)

https://www.cybersecurity360.it/nuove-minacce/minacce-alla-sicurezza-nella-supply-chain-ecco-come-contrastare-gli-attacchi-piu-diffusi/

Cybersecurity360.it *- Andrea Michinelli – agosto 2021*

Beijing has a new legal architecture for sweeping control over user data China's vision on data governance is becoming clearer. For years, China, like other countries, has been exploring ways to harness and also secure the power of the vast troves of data held by companies and government agencies. In July, when it launched a cybersecurity probe into ride-hailing giant Didi Chuxing, many saw it as the start of a new era for state control over data in China. In the remaining months of a year that has already seen its tech regulatory crackdown intensify, China will implement no fewer than three new laws and rules governing data privacy and security, including at least one specific one for the automotive sector.

Together they paint a much clearer picture of Beijing's vision for private data: to govern it as a key national asset within its borders, while trying to further unlock data's potential, seen by Beijing as a business input of similar importance as land and capital. "The hope from Beijing's perspective is to unleash the data potential of 1.4 billion consumers, producers, and innovators, plus the mountain of industrial data that the country produces and see it yield economic fruit," said Jacob Gunter, senior analyst with German think tank MERICS.

China's new data security and privacy laws

China had largely allowed tech firms to develop with little oversight over how they collected or used data, apart from provisions for user information to be shared with the government in a variety of circumstances. Then in 2017, China implemented a major new legislation in the data governance space, the Cybersecurity Law, to categorize and supervise data, with data localization a key focus of that law. That was followed by companies like Apple and others setting up data centers in China. The rules taking effect over the next three months strengthen that approach but also extend it far more broadly. At the national level, the Cyberspace Administration, which has become a "super agency" under Chinese president Xi Jinping's watch, will coordinate with departments under the State Council, sometimes referred to as China's cabinet, to implement the data laws.*(Continua)*

Https://qz.com/2051268/china-aims-to-control-but-also-unleash-the-economic-power-of-data/

QZ *- Jane Li- August 30, 2021*

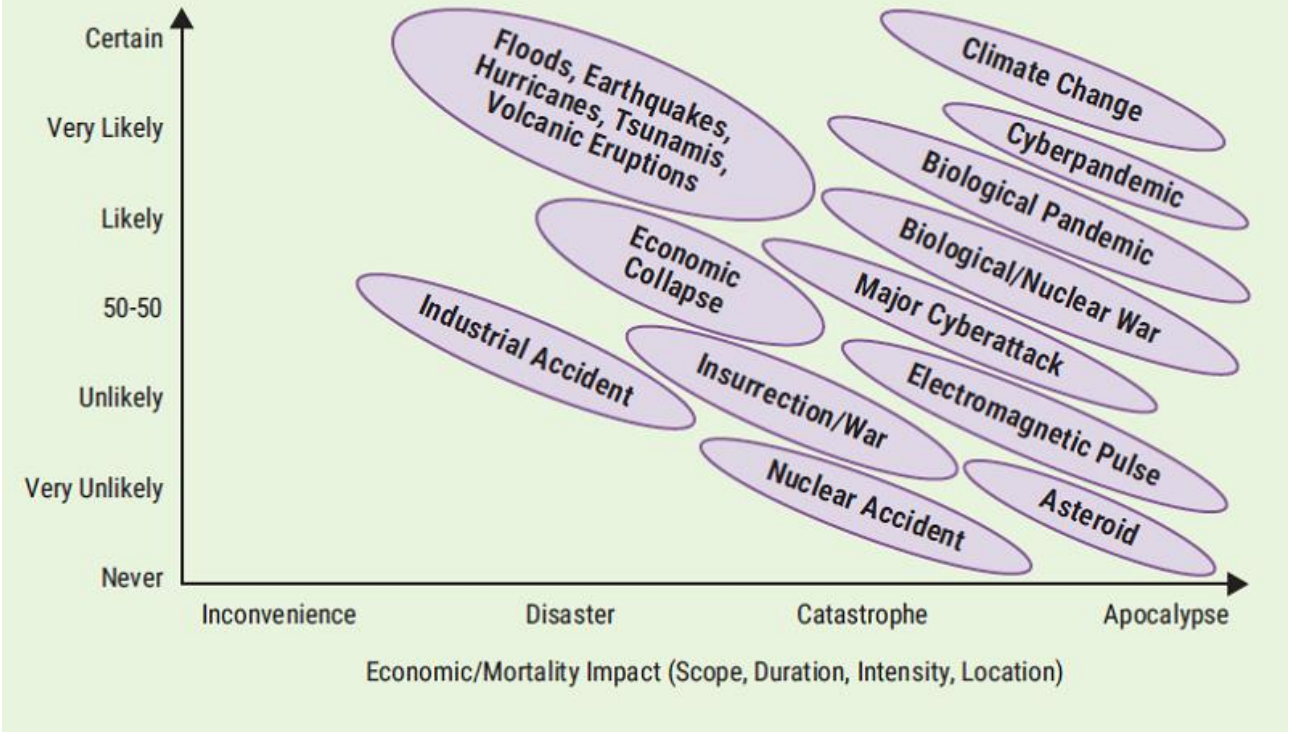
Accessing Data and Maintaining Privacy Before During and After Catastrophic Events. The basic precepts of privacy do not change in the face of catastrophes, but the type and amount of personally identifiable information (PII) used and generated and the need for legitimate access to those data increase substantially. There are different requirements for data collection, storage, access and disposal for a range of catastrophic events. It is important to understand how those data might best be protected throughout their life cycles to ensure the privacy rights of individuals and still provide what is needed for first responders and assistance agencies. It is also important to discuss the continuity and restoration of IT systems and business processes and the recovery of data and access affected by catastrophes.

There are substantial differences between regular contingency planning—business continuity planning (BCP) and disaster recovery planning (DRP)—and catastrophe contingency planning (CCP).[1] These differences make for increased difficulty and complexity in recovering both systems and the sensitive data that they contain and ensuring that only authorized and authenticated users have access.

Types of Catastrophic Events

The terms disaster, catastrophe and apocalypse are used to describe increasingly destructive, high-impact events. Figure 1 shows examples of such events, with impact plotted against likelihood. The diagram is illustrative rather than definitive. The placement and magnitude of the incidents are based on estimates by the World Economic Forum, the Global Challenges Foundation and the other subject matter expert opinions.

Figure 1—Catastrophic Events by Likelihood and Impact



In figure 1, the orientation of the ovals implies that less impactful events are more common than those of greater impact. For example, less powerful earthquakes occur more frequently compared to those

that are devastating, such as the 2010 earthquake that destroyed Port-au-Prince, Haiti, leaving an estimated 250,000 dead, 300,000 injured and 1.5 million homeless.(*Continua)*

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/accessing-data-and-maintaining-privacy-before-during-and-after-catastrophic-events
ISACA JOURNAL - C. Warren Axelrod,- 1 September 2021

Rockwell Automation: We cannot allow cyberattacks to be the new normal
The pandemic has exposed the vulnerabilities of the global manufacturing and supply-chain processes long hidden beneath the surface**.**
Cybersecurity has been a decades-long "grey rhino" in the wings of this "black swan" event. Last year, a Tokopedia data breach jeopardised more than 15 million user accounts, and cybercrime accounted for 43 percent of all crime in Singapore. Interconnectivity in a digital landscape may bring greater agility and convenience to manufacturers but the same benefits apply to malevolent players which are now no longer encumbered by geography.
Much like multi-layered anti-COVID measures, from defense (face masks and hand sanitisers) to prevention (lockdowns), rapid detection (PCR kits), and a cure (vaccines and antiviral drugs), corporations need to apply the same robust approach to protecting critical infrastructure.
Convergence of IT and OT
Increased interconnectivity also extends to hackers. Companies need to understand that there is no "air gap" between Information Technology (IT) and Operational Technology (OT) – the technology directly monitoring and or controlling industrial equipment, assets, and processes. These are not separate entities but two halves of a whole enterprise. While many have taken measures to secure IT, their OT systems remain under-protected, becoming a convenient "backdoor" for hackers to breach. Ransomware incidents have become increasingly frequent in manufacturing. Ransomware attackers can penetrate a chink in the armour within minutes and spend months "dormant." They silently infiltrate the entire network and stay undetected for months while gathering data and critical information before striking. A recurring issue in OT security is legacy infrastructure, built decades before high-speed internet was commonplace. This means older machinery, equipment and computer systems are a worrying blind spot to IT and security operations teams and can also result in exposure. For example, a factory's central conveyor belt might still run on an outdated edition of Windows XP no longer supported by its developer, nor compatible with the latest updates and protections. There is a lot of complexity in the OT layer for manufacturers to address, alongside balancing the costs to modernise. This process is often deprioritised and delayed. Modernisation takes time and requires multi-year transformation. But by making these changes now, organisations can immediately adopt best practices to build a holistically secure IT/OT network environment to neutralise potential threats.
The myth of the panacea
Similar to how we have managed to bring disease outbreaks such as polio and smallpox under control, a multi-layered defence strategy is needed to detect and deter malicious players. Organisations should start with a holistic enterprise-wide security assessment that includes: *(Continua)*
https://itwire.com/guest-articles/guest-opinion/rockwell-automation-we-cannot-allow-cyberattacks-to-be-the-new-normal.html
ITWIRE - *Sabyasachi Goswami – September ,2, 2021*

Back to school 2021, c'è un ospite a sorpresa: l'attacco ransomware *Dopo gli attacchi contro la sanità (come nel caso della Regione Lazio), la riapertura di migliaia di istituti scolastici che si sono*

digitalizzati in fretta e furia durante la pandemia – spesso senza adottare adeguati protocolli di sicurezza – rappresenta un'occasione ghiotta per gli hacker A fine agosto, il gruppo olandese ROC Mondriaan, che gestisce 26 scuole superiori a L'Aia e nelle città vicine per un totale di oltre 25.000 studenti, ha denunciato un attacco informatico contro i suoi sistemi. Il tutto a pochi giorni dalla riapertura degli istituti. "Si torna alle basi usando carta e penna", ha detto lunedì il preside di una scuola ROC Mondriaan all'Aia. Quello olandese è soltanto un episodio, l'ultimo, di attacchi contro le scuole che stanno riaprendo in tutta Europa e che gestiscono dati sensibili come le valutazioni degli studenti e informazioni personali come indirizzi, numeri di telefono, condizioni di salute e informazioni familiari. Un rapporto pubblicato a luglio dalla società di cybersicurezza Sophos ha mostrato che il 44% di quasi 500 organizzazioni educative intervistate in tutto il mondo sono state colpite da un attacco *ransomware* lo scorso anno. Tra quelle colpite, un terzo ha pagato un riscatto per riavere i propri dati. Un'altra azienda di cybersecurity, Proofpoint, ha spiegato che il 70 per cento dei funzionari di cybersecurity intervistati del settore dell'istruzione europeo si attendono un "cyberattacco materiale" nei prossimi 12 mesi, con il *ransomware* tra le minacce più temute. "Le campagne *ransomware* che stiamo vedendo ora", concentrate in particolare sulla sanità (come il caso della Regione Lazio) e spesso provenenti da Russia e Cina, "sono solo destinate a continuare", ha spiegato Rob Krug, ingegnere di sicurezza della società ceca di cybersecurity Avast, citato da *Politico*. "Le scuole, che siano istituzioni private o governative, si troveranno spesso nel mirino degli aggressori semplicemente perché hanno dimostrato di essere obiettivi facili in passato". *(Continua)*
https://formiche.net/2021/09/back-to-school-2021-ransomware/
FORMICHE *Federica De Vincentis 03/09/2021*

This is the perfect ransomware victim, according to cybercriminals. An investigation into what ransomware groups want has painted the picture of the perfect target. Researchers have explored what the perfect victim looks like to today's ransomware groups
On Monday, KELA published a report on listings made by ransomware operators in the underground, including access requests -- the way to gain an initial foothold into a target system -- revealing that many want to buy a way into US companies with a minimum revenue of over $100 million. Initial access is now big business. Ransomware groups such as Blackmatter and Lockbit may cut out some of the legwork involved in a cyberattack by purchasing access, including working credentials or the knowledge of a vulnerability in a corporate system. When you consider a successful ransomware campaign can result in payments worth millions of dollars, this cost becomes inconsequential -- and can mean that cybercriminals can free up time to strike more targets.
The cybersecurity company's findings, based on observations in dark web forums during July 2021, suggest that threat actors are seeking large US firms, but Canadian, Australian, and European targets are also considered.
Russian targets are usually rejected immediately, and others are considered "unwanted" -- including those located in developing countries -- likely because potential payouts are low. Roughly half of the ransomware operators will, however, reject offers for access into organizations in the healthcare and education sector, no matter the country. In some cases, government entities and non-profits are also off the table. In addition, there are preferred methods of access. Remote Desktop Protocol (RDP), Virtual Private Network (VPN)-based access prove popular. Specifically, access to products developed by companies including Citrix, Palo Alto Networks, VMWare, Cisco, and Fortinet. "As for the level of privileges, some attackers stated they prefer domain admin rights, though it does not seem to be critical," the report states.

KELA also found offerings for e-commerce panels, unsecured databases, and Microsoft Exchange servers -- although these may be more appealing for data stealers and criminals attempting to implant spyware and cryptocurrency miners.
"All these types of access are undoubtedly dangerous and can enable threat actors to perform various malicious actions, but they rarely provide access to a corporate network," the researchers noted.
Roughly 40% of listings were created by players in the Ransomware-as-a-Service (RaaS) space.
Ransomware operators are willing to pay, on average, up to $100 000 for valuable initial access services*.(Continua)*
https://www.zdnet.com/article/this-is-the-perfect-ransomware-victim-according-to-cybercriminals/
***ZeroDAY** - Charlie Osborne - September 6, 2021*

Germany has protested to Russia over attempts to steal data from lawmakers and use them to spread disinformation ahead of the upcoming election. Germany has formally protested to Russia over a series of cyber attacks aimed at stealing data from lawmakers that could be used to arrange disinformation campaigns before the upcoming German election.
The spokeswoman for the Foreign Ministry, Andrea Sasse, said that threat actor tracked as Ghostwriter has been "combining conventional cyberattacks with disinformation and influence operations." in attacks against Germany. The alleged state-sponsored hackers conducted phishing attacks against federal and state lawmakers to steal their personal login details.
"These attacks could serve as preparations for influence operations such as disinformation campaigns connected with the parliamentary election," Sasse told reporters in Berlin. "The German government has reliable information on the basis of which Ghostwriter activities can be attributed to cyber-actors of the Russian state and, specifically, Russia's GRU military intelligence service," she added. It "views this unacceptable activity as a danger to the security of the Federal Republic of Germany and for the process of democratic decision-making, and as a severe strain on bilateral relations."
The government of Berlin calls on the Kremlin to immediately halt these campaigns.
The German government considers the attacks completely unacceptable and warns of a possible response if they will not end. In March, German newspaper Der Spiegel revealed that email accounts of multiple members of the German Parliament (Bundestag) were targeted with a spearphishing attack.
The attackers are suspected to be hackers of the tracked as Ghostwriter group that works under the control of the Russian military secret service GRU*. (Continua*)
https://securityaffairs.co/wordpress/121958/intelligence/germany-protests-to-russia-attacks.html
***Security Affairs** - Pierluigi Paganini- September 8, 2021*

PROSSIMI EVENTI

A Roma la 7th EDEN Conference on data protection in law enforcement - Si terrà a Roma il 18 e 19 ottobre p.v., all'Auditorium della tecnica, la 7th EDEN Conference on data protection in law enforcement.
È una interessante conferenza internazionale, organizzata da ERA (Accademia Europea di Diritto) in collaborazione con la Polizia Italiana ed Europol's Data Protection Experts Network (EDEN) diritto, nella quale si affronteranno temi di data protection, AI, machine learning, data bias ecc.
Prossimamente sarà resa nota l'agenda con il programma e la descrizione dei panel. Il link all'evento è il seguente: https://www.era.int/cgi-

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

bin/cms?_SID=885ede4b6519453fd72b2911c71b71b8835ef2200078460845008 4&_sprache=en&_bereich=artikel&_aktion=detail&idartikel=130784

A causa dell'emergenza Covid 19 gli eventi in presenza sono ancora rinviati a data da destinarsi. Stiamo programmando l'attività dei Colloquia in modalità online. Vi terremo informati.

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Palestro 95 – 00185 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo è sufficiente usare il seguente link: http://www.linkedin.com/ groups/96335
Versione stampabile della	Nella sezione "Newsletter "del sito

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

newsletter http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.

Comitato di Redazione
Alberto Traballesi
Glauco Bertocchi
Silvano Bari
ai quali potete inviare suggerimenti e quesiti scrivendo a:
segreteria@infrastrutturecritiche.it

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.