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 2022	N. 2/ 2022	Febbraio 2022

Crisi in Ucraina: quali rischi per la cybersecurity in Occidente?

Il 15 febbraio, nella stessa giornata in cui le tensioni in Ucraina sembrano iniziare ad allentarsi, è stata riportata la notizia di un attacco hacker nei confronti di alcune istituzioni del Paese, sferrato probabilmente da gruppi hacker più o meno collegati con le forze armate russe. In particolare, l'attacco che ha bloccato l'accesso al sito Web del ministero della Difesa ucraino, avrebbe coinvolto anche due istituti bancari, come riportato dal centro per la sicurezza delle informazioni dell'Ucraina (Fonte Reuters: Ukraine reports cyber attack on defence ministry website, banks). Il rischio di azioni di questo tipo era già stato previsto dal Segretario generale della NATO Stoltenberg durante la sua recente visita in Romania, presso la base di Costanza. In tale occasione, Stoltenberg aveva infatti avvertito che il "pericolo non è confinato a una "piena invasione militare" bensì ad "azioni ibride", comprese quelle "cibernetiche", o a un tentativo di "ribaltare il governo di Kiev"" (Fonte Ansa: Stoltenberg, '007 russi in Ucraina, c'è rischio di golpe').

Tuttavia, è importante ricordare come in realtà la Russia non sia nuova ad attacchi cyber nei confronti dell'Ucraina. Fin dal 2014 infatti vi sono state una serie di azioni condotte nel cyberspazio nei confronti del governo di Kiev. In particolare, la Russia ha interferito nelle elezioni ucraine[1], ha preso di mira la sua rete elettrica[2], ha alterato i suoi siti web governativi[3] e ha compiuto azioni di disinformazione[4]. Strategicamente, le operazioni informatiche russe sono state mirate ad indebolire e delegittimare il governo ucraino e le organizzazioni del settore privato.

Tatticamente, invece, hanno mirato a influenzare, spaventare e sottomettere la popolazione (Fonte The Conversation: Russia has been at war with Ukraine for years – in cyberspace). Se da un lato le possibilità di una invasione sembrano ridursi, dopo le notizie di distensione giunte a seguito dell'incontro Putin – Scholz e del parziale ritiro delle forze armate russe (Fonte corriere.it: Scholz e Putin: l'ora di trattare. Dai russi primo ritiro parziale), dall'altro risulta sempre più verosimile l'aumento dell'assertività russa in ambito cyber. In particolare, già a gennaio, in un comunicato stampa del Dipartimento del Tesoro degli Stati Uniti, l'amministrazione Biden ha accusato la Russia di attuare un piano di information warfare risalente al 2020 per "destabilizzare la situazione politica in Ucraina e gettare le basi per la creazione di un nuovo governo controllato dalla Russia in Ucraina" (Fonte thecipherbrief.com: A New Path to Cyber Conflict with Russia). Il piano, secondo il comunicato del Tesoro, includeva "l'identificazione e la cooptazione di individui filo-russi in Ucraina e la diffamazione di eminenti ucraini considerati filo-occidentali, che avrebbero ostacolato gli sforzi russi per portare l'Ucraina sotto il suo controllo". "La Russia ha ordinato ai suoi servizi di intelligence di reclutare gli attuali ed ex funzionari del governo ucraino per prepararsi a prendere il governo dell'Ucraina e per controllare le infrastrutture critiche dell'Ucraina con una forza russa di occupazione", secondo il comunicato del Tesoro. La Russia, in precedenti incursioni in Ucraina, "ha perseguito ampie operazioni informatiche contro le

[1] https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election/
[2] https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/
[3] https://www.pcmag.com/news/ukrainian-government-websites-defaced-amid-threat-of-russian-invasion
[4] https://www.state.gov/fact-vs-fiction-russian-disinformation-on-ukraine/

infrastrutture critiche", ha affermato il Tesoro, aggiungendo che gli operativi di Mosca "si sono concentrati sull'interruzione di un settore delle infrastrutture critiche in particolare: il settore energetico ucraino. La Russia ha anche degradato l'accesso dell'Ucraina ai prodotti energetici in pieno inverno".

Inoltre, il 15 gennaio, Microsoft ha annunciato che i suoi investigatori hanno scoperto un malware distruttivo in dozzine di organizzazioni governative, senza scopo di lucro e di tecnologia dell'informazione ucraine. Stranamente, il malware mostrava una richiesta di riscatto, ma sembra essersi trattato di uno stratagemma poiché non veniva mostrato alcun modo per decrittografare le informazioni nel caso di pagamento del riscatto. A fine gennaio, la *Cybersecurity and Infrastructure Security Agency* (CISA) degli Stati Uniti ha confermato i resoconti della stampa secondo cui "entità pubbliche e private in Ucraina hanno subito una serie di incidenti informatici dannosi, tra cui defacement del web e segnalazioni del settore privato di malware potenzialmente distruttivi sui loro sistemi". Apparentemente riferendosi alla divulgazione di Microsoft, la CISA ha affermato che il malware identificato era simile a *NotPetya*. La CISA ha descritto tale scoperta come "particolarmente allarmante" perché *NotPetya* è stata ritenuta dalla CIA una creazione del GRU russo dopo essere stata utilizzata nel 2017 contro l'Ucraina, dove ha causato danni diffusi alle infrastrutture critiche. Anch'esso si è comportato più come un malware distruttivo piuttosto che come un ransomware (Fonte thecipherbrief.com: A New Path to Cyber Conflict with Russia).

Se da un lato la destabilizzazione dell'Ucraina al fine di favorire un cambio di potere mediante azioni di guerra ibrida comprendenti attacchi cyber risulta esser la chiara strategia perseguita attualmente dal governo di Mosca, meno chiaro risulta essere il confine oltre il quale Putin non sarà disposto a spingersi. Per esempio, BBC prospetta un possibile ampliamento dello scenario: l'eventuale conflitto militare rimarrebbe ovviamente confinato in Ucraina, ma gli attacchi informatici potrebbero andare ben oltre i suoi confini fisici. È per questo che le organizzazioni britanniche sono state esortate a rafforzare le proprie difese informatiche. Il National Cyber Security Centre (NCSC) ha pubblicato nuove linee guida, e sebbene sia stato chiarito che non si conoscono al momento minacce specifiche alle infrastrutture inglesi, è anche chiaro che il rischio sia stato messo in conto.

Lo stesso ha fatto NSA, prendendo parte a una serie di riunioni sulla sicurezza che hanno valutato il possibile impatto interno degli eventi in Ucraina. Lo scenario più preoccupante è che la Russia bersagli le infrastrutture occidentali con attacchi simili a quello alle centrali elettriche ucraine del 2015. Un attacco al settore finanziario potrebbe impedire agli ucraini di disporre del denaro per sostentarsi, un attacco alle infrastrutture di comunicazione potrebbe paralizzare e isolare l'intero Paese (Fonte securityopenlab.it: Ucraina e Russia, se la cyber guerra arrivasse in Occidente?).

Per quanto tale scenario risulti al momento molto improbabile, le azioni di cyber warfare russe in Ucraina negli ultimi sette anni e il loro rinnovato intensificarsi sono una chiara dimostrazione come, nel confronto con l'Occidente, la Russia abbia una ulteriore significativa arma di pressione (oltre a quella già considerevole del controllo di una significativa percentuale delle forniture di gas naturale di molti Paesi europei, in primis Germania e Italia).

Il fatto che gli attacchi cyber russi si siano per ora limitati al territorio ucraino non significa che ciò possa valere anche in futuro, soprattutto nel caso di un ulteriore acuirsi delle tensioni che potrebbe venir causato dall'incorrere di nuove sanzioni nei confronti della Russia o da un percorso di avvicinamento dell'Ucraina alla NATO o alla UE.

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

Angelo Socal

Laureato in Ingegneria Elettronica, ha conseguito un Master in "Geopolitica e Sicurezza Globale" presso "la Sapienza" e un Master in "Sicurezza Economica, Geopolitica e Intelligence (SEGI)" presso la "Società Italiana per l'Organizzazione Internazionale (SIOI)". Attualmente è Analista e Consulente di Sicurezza in Hermes Bay, dove si occupa di Enterprise Risk Management, Business Intelligence e Cyber Security. Inoltre, ha conseguito esperienze di docenza su diverse tematiche, tra cui Protezione delle Infrastrutture Critiche, Risk Management, Open Source Intelligence (OSINT) e Cyber Security presso diverse aziende, istituzioni e università.

ATTIVITA' DELL'ASSOCIAZIONE

ELEZIONI PER IL RINNOVO DEL CONSIGLIO DIRETTIVO DI AIIC

Il Consiglio Direttivo uscente, nella sua riunione del 28 gennaio 2022, ha deliberato di fissare al 6 e 7 giugno 2022, tramite piattaforma online, la data per le elezioni del nuovo Consiglio Direttivo.
Tutte le informazioni e il Regolamento Elettorale verranno messi a disposizione dei Soci quanto prima.

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:

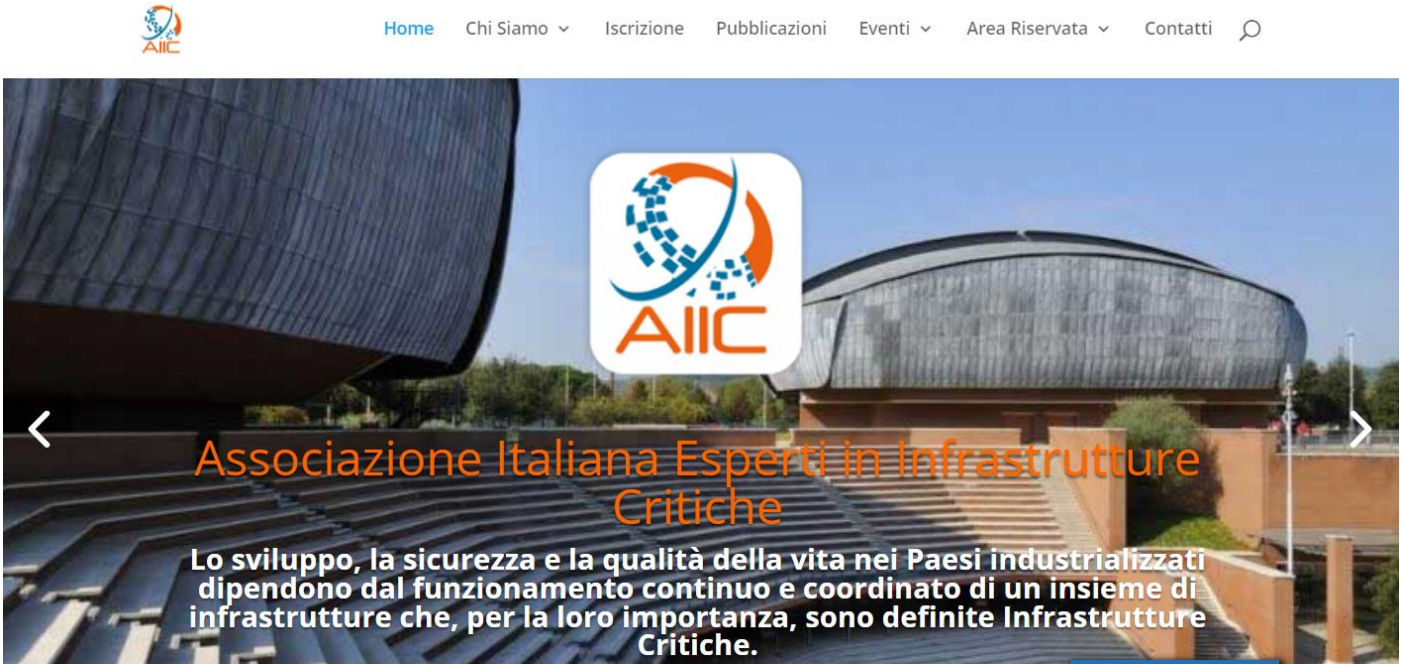
- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare 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 – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.

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'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.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.
Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.
Potete scriverci al nostro solito indirizzo email: segreteria@infrastrutturecritiche.it



GRUPPI DI LAVORO AIIC

Sono terminati i due Gruppi di Lavoro AIIC su "Disciplina normativa della criticità" coordinato da Luisa Franchina e su "Protezione degli spazi pubblici" coordinato da Sandro Bologna. I risultati, che verranno esposti in due apposite pubblicazioni, saranno presto disponibili attraverso il sito dell'Associazione e verranno presentati, ai soci e ai non soci, in occasione di prossimi incontri, in presenza o on-line.

RIPRENDONO I COLLOQUIA

Riprenderanno a breve i Colloquia, gli appuntamenti tra soci e simpatizzanti sui vari temi legati alle infrastrutture critiche.
Stiamo organizzando per il giorno 29 marzo p.v. una sessione dedicata alla sicurezza di alcune particolari infrastrutture connesse in rete.
Vi forniremo ulteriori particolari appena possibile.

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

Vi ricordiamo comunque che ogni socio può suggerire un argomento e proporsi come relatore in uno dei nostri incontri: è sufficiente scrivere una mail a segreteria@infrastrutturecritiche.it.

NEWS E AVVENIMENTI

Manutenzione e sicurezza, un insieme imprescindibile - La riflessione proposta approfondisce la funzione strategica della manutenzione come misura generale di tutela della sicurezza, per arrivare a prospettare la necessità di coltivare una cultura della manutenzione che va di pari passo con quella della sicurezza.
L'insieme sicurezza e manutenzione rispecchia la doppia faccia di una stessa medaglia. Il contributo evidenzia i vantaggi dell'adozione di un sistema di gestione della manutenzione, che può fare da motore al passaggio da una politica correttiva/riparativa a quella preventiva, nonché di qualificazione degli addetti alla manutenzione.
Manutenzione e sicurezza, un rapporto di bilateralità
Partiamo dall'etimologia del termine manutenzione che deriva dalla locuzione del latino medievale manu tenere, tenere con mano, tenere una cosa in modo che duri a lungo e rimanga in essere in efficienza. La manutenzione costituisce così un'attività strategica fondamentale per la conservazione e la sicurtà delle cose della nostra vita quotidiana, lavorativa e non, ed impatta prepotentemente sull'efficienza funzionale e sulla sicurezza degli ambienti, degli impianti, delle attrezzature e dei dispositivi, elementi indispensabili per garantire l'obiettivo principale, la sicurezza dei lavoratori e delle persone in generale.
Negli ambienti di lavoro questa prospettiva di bilateralità nel rapporto tra sicurezza e manutenzione è consolidata dalle norme di riferimento a tutela della salute e della sicurezza dei lavoratori e le norme, si sa, costituiscono un aspetto fondamentale per stabilire e indirizzare verso un comportamento condiviso. (continua...)
https://www.ingenio-web.it/33209-manutenzione-e-sicurezza-un-insieme-imprescindibile
INGENIO - *Bergagnin Stefano, Somma Rita - 18/01/2022*

La sicurezza antincendio nelle strutture sanitarie - In questo articolo si parla della sicurezza antincendio nelle strutture sanitarie, e in particolare di cosa prescrive la nuova Regola Tecnica che integra la Sezione V del Codice di Prevenzione Incendi e in quali casi si applica.
I provvedimenti da adottare nelle varie situazioni, la classificazione degli edifici in base alla tipologia dei servizi erogati, l'importanza della strumentazione. Il ruolo strategico dell'analisi dei rischi per individuare eventuali criticità.
L'articolo fa parte dell'inserto Block Notes della rivista A&B curata dagli Ingegneri della provincia di Genova che ha realizzato un documento monotematico contenente le Linee Guida per rinnovare la medicina territoriale con approccio ingegneristico.
(continua)
https://www.ingenio-web.it/33174-la-sicurezza-antincendio-nelle-strutture-sanitarie
INGENIO *- Bonavita Francesco, 18/01/2022*

Industrial Cybersecurity: cosa ci aspetta nel 2022 secondo Nozomi Networks - Ransomware sempre più orientato verso l'Europa e realtà di più piccole dimensioni, attacchi da parte di stati nazionali, una più stretta collaborazione tra pubblico e privato per proteggere le infrastrutture critiche, il crescente ricorso a soluzioni iperconvergenti, una forte attenzione alla sicurezza della supply chain e la definitiva consacrazione di Zero Trust

Indice degli argomenti

Ransomware: direzione Europa, nel mirino anche piccole realtà
Aumentano gli attacchi da stati nazionali
Collaborazione pubblico-privato, Zero Trust e iperconvergenza: le armi contro i cyber attack
(continua)

https://www.internet4things.it/sicurezza-iot/industrial-cybersecurity-cosa-ci-aspetta-nel-2022-secondo-nozomi-networks/

INTERNET4THINGS - *Claudia Costa, 18 Gennaio 2022*

Il 2022 dell'IoT tra piattaforme, interoperabilità e sicurezza - C'è una evoluzione costante che interessa tutto il mondo dell'Internet of Things. Dalle logiche di piattaforma nascono opportunità che abbracciano tutti i mondi e tutti i settori. Cosa ci aspettiamo in questo 2022?

Da tempo diciamo che l'Internet of Things (IoT) è una di quelle tecnologie che sta raggiungendo un nuovo livello di maturità. Prova ne è il fatto che vendor e analisti hanno smesso di misurare il mercato in base al numero di dispositivi venduti, ma in relazione alla numerosità e alla tipologia di applicazioni complete e funzionati sulle quali si lavora.

Indice degli argomenti

Un mercato sempre più maturo ha bisogno di piattaforme
Dalle applicazioni tradizionali alla sostenibilità: dove gioca la sua partita l'IoT
L'IoT Edge per la bassa latenza e per la privacy, Matter per l'interoperabilità
La sicurezza resta il vulnus
(continua….)

https://www.internet4things.it/iot-library/il-2022-delliot-tra-piattaforme-interoperabilita-e-sicurezza/

INTERNET4THINGS *- Maria Teresa Della Mura, 14 Gennaio 2022*

Verso il Perimetro di Sicurezza Nazionale Cibernetica: dalla localizzazione dei dati al nuovo ecosistema tecnologico - Lavori in corso per strutturare il nuovo Perimetro di Sicurezza Nazionale Cibernetica. Ecco gli obiettivi e alcune delle criticità individuate dall'Avv. Stefano Mele.

Tra gli obiettivi a livello governativo per i prossimi anni c'è l'istituzione del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) che coinvolgerà parte della Pubblica Amministrazione e delle aziende operanti in settori "sensibili". ZeroUno ne ha parlato con l'Avv. Stefano Mele, Partner presso Gianni&Origoni, ove è il Responsabile del Dipartimento Cybersecurity Law e co-Responsabile del Dipartimento Privacy.

ZeroUno: Quali sono le novità per le pubbliche amministrazioni e le aziende private che derivano dalla normativa sul Perimetro di Sicurezza Nazionale Cibernetica?

Il Perimetro di Sicurezza Nazionale Cibernetica guarda non a tutte le aziende e a tutte le pubbliche amministrazioni, perché non tutte le aziende e tutte le pubbliche amministrazioni sono importanti per la nostra sicurezza nazionale. Questa normativa, infatti, si focalizza esclusivamente su due ampie macro-categorie: la prima è quella dei soggetti pubblici che svolgono una funzione essenziale per lo

Stato, come ad esempio gli organi centrali e i ministeri. La seconda, è quella dei soggetti pubblici e privati che svolgono una funzione essenziale per gli interessi dello Stato, ove rientrano tutti quei soggetti che, per intenderci, erogano un servizio essenziale per i cittadini, come, ad esempio, le telecomunicazioni, i trasporti, l'energia, i sistemi bancari e finanziari, o ancora le infrastrutture digitali e tecnologiche. In definitiva, la normativa sul Perimetro di Sicurezza Nazionale Cibernetica riguarda tutti quei soggetti pubblici e privati per i quali un eventuale incidente (non solo un attacco cyber) posso avere un impatto rilevante per la nostra sicurezza nazionale. *(continua)*
https://www.zerounoweb.it/techtarget/searchsecurity/verso-il-perimetro-di-sicurezza-nazionale-cibernetica-dalla-localizzazione-dei-dati-al-nuovo-ecosistema-tecnologico/
ZEROUNOWEB *- Marco Schiaffino, 27 Gen 2022*

Sanità Digitale, uno sguardo al 2022: trend e prospettive - Dopo un 2021 da record in quanto ad investimenti in sanità digitale, il 2022 promette ulteriori passi avanti grazie alle risorse del PNRR. Telemedicina e monitoraggio remoto, AI e blockchain sono i trend di maggiore interesse.
Il 2021 è stato un anno importante nella sanità digitale. Riferendosi al mercato americano, Rock Health parla infatti di "grandi cambiamenti nell'healthcare" con riferimento alle infrastrutture, ai modelli di business e anche alla maggiore disponibilità di talenti, che renderanno ancor più tangibili gli effetti della trasformazione digitale a partire da quest'anno.
Indice degli argomenti
Un mercato in fortissima crescita in tutto il mondo
Dalla telemedicina a blockchain, i trend del 2022 in sanità digitale
Telemedicina, arriva la Piattaforma Nazionale
L'anno delle terapie digitali
Remote Patient Monitoring
La centralità della Patient Experience
Decentralizzazione dei dati sanitari
Intelligenza Artificiale sempre più pervasiva (continua….)
https://www.zerounoweb.it/trends/sanita-digitale-uno-sguardo-al-2022-trend-e-prospettive/
ZEROUNOWEB *- Emanuele Villa, 31 Gen 2022*

Fleets Can Take Steps to Reduce Risk of Cybersecurity Threats Cybersecurity breaches are an ever-present danger for all types of businesses, and freight transportation companies are no exception.It may not be possible to eliminate this threat entirely, but with the right safeguards in place, trucking and logistics companies can reduce the risk of being hacked or falling victim to a ransomware attack, industry experts said.
"We are a heavily targeted industry," said Cory Staheli, chief information officer at motor carrier Trans-System Inc. Staheli believes that hackers often perceive trucking companies as easy targets based on the assumption that they lack the sophistication and resources to properly protect themselves online. And those hackers are not merely kids in a basement getting into mischief. "We need to understand what we're up against," Staheli said. "These guys are highly organized criminals. They are trying everything they can to take our money from us."
Trans-System, based in Cheney, Wash., is the parent corporation of three trucking companies — flatbed hauler System Transport, TWT Refrigerated Service and bulk carrier James J. Williams. Trans-System ranks No. 95 on the Transport Topics Top 100 list of the largest for-hire carriers in North America.

Industry experts said cyberattacks are increasing in both frequency and complexity. It's not a question of if, but when a cybersecurity breach will happen at your company, said Joe Russo, head of information technology at Isaac Instruments, a supplier of electronic logging devices and fleet-management technology.
Wally Stegall, a corporate technical fellow with fleet telematics vendor Morey Corp., agreed.
"No fortress is impregnable," Stegall said. "In cybersecurity, that is just a fact."
In recent years, the increase in remote work has created even more security challenges.
As the COVID-19 pandemic took hold and working from home became much more common, it provided easier access for cyber criminals, Russo said in a presentation during Isaac Instruments' virtual user conference in November.
Cyberattacks increased three- to five-fold from the pre-COVID days, he said, primarily because many organizations were not adequately prepared for the abrupt shift to remote work.
"They weren't prepared to give everyone their own laptop so people used their personal laptop," Russo said. "If you do that, you don't know if that personal laptop is protected or had security tools. That is how we've seen an increase in breaches — through those home devices that were never patched, not protected, had back doors, had the threat agent waiting to collect the keyboard entry to see how they connect back to the home office. Then he's opened the door. He's in. If you don't have countermeasures, they have accessed all the data." (continua…)
https://www.dailyadvent.com/news/a879fdbfa24e9635969c76d00500be95-Fleets-Can-Take-Steps-to-Reduce-Risk-of-Cybersecurity-Threats
***Dailyevent**-Hilary Daninhirsch -February 1, 2022*

NEW YORK Adams eyes expansion of highly controversial police surveillance technology . The Democratic mayor's bullishness and the resources at his fingertips stand to put New York at the forefront of an evolving national debate over safety, privacy and the racial and gender biases tied to the controversial software.
NEW YORK — Civil rights groups sued over its constitutionality. State legislatures are studying ts efficacy. San Francisco declared it antithetical to democracy.
But the mayor of the nation's most populous city is fully embracing the use of facial recognition technology by the police and is now exploring a dramatic expansion in how it is used. Eric Adams, a centrist Democrat, is so convinced modern technology can accurately and ethically help identify perpetrators of crimes he has incorporated it into his plan for fighting an outbreak of violence in New York.
"If you're on Facebook, Instagram, Twitter — no matter what, they can see and identify who you are without violating the rights of people," Adams said late last month as he pushed a new plan to end gun violence. "It's going to be used for investigatory purposes."
Facial recognition software has long been employed by governments across the world to assist in criminal probes and to screen people entering sensitive sites, from sports stadiums to customs checkpoints. An image captured from a surveillance video is compared to a photo database of known individuals, which increasingly includes billions of pictures scraped from social media. The software throws up a flag when, with some degree of probability, it spots a match.
But as other American cities have retreated from the technology or banned it altogether, Adams' bullishness and the resources at his fingertips — the city is set to spend around $11 billion on the NYPD this budget cycle — stand to put New York at the forefront of an evolving national debate over safety, privacy and the racial and gender biases tied to the controversial software.

The NYPD has been using facial recognition technology for more than a decade, prompting at least six lawsuits and inspiring a New York statute mandating reams of public reporting. The same software used by the city, DataWorks Plus, led to the wrongful arrest of two men in Detroit.
Police officials have credited the tool with helping to solve murders, rapes and missing person cases, and they stress it is used fairly and only in a narrow capacity.
Now the mayor wants to go further.
"We will also move forward on using the latest in technology to identify problems, follow up on leads and collect evidence — from facial recognition technology to new tools that can spot those carrying weapons, we will use every available method to keep our people safe," Adams, a retired police captain, said at a Jan. 24 press briefing.
A week later, he alluded to replacing metal detectors at public schools with new technology to scan students for weapons. A City Hall aide separately said the administration is exploring the use of infrared or thermal imaging cameras in the buildings. (continua…)
https://www.politico.com/news/2022/02/08/adams-police-surveillance-technology-00006230
***POLITICO**-SALLY GOLDENBERG,JOE ANUTA- 02/08/2022*

Cybersecurity and Data Privacy – What to expect in 2022

Threats to cybersecurity and data privacy are constantly increasing both in volume and complexity. This trend is expected to continue in 2022. In a bid to protect cybersecurity and ensure data is properly safeguarded, countries around the world are introducing new laws focused on cybersecurity and data protection. Armed with new legal frameworks, regulators and law enforcement are placing onerous obligations on organisations who fall victim to cybersecurity breaches. There are shorter deadlines in which to notify the authorities of data breaches and ever increasing fines and penalties for businesses that fail to respond swiftly and appropriately to a cyberattack.
In this ever-changing area what is on the horizon for 2022?
Legal Changes
The United Kingdom, fresh from leaving the European Union has already indicated that there will be data privacy law changes. Chancellor Rishi Sunak has said that the General Data Protection Rules (GDPR) are not necessary and pointed to what he called "sensible countries" such as Japan, Switzerland and Canada who have established and respected data rules. The Chancellor has explained that the UK Government wants to "protect individual data but we don't want to hinder innovation, and the whole view is that there are things that we can change that will be pro-innovation whilst protecting rights and getting rid of some of the box-ticking and ending up in a good place that is net positive for the UK".
In the US, following on from the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) other States are enacting their own privacy legislation. The Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (ColoPA), and A.430/S.2628 in New York; will be effective 1st January 2023, 1st July 2023, and May 2022 respectively. Many other States have active bills working their way through legislature, with at least 45 states and Puerto Rico having introduced or considered more than 250 bills or resolutions through 2021 that deal with cybersecurity.
In the last few months China's new data protection law, the Personal Information Protection Law (PIPL) took effect. Broadly, it is similar to the GDPR in a number of key aspects. It has extra-territorial reach. In some areas it introduces more stringent requirements than under the GDPR. Organisations who transfer or gather data that comes within the scope of PIPL need to take steps urgently to ensure they are complying.

The United Arab Emirates have introduced data protection legislation this month, Federal Decree Law on the Protection of Personal Data. It has notable similarities to the GDPR. It also has extra-territorial reach. The law is so new that it is not yet known how it will be applied by the UAE authorities.
Cyber Attack Trends (continua…)
https://www.jdsupra.com/legalnews/cybersecurity-and-data-privacy-what-to-2900519/
JDSUPRA - *Andrew Thornton-Dibb, Francesca Titus -February 2, 2022*

You've got backup – but how safe are you? Most businesses have backup facilities in place to help them in the event of a data breach or physical disaster that renders their offices or data unusable. But how many know that they can retrieve that data and have their business up and running again in minutes?
Server room floods, ransomware, fires – however your data is damaged, lost or digitally encrypted – do you know how quickly you can retrieve it or even if you can? iland found in a recent survey that just 50% of businesses are testing their disaster recovery (DR) plans only annually or at less frequent intervals, while seven percent did not test their DR at all. Of the organisations testing less frequently, half said their disaster recovery plan may be inadequate based on their most recent DR test, while 12% encountered issues that would result in sustained downtime. Zero respondents said that their DR test was completely or moderately successful. Everyone reported experiencing issues.
So, with most companies remaining badly behind the curve, what steps are needed to ensure that you can retrieve your data after a data breach or disaster?
Understanding your data
The datasets of organisations are huge, but the ability to retrieve 100s of terabytes in minutes is like having a spare car in your garage just in case your main one doesn't work – it's expensive to have it all waiting on the off chance you need it. And the faster you need it back, the more it costs.
Therefore, a core aspect of a DR strategy is to prioritise the data that is most critical to the business and focus your efforts around protecting that data first. To understand your data, look at your entire estate and define what's critical to your business operations. Prioritise it in order of how it would impact customer delivery most if lost. It will give you a focus, and in turn, you can develop measures to minimise data loss in the event of a cyber-attack or disaster. You can also catalogue it by how much data can be lost by invoking a recovery (RPO) and its priority for recovery (RTO). (continua…)
https://www.globalbankingandfinance.com/youve-got-backup-but-how-safe-are-you/
GLOBALBANKING-Ian Richardson -*2022-02-08*

Texas alleges Facebook's facial recognition practices violated privacy protections
Texas is suing Facebook over allegations that the social media giant violated Texans' privacy through the company's previous use of facial recognition technology, according to a complaint filed Monday. "Facebook will no longer take advantage of people and their children with the intent to turn a profit at the expense of one's safety and well-being," Texas Attorney General Ken Paxton (R) said in a statement. "This is yet another example of Big Tech's deceitful business practices and it must stop. I will continue to fight for Texans' privacy and security."
The lawsuit alleges Facebook, now under the parent company Meta, captured biometric data of Texans for commercial purposes without their informed consent and failed to destroy collected identifiers within a reasonable time.

The lawsuit also alleges that Facebook violated the privacy of people who were not even users on the platform by collecting biometric identifiers from photos and videos "innocently uploaded by friends and family who did use Facebook."
"There was no way for such non-users to know of or contest this exploitation," the complaint states.
The lawsuit was first reported by The Wall Street Journal. A person familiar with the matter told the Journal the lawsuit seeks civil penalties in the hundreds of billions of dollars.
A Meta spokesperson denied the allegations in the lawsuit.
"These claims are without merit and we will defend ourselves vigorously," the spokesperson said in a statement.
Facebook settled a separate class-action lawsuit, based around Illinois privacy law, over its use of facial recognition for about $650 million in 2020.(continua…)
Https://thehill.com/policy/technology/594139-texas-alleges-facebooks-facial-recognition-practices-violated-privacy
THE HILL *- REBECCA KLAR-02/14/22*

Russia-linked threat actors breached US cleared defense contractors (CDCs)

Russia-linked threat actors have breached the network of U.S. cleared defense contractors (CDCs) since at least January 2020.
According to a joint alert published by the FBI, NSA, and CISA, Russia-linked threat actors conducted a cyber espionage campaign aimed at US cleared defense contractors to steal sensitive info related to intelligence programs and capabilities.
CDCs support contracts for the U.S. Department of Defense (DoD) and Intelligence Community in multiple areas:

- Command, control, communications, and combat systems;
- Intelligence, surveillance, reconnaissance, and targeting;
- Weapons and missile development;
- Vehicle and aircraft design; and
- Software development, data analytics, computers, and logistics.

The campaign has been active since at least January 2020 and several US cleared defense contractors were breached by the nation-state actors.
The attackers targeted CDCs and subcontractors of any size with varying levels of cybersecurity protocols and resources.
"From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors." reads the joint alert. "The actors leverage access to CDC networks to obtain sensitive data about U.S. defense and intelligence programs and capabilities. Compromised entities have included CDCs supporting the U.S. Army, U.S. Air Force, U.S. Navy, U.S. Space Force, and DoD and Intelligence programs."
Threat actors employed similar tactics in many attempts to compromise enterprise and cloud networks. Attackers seem to focus their efforts on attacks against organizations using Microsoft 365 (M365) environment. The actors were able to maintain persistence by using legitimate credentials and a variety of malware that was used for data exfiltration. In some cases, cyberspies have maintained persistence for at least six months.
"These continued intrusions have enabled the actors to acquire sensitive, unclassified information, as well as CDC-proprietary and export-controlled technology." states the report. "By acquiring proprietary internal documents and email communications, adversaries may be able to adjust their own military plans

and priorities, hasten technological development efforts, inform foreign policymakers of U.S. intentions, and target potential sources for recruitment."
The alert provides recommendations on how to detect malicious activity and respond in case of compromise. (continua…)
HTTPS://SECURITYAFFAIRS.CO/WORDPRESS/128099/CYBER-WARFARE-2/RUSSIAN-HACKERS-BREACHED-CLEARED-DEFENSE-CONTRACTORS.HTML
Security Affairs *-Pierluigi Paganini - February 16, 2022*

La risposta di Usa e alleati agli attacchi cyber in Ucraina
Colpiti ministeri e banche di Kiev. Sventata un'offensiva contro l'intelligence. "Ecco perché non è una minaccia alla sicurezza nazionale", spiega l'avvocato Mele (Gianni&Origoni). L'Occidente lavora ad azioni di ritorsione o sanzioni a seconda della gravità delle aggressioni. Ma la portata delle stesse e le difficoltà nell'attribuzione delle responsabilità rappresentano una zona grigia già sfruttata dalla Russia
Gli Stati Uniti e i loro alleati sono pronti a rispondere agli attacchi informatici russi contro l'Ucraina con azioni di ritorsione o sanzioni a seconda della gravità delle offensive. È quanto dichiarato da funzionari americani ed europei poche ore dopo l'attacco che nella giornata di martedì 15 febbraio ha colpito due banche statali ucraine, PrivatBank e Oschadbank, e il sito web del ministero della Difesa. Il governo di Kiev l'ha definito il più grande attacco DDoS (Distributed Denial of Service) nella storia del Paese e ha spiegato che ne è stato bloccato uno contro il Servizio di sicurezza statale.
Come ha ricordato all'agenzia Reuters un diplomatico europeo, gli attacchi cibernetici sono una componente storica della strategia di Mosca, che li ha già utilizzati nei passati confronti militari con Georgia e con la stessa Ucraina. È la guerra ibrida, fatta anche di campagne di disinformazione. "Fa parte del loro manuale", ha detto il diplomatico, sottolineando la volontà occidentale di un'azione concertata per inchiodare la Russia per i cyberattacchi e altri "comportamenti scorretti".
Tuttavia, il pacchetto di sanzioni che i funzionari statunitensi, europei e canadesi hanno elaborato in caso di invasione russa dell'Ucraina non prevede un piano per la risposta agli attacchi informatici.
Ciò è frutto, almeno in parte, delle difficoltà di attribuire le responsabilità di attacchi DDoS, processo che può richiedere anche molto tempo. Inoltre, ci sono anche Paesi, come la Francia per esempio, piuttosto restii a puntare pubblicamente il dito contro i criminali informatici, specie se alle loro spalle c'è uno Stato.
L'altro aspetto da considerare in queste valutazioni è la portata dall'attacco. "Stando a quanto noto finora, non definirei l'attacco che martedì ha colpito l'Ucraina come un minaccia alla sicurezza nazionale", spiega **Stefano Mele**, partner e responsabile della cybersecurity dello Studio Gianni&Origoni, a *Formiche.net*. "La Russia ha una lunga tradizione di attacchi portati volutamente sotto la soglia dell'uso della forza secondo il diritto internazionale, in modo da impedire una risposta", osserva. (continua…)
https://formiche.net/2022/02/attacco-hacker-ucraina-stefano-mele/
Formiche *- Gabriele Carrer - 16/02/2022*

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/

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

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 newsletter	Nella sezione "Newsletter"del sito 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.