Newsletter

ANNO 2024	n. 02/ 2024	febbraio 2024

Attacchi informatici in aumento: il "2023 Global Threat Roundup" di Forescout conferma tendenze allarmanti

Negli ultimi anni, la sicurezza informatica è stata sempre più oggetto di analisi approfondite da parte di diverse aziende specializzate. I loro report offrono una panoramica completa delle tendenze e delle problematiche che caratterizzano l'attuale contesto della cybersecurity. Tra i report più recenti, emerge il "Global Threat Roundup" di Forescout che fornisce un quadro aggiornato delle minacce globali odierne. L'analisi dei dati provenienti dall'Adversary Engagement Environment (AEE) dell'azienda, evidenzia un significativo aumento degli attacchi informatici, con oltre 420 milioni di incidenti registrati tra gennaio e dicembre 2023. Questo incremento del 30% rispetto all'anno precedente dimostra la crescente sofisticazione e audacia degli attaccanti. Il rapporto rivela che nel corso del 2023 gli attori malevoli, principalmente costituiti da cybercriminali e "state-sponsored actors", hanno preso di mira 163 Paesi. Gli Stati Uniti si trovano al vertice della lista dei bersagli con 168 attaccanti accertati, seguiti dal Regno Unito (88) e dalla Germania (77). La maggior concentrazione di minacce è stata individuata in Cina (155 attori), Russia (88) e Iran (45), i quali, insieme ospitano la metà dei gruppi di attaccanti a livello globale. Tra i settori più colpiti, emerge una significativa risonanza nei contesti governativi e finanziari, dove la complessità delle infrastrutture e l'ampia portata di dati sensibili rendono tali settori particolarmente vulnerabili agli attacchi informatici in continua evoluzione. Una delle evidenze più preoccupanti del rapporto è l'aumento degli attacchi informatici provenienti dalla Cina. Nel 2023 gli attacchi hanno avuto origine da 212 Paesi, mentre i primi dieci Paesi hanno rappresentato il 77% del traffico dannoso, la Cina, al secondo posto nella classifica, si è distinta con un significativo aumento del suo volume di attacchi rispetto all'anno precedente (+4%). Questa tendenza solleva preoccupazioni significative, richiamando l'attenzione sulla necessità di una collaborazione internazionale più stretta per affrontare le sfide della sicurezza informatica e sviluppare strategie efficaci di difesa cibernetica. Le web application (28% degli attacchi) e i protocolli di accesso remoto (26%) sono emersi come le tipologie di servizi più colpiti nel 2023. Gli attaccanti hanno sfruttato le vulnerabilità in questi servizi per ottenere l'accesso non autorizzato a reti e sistemi, spesso con l'intenzione di rubare dati sensibili o interrompere le operazioni. Inoltre, i cybercriminali stanno orientando sempre più i loro attacchi sui dispositivi IoT (Internet of Things) e sulle componenti delle infrastrutture di rete per ottenere l'accesso alle reti aziendali. Il rapporto ha rilevato un aumento dell'uso di exploit contro i dispositivi IoT, probabilmente a causa della loro crescente diffusione e della loro spesso debole postura di sicurezza. In modo preoccupante si evidenzia che la Cybersecurity and Infrastructure Security Agency (CISA), un'agenzia statunitense, nelle sue documentazioni aggiornate, copre solo circa il 35% delle vulnerabilità sfruttate conosciute. Ciò suggerisce che le organizzazioni potrebbero essere soggette agli attacchi che sfruttano vulnerabilità non ancora note o pubblicamente divulgate. In merito alle tipologie di malware utilizzate, i trojan di accesso remoto (RAT) (26%), gli infostealer (26%) e le botnet (22%) rimangono gli strumenti più popolari. Questo scenario riflette una diversificazione delle minacce digitali, con attaccanti che sfruttano una gamma sempre più ampia di vettori e strategie per compromettere la sicurezza delle reti e dei sistemi informativi.

Il “2023 Global Threat Roundup” di Forescout si colloca nella serie di report (che include anche quelli di origine non aziendale come il rapporto Clusit e il “Threat Landscape” di ENISA) che complessivamente delineano una situazione di crescente allarme per la sicurezza informatica a livello globale. Emergono le sfide crescenti e l'ampia portata delle minacce digitali che mettono a rischio organizzazioni di ogni settore e dimensione. Si evidenzia anche una costante evoluzione delle minacce informatiche e la conseguente necessità di adottare un approccio possibilmente proattivo alla sicurezza informatica. La complessità e la sofisticazione degli attacchi impongono a tutte le organizzazioni, pubbliche e private, di rivedere e potenziare costantemente le proprie difese e di adattarsi dinamicamente alle nuove tecniche usate dagli aggressori.

Marco Raul Massoni Laureato in “Scienze della Politica” presso l’Università degli Studi di Macerata. Ha conseguito un master 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 svolge attività di consulenza in materia di cybersecurity

ATTIVITA’ DELL’ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2024

Il 31 dicembre 2023 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare con sollecitudine l’iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale “rinnovo socio ordinario nome e cognome anno 2024”.
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it.
Ricordiamo che **la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2024. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione versando anche il contributo per le spese di segreteria.**
La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è 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.
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*

MANIFESTAZIONE DI INTERESSE

VISITA GUIDATA
AL CORPO NAZIONALE DEI VIGILI DEL FUOCO

Riprendendo il nostro programma di visite sul campo, abbiamo la disponibilità di massima ad organizzare una **visita guidata** presso il **Centro Studi ed Esperienze (CSE) del Corpo Nazionale Italiano dei Vigili del Fuoco** situato in Roma, via delle Capannelle.

Il programma di massima prevede:

- presentazione delle principali attività del Centro Sudi ed Esperienze;
- visita ai laboratori di prova dei materiali (Scienza delle costruzioni, Difesa Atomica, Macchine e Termotecnica, Elettrotecnica, Idraulica);
- indicazioni sull'utilizzo dei materiali nella realtà delle costruzioni civili e industriali;
- attività del Nucleo Investigativo Antincendio (NIA).

La visita potrebbe essere effettuata nel **periodo metà marzo-aprile 2024**, durata prevista 3 ore, luogo di incontro via delle Capannelle – Roma, da raggiungersi con mezzi propri.

Poiché la visita è soggetta ad un numero minimo ed uno massimo di partecipanti, e bisogna prevedere i tempi per i permessi di ingresso, chiediamo di esprimere il proprio interesse – non vincolante – a partecipare, rispondendo via mail a: segreteria@infrastrutturecritiche.it entro il giorno 29 febbraio p.v.
Qualora si raggiunga il numero minimo di interessati, procederemo con l'organizzazione e l'apertura delle iscrizioni.

Attenzione! La visita è riservata ai soli soci AIIC in regola con il pagamento delle quote sociali. I signori non-soci che volessero partecipare, possono iscriversi all'Associazione AIIC usufruendo di una quota di associazione minima (euro 50 anno + 10 una tantum).
Le modalità per l'iscrizione si trovano sul sito www.infrastrutturecritiche.it o si possono richiedere inviando una mail a segreteria@infrastrutturecritiche.it

Il Centro Studi ed Esperienze (CSE) del Corpo Nazionale Italiano dei Vigili del Fuoco è stato istituito nel 1961 ed è ospitato nelle Scuole Centrali Antincendi di Capannelle a Roma.
Da oltre sessanta anni il contributo del Centro Studi è stato di ricerca applicata attraverso i suoi laboratori di prova dei materiali (Scienza delle costruzioni, Difesa Atomica, Macchine e Termotecnica, Elettrotecnica, Idraulica) con le correlate indicazioni in merito al loro utilizzo nella realtà delle costruzioni civili e industriali del Paese. Nell'ultima legge di riordino del Corpo Nazionale il CSE è stato integrato dalle attività del Nucleo Investigativo Antincendio (NIA).

Un cordiale saluto a tutti.

Silvano Bari
Vice presidente AIIC

NEWS E AVVENIMENTI

Perché il riconoscimento facciale sarà incubo inevitabile: i segnali forti - Un'inchiesta del Telegraph toglie il velo all'utilizzo "disinvolto" del riconoscimento facciale da parte della polizia giudiziaria del Regno Unito. In Italia è stato introdotto un divieto generale di utilizzo di queste tecnologie che probabilmente permarrà fino a che l'AI Act non sarà approvato definitivamente. Ma di certo dovremo imparare a conviverci

Le foto dei passaporti dei cittadini britannici vengono utilizzate per indagini di polizia: solo nei primi nove mesi del 2023 un passaporto su tre è stato "controllato" per il matching in indagini di polizia. In Europa – e in Italia – non è ancora possibile (e speriamo che resti così a lungo). È quanto emerge da un'inchiesta pubblicata dal quotidiano britannico Telegraph, che ha svelato quanto diffuso sia sull'utilizzo del riconoscimento facciale in Gran Bretagna.

Indice degli argomenti

Cosa emerge dall'inchiesta UK sull'uso massivo del riconoscimento facciale

Riconoscimento facciale, la posizione Ue

Lo stato dell'arte in Italia

Conclusioni

(continua…)

https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-una-realta-inquietante-a-cui-dobbiamo-abituarci/

Agenda Digitale *- Massimo Borgobello – 12 gennaio 2024*

Come mettere sotto controllo attacchi terroristici diretti ad una folla - Un prezioso strumento informatico, che permette di inquadrare il rischio di attacchi terroristici diretti a raggruppamenti di persone, offrendo anche indicazioni sulle possibili strategie di mitigazione e messa sotto controllo di questi drammatici eventi.

Gli attacchi di massa al pubblico, siano essi motivati da ragioni personali o ideologiche, come ad esempio il caso di un attacco terroristico di origine religiosa, causano molta preoccupazione e paura. Ciononostante, spesso è possibile intraprendere azioni che possono consentire di prevenire, difendersi e rispondere agli attacchi di massa.

Un recente progetto di ricerca finanziato dal NIJ (National Institute of Justice) ha analizzato oltre 600 scenari di attacchi di massa, centinaia di articoli e risorse e dozzine di interviste ad esperti, per sviluppare il Mass Attacks Defense Toolkit 2, un toolkit educativo online con strategie, indicazioni e collegamenti a risorse aggiuntive. Il toolkit è disponibile al link https://www.rand.org/pubs/tools/TLA1613-1.html

Ecco le cinque principali aree esaminate nel documento. *(continua…)*

https://www.puntosicuro.it/criminalita-C-105/come-mettere-sotto-controllo-attacchi-terroristici-diretti-ad-una-folla-AR-23950/

PuntoSicuro *- Adalberto Biasiotti - 17/01/2024*

Rafforzamento della resilienza cibernetica in Italia: nuovi fondi e iniziative strategiche

Prosegue il percorso dell'Italia verso un rafforzamento delle misure di contrasto ai crimini informatici a tutela delle infrastrutture digitali nazionali. Ecco come verranno gestiti i nuovi finanziamenti europei destinati al potenziamento della sicurezza del Paese e le iniziative intraprese per affrontare le sfide della cyber security

Il ministro della Giustizia Carlo Nordio ha di recente ribadito la volontà del governo italiano di **rafforzare**, in linea con le disposizioni intraprese per fronteggiare le minacce nel dominio cyberspazio, le **misure volte al contrasto dei crimini informatici** a tutela delle infrastrutture digitali nazionali.

Tale necessità deriva dall'incremento delle minacce informatiche che l'Italia si trova ad affrontare: secondo l'ultimo **rapporto Clusit**, infatti, nel primo semestre 2023 gli attacchi subiti dall'Italia sono aumentati del +40% rispetto al 2022. In termini percentuali, inoltre, questo aumento si presenta maggiore rispetto alla crescita osservata a livello globale, che nello stesso periodo di riferimento è pari all'11%.

Nel contesto italiano, le istituzioni risultano essere le più colpite. Queste, infatti, rappresentano il 23% del totale degli attacchi infornatici registrati nel Paese, seguite dal settore manifatturiero con il 17%. Per quanto concerne la tipologia, gli **attacchi DDoS** hanno registrato un aumento del 30%, cinque volte la media globale, ma anche gli **attacchi di phishing** e **ingegneria sociale** incidono maggiormente in Italia (14%) rispetto al resto del mondo (8,6%).

Indice degli argomenti

Gli obiettivi della nuova strategia cyber italiana

A fronte di questo scenario, l'Italia ha maturato la decisione di definire una strategia che possa permetterle di conseguire un duplice obiettivo.

Da un lato contrastare l'incremento degli attacchi, in considerazione non solo ai danni connessi ma anche all'ingente dispendio di energie e di risorse, specialmente economiche, per poter porre un argine al fenomeno.

Dall'altro implementare misure volte a promuovere lo sviluppo di azioni coerenti non solo con gli interessi nazionali, ma anche in sintonia con la necessità di proteggere le infrastrutture digitali in un contesto più ampio, collaborando con le istituzioni europee e gli stati membri, al fine di ampliare la coesione e il supporto nell'ambito della cyber sicurezza.

Cyber security: serve maggiore coordinamento europeo

La necessità di un maggiore coordinamento a livello europeo in ambito cyber security è stata **espressa** anche nel contesto dell'Euro Cyber Resilience Board (ECRB), un forum di discussione strategica tra infrastrutture di mercato finanziario europee, fornitori di servizi essenziali, supervisori delle banche centrali e altre autorità europee, tra i cui obiettivi è incluso l'incremento della consapevolezza sulla resilienza cibernetica.

In occasione del nono meeting dell'ERCB, infatti, Piero Cipollone, membro del comitato esecutivo della banca centrale europea, ha rimarcato come una inadeguata risposta al malfunzionamento del sistema finanziario a causa dei danni provocati dagli attacchi informatici possa condurre ad una condizione di rischio sistemico.(continua…)

https://www.cybersecurity360.it/cybersecurity-nazionale/rafforzamento-della-resilienza-cibernetica-in-italia-nuovi-fondi-e-iniziative-strategiche/
Cybersecurity360 *- Luisa Franchina, Matteo Cicarelli, Virginia Bernini - 25 Gen 2024*

Pwn2Own 2024: Tesla Hacks, Dozens of Zero-Days in Electrical Vehicles

Hacking teams pick apart electrical vehicles (EVs), exposing them for what they are: safety-critical computers without commensurate security.

In just two days at Pwn2Own 2024 in Tokyo, researchers have compromised a bevy of electric vehicle chargers, operating systems, Tesla components, and unearthed dozens of zero-day vulnerabilities along the way.

Last year's Pwn2Own in Vancouver flirted with cars as an attack surface, adding Teslas into the mix alongside competitions to hack more traditional servers, enterprise applications, browsers, and the like. But this year's event went full pedal to the metal, and the results have been enlightening. On the first day alone, contestants demonstrated 24 unique zero-days, earning them $722,500 in winnings. Day two saw 20 new exploits, and the final, third day promises nine more still.

"Vehicles are increasingly becoming a complex system of systems," says Dustin Childs, head of threat awareness for Trend Micro's Zero Day Initiative (ZDI), the group hosting the event. "There hasn't been a lot of research into this area in the past, and based on our experience, that lack of external scrutiny means there could be a lot of security issues."

Hacking Into Teslas

The headline-grabbing event at last year's Pwn2Own was when a team from Toulouse-based Synacktiv managed to breach a Tesla Model 3 in under two minutes.

This year, Synacktiv has returned with exploits of the Ubiquiti Connect and JuiceBox 40 Smart EV charging stations, the ChargePoint Home Flex (an at-home EV charging tool), and the self-explanatory Automotive Grade Linux. Its most notable achievements, though, have been a three-bug exploit chain against Tesla's modem, and a two-bug chain against its infotainment system, each earning a $100,000 cash prize.

According to the rules of the event, vendors have 90 days to remediate their security flaws before they're allowed to be publicly disclosed. But in an email from Tokyo, the Synacktiv crackers gave Dark Reading a high-level overview of what the attacks looked like:

"The attack is sent from a GSM antenna emulating a fake BTS (rogue telecom operator). A first vulnerability gives root access to the modem card of the Tesla," they wrote. "A second attack jumps from the modem to the infotainment system. And bypassing the security features on this process, it's possible to access multiple equipment on the car such as the headlights, the windshield wipers, or to open the trunk and the doors."

With Teslas, says Synacktiv CEO Renaud Feil, "it's a two-sided coin. It's a car that has a huge attack surface — everything is IT in a Tesla. But they also have a strong security team and they try to pay a lot of attention to security. So it's a huge target, but it's a difficult target."

Modern Cars at a Crossroads

"The attack surface of the car it's growing, and it's getting more and more interesting, because manufacturers are adding wireless connectivities, and applications that allow you to access the car remotely over the Internet," Feil says. (continua…)

https://www.darkreading.com/ics-ot-security/pwn2own-2024-teslas-hacked-dozens-new-zero-days-evs
DARKREADING *- Nate Nelson- January 25, 2024*

DDL Cybersicurezza: ambizioni alte, ma mancano i fondi

Il Consiglio dei Ministri ha approvato un disegno di legge per rafforzare la cybersicurezza, potenziando l'ACN e istituendo l'obbligo di segnalazione rapida di incidenti informatici. Il ddl introduce sanzioni per mancate notifiche e crea la figura del referente per la cybersicurezza nelle PA, ma non prevede fondi aggiuntivi per implementare le misure e lascia fuori…

Il nuovo disegno di legge in materia di reati informatici e di rafforzamento della cybersicurezza nazionale, approvato il 25 gennaio dal Consiglio dei Ministri, pone le basi per rispondere alle sfide imposte dal mondo digitale, ma solleva interrogativi e dubbi, soprattutto per quanto riguarda l'assenza dell'Intelligenza Artificiale (IA) e la mancanza di risorse economiche.

Indice degli argomenti

Nuove misure per rafforzare la difesa digitale del paese: il ruolo dell'ACN

Partiamo da un'analisi delle nuove disposizioni-. In un contesto sempre più vulnerabile alle minacce informatiche, il governo ha deciso di potenziare le funzioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), con un particolare focus sul coordinamento con l'Autorità giudiziaria in caso di attacchi informatici.

Lo stesso coordinamento operativo è previsto anche tra i servizi di informazione per la sicurezza (DIS) e l'Agenzia per la cybersicurezza nazionale.

Il cuore di queste nuove disposizioni è rappresentato da specifiche procedure che mirano a rendere più immediato l'intervento dell'ACN per prevenire attacchi e mitigare le conseguenze, garantendo il rapido ripristino delle funzionalità dei sistemi informatici.

L'obbligo di segnalazione e notifica per determinati soggetti pubblici

Infatti, un importante passo avanti è stato compiuto attraverso l'istituzione di un obbligo di segnalazione e notifica per determinati soggetti pubblici. Le pubbliche amministrazioni centrali, con le rispettive società in-house, le Regioni e le Province autonome di Trento e Bolzano, i comuni con una popolazione superiore ai 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e le aziende sanitarie locali, devono segnalare e notificare gli incidenti informatici subiti aventi impatto su reti, sistemi informativi e servizi informatici.

I soggetti indicati devono segnalare tempestivamente all'ACN, e in ogni caso entro 24 ore dalla scoperta dell'incidente, fornendo una notifica completa entro 72 ore dalla stessa data.

Le sanzioni in caso di mancata notifica

Le sanzioni per la mancata notifica sono incisive. (continua…)

https://www.agendadigitale.eu/sicurezza/ddl-cybersicurezza-ambizioni-alte-ma-mancano-i-fondi/

AgendaDigitale **-** *Andrea Tironi -26 gennaio 2024*

Grandi infrastrutture: le sfide tecniche dei sistemi per il monitoraggio strutturale di ponti e gallerie - Le grandi infrastrutture sopra e sotto terra rappresentano il centro nevralgico della rete di trasporti nazionale. Pertanto, queste richiedono un costante sorveglianza delle loro condizioni.

Tuttavia, gli obbiettivi del monitoraggio di ponti e gallerie, specialmente se situati in aree di rischio sismico, divergono. È quindi cruciale comprenderne a fondo le diverse priorità. Solo dopo aver acquisito questa comprensione è possibile valutare le tecniche da impiegare. *(continua…)*
https://www.ingenio-web.it/articoli/grandi-infrastrutture-le-sfide-tecniche-dei-sistemi-per-il-monitoraggio-strutturale-di-ponti-e-gallerie/
***Ingenio** - Bernardino Chiaia | Marco Civera | Matteo Dalmasso | Valerio De Biagi – 29/01/2024*

How advanced manufacturing can improve supply chain resilience and cybersecurity

- The manufacturing industry is experiencing increasing cyber-attacks, month by month.
- The World Economic Forum's New Narrative demonstrates how the sector can overcome challenges to resilience.
- Manufacturing leaders explain how action today can future-proof the factories of tomorrow.

In 2022, manufacturing had the highest share of cyber-attacks among leading industries worldwide and the third quarter of 2023 marked a 15% increase over the previous. As the manufacturing landscape grapples with this escalating threat, the cost of fortifying digital defences in the cloud era has become exponentially challenging.
This turbulent scenario underscores the urgent need for a swift yet meticulous strategic investment in cybersecurity. In this era of unprecedented technological advancement, safeguarding manufacturing operations has transcended from a luxury to an imperative.
Against this backdrop, advanced manufacturing leaders composed the New Narrative for Advanced Manufacturing, aimed at increasing capacity for sustainability, efficiency, resiliency, innovation and people in the future of manufacturing. Although these impact areas are intertwined and reinforce each other, three co-authors of the New Narrative step forward to share their perspectives on the pivotal role of cybersecurity in fortifying manufacturing resilience. Here are their insights.
People, process and technology
Barbara Frei, Executive Vice President Industrial Automation, Member of the Executive Committee, Schneider Electric
"By reducing the risks and protecting the digital economy, our society will be able to realize the digital dividends of the fourth industrial revolution.
"In the manufacturing industry, cybersecurity should not be viewed solely as a defensive practice but as a means to proactively drive larger value outcomes. Often, cybersecurity is only seen as a "necessary evil" driven by IT considerations. However, industrial companies can leverage cybersecurity to create significant value by involving a broader group of stakeholders in their cybersecurity practices.
"As a technology supplier assisting customers in their digital transformation, Schneider Electric has observed that many industries and manufacturing plants remain limited at the proof-of-concept stage, often because cybersecurity was not initially considered in these pilot projects. Prioritizing cybersecurity within the prism of "people, process and technology" from the outset of a digital transformation programme enables and fosters the convergence of IT and OT (operational technology). (continua…)
https://www.weforum.org/agenda/2024/01/advanced-manufacturing-improve-supply-chain-resilience-cybersecurity/
***WEFORUM** - Maya Ben Dror - 31 Jan 2024*

China Infiltrates US Critical Infrastructure in Ramp-up to Conflict

Threat actors linked to the People's Republic of China, such as Volt Typhoon, continue to "pre-position" themselves in the critical infrastructure of the United States, according to military and law enforcement officials.

The People's Republic of China is accelerating the development of its military capabilities — including cyber operations — because it believes it will need to deter and confront the United States, US officials said yesterday.

And indeed, China-linked cyberattackers have increasingly focused on critical infrastructure systems in particular as part of a campaign by Beijing to be ready for a broader conflict, according to experts — a distinct change in strategy by China, the experts said. For instance, the highly active threat group Volt Typhoon (aka Bronze Silhouette and Vanguard Panda) has conducted attacks against the US government and defense contractors since at least 2021, but since last May it has been recognized as a threat to critical infrastructure and military bases. In fact, it's seen as such a clear threat that it was recently disrupted by the US government and private sector companies, officials said this week.

"Over the last two years, we have become increasingly concerned about a strategic shift in PRC malicious cyber activity against US critical infrastructure," Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA) at the US Department of Homeland Security, stated in written testimony on Jan. 31 to the US House of Representative's Select Committee on the Strategic Competition Party.

She added, "We are deeply concerned that PRC actors — particularly a group referred to in industry reporting as Volt Typhoon — are seeking to compromise US critical infrastructure to pre-position for disruptive or destructive cyberattacks against that infrastructure in the event of a conflict, to prevent the United States from projecting power into Asia or to cause societal chaos inside the United States."

China Is the "Defining Cyber Threat of This Era"

Cyberattacks from China-linked groups have been a standard attribute of the last two decades. For the most part, however, the attacks have either been cybercriminal efforts looking for a payday or espionage operations targeted at stealing government secrets and corporate intellectual property. (continua…)

https://www.darkreading.com/cyberattacks-data-breaches/china-infiltrates-us-critical-infrastructure-ramp-up-conflict

DarkReading - *Robert Lemos - February 1, 2024*

Attacchi cyber all'industria spaziale: difendiamola prima del disastro

L'industria spaziale euro-atlantica si trova in una posizione di vulnerabilità rispetto alle minacce cyber. Le debolezze dei sistemi spaziali potrebbero compromettere infrastrutture fondamentali, tra cui l'agroindustria, le forze armate e il comparto dei trasporti. Esaminiamo le maggiori criticità e le possibili soluzioni

Gli elementi spaziali euro-atlantici, inclusi satelliti e centri di comando delle missioni, sono frequentemente bersaglio di attacchi cibernetici. Malgrado l'avanzamento tecnologico del settore spaziale, i progressi nella sicurezza informatica non hanno tenuto il passo con quelli di altri settori tecnologicamente avanzati.

La presenza diffusa di vulnerabilità e percorsi di attacco non monitorati evidenzia le significative difficoltà che i sistemi spaziali, dai nanotecnologici CubeSats ai rover ultravanzati, incontrano in termini di sicurezza delle informazioni digitali. Nonostante alcune di queste problematiche siano comuni ad

altri settori, i sistemi spaziali USA-UE si confrontano con un'enorme pletora di rischi InfoSec che rende più complesse le capacità risolutive del settore.

Indice degli argomenti

Le vulnerabilità InfoSec delle infrastrutture spaziali euro-atlantiche

Le infrastrutture critiche sono definite, secondo i massimi esperti mondiali del **Dipartimento della Sicurezza Interna degli Stati Uniti**, come l'insieme di settori fondamentali di una qualsiasi nazione che, se attaccati, porterebbero ad un relativo periodo di paura e caos. Tra questi, la maggior parte delle infrastrutture critiche si basa anche sui sistemi spaziali: definiamo "sistemi spaziali" come risorse che esistono nello spazio orbitale, suborbitale o esterno, o sistemi di controllo cielo-crosta terrestre sulla Terra, compresi i siti di lancio, adatte per tutte le predette risorse.

Le agenzie spaziali e le organizzazioni di risorse spaziali sono enti euro-atlantici che costruiscono, gestiscono, manutengono o possiedono i sistemi spaziali euro-atlantici.

La dipendenza delle infrastrutture critiche dai sistemi spaziali

Alcuni esempi della dipendenza delle infrastrutture critiche dai sistemi spaziali includono la dipendenza dell'agroindustria dai satelliti meteorologici e climatici, la dipendenza dell'esercito euro-atlantico dai satelliti di intelligence, la dipendenza del settore dei trasporti dai satelliti del sistema di posizionamento globale (GPS) e le numerose industrie che si affidano alle risorse spaziali per un tempo determinato che vanno, ad esempio, dalla trasmissione di dati di rete al settore finanziario, ai distributori di energia, e così via.

Diversi settori delle infrastrutture critiche euro-atlantiche dipendono dai sistemi spaziali per le comunicazioni globali: quotidianamente ci affidiamo anche ai sistemi spaziali per le scoperte scientifiche, come quelle dei grandi telescopi internazionali, che spesso richiedono attrezzature altamente specializzate e avanzate. (continua…)

https://www.agendadigitale.eu/sicurezza/sistemi-spaziali-euro-atlantici-asset-cruciali-troppo-vulnerabili-i-ritardi-da-colmare/

Agenda Digitale *- Luciano Magaldi - 1 feb 2024*

AI Act, via libera di tutti i Paesi UE: ecco l'approccio europeo all'intelligenza artificiale

Altra tappa superata e il traguardo finale si fa sempre più vicino: lo scorso 2 febbraio 2024, infatti, è arrivato il via libera, all'unanimità, dei Paesi UE sull'AI Act, il primo testo di legge al mondo sull'intelligenza artificiale. Facciamo il punto, ricapitolando brevemente

Gli ambasciatori dei 27 paesi dell'Unione Europea (Coreper) hanno votato all'unanimità, lo scorso 2 febbraio 2024, l'ultimo testo (in bozza) dell'AI Act, approvando l'accordo politico che era stato raggiunto a dicembre, dopo un'estenuante negoziazione.

Dunque, il primo testo al mondo che intende regolamentare l'intelligenza artificiale è prossimo alla sua votazione finale prevista per il 24 aprile 2024.

Si tratta ora di seguire gli ultimi sviluppi, ma intanto facciamo un rapido punto.

Indice degli argomenti

- **Breve recap temporale di questi ultimi mesi**
- **AI Act: i punti chiave, in estrema sintesi**
- **AI Act: la UE chiude il cerchio nonostante critiche e opposizioni**
  - Il ruolo chiave dell'Italia: la dichiarazione del sottosegretario Butti
  - Brando Benifei, un importante traguardo dopo due anni di lavoro
- **Gli impatti dell'AI Act**
  - Impatti sugli individui
  - Impatto sulla tecnologia e sulle aziende
- **I prossimi passi**

Breve recap temporale di questi ultimi mesi

Come sappiamo, il 9 dicembre 2023 il trilogo ha raggiunto l'intesa (politica) sui principali nodi critici dell'AI Act.

Il 21 gennaio 2024, è stato presentato dalla Commissione in una riunione tecnica la versione finale del testo, in sintesi qui.

Quindi, il 2 febbraio 2024 c'è stato il via libera all'unanimità di tutti i Paesi della UE, sciogliendo ogni riserva. Insomma, l'ultimo testo possiamo dire che convinca tutti.

AI Act: i punti chiave, in estrema sintesi

Ricapitoliamo anche i punti cardine sui quali il testo, alla luce dell'ultima bozza, si basa.

Anzitutto una definizione che si rifà ai principi dell'OCSE, promuovendo un uso dell'IA innovativo e affidabile nel pieno rispetto dei diritti umani e dei valori democratici; o almeno questo è il radicato intento. Un approccio basato sul rischio è l'altro cuore della disciplina. Ne deriva che tanto più alto sarà il rischio, quanto più rigide saranno le regole.

Se provassimo a riassumere per punti gli aspetti chiave diremmo che si è voluto fondare l'AI Act su:

1. regole da applicare ai sistemi di AI per finalità generali ad alto impatto comportanti rischi sistemici in futuro, nonché sui sistemi di AI ad alto rischio;
2. sistemi di governance rivisti anche alla luce di alcuni poteri di esecuzione europei;
3. un elenco più ampliato dei divieti, pur potendo utilizzare l'identificazione biometrica remota da parte delle Autorità, fatte salve le tutele;
4. una rafforzata protezione dei diritti imponendo agli operatori dei sistemi di AI ad alto rischio di dover effettuare una valutazione d'impatto prima di poter utilizzare un sistema di AI.

AI Act: la UE chiude il cerchio nonostante critiche e opposizioni

Il risultato raggiunto non è affatto scontato. (continua…)

https://www.cybersecurity360.it/news/ai-act-via-libera-di-tutti-i-paesi-ue-ecco-lapproccio-europeo-allintelligenza-artificiale/

Cybersecurity360 - *Chiara Ponti -05 Feb 2024*

L'inversione dei poli magnetici del Sole è imminente: quali saranno le conseguenze per la Terra? - L'inversione dei poli magnetici, fenomeno che si rinnova circa ogni 11 anni, riveste un ruolo determinante nel condizionare il sistema spaziale terrestre. L'inversione magnetica in sé ha un impatto ridotto sul clima del nostro pianeta, ma negli intervalli che la precedono si intensifica l'attività magnetica solare con effetti particolari, quali eruzioni solari ed espulsioni di massa coronale. Questi eventi proiettano nello spazio particelle cariche ad alta energia che, interagendo con il campo magnetico terrestre, possono compromettere il funzionamento dei satelliti di comunicazione e lo sviluppo di

fenomeni significativi sulla Terra, quali *eruzioni solari ed espulsioni di massa coronale*. Le *espulsioni di massa coronale*, ad esempio, possono pregiudicare la stabilità delle reti energetiche terrestri, perché possono indurre correnti elettriche al suolo in grado di *danneggiare i trasformatori o altre componenti critiche delle infrastrutture elettriche*, aumentando il rischio di estesi *blackout*.
https://www.greenme.it/scienza-e-tecnologia/astronomia/inversione-dei-poli-magnetici-del-sole-imminente-quali-conseguenze-per-la-terra/
greenMe – *Ilaria Rossella Pagliaro – 05/02/2024*

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 Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della	Nella sezione "Newsletter"del sito

newsletter

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

Comitato di Redazione

Alberto Traballesi
Glauco Bertocchi
Silvano Bari
Gianluca Cipriani
Marco Raul Massoni

ai quali potete inviare suggerimenti e quesiti scrivendo a:
segreteria@infrastrutturecritiche.it