AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2024 | **n. 07/2024** | **luglio 2024**

Nuovi ransomware nel panorama Cyber e solite vecchie costrizioni per indurre a pagare il riscatto

Un attacco informatico ransomware si verifica quando viene utilizzato un software dannoso per negare a un utente o a un'azienda l'accesso a un sistema informatico o ai dati. Il malware tipicamente richiede un pagamento per lo sblocco dei file. L'evoluzione dei ransomware è costante e se inizialmente questo tipo di software malevolo utilizzava un'unica forma di minaccia per ottenere un pagamento (mediante crittografia di file e servizi) , nel corso degli anni ha raddoppiato e addirittura triplicato la pressione sulle vittime per forzarle al pagamento: non più solo blocco dei sistemi, ma anche l'esfiltrazione dei dati con minaccia di rivendita nel dark web, fino a minacciare il contatto con i clienti e informarli direttamente della falla che coinvolge anche i loro dati, con un effetto disastroso sulla reputazione della vittima principale.
Gli attacchi ransomware hanno registrato complessivamente una recrudescenza nel 2023, con una focalizzazione particolare sui settori sanitario internazionale, a livello di governo locale e istruzione a fronte di una diminuzione in altri settori chiave. Secondo i dati Recorded future sul 2023 infatti, a dicembre 2023 le bande di ransomware hanno pubblicato 356 vittime sui loro siti di estorsione, in calo rispetto alle 369 vittime del mese precedente, ma ben al di sopra delle 241 vittime pubblicate a dicembre 2022. In particolare, gli esperti dell'azienda di sicurezza affermano che c'è stato un "aumento del 70% negli attacchi ransomware segnalati anno dopo anno. Una mappa aggiornata degli attacchi ransomware dal 2018 a oggi per gli Stati Uniti è fornita dall'azienda Comparitech. Per l'Italia è il progetto italiano DRM – Dashboard Ransomware Monitor, che tiene sotto controllo in tempo reale tutti i gruppi criminali ransomware. Dalla dashboard selezionando il paese "Italy" è possibile avere evidenza delle rivendicazioni avvenute in Italia.
Fra i ransomware di nuova generazione a cui prestare attenzione possiamo annoverare: **Dark-Power, Cactus 3AM, senza dimenticare Luna e Black Basta.**
Il **ransomware Dark Power,** un ceppo di ransomware relativamente nuovo, è stato lanciato all'inizio di febbraio 2023. Si tratta di una razza rara di ransomware, poiché è stata scritta nel linguaggio di programmazione Nim. Il ransomware prende di mira le piattaforme Microsoft Windows e alcuni servizi specifici sul computer della vittima disabilitandoli, inclusi i servizi di backup e anti-malware. Anche il servizio Copia Shadow del volume (VSS) viene interrotto per impedire al ransomware di rilevare file bloccati durante il processo di crittografia. La richiesta di riscatto di Dark Power è un file PDF, creato utilizzando Adobe Illustrator 26.0. La nota afferma che tutti i file nel backup, nel server Outlook e nei database sono stati crittografati e che è possibile ripristinare tutto, ma le vittime devono seguire le istruzioni fornite. La richiesta di riscatto avverte il destinatario di non tentare di modificare i file da solo, di utilizzare software di terze parti per ripristinare i propri dati o soluzioni antivirus poiché ciò potrebbe danneggiare la chiave privata e comportare la perdita di tutti i dati. La richiesta di riscatto richiede un pagamento di $ 10.000 USD a un indirizzo blockchain Monero, con un sito Web Tor (power[redacted].onion) fornito per il pagamento e la comunicazione.
CACTUS è stato scoperto a maggio 2023 dai ricercatori dell'azienda di sicurezza Kroll. La particolarità della minaccia è che, a differenza di quelle precedenti analizzate, riesce ad eludere le difese degli

antivirus perché si insedia nei dispositivi da infettare già crittografata. Cactus non viene rilevato dai software di difesa che non vedono in lui alcuna problematica di sicurezza. Un altro elemento distintivo di Cactus è la sua capacità di cambiare continuamente l'estensione ai file presi di mira dal processo di crittografia, un'operazione che permette di guadagnare più tempo, rallentando il lavoro di scoperta dei file cifrati da parte degli antivirus, per cercare di salvare le informazioni ancora intatte. (fonte Ansa).

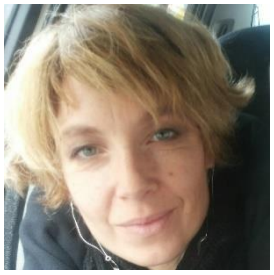
Il Ransomware denominato 3AM sembra essere di una famiglia di malware completamente nuova. Scritto in Rust, un linguaggio di programmazione (sviluppato da Mozilla) noto per la sua robustezza e prestazioni, il malware tenta di interrompere numerosi servizi, tra cui i software di sicurezza e i tool per il backup dei dati, cercando di compromettere il sistema il più possibile. Anche 3AM cerca di eliminare le copie dei dati Volume Shadow (VSS), rendendo estremamente difficile il recupero dei file criptati. Il suo nome deriva dal fatto che attua un terzo livello di pressione sulla vittima: condivide infatti, la notizia di una fuga di dati con i follower dei social media della vittima e utilizza bot per rispondere ad account di alto rango su X (ex Twitter) con messaggi che puntano a fughe di dati. Inoltre, i file criptati da 3AM presentano l'estensione ". threamtime". L'attività del gruppo di ransomware 3AM è stata documentata pubblicamente per la prima volta a metà settembre 2023.

È di ottobre 2023 invece, la notizia che il gruppo ransomware **Rhysida** era arrivato a manifestarsi in Italia. Rhysida, una variante ransomware emergente, utilizzata prevalentemente contro i settori dell'istruzione, della sanità, della produzione, dell'informatica e della pubblica amministrazione da maggio 2023. L'agenzia americana CISA ha dedicato un'intera scheda al gruppo e alle sue modalità d'azione. Le informazioni contenute nell'avviso dell'agenzia americana derivano dalle relative indagini di risposta agli incidenti e dall'analisi del malware di campioni scoperti sulle reti delle vittime. Rhysida sembra essere un ransomware-as-a-service (RaaS) per cui gli strumenti e le infrastrutture del ransomware vengono affittati secondo un modello di condivisione degli utili ed eventuali riscatti pagati vengono poi suddivisi tra il gruppo e gli affiliati. Gli attori di Rhysida sfruttano servizi remoti rivolti all'esterno per accedere inizialmente e persistere all'interno di una rete. I servizi remoti, come le reti private virtuali (VPN), consentono agli utenti di connettersi alle risorse di rete aziendali interne da posizioni esterne. Gli attaccanti Rhysida si autenticano su punti di accesso VPN interni con credenziali valide compromesse, in particolare a causa delle organizzazioni in cui l'MFA non è abilitato per impostazione predefinita.

Altri ransomware particolarmente temibili del 2023 sono stati Luna e Black Basta: il primo scoperto a giugno 2023, scritto in Rust (come 3AM), è in grado di criptare sia dispositivi Windows che Linux, così come immagini di macchine virtuali ESXi. Il secondo, è stato scoperto per la prima volta a febbraio 2023 e ad oggi, ne sono state scoperte due versioni: una per Windows e una per Linux che prende di mira principalmente le immagini delle macchine virtuali ESXi. Una caratteristica distintiva della versione per Windows è che avvia il sistema in modalità provvisoria prima di criptarlo, il che permette al malware di eludere il rilevamento da parte delle soluzioni di sicurezza, molte delle quali non funzionano in modalità provvisoria (Fonte kaspersky). L'agente malevolo Black Basta è stato responsabile di oltre 300 attacchi documentati ed ha fruttato ai suoi creatori oltre 100 milioni di dollari in riscatti. Da gennaio 2024 fa un po' meno paura perché è stato reso disponibile gratuitamente un decryptor per le sue vittime. I ricercatori di SRLabs hanno individuato un punto debole nell'algoritmo di crittografia del ransomware riuscendo a recuperare una chiave da 64 byte, attraverso cui è stato possibile creare uno strumento, poi distribuito a titolo gratuito, che permette di recuperare almeno una parte dei file presi di mira dai cybercriminali. Il tool in questione è disponibile al download dal **sito GitHub**. Tuttavia, il decryptor è efficace solo in caso di attacco precedente allo scorso Natale perché i criminali informatici, sembra abbiano già corretto la vulnerabilità nel ransomware che è tornato efficace.

Le informazioni sull'esatto vettore di infezione utilizzato di Dark Power, non sono ancora disponibili, ma per infettare i computer, gli attaccanti di qualsiasi ransomware utilizzano solitamente una serie di

tattiche per ingannare gli utenti. I metodi comuni includono l'invio di e-mail contenenti allegati o collegamenti dannosi o l'utilizzo di pagine Web che ospitano software piratato, strumenti di cracking e generatori di chiavi. Inoltre, i criminali informatici sfruttano reti P2P, downloader di terze parti, siti Web di hosting di file gratuiti, programmi di installazione ingannevoli e strumenti di aggiornamento software falsi per convincere gli utenti a scaricare ed eseguire ransomware. I file utilizzati per distribuire malware includono documenti MS Office e PDF dannosi, file JavaScript, eseguibili, file ISO e archivi contenenti file dannosi.
Per difendersi dagli attacchi ransomware è utile consultare il sito del no more ransom project che offre consigli di prevenzione e strumenti di decrittazione per evitare di dover pagare.
In generale è consigliabile restare aggiornati sui nuovi ransomware e sulle loro tecniche e tattiche e procedure di attacco attuando difese preventive.



Alessia Valentini

Consulente di Cybersecurity, Advisor e Giornalista. Fa parte delle "Women for Security" la community di Cyberladies nata nell'ambito del Clusit. È Giornalista presso l'ODG del Lazio dal 2013. Ha conseguito la certificazione CISA /ISACA nel 2017. È stata consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016.

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 informazioni, alla mail segreteria@infrastrutturecritiche.it.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

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*

COLLABORAZIONE ALLE ATTIVITA' AIIC

Si invitano tutti i soci a partecipare alle attività sociali (newsletter, webinar, ecc.) inviando articoli, segnalazioni o dando la disponibilità a tenere webinar o seminari o a partecipare alla stesura e redazione della newsletter mensile.
La mail cui scrivere è segreteria@infrastrutturecritiche.it

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

NEWS E AVVENIMENTI

A Look at the Riskiest Connected Devices of 2024
VoIP gear, hypervisors, medical equipment, building automation, printers, and more pose broad risk to organizations, with many facing danger from a combo of IT, IoT, and OT all at once. This listicle breaks it down.
For nearly every organization, the cyberattack threat landscape is made up of a mix of IT, Internet of Things (IoT), and operational technology (OT) like HVAC systems, offering plenty of "ways in" for cyber threat actors. Plus, the medical field has its own specialized set of IoT equipment, extending the targeting options for would-be bad guys even further.
To help organizations assess where danger might be lurking this modern, complex device landscape, Forescout Research–Vedere Labs examined nearly 19 million devices to determine which categories represent the greatest risk to organizations. The findings are based on the potential for misconfiguration, the number of vulnerabilities found, exposure to the Internet, and the potential impact to an organization in the case of compromise.
Baseline data points include the fact that IT devices still account for most vulnerabilities (58%), but that the category is down from 78% in 2023. IoT vulnerabilities, however, were up a whopping 136%, increasing the percentage of known bugs from 14% last year to 33% today.
Overall, the most vulnerable device types are: wireless access points (WAPs), routers, printers, voice-over-IP (VoIP) devices, and IP cameras. The most-exposed unmanaged gear includes VoIP devices, networking infrastructure, and printers. (continua…)
https://www.darkreading.com/cyber-risk/riskiest-connected-devices-2024
***DARKREADING** - Tara Seals - June 10, 2024*

Cyber security nell'Industria 4.0 e 5.0: impatti e punti deboli da proteggere - Con l'approssimarsi del nuovo decreto attuativo, che dovrebbe dare il via definitivo all'Industria 5.0, tornano d'attualità tutti i temi che riguardano l'Industry 4.0, tra cui gli aspetti relativi alla cyber security, spesso trascurati in questi ambiti. Ecco gli aspetti fondamentali da considerare per proteggere gli asset tecnologici
https://www.cybersecurity360.it/soluzioni-aziendali/cyber-security-nellindustria-4-0-e-5-0-impatti-e-punti-deboli-da-proteggere
***Cybersecurity360 -** Marco Gentilini,12 giu 2024*

Uso di nuove tecnologie cost-effective per la gestione del patrimonio di ponti e viadotti esistenti
I ponti rappresentano una componente critica delle reti stradali e la loro sicurezza è attualmente oggetto di interesse primario. Durante la loro vita, i ponti sono soggetti a diversi fenomeni naturali e antropici che ne incrementano la vulnerabilità, e necessitano di ispezioni che ne accertino periodicamente lo stato di salute. Per supportare le tecniche di ispezione tradizionali, il presente articolo fornisce una panoramica sulle nuove tecnologie efficienti e a basso costo che possono essere impiegate per la gestione del patrimonio di ponti esistenti.
(continua…)
https://www.ingenio-web.it/articoli/uso-di-nuove-tecnologie-cost-effective-per-la-gestione-del-patrimonio-di-ponti-e-viadotti-esistenti
***Ingenio** – Mirko Calò, Angelo Cardellicchio, Alessandro Nettis, Andrea Nettis, Sergio Ruggieri, Giuseppina Uva, 17 giugno 2024*

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Certificazioni cloud europee, rimossi i requisiti di sovranità: cosa cambia?

A Bruxelles è in discussione una versione aggiornata dell'European Cybersecurity Certification Scheme (EUCS) per i servizi cloud, che ha rimosso i requisiti di sovranità. Questo cambiamento, voluto da varie organizzazioni e Stati membri, mira a migliorare la competitività globale ma ha sollevato preoccupazioni tra i fornitori di servizi cloud europei

In questi giorni è in discussione a Bruxelles una versione rivista del regolamento europeo sulla certificazione della cybersecurity per i servizi cloud, noto come **European Cybersecurity Certification Scheme (EUCS)** for Cloud Services. Il documento, pubblicato per la prima volta dall'ENISA il 22 dicembre 2020, ha subito infatti a marzo 2024 un nuovo aggiornamento, il quale ha visto **rimuovere dalla proposta i requisiti di sovranità**, che imponevano ai colossi tecnologici statunitensi di creare joint venture o collaborare con aziende europee per poter gestire i dati all'interno dell'UE.

Indice degli argomenti

L'aggiornamento del marzo 2024: una svolta nelle regole?

La necessità di questo nuovo aggiornamento nasce proprio dalle contestazioni a questi requisiti, portate avanti da una serie di organizzazioni, tra cui **la Camera di Commercio Americana in Europa** – che già nel giugno 2022 aveva rilasciato un **position paper sull'argomento**, nel quale dichiarava che le discussioni sull'EUCS hanno mancato di trasparenza e coinvolgimento degli stakeholder – ma anche da **gruppi industriali e aziende** sia esteri che europei, lobbisti e mediatori, come la **Japan Association of New Economy**, centri di ricerca, come il Centro Europeo per l'economia politica internazionale (ECIPE), che a febbraio **chiedeva all'ENISA di abbandonare questi requisiti**, sostenendo che comporterebbero significative perdite economiche per gli Stati membri dell'UE e che potrebbero indebolire la competitività dell'industria europea, aumentando i rischi di sicurezza informatica e creando inefficienze operative, nonché al**cuni Stati membri dell'UE, come ad esempio il Belgio**, che sempre a febbraio ha proposto di separare i requisiti di sovranità dai requisiti funzionali, certificando solo i secondi, mentre le dichiarazioni di sovranità sarebbero state incluse nell'International Company Profile Attestation (ICPA) solo per il livello di certificazione più alto.

Se ne era parlato a febbraio, quando **l'ECIPE** (Centro Europeo per l'economia politica internazionale) aveva pubblicato un Occasional Paper N. 04/2023 intitolato "The Economic Impacts of the Proposed EUCS Exclusionary Requirements Estimates for EU Member States", redatto a cura del direttore e di un dirigente del Centro, entrambi con pregresse esperienze di lavoro in Asia. Il paper riguardava lo schema di certificazione per la cyber security dei servizi Cloud (EUCS, "European Cybersecurity Certification Scheme for Cloud Services") presentato a settembre dall'Agenzia per la Sicurezza delle Reti e dell'Informazione Europea, ENISA e argomentava possibili perdite nei PIL nazionali europei a causa di queste restrizioni legate alle proprietà extra europee di produzione ICT e alle restrizioni sulle localizzazioni delle case madri produttrici, sullo staff e sulla geolocalizzazione dei dati. (continua…)

https://www.agendadigitale.eu/sicurezza/certificazioni-cloud-europee-rimossi-i-requisiti-di-sovranita-cosa-cambia/

AgendaDigitale - *Luisa Franchina - Maria Beatrice Versaci - 20 giu 2024*

Threat Actor May Have Accessed Sensitive Info on CISA Chemical App

An unknown adversary compromised a CISA app containing the data via a vulnerability in the Ivanti Connect Secure appliance this January.

An unknown threat actor may have accessed critical information on US chemical facilities by compromising the US Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Security Assessment Tool (CSAT) earlier this year, by way of known Ivanti flaws.

Data the adversary may have accessed includes the types and quantities of chemicals stored at different facilities, facility-specific security vulnerability assessments, site security plans, and personnel identity information of individuals who might have sought access to restricted areas at high-risk facilities.

Anti-Terror Related Data

CISA required chemical facilities around the country to provide this information as part of the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards (CFATS) program to enhance security at high-risk chemical facilities in the US. CFATS expired in July 2023. According to CISA, a threat actor may have accessed data in its CSAT application after chaining together several zero-day vulnerabilities Ivanti disclosed earlier this year in its Connect Secure appliance. In a notification letter to stakeholders, DHS associate director Kelly Murray said the intrusion happened during a two-day period, sometime between Jan. 23 and Jan. 26, 2024.

After gaining access to the Ivanti appliance, the threat actor deployed a web shell on it that enabled remote command execution and arbitrary file writes to the underlying system, Murray said. The attacker accessed the web shell several times during the two-day period but there is no evidence of any data exfiltration or lateral movement beyond the Ivanti device, she said.

"While CISA's investigation found no evidence of exfiltration of data, this may have resulted in the potential unauthorized access of Top-Screen surveys, Security Vulnerability Assessments, Site Security Plans, Personnel Surety Program submissions, and CSAT user accounts," Murray said. "All information in CSAT was encrypted using AES 256 encryption and information from each application had additional security controls limiting the likelihood of lateral access," she noted. (continua…)

https://www.darkreading.com/cyberattacks-data-breaches/threat-actor-may-have-accessed-sensitive-info-on-cisa-chemical-app

***DARKREADING** - Jai Vijayan - June 25, 2024*

Gli aspetti tecnologici e di protezione dei dati personali degli applicativi di riconoscimento facciale - Negli ultimi tempi le cronache hanno dedicato molta attenzione agli applicativi di riconoscimento facciale, che stanno trovando campi di applicazione sempre più vasti. È recentissima la notizia che la società aeroporti di Milano- SEA- ha cominciato ad applicare questa tecnologia per gestire in modo automatizzato la registrazione dei passeggeri ed il rilascio delle carte di imbarco.

Un uso appropriato di queste tecnologie deve prendere in considerazione due aspetti:

gli aspetti tecnologici,

gli aspetti di protezione dei dati personali.

Vediamo insieme questi due aspetti.

(continua…)

https://www.puntosicuro.it/privacy-C-89/i-mille-problemi-legati-agli-applicativi-di-riconoscimento-facciale-AR-24446

***PuntoSicuro** – Adalberto Biasiotti, 28 Giugno 2024*

Nist cybersecurity framework, cosa cambia con la versione 2.0

La nuova versione del Nist cybersecurity framework pone l'accento sulla governance del rischio, ma sono priorità anche la formazione e la gestione efficace del rischio

Il **National Institute of Standards and Technology** (NIST) ha aggiornato il suo Cybersecurity Framework (CSF) dalla Versione 1.1 **alla Versione 2.0**, con lo scopo di migliorare la gestione dei rischi informatici in un contesto, quello del mondo digitale, sempre più complesso e dinamico.

Di seguito verranno evidenziate i cambiamenti e le integrazioni che il CSF ha subito nel processo di aggiornamento e le priorità da affrontare sul fronte **cybersecurity**.

Indice degli argomenti

Nist 2.0, novità a livello strutturale

Il NIST CSF è strutturato in tre componenti principali: il Framework Core, i Tiers di implementazione e i Profili. La Versione 2.0 mantiene questa struttura ma introduce modifiche chiave per migliorare la chiarezza e l'efficacia del Framework.

- **Framework Core**. Il Framework Core è un insieme di attività organizzate per raggiungere specifici obiettivi di sicurezza. Queste attività sono suddivise in Funzioni, Categorie e Sottocategorie. Nella versione 1.1, il Core era composto da cinque Funzioni principali: Identify, Protect, Detect, Respond, e Recover. Nella nuova versione 2.0, è stata introdotta la funzione "**Govern**" che racchiude attività di natura organizzativa e gestione relativamente alla strategia di sicurezza perseguita dal CSF.
- **Tiers di implementazione**. I Tiers di implementazione forniscono un contesto su come un'organizzazione gestisce il rischio di cybersecurity. La Versione 2.0 raffina ulteriormente questo concetto, descrivendo il livello di rigore delle pratiche di governance e gestione del rischio di cybersecurity.
- **Profili**. Nella Versione 1.1 del CSF i Profili erano utilizzati per mappare lo stato attuale delle pratiche di cybersecurity di un'organizzazione (Profilo Corrente) rispetto agli obiettivi desiderati (Profilo Target). Questo permetteva alle organizzazioni di identificare le lacune e sviluppare piani di azione per colmare queste lacune, migliorando così la loro postura di cybersecurity. La versione 2.0 fornisce un approccio più strutturato per creare e utilizzare i Profili, inclusi passaggi dettagliati per la loro preparazione e utilizzo continuo. Vi è poi anche l'introduzione dei **Community Profiles**, una nuova caratteristica che offre un punto di partenza comune per organizzazioni con interessi e obiettivi condivisi. Questi profili sono tipicamente sviluppati per un particolare settore, sottosettore, tecnologia, tipo di minaccia o altro caso d'uso. Un'organizzazione può utilizzare un Community Profile come base per il proprio Profilo Target, adattandolo alle proprie esigenze specifiche. (continua…)

https://www.agendadigitale.eu/sicurezza/nist-cybersecurity-framework-cosa-cambia-con-la-versione-2-0/

AGENDA DIGITALE -*Simone Bonavita, Alessandro Cortina - 28 giu 2024*

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Gestione dei fornitori: come implementare un Cybersecurity Supply Chain Risk Management

Le evoluzioni normative del DORA e della NIS 2 hanno spinto molte organizzazioni a investire sul rafforzamento della mitigazione del rischio cyber nell'ecosistema dei fornitori. Ecco come implementare un Cybersecurity Supply Chain Risk Management come indicato dalla NIST SP 800-161

La **gestione del rischio informatico derivante dalla supply chain** comporta spesso un elevato effort in termini di risorse e spending.

A seguito delle recenti evoluzioni normative ed in particolare con riferimento al **Digital Operational Resilience Act (DORA)** e alla **NIS 2** diverse organizzazioni stanno investendo sul **rafforzamento della mitigazione del rischio cyber nell'ecosistema dei fornitori**.

Le best practice, quali ad esempio la NIST SP 800-161 forniscono degli spunti utili a comprendere gli elementi funzionali all'implementazione di presidi di rafforzamento della cyber in ambito supply chain.

Il Cybersecurity Supply Chain Risk Management (C-SCRM) descritto dalla best practice riportata rappresenta un sistema di gestione dei rischi di cyber security lungo tutta la catena di fornitura, finalizzato inoltre allo sviluppo di strategie di risposta, politiche, processi e procedure adeguate.

Il C-SCRM richiede un elevato livello di maturità della cyber security posture e un commitment da parte del top management suggerendo un'efficace applicabilità soprattutto nell'ambito di grandi aziende con elevate capacità di cyber security.

Tuttavia, è comunque possibile declinare il C-SCRM in contesti aziendali meno estesi, identificando alcune azioni chiave da implementare in ottica quick win. La presente analisi ha il duplice obiettivo di descrivere le caratteristiche del C-SCRM e di fornire alcuni spunti di riflessione in merito all'implementazione dello stesso in vari contesti aziendali.

Indice degli argomenti

Gestione dei fornitori: quadro di riferimento

L'efficienza della supply chain determina la capacità delle organizzazioni di condurre attività di business, tra cui la commercializzazione di prodotti e servizi, e di conseguenza questa risulta funzionale al raggiungere gli obiettivi strategici.

Se consideriamo la progressiva digitalizzazione dei processi aziendali e l'evoluzione del contesto di minaccia, la mitigazione del rischio cyber risulta di particolare rilevanza al fine di garantire l'efficienza della supply chain.

Nonostante l'interconnessione operativa tra aziende e fornitori spesso in realtà non emergono sinergie significative nell'ambito della risposta agli incidenti informatici e rispetto ad iniziative di prevenzione del rischio.

(Continua…)

https://www.cybersecurity360.it/legal/gestione-dei-fornitori-come-implementare-un-cybersecurity-supply-chain-risk-management/?utm_campaign=cybersec_nl_20240703&utm_source=cybersec_nl_20240703&utm_medium=email&sfdcid=0030O000002LXHlXQAX

Cybersecurity 360 - *Lorenzo Vacca - 26 giu 2024*

Attacco alla supply chain: il caso Polyfill.io e le sue implicazioni

Oltre 100mila siti Web a rischio di vulnerabilità grazie a un malware contenuto in Polyfill.io, una libreria di terze parti largamente utilizzata nel mondo, recentemente acquisita da un'organizzazione cinese. Una pericolosa minaccia che ci ricorda l'elevato rischio degli attacchi alla supply chain

La scorsa settimana, un **evento di proporzioni epiche** ha scosso il mondo del web development: **Polyfill.io**, un servizio utilizzato da oltre 100.000 siti web per migliorare la compatibilità JavaScript sui browser più vecchi, è stato accusato di distribuire malware attraverso le sue funzioni.

Questo **attacco alla catena di fornitura** ha colpito direttamente milioni di utenti in tutto il mondo, sollevando **gravi preoccupazioni sulla sicurezza del software e sulla fiducia nei fornitori di terze parti**.

Indice degli argomenti

Polyfill.io: cronaca degli eventi

La vicenda ha preso una piega rilevante quando è emerso che Polyfill.io era stato venduto all'inizio dell'anno a un'organizzazione cinese. Da quel momento, il servizio, una volta affidabile, ha iniziato a distribuire codice malevolo.

Gli script generati dinamicamente da "cdn.polyfill.io" hanno iniziato a reindirizzare gli utenti a siti pornografici e di scommesse sportive, oltre a mettere in pericolo la sicurezza dei dati attraverso tecniche come il clickjacking.

La società di monitoraggio della sicurezza C/side, attraverso il suo fondatore Simon Wijckmans, ha lanciato l'allarme. In un avviso rivolto ai proprietari di siti web, Wijckmans ha avvertito: "Controllate il codice per qualsiasi utilizzo del dominio polyfill[.]io e rimuovetelo dalle vostre applicazioni".

Questo avviso ha messo in evidenza il rischio immediato per circa 100.000 siti web che utilizzavano il servizio compromesso.

La risposta di Polyfill.io

Invece di adottare una posizione di collaborazione e trasparenza, la prima reazione di Polyfill.io è stata quella di accusare i media e Cloudflare di diffamazione. Questa scelta ha ulteriormente danneggiato la loro reputazione, facendo sembrare l'azienda più interessata a difendersi piuttosto che a risolvere il problema. (continua…)

https://www.cybersecurity360.it/nuove-minacce/attacco-alla-supply-chain-il-caso-polyfill-io-e-le-sue-implicazioni/?utm_campaign=cybersec_nl_20240703&utm_source=cybersec_nl_20240703&utm_medium=email&sfdcid=0030O00002LXHlXQAX

Cybersecurity360 *-Dario Fadda - 2 lug 2024*

Il nuovo Regolamento per il cloud della PA: novità e impatti

L'Agenzia per la cybersicurezza nazionale, con il Dipartimento per la trasformazione digitale, ha adottato il Regolamento unico per le infrastrutture digitali e i servizi cloud della PA. Il Regolamento, in vigore dal primo agosto 2024, definisce misure di sicurezza, qualità e modalità di migrazione per supportare la transizione digitale

L'Agenzia per la cybersicurezza nazionale ha adottato, d'intesa con il Dipartimento per la trasformazione digitale, il Regolamento unico per le infrastrutture digitali e i servizi cloud per la Pubblica Amministrazione con Decreto Direttoriale n. 21007/24 del 27 giugno 2024.

In seguito all'adozione delle nuove disposizioni, termina il periodo transitorio della regolazione dei servizi cloud. La norma entrerà in vigore dal primo agosto 2024 per consentire l'assorbimento delle novità da parte delle Pubbliche Amministrazioni.

Indice degli argomenti

Finalità del nuovo Regolamento

Il nuovo Regolamento è stato pensato come uno strumento di guida per le Pubbliche Amministrazioni nell'individuazione delle possibili soluzioni cloud, attraverso una descrizione dettagliata e metodologica della caratterizzazione e classificazione dei dati e dei servizi digitali.
Nel Regolamento, dunque, sono definite una serie di finalità, le quali sono:

- stabilire le misure e i requisiti per il raggiungimento dei livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA;
- definire le caratteristiche di qualità, sicurezza, *performance*, scalabilità e portabilità dei servizi *cloud* per la PA;
- individuare i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni, stabilendo anche le modalità per la classificazione dei dati e dei servizi digitali;
- definire le modalità del procedimento di qualificazione dei servizi cloud per le Pubbliche Amministrazioni, di cui la PA può approvvigionarsi ricorrendo al libero mercato.

La classificazione di dati e servizi digitali

Per quanto concerne la classificazione, le Pubbliche Amministrazioni dovranno predisporre e aggiornare un elenco dei propri dati e servizi digitali sulla base della loro caratterizzazione. La classificazione comprende tre classi di dati e servizi digitali:

- "**ordinari**", in cui rientrano dati e servizi la cui compromissione non determini pregiudizi al mantenimento di funzioni considerevoli per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese;
- "**critici**", in cui rientrano dati e servizi la cui compromissione può scaturire in danni rilevanti per l'esercizio delle summenzionate funzioni;
- "**strategici**", la cui compromissione può rappresentare un rischio elevato alla sicurezza nazionale.

Aggiornamento di elenchi e classificazione

L' elenco e la classificazione saranno aggiornati con cadenza almeno biennale, oppure in presenza di dati e servizi digitali nuovi, e trasmessi all'Agenzia per la cybersicurezza nazionale (ACN), la quale avrà novanta giorni per fornire un riscontro di conformità. (continua…)
https://www.agendadigitale.eu/infrastrutture/il-nuovo-regolamento-per-il-cloud-della-pa-novita-e-impatti/
AgendaDigitale *-Luisa Franchina- Corrado Fulgenzi - 2 lug 2024*

UN telecom watchdog wags finger at Russia for satellite interference
European neighbors say interference comes from Moscow and Kaliningrad, Kremlin claims it didn't find anything
The UN's Radio Regulations Board (RRB) has asked Russia to play nice with Europe and not interfere with satellites.
The RRB, a part of the International Telecommunication Union (ITU), the telecom agency for the United Nations, held its 96th meeting last week to discuss a number of topics, including alleged satellite interference several European countries suspect is coming from Russia. France, Sweden, the Netherlands, Luxembourg, and Ukraine all said they had experienced some sort of interference in the last few months.
The disruption has resulted in taking down broadcasts and even TV hijacking in two cases, which involved children's TV shows in the Netherlands being replaced with Russian war videos.
Although Russia has denied any knowledge of the interference, telling the RRB it hasn't detected any whatsoever, the evidence is stacking up against the country. The interference has largely targeted channels with Ukrainian programming, and Sweden claims it only started seeing meddling after it joined NATO.
Perhaps most damning of all, two satellite operators traced the interference to three sites: Russia's capital city Moscow, the Kaliningrad exclave next to Poland and Lithuania, and Pavlovka, though it remains unclear which Pavlovka, as there are more than one located in Russia. (continua…)
https://www.theregister.com/2024/07/02/russia_satellite_interference/
TheRegister -*Matthew Connatser -2 Jul 2024*

IA e social zombing, mix devastante per le aziende: come proteggersi - Il Social Zombing compromette la reputazione online senza bisogno di furto di password, attraverso attività come follower falsi e recensioni fake. L'intelligenza artificiale generativa amplifica tali attacchi, rendendoli più sofisticati e dannosi. Monitoraggio costante e proattività sono essenziali per difendersi da queste insidie digitali *(continua).*
https://www.agendadigitale.eu/sicurezza/ia-e-social-zombing-mix-devastante-per-le-aziende-come-proteggersi/
Agenda Digitale *- Gabriele Gobbo, 5 lug 2024*

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

NOTIZIE D'INTERESSE:

Con questo numero la newsletter AIIC va in vacanza. Ci rivedremo a settembre.
Buone vacanze a tutti!

Il Comitato di Redazione

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

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
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 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 Gianluca Cipriani *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.