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. 10/ 2022	Novembre 2022

Il nuovo Threat Landscape di ENISA

Il 3 novembre 2022 è stato pubblicato il nuovo "Threat Landscape" di ENISA (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022) nel quale viene fornita una panoramica relativa alle minacce afferenti la sfera cibernetica. Da una iniziale analisi del report, si evince che l'invasione russa dell'Ucraina ha influenzato notevolmente le statistiche relative ai vettori di attacco cibernetici. Infatti, soffermando l'attenzione sul bimestre febbraio – marzo è possibile notare che il numero di incidenti informatici è notevolmente aumentato. Tuttavia, complessivamente, nel 2022, secondo quanto emerso dal report di ENISA gli incidenti informatici sono diminuiti rispetto all'anno precedente. Il dato preoccupante riguarda l'aumento degli incidenti categorizzati "Near" che, secondo la classificazione di ENISA, sono quelli avvenuti all'interno dell'Unione Europea.
Nel complesso, i principali attori delle minacce non differiscono molto rispetto al report dall'anno 2021; nel dettaglio questi sono state-sponsored, gruppi di cyber-criminali, hacker mercenari e hacktivisti. Analogamente, le otto principali categorie di minacce identificate (ransomware, malware, social engineering, data threats, Denial of Service, web threats, campagne di disinformazione e attacchi alla supply chain) sono apparse anche nell'edizione 2021 del rapporto. Nell'ultima edizione della pubblicazione resta escluso il cryptojacking.
Con oltre 10 TB di dati rubati mensilmente durante il periodo oggetto di analisi, il ransomware rimane la minaccia primaria, come evidenziato dallo studio di ENISA. Più in generale, l'uso di malware è tornato ad aumentare dopo la diminuzione notata nel 2021 e legata alla pandemia di COVID-19.
L'ENISA ha anche rilevato un aumento degli attacchi Denial-of-Service dall'estate del 2022. È importante sottolineare l'attacco DDoS diretto ad un cliente dell'Europa orientale dell'azienda americana Akamai nel luglio 2022 si è rivelato il più grande mai lanciato in Europa.
Continuando l'analisi della pubblicazione di ENISA, per quanto concerne le tipologie di attacco, dal si evince che:

- sono in netto aumento gli attacchi che sfruttano gli exploit zero-day;
- le tecniche di estorsione relative ai cyber attacchi sono in rapida evoluzione;
- la disinformazione avviene anche attraverso l'impiego di intelligenza artificiale;
- le diverse tipologie di phishing riescono ad adattarsi sempre più ai diversi contesti;
- l'efficacia gli attacchi DDoS è in costante crescita e questi prendono di mira le reti mobili e gli IoT;
- aumentano gli attacchi di interruzione e reindirizzamento del traffico internet.

Relativamente ai settori colpiti dagli attacchi informatici, sebbene nessun di questi sia stato risparmiato, le Pubbliche Amministrazioni sono ancora il principale obiettivo, rappresentando il 24,21% di tutti gli incidenti segnalati. Gli attacchi verso il settore pubblico, insieme a quelli diretti verso i fornitori di servizi digitali, hanno rappresentato il 50% di tutte le minacce, mentre l'altra metà è condivisa da tutti gli altri settori dell'economia.
In sintesi, il documento rilasciato da ENISA è il risultato di un'attività di raccolta di contenuti open source come articoli, opinioni di esperti, report di intelligence, analisi degli incidenti e report di ricerca sulla sicurezza, nonché interviste con i membri del gruppo di lavoro ENISA Cyber Threat Landscape.

Il rapporto annuale sul panorama delle minacce dell'ENISA ha lo scopo di supportare gli addetti ai lavori e gli specialisti della sicurezza a definire strategie per difendere i cittadini e le organizzazioni negli Stati membri dell'UE.

Gianluca Cipriani Ha conseguito la laurea in "Scienze Politiche" presso l'Università degli Studi "Roma Tre" e si è specializzato in "Relazioni Internazionali" presso l'Università degli Studi "Roma Tre" con un percorso incentrato sulla strategia militare e sicurezza internazionale. Dopo anni di esperienza come analista di geopolitica, attualmente svolge attività di consulenza in materia di cybersecurity.

Andrea Agostino Fumagalli Laureato in "Giurisprudenza" presso l'Università degli Studi di Milano con tesi in Informatica Giuridica Avanzata, ha maturato diverse esperienze lavorative nell'ambito legale e di compliance, occupandosi di sicurezza delle informazioni. Attualmente svolge attività di consulenza in materia di cybersecurity.

ATTIVITA' DELL'ASSOCIAZIONE

ATTIVITA' DI EDUCATION

Sono in corso di programmazione le attività di formazione per soci e simpatizzanti che si svolgeranno nell'ultima parte dell'anno 2022.

Anzitutto, l'accordo con IsacaRoma consentirà ai soci AIIC di partecipare ai loro seminari (svolti principalmente in modalità webinar) su cybersecurity, risk management e protezione dei dati.

Per quanto riguarda i nostri "Colloquia", abbiamo in cantiere per metà novembre un evento molto interessante sulla protezione delle infrastrutture critiche tramite "droni" mentre stiamo organizzando, con una startup del settore, un evento di illustrazione di soluzioni innovative di predizione e anticipazione degli eventi negativi per tendere al rischio minimo nelle realtà RIR (Rischio Incidente Rilevante) e in generale dove il Real Time Risk Management e la Resilience Engineering rappresentano aspetti qualificanti e determinanti nella gestione.
Stiamo valutando le modalità di svolgimento di questi eventi, possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, stiamo già prendendo accordi per una ripresa delle visite aziendali presso enti/imprese di rilevanza nazionale.
Vi terremo informati.

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 anche che proprio per fornire un valore aggiunto ai nostri associati, alcuni eventi saranno riservati soltanto a chi è in regola con il pagamento delle quote associative.

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.

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 accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Association 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 180.000 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.
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*

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

GRUPPI DI LAVORO AIIC

"Resilienza delle Infrastrutture Critiche e Cambiamenti Climatici"
Il Consiglio Direttivo AIIC nella sua riunione del 19 Settembre 2022 ha approvato la nascita del GdL ***"Resilienza delle Infrastrutture Critiche e Cambiamenti Climatici"***.
Le nuove infrastrutture dovranno essere pianificate, progettate, costruite e gestite tenendo nella dovuta considerazione le minacce sistemiche che possono verificarsi nel corso della loro vita, inclusi i cambiamenti climatici, e nel rispetto dei vincoli di sviluppo sostenibile. Dovranno essere progettate e pensate per contribuire al raggiungimento degli Obiettivi di Sviluppo Sostenibile dell'Agenda 2030, in particolare l'SDG 9 "Costruire un'infrastruttura resiliente e promuovere l'innovazione ed una industrializzazione equa, responsabile e sostenibile".
Coordinatore: Sandro Bologna
Data inizio lavori: 01.11.2022
Durata max: 12 mesi
La lista degli argomenti proposti è contenuta nel sito sociale alla pagina
https://infrastrutturecritiche.it/resilienza-delle-infrastrutture-critiche-e-cambiamenti-climatici/
Tutti i Soci AIIC che intendono partecipare sono invitati a manifestare la loro disponibilità entro il 31 Ottobre 2022, inviando una mail al Coordinatore s.bologna@infrastrutturecritiche.it e per conoscenza alla Segreteria segreteria@infrastrutturecritiche.it.

GDL - La Direttiva NIS 2 e la gestione degli incidenti di cybersecurity
Il Consiglio Direttivo AIIC ha approvato la nascita del GdL "**La Direttiva NIS 2 e la gestione degli incidenti di cybersecurity"**.
Tutti i Soci AIIC che intendono partecipare sono invitati a manifestare la loro disponibilità **entro il 15 novembre 2022**, mandando una mail alla Segreteria segreteria@infrastrutturecritiche.it e per conoscenza al Coordinatore r.dalessandro@infrastrutturecritiche.it.
Promotori del Gruppo di Lavoro: Stefano Aterno e Raffaella D'Alessandro
Coordinatore: Raffaella D'Alessandro
Data inizio lavori: 16.11.2022
Durata max: 8 mesi
Descrizione del GdL e lista degli argomenti trattati
La Commissione europea ha già aperto i lavori per il naturale successore della Direttiva NIS: la Direttiva NIS2. La Direttiva NIS2 opererà lungo una direzione di continuità con la NIS. Reinterpreterà le disposizioni per adeguarsi al considerevole aumento di traffico nella rete e delle relative superfici di attacco. E' previsto l'ampliamento dei settori di attività, e saranno coinvolte un numero e una varietà sempre maggiore di organizzazioni. La NIS2 amplia sia la lista dei requisiti minimi che le aziende devono garantire, sia il loro livello di coinvolgimento, estendendo di fatto la platea dei soggetti coinvolti, nella logica di rendere più sicure le intere supply chain. Dal punto di vista della cybersecurity si rende necessario scongiurare che un'infrastruttura critica possa essere messa in pericolo a causa delle vulnerabilità di un fornitore terzo che non garantisce la necessaria affidabilità, pur partecipando alla catena principale. La NIS2 responsabilizzerà anche le PMI che erano rimaste ben al di fuori della portata della NIS originale e che oggi potrebbero ritrovarsi coinvolte.
Lo studio si pone l'obiettivo di fornire le indicazioni necessarie per comprendere i principi essenziali della Direttiva NIS 2 e di fornire un focus in merito alla gestione degli incidenti di cybersecurity.

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

La lista degli argomenti proposti è contenuta nel sito sociale alla pagina
https://infrastrutturecritiche.it/gdl-la-direttiva-nis-2-e-la-gestione-degli-incidenti-di-cybersecurity/

Ricordiamo che la partecipazione ai Gruppi di Lavoro AIIC è riservata ai soci AIIC in regola con il pagamento delle quote sociali.
A questo proposito, il Consiglio Direttivo ha deciso una facilitazione per chi volesse partecipare associandosi – come nuovo socio – ad AIIC, e cioè di considerare valida la quota associativa versata in questo periodo di fine 2022 anche per l'intero anno 2023.

NEWS E AVVENIMENTI

AGENZIA CYBERSECURITY: VIA A CONCORSO PER ASSUNZIONE 60 RISORSE
31 ottobre 2022 – Contratti a tempo indeterminato. Sette i profili richiesti con esperienza post diploma di almeno tre anni. Candidature fino al 28 novembre. Il direttore Baldoni: "Cerchiamo i migliori tecnici che vogliano impegnare il proprio talento e le proprie competenze al servizio dell'interesse del Paese"
https://www.corrierecomunicazioni.it/cyber-security/agenzia-cybersecurity-via-a-concorso-per-assunzione-60-risorse/)
https://www.inpa.gov.it/bandi-e-avvisi/dettaglio-bando-avviso/?concorso_id=313ae6cdad854cc38db0aea7aa891c72

INTELLIGENZA ARTIFICIALE GENERATIVA: LE APPLICAZIONI
C'è una nuova buzzword che sta galvanizzando l'attenzione della Silicon Valley "Generative AI". Col termine Intelligenza Artificiale generativa ci si riferisce all'utilizzo di tecniche di machine learning e deep learning per generare contenuti nuovi sulla base di dati pregressi. In particolare, parliamo dell'utilizzo di modelli linguistici di grandi dimensioni (Large Language Models) che permettono di ottenere testi, immagini, video, codice inedito a partire da un input testuale. Intelligenza Artificiale Generativa: le applicazioni
Le fasi dell'IA Generativa
Si tratta di un campo non nuovo, ma che ha subìto un'accelerazione rapida in quest'ultimo anno. Il perché è presto detto: oggi abbiamo più dati che in passato, più potenza computazione e dei migliori algoritmi generativi. E siamo solo all'inizio: *Sequoia Capital* prevede un impatto economico di trilioni di dollari nei prossimi anni.
Fino al 2015 per permettere ad una macchina di comprendere il linguaggio si usavano modelli linguistici non molto ampi. Erano efficaci per compiti molto specifici come previsioni di eventi, individuazione di spam, traduzioni basilari. Ma nel 2017 arriva la svolta: un paper di Google Research introduce una nuova architettura di rete neurale chiamata "transformer", in grado di generare modelli linguistici di qualità più elevata, impiegando meno tempo di addestramento. Inoltre questi transformer possono essere personalizzati facilmente per operare in domini specifici. Iniziano ad essere messi alla prova da aziende come Microsoft, Google, OpenAI e, così, nel 2000 si assiste al primo salto di specie: *GPT-3* è il modello che funziona meglio per la creazione di testi.
Ma questi modelli sono difficili da far funzionare, richiedono architetture hardware complesse, GPU potenti per cui sono disponibili a poche aziende. Piano piano i costi iniziano a calare e, oggi, sono

spuntati i primi software stand alone e web based che stanno aprendo le porte ai test di massa (vedi post sulla *generazione di immagini da testo*). DALL-E 2, rilasciato in beta a luglio, è usato da oltre 1,5 milioni di persone che producono più di 2 milioni di immagini al giorno. Midjourney, aperto prima al pubblico, ha più di 3 milioni di utenti.
La prossima fase sarà quella dell'integrazione di questi metodi di generazione all'interno di prodotti già ampiamente utilizzati dalle persone. Microsoft ha già annunciato che Dall-E si potrà *usare dentro Bing* e sono stati creati plugin per utilizzare *Stable Diffusion* nei prodotti Adobe *(continua….).*
https://vincos.it/2022/10/29/intelligenza-artificiale-generativa-le-applicazioni/
VINCOS *– Redazione- 29 ottobre 2022 –*

CYBERCRIME, 25 CAMPAGNE CONTRO L'ITALIA LA SCORSA SETTIMANA
L'**Italia** è stata presa di mira da 25 campagne del **cybercrime**, di cui 18 mirate espressamente al nostro paese. Lo denunciano gli esperti di cybersecurity del CERT-AgID, che hanno rilevato 13 temi sfruttati e otto famiglie **malware**:

- Lokibot – Campagne generiche a tema "Ordine" e "Delivery" veicolate tramite email con allegati ACE e GZ;
- AgentTesla – Campagne italiane a tema "Ordine" e "Assicurazioni" veicolata tramite email con allegati file LZH;
- Qakbot – Campagne a tema "Resend" veicolate tramite email con allegati ZIP e ISO;

(continua**…)**
https://www.difesaesicurezza.com/cyber/cybercrime-25-campagne-contro-italia-la-scorsa-settimana/
Difesa e Sicurezza -Francesco Bussoletti- 31 ottobre 2022

Chi apre TikTok si "apre" all'occhio cinese *La piattaforma può ora accedere ai dati degli utenti europei da altri Paesi (anche dalla Cina). Torna sotto ai riflettori la questione dei social utilizzati come mezzo di spionaggio. Il lavoro della presidenza Biden, la Corte di Giustizia Europea e le rassicurazioni dell'azienda cinese*
La piattaforma cinese TikTok *sta aggiornando* i propri termini e condizioni della privacy nel Regno Unito, nella zona economica europea e in Svizzera. L'app sta provvedendo a informare gli utenti dell'area del fatto che dipendenti della piattaforma fuori dal continente europeo possano ora accedere ai loro dati. I Paesi in cui i dati degli utenti europei sono soggetti all'accesso sono Brasile, Canada, Israele, Cina, Stati Uniti, Singapore, Giappone, Malesia, Filippine e Corea del Sud.
TikTok *afferma* che l'accesso ai dati da remoto viene effettuato per ragioni di controllo della performance, manutenzione, misurazione degli algoritmi, prevenire la diffusione di account *fake* e *bot*. Afferma anche che la pratica rispetta la legislazione europea sulla protezione dei dati, il cosiddetto Gdpr.
La questione del *data flow* tra un Paese comunitario e uno extra-comunitario è piuttosto complessa. Gli accordi contrattuali tra aziende cinesi ed europee non prevedono che il governo del Paese destinatario non possa accedere a quei dati. Il problema, però, è che la Corte di Giustizia Europea si è espressa un paio di anni fa affermando che il trasferimento di dati al di fuori dell'Unione deve tenere conto del livello di protezione degli stessi, con particolare riferimento all'accesso da parte di entità statuali.
Per dirla in maniera semplice, le norme comunitarie vorrebbero evitare che il governo cinese (o entità a esso collegate) possa mettere il naso nel flusso di dati della piattaforma proveniente dall'Europa. Ma, al contrario, non esistono norme contrattuali tra le aziende che possano impedirlo.
Un problema di spionaggio quindi? Non è detto. (continua…)

https://formiche.net/2022/11/tiktok-privacy-spionaggio-dati/
FORMICHE- *Matteo Turato- 03/11/2022*

The Art of Calculating the Cost of Risk Insurance and legislation affect how enterprises balance between protecting against breaches and recovering from them.

In 409 A.D., when Flavius Honorius, the ruler of Rome, saw the invading hordes of Visigoths, he must have wondered whether he should have invested more gold into his perimeter defenses. History tells us that such an investment would have been appropriate, but perhaps Honorius' risk analysis never took into consideration the size and scope of a politically sponsored attack.

Centuries later, political and corporate leaders still face similar questions. Do we invest further in physical and digital security to protect our assets? Are our endpoints secure from malware and breaches? If attackers successfully enter the network, do we have the tools to defend it without compromising resources and data?

A key consideration today is whether enterprises should invest in proactive defenses to identify, detect, and protect the network, or whether they should focus on a reactive approach, responding and recovering from a cybersecurity event should one occur. These approaches are components of the National Institute of Standards and Technology (NIST) *Cybersecurity Framework*, which "integrates industry standards and best practices to help organizations manage their cybersecurity risks," according to the NIST website.

"Being proactive doesn't necessarily mean startups need heavy investments in technology," says John Hellickson, field CISO at Coalfire. "Instead, one could ensure the foundational elements, setting reasonable security policies and standards, implementing security from the start when standing up new IT infrastructure, and following secure coding guidelines when it comes to building applications is executed early on.

"As organizations grow, [they] should implement more comprehensive information security program elements, proactively assessing risks to mitigate those outside of the risk tolerance before likely threats are realized. Since every organization is unique, finding the right amount of investment is more of an art than science."

Enterprises have considerable motivations to be proactive at cybersecurity. Earlier this year, US Securities and Exchange Commission (SEC) Chairman Gary Gensler *proposed several new rules* that would put increased responsibility on C-suites and boards of directors to defend against data breaches. While the rules have yet to be ratified, some organizations already are implementing the proposed rules, including adding cybersecurity experts to corporate boards. To date, Gensler has proposed nearly *50 new rules*.

Cyber Insurance Influences Risk Assessment

Another motivation is *obtaining cyber insurance*. Without appropriate security controls in place, enterprises can find it difficult to engage a broker or carrier that would risk writing a policy. Even if the policy is written, the prospect still needs to get underwriters' approval before the carrier binds the policy. *(continua…)*

https://www.darkreading.com/edge-articles/the-art-of-calculating-the-cost-of-risk
Darkreading *-Stephen Lawton- November 02, 2022*

Infrastrutture critiche, a Bologna il living lab per la resilienza Realizzato nell'ambito del progetto europeo Precinct, l'hub avrà il compito di testare la piattaforma ecosistemica per le performance delle reti. In campo Lepida

A settembre è stato avviato il Living Lab (LL) di Bologna volto a implementare e testare la piattaforma ecosistemica del progetto europeo Precinct, dedicata all'incremento della resilienza delle infrastrutture critiche (IC). La rete pubblica di Lepida svolge un duplice ruolo: è sia una IC e connette anche le altre IC coinvolte nell'area sperimentale ovvero l'Aeroporto, la Stazione Centrale e i loro transiti per il trasporto passeggeri (People Mover e autobus). Lepida mette a disposizione le proprie tecnologie, conoscenze e competenze.

Indice degli argomenti

- *L'obiettivo del progetto Precinct*
- *Le soluzioni*

L'obiettivo è condividere un approccio comune e integrato di gestione della sicurezza cyber-fisica (continua….)

https://www.corrierecomunicazioni.it/digital-economy/infrastrutture-critiche-a-bologna-il-living-lab-per-la-resilienza/

***CORCOM**- Redazione-02 Nov 2022*

Cyber resilience: best practice per ridurre il rischio di attacco alle identità e agli accessi digitali

L'adozione di tecniche di Attack Path Management e Group Policy Management, insieme all'implementazione di misure di resilienza informatica, consentono di creare un'efficace strategia di sicurezza basata su una solida valutazione del rischio aziendale

Quasi tutte le organizzazioni di medie e grandi dimensioni soffrono di un'**espansione incontrollata degli account**. La distinzione fra account "utente" e "di servizio" è essenziale perché la proliferazione non gestita causa un aumento della superficie di attacco sia delle utenze "standard" che di quelle legate ad account privilegiati.

In generale, la gestione delle identità secondo buone prassi è necessaria in tutti gli ambienti e sistemi: AWS e G-Suite, ma in Active Directory questo problema è critico perché si assiste a "foreste" di account cresciute a un livello tale che gli account non possono più essere gestiti manualmente.

Per gli esperti di sicurezza informatica, gli account di servizio possono essere equiparati a una "bomba a orologeria" a causa dei maggiori privilegi di accesso ad essi associati, tuttavia, anche la mancata gestione delle evoluzioni degli account utente costituisce un concreto rischio di security. Il monitoraggio dell'account e i controlli di gestione prevengono attività non autorizzate che possono portare alla perdita dei dati coperti.

Se implementati correttamente, questi controlli consentono ai proprietari e agli amministratori delle risorse di analizzare con precisione chi ha accesso ai dati coperti e di rilevare l'eventuale accesso inappropriato prima che si verifichino eventi di perdita di dati.

Indice degli argomenti

- *Introduzione alla gestione degli account utente con Active Directory*
- *Errori di gestione e challenge di sicurezza*
- *Buone prassi e strumenti per la risoluzione*
- *Le soluzioni di sicurezza secondo Quest*

Introduzione alla gestione degli account utente con Active Directory

Il sistema di Active Directory (AD) è presente in molte organizzazioni in tutto il mondo per fornire servizi di rete in modo che utenti e computer possano autenticarsi facilmente ed essere autorizzati ad

accedere alle risorse di rete o ad accedere ai sistemi Windows. AD consente, inoltre, agli amministratori di sistema e ai team dell'infrastruttura di gestire le reti di computer aziendali. AD, infatti, abilita l'accesso di utenti e di computer a diverse risorse di rete: cassette postali, stampanti, file condivisi, risorse in cloud tramite *Single Sign-On (continua….)*.
https://www.cybersecurity360.it/soluzioni-aziendali/cyber-resilience-best-practice-per-ridurre-il-rischio-di-attacco-alle-identita-e-agli-accessi-digitali/
Cybersecurity360 *Alessia Valentini -4/11/2022*

Il riscatto non si paga. Lezione australiana sul ransomware

L'amministratore delegato di Medibank, colosso delle assicurazioni sanitarie, ammette che la società è stata attaccata. Violati i dati di quasi 10 milioni di clienti. No alle richieste estorsive: cedere incoraggerebbe gli aggressori. Secondo l'avvocato Mele il governo italiano dovrebbe vietare i pagamenti aggiungendo una norma al Codice penale

Cedere sul riscatto rischia di "incoraggiare i criminali a estorcere direttamente i nostri clienti, e c'è una forte possibilità che pagare metta in pericolo altre persone rendendo l'Australia un bersaglio più grande". A parlare così all'*Australian Financial Review* è **David Koczkar**, che dopo molte critiche ha ammesso le difficoltà di Medibank, la società di cui è amministratore delegato, uno dei maggiori fornitori di assicurazioni sanitarie private d'Australia, recentemente vittima di un pesante attacco hacker che ha colpito i dati di 9,7 milioni di clienti.

Dopo quasi quattro settimane, la società ha ammesso il furto dei dati precedentemente escluso. "Stiamo operando sulla base del fatto che, poiché non ci si può fidare dei criminali, tutti i dati sono stati rubati e questo ci aiuterà a fornire la migliore protezione ai nostri clienti e a contattarli in base alle loro circostanze individuali", ha dichiarato Koczkar spiegando che il problema è stato un furto di password rubata e non l'inadeguatezza dei sistemi.

L'Australia è uno dei Paesi che la scorsa settimana hanno partecipato al *secondo vertice internazionale della Counter Ransomware Initiative* ospitato alla Casa Bianca. Con questa iniziativa, l'amministrazione Biden "sta intraprendendo azioni concrete con i nostri partner internazionali per proteggere i nostri cittadini e le nostre imprese dai criminali informatici", *si legge in una nota diffusa dalla Casa Bianca dopo l'incontro*. *In un briefing con la stampa prima dell'appuntamento*, un alto funzionario della Casa Bianca ha spiegato: "Non si tratta tanto della Russia quanto di come noi, come insieme di Paesi, rendiamo più difficile, più costoso e più rischioso il lavoro degli attori del ransomware". Tra le iniziative della Counter Ransomware Initiative c'è una task force internazionale contro il ransomware, presieduta dall'Australia, per coordinare le attività di resilienza, *disruption* e contrasto alla finanza illecita.

Il summit ha concluso, ha spiegato Roberto Baldoni, direttore generale dell'Agenzia per la cybersicurezza nazionale, "un anno di attività che ha visto l'Agenzia lavorare a stretto contatto con il ministero degli Affari esteri, il ministero dell'Interno e la Polizia postale, oltre che il ministero dell'Economia e delle finanze per definire l'insieme delle iniziative internazionali da mettere in campo per il contrasto alla minaccia ransomware": l'Agenzia è stata impegnata nel potenziare la resilienza del Paese in merito agli attacchi cyber, la Farnesina nella fondamentale attività di *cyber diplomacy* a livello internazionale, le strutture del Mef impegnate nel contrastare la capacità di trarre profitto dalle azioni malevoli, anche sfruttando pagamenti in criptovaluta, e la Polizia postale guidata da Ivano Gabrielli nelle iniziative di *disruption* dei gruppi criminali.

L'ammissione di Koczkar è a suo modo storica e racconta come siano sempre di più le aziende che dichiarano pubblicamente il loro no al pagamento di riscatti (continua….)
https://formiche.net/2022/11/ransomware-australia-niente-riscatto/
FORMICHE *- Gabriele Carrer -07/11/2022 –*

US to Japan: We'll help you make chips. Now about that China ban...

The two not explicitly linked together but USA still working hard to hurt China semiconductor imports
As Washington tries to persuade allies to join its China chip technology export ban, Japan is preparing for a joint research project with the US on the development of next generation advanced semiconductors.
According to reports, Japan is aiming to allocate 350 billion yen ($2.38 billion) on the US collaboration. *Nikkei Asia* claims a secondary supplementary budget bill for Japan's current fiscal year will also include 450 billion yen ($3.07 billion) for production of advanced chips, as well as 370 billion yen ($2.52 billion) for securing materials essential for manufacturing.
This latest move follows increasing efforts by the US to build closer ties with allied nations in the Pacific region. Last year, Washington and Tokyo announced the launch of the *US-Japan Partnership on Trade*, to advance bilateral collaboration on trade-related topics and "issues of common interest", the latter of which included semiconductor manufacturing.
Earlier this year, it was reported that the US was working with Japan to help the latter to put in place the ability to design and manufacture cutting edge *2nm chips* within the next few years.
Just this morning, Japan announced it is joining *NATO's cyber defense center*.
This latest news falls in lockstep with these plans, as Nikkei states that the joint research hub will be established by the end of the year with the goal of developing and putting in place the ability to mass produce 2nm semiconductors by the latter half of the decade.
Participating institutions include the University of Tokyo, the National Institute of Advanced Industrial Science and Technology and science institute Riken, as well as research institutions from Europe and the US.
According to Nikkei, the 450 billion yen will be spent on building production hubs for advanced semiconductors, with subsidies for companies such as TSMC, Kioxia, and Micron Technology to site semiconductor fabrication plants in Japan, in a similar fashion to the US government's CHIPS Act which offers subsidies for companies to set up shop there (continua….).
https://www.theregister.com/2022/11/07/us_japan_2nm_chips/
TheRegister- Dan Robinson -7 Nov 2022 // 14:30 UTC

Water sector in the US and Israel still unprepared to defeat cyber attacks

Expert warns that the US and Israel are still unprepared to defeat a cyber attack against organizations in the water sector**.** Ariel Stern, a former Israeli Air Force captain, warns that the US and Israel are still unprepared to defeat a cyber attack against the water sector that could be orchestrated by enemy states like Iran. Stern highlighted the dangers for providers of critical infrastructure and issued his warning following the *ransomware attack* that in August disrupted the IT operations of South Staffordshire Water, a UK company supplying drinking water to 1.6M consumers daily. The intelligence officer pointed out that nations like Russia, Iran, North Korea, and China have the capabilities to hit the water sector with dramatic consequences.
"He flagged that the main adversary in this sphere for Israel is Iran, but cautioned that even after past cyber attacks on Israel's and America's water sector in recent years, "we don't have top minds in the water industry."" *reported The Jerusalem Post.* ""Most water sector workers are civil engineers. How can they ignore it [cyber dangers]? They are very sophisticated within their domain relating to pipes, water flows, ground stabilization and chemistry," but not with regard to blocking hackers."

One of the main problems for the industry is the lack of proper training for cyber defense.
A cyber attack against a water facility or an organization in the water sector could have a widespread impact because many infrastructures serve wide areas including many cities and states, and protecting them it is not easy.
In many cases, the IT and OT networks are not separated and are not designed to be resilient to cyber-attacks.
Stern explained that there are 55,000 distinct water operators in the US, but the majority of the population is served by a small number of those operators that are exposed to cyber attacks. He urges these organizations to rapidly adopt necessary defense measures(continua…)
https://securityaffairs.co/wordpress/138185/hacking/water-sector-us-israel-cyberattacks.html
Security Affairs *-Pierluigi Paganini- November 7, 2022*

Attacchi DDoS: negli smart attack gli hacktivist lasciano il posto ai professionisti Secondo Kaspersky, gli attacchi Distributed Denial of Service (DDoS) diventano *smart attack*. Negli attacchi DDoS del terzo trimestre 2022, gli hacktivist fanno un passo indietro, per lasciare il posto ai professionisti.
"Il rapporto pubblicato da Kaspersky", commenta Pierluigi Paganini, analista di cyber security e CEO Cybhorus, "è in linea con quanto emerso dalle analisi delle principali aziende che si occupano di mitigare attacchi DDoS". Ecco i dati nei dettagli.

- Smart attack in forte aumento
- I professionisti del DDoS

Smart attack in forte aumento
Gli attacchi DDoS sono saliti in maniera importante nel Q3 2022, in particolare quelli lanciati da professionisti.
Tuttavia "gli attacchi sono decisamente più complessi", spiega Paganini, "un processo evolutivo dovuto alla necessità di superare le crescenti difese delle principali organizzazioni su scala globale".
Gli smart attack infatti raddoppiano rispetto al medesimo periodo dell'anno prima. Gli attacchi DDoS sofisticati aumentano in maniera importante. Nel primo semestre del 2022, il numero di attacchi da parte degli hacktivist ha registrato una significativa crescita, ma la loro attività è in declino verticale nel terzo.
Infatti "essendo invariati i settori presi di mira da questi attacchi", sottolinea Paganini, "gli esperti sono propensi a considerare queste attività come parte di operazioni condotte da gruppi di mercenari specializzati".(continua…)
https://www.cybersecurity360.it/news/attacchi-ddos-negli-smart-attack-gli-hacktivist-lasciano-il-posto-ai-professionisti/#:~:text=Attacchi%20DDoS%3A%20negli%20smart%20attack%20gli%20hacktivist%20lasciano%20il%20posto%20ai%20professionisti,-Home&text=Secondo%20Kaspersky%2C%20gli%20attacchi%20Distributed,lasciare%20il%20posto%20ai%20professionisti..
Cybersecurity360*- Mirella Castigli -8/11/2022*

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

NOTIZIE D'INTERESSE:

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

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

RIFERIMENTI DELL'ASSOCIAZIONE

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

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

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

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

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

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

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