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

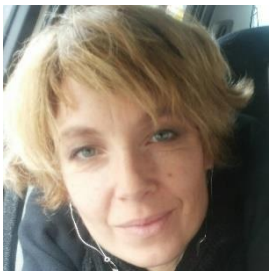
ANNO 2023 **n. 11/ 2023** **dicembre 2023**

Passkey come "new normal" per dire addio alle password

Se ne parla da un po' nella community IT e di Cybersecurity: sia chiama tecnologia Passkey e promette di mandare in pensione le password e il Codice One Time Password (OTP) nel processo di Autenticazione a doppio fattore (di riconoscimento).
Le password presentano problemi di sicurezza, che se sfruttati generano violazioni, phishing e identità rubate, e possono essere scomode da ricordare per gli utenti, specialmente quando sono molteplici e per ogni sito devono essere ricordate o custodite in qualche modo o app che, a sua volta, non sia violabile dai criminali.
Le passkey sono un nuovo tipo di credenziale che sfrutta l'autenticazione biometrica, come l'impronta digitale o il riconoscimento facciale, oppure un PIN o una sequenza di scorrimento utilizzata con gli Android per l'accesso.
Google nel suo blog spiega in dettaglio di cosa si tratta: Le passkey sono state create con un nuovo standard web, lo standard di sicurezza Web Authentication API o WebAuthn, che utilizza la crittografia a chiave pubblica per verificare l'identità e per l'accesso e sostituisce l'accoppiata "nome utente e password". Ogni chiave è unica e creata con dati crittografati per una maggiore sicurezza.
WebAuthn è la stessa soluzione utilizzata dalle app di messaggistica sicura, per crittografare le conversazioni e dai processori di pagamento online, per assicurarsi che i dettagli della carta di credito non vengano rubati; quindi, è ben compresa e ampiamente utilizzata. Quando si crea account per un servizio che utilizza WebAuthn, invece di generare una password che corrisponda ad alcuni criteri arbitrari, il dispositivo creerà una coppia univoca di chiavi matematicamente correlate. Una è chiamata chiave pubblica e l'altra è chiamata chiave privata. La chiave pubblica è archiviata sui server del servizio, ma non importa se gli hacker lo rubano o se viene divulgato in altro modo, proprio perché è condivisibile e quindi può essere di dominio pubblico senza che ciò influisca sulla sicurezza. La chiave privata, invece, è archiviata in modo sicuro sul dispositivo e deve rimanere segreta. Ad ogni accesso dell'utente il dispositivo di accesso viene "sfidato" presentando la chiave pubblica. Poiché le due chiavi sono matematicamente correlate, se e solo se il dispositivo risponde alla sfida usando la chiave privata (senza trasmetterla) allora l'accesso sarà garantito. Non ci sono informazioni che i criminali possano rubare…
Quindi all'accesso ad un account che utilizza WebAuthn, il dispositivo o browser web chiederà di sbloccare l'account utilizzando un PIN o un'opzione biometrica come FaceID o TouchID. E tutte le operazioni relative alla chiave pubblica e privata verranno eseguite automaticamente in background.
Apple e Google hanno aggiornato il software del telefono e i browser web a fine 2022 per utilizzare la tecnologia passkey. In particolare, Google informa degli aggiornamenti sull'implementazione delle esperienze passkey sia su Chrome che su Android, servizi come Docusign, Kayak, PayPal, Shopify e Yahoo! (Google blog). L'adozione delle passkey si sta diffondendo a macchia d'olio: oltre alle applicazioni di Google, Gmail e YouTube la funzionalità è già attiva per alcune app da Uber a eBay, da PayPal a Microsoft e potrà progressivamente estendersi, grazie alla partecipazione dei colossi del settore all'alleanza Fido (Fast Identity Online) perché l'obiettivo finale è creare un metodo unico e condiviso per l'accesso sicuro alle piattaforme digitali.
Naturalmente "non è tutto oro quello che luccica" perché anche le passkey sono soggette a rischi. Igor Kuznetsov, Director, Global Research and Analysis Team (GReAT) di Kaspersky fa sapere che

nonostante ogni passkey sia collegata a un sito web specifico, in modo da impedirne l'uso su siti fraudolenti, sono soggette alle stesse minacce che colpiscono qualsiasi metodo di autenticazione. Questo significa che se il dispositivo utilizzato per il login (computer o telefono) viene compromesso, i criminali informatici possono utilizzare il social engineering per ingannare l'utente e farlo accedere a un'applicazione fraudolenta o rubare i dati dopo un login riuscito. È inoltre importante ricordare che, per impostazione predefinita, le passkey sono sincronizzate con i servizi cloud del provider, come Google o Apple, entrambi membri dell'alleanza FIDO. In caso di compromissione dell'account del provider (ad esempio, un account Google o un ID Apple), la sicurezza della passkey diventa vulnerabile. Come sempre gli esperti suggeriscono di affiancare alle passkey una protezione applicativa del dispositivo, curare l'aggiornamento regolare del software e fare attenzione a chiamate, sms, link sospetti.
Per approfondimenti si può consultare anche la guida on line pubblicata da Mirella Castigli.

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 scadrà il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo 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 2023".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

Il Consiglio Direttivo di AIIC ha deciso una facilitazione per chi si iscriverà come nuovo socio: a partire dal mese di ottobre 2023, pagando la relativa quota sociale, il nuovo socio avrà diritto a vedere la propria iscrizione valida fino a tutto l'anno 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

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*

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

Il riconoscimento biometrico è decisamente attraente, ma… - Il General Accounting Office americano ha analizzato una delle più grandi banche dati biometriche del mondo, quella utilizzata dal DHS - Dipartimento della sicurezza interna degli Stati Uniti. Le carenze sono numerose e le preoccupazioni significative.
Il DHS-Department of homeland security, utilizza un archivio di dati biometrici, che è stato attivato la bellezza di 29 anni fa e che ancora oggi viene costantemente aggiornato. Questo archivio offre dei servizi di gestione dell'identità, basata sul riconoscimento di caratteristiche biometriche, come ad esempio le impronte digitali. Ad oggi questo sistema archivia la bellezza di 290 milioni di identità biometriche. Nel 2016 il Dipartimento ha avviato un programma per la sostituzione di questo archivio, che indubbiamente ormai mostrava i suoi anni.
Il programma di sostituzione però non è stato rispettato ed è stata individuata una nuova data, per l'attivazione di un sistema sostitutivo. Ad oggi il programma è in ritardo di ben quattro anni.
Il nuovo programma è stato battezzato con l'acronimo HART – Homeland advanced recognition technology. Tanto per cominciare, certamente i lettori non saranno sorpresi se il costo iniziale previsto è ad oggi cresciuto della bellezza di 354 milioni di dollari. Inoltre, con ogni probabilità dovrà essere definito una nuova data di entrata in funzione di questo sistema, perché i problemi da superare non sono certamente pochi. Ad esempio, ad oggi il programma non sembra in grado di soddisfare i requisiti di protezione criptografica dei dati, in grado di resistere alle nuove tecnologie di attacco.
(continua)
https://www.puntosicuro.it/security-C-125/il-riconoscimento-biometrico-decisamente-attraente-ma-AR-23780
PuntoSicuro – *Adalberto Biasiotti, 3/11/2023*

Come i cambiamenti climatici condizionano le frane - I cambiamenti climatici in atto e previsti non hanno precedenti. L'aumento della frequenza e dell'intensità degli eventi meteorologici estremi desta particolare attenzione, poiché ha importanti risvolti sulle frane e sul dissesto geo-idrologico. Valutare come i cambiamenti climatici condizionano la numerosità, la tipologia, la distribuzione e la frequenza delle frane non è un'attività semplice, ma quanto mai necessaria.
Il riscaldamento globale è un fatto inequivocabile, con cambiamenti in atto che non hanno precedenti, come confermano gli ultimi rapporti dell'Intergovernmental Panel on Climate Change (IPCC).
Pensando agli effetti dei cambiamenti del clima vengono subito in mente l'aumento delle temperature, le ondate di siccità, la fusione dei ghiacciai e l'innalzamento del livello del mare.
L'aumento della frequenza e dell'intensità degli eventi meteorologici estremi è un problema altrettanto preoccupante. Quest'ultimo – e non solo – ha importanti risvolti su numerosi fenomeni di dissesto geo-idrologico, come le frane.
L'analisi degli impatti che i cambiamenti climatici possono avere sui fenomeni di instabilità dei versanti è un problema complesso, che necessita di conoscenze e azioni efficaci e di un approccio olistico e multidisciplinare.
(continua)
https://www.ingenio-web.it/articoli/come-i-cambiamenti-climatici-condizionano-le-frane/
Ingenio - *Stefano Luigi Gariano, 3.11.2023*

Infrastrutture critiche: Commend per le comunicazioni di Trentino Trasporti

In ambito ferroviario, nelle situazioni di emergenza o quando serve fornire indicazioni di servizio, **la comunicazione deve essere chiara, tempestiva ed affidabile** in qualsiasi momento. Lo richiedono, tra le altre, normative chiave come la Direttiva NIS2. Commend Italia ha collaborato con **Trentino Trasporti** - la società responsabile del trasporto pubblico della Provincia Autonoma di Trento - per raggiungere questo obiettivo nelle gallerie e nelle stazioni della linea ferroviaria Trento-Malè-Mezzana. La sfida che Trentino Trasporti ha posto a Commend ha riguardato la realizzazione di un sistema flessibile e modulare di comunicazione, in grado di interfacciarsi con i sistemi di controllo esistenti. Il sistema doveva **garantire comunicazioni, sia di emergenza sia di servizio**, con un'elevata intelligibilità, anche in condizioni rumorose o all'interno delle numerose gallerie che caratterizzano il tratto gestito dalla società di trasporti trentina.

Le richieste del cliente erano molte. Occorreva garantire una gestione efficace delle comunicazioni all'interno delle gallerie sfruttando l'infrastruttura esistente. Erano necessarie comunicazioni rapide ed efficienti con il posto operatore DCO presso la sede di Trento. Per questioni di **sicurezza e ridondanza**, il sistema doveva interfacciarsi con il sistema telefonico, per poter inoltrare le chiamate ad altri utenti in caso di necessità.

Il sistema interfonico doveva essere **virtualizzabile e ridondabile**, installato su server esistenti. Doveva essere facilmente scalabile in termini di funzioni, apparati, interfacce. (Continua…)

https://www.securityopenlab.it/news/3167/infrastrutture-critiche-commend-per-le-comunicazioni-di-trentino-trasporti.html

Security Open Lab *– Redazione Security – 13 Nov 2023*

Inaugurata a Milano la cabina elettrica "fantasma" in grado di resistere al cambiamento climatico. Unareti ha inaugurato oggi una cabina elettrica "fantasma", perché interrata, in grado di resistere agli eventi determinati dai cambiamenti climatici come l'esondazione del **Seveso**, consente l'installazione interrata in un contesto metropolitano dove è sempre più difficile individuare nuovi spazi e non necessita di manutenzione periodica. La nuova infrastruttura installata in via Rubattino è stata presentata oggi dall'amministratore delegato di A2A, **Renato Mazzoncini** e dall'assessora al verde e ambiente del Comune di Milano, **Elena Grandi**. "Il ' fantasma' che abbiamo inaugurato oggi è una cabina secondaria compatta, che sta sotto terra per dare energia ai nostri concittadini, senza togliere spazio prezioso al suolo pubblico di Milano ed è fondamentale per poter crescere in termini di potenza elettrica". Milano, ha proseguito **Mazzoncin**i, è una città particolare, "ha una potenza elettrica con una densità cinque volte quella di Roma, quasi 9 megawatt al chilometro quadrato, distribuiamo sette terawatt/ora di energia, quasi il 2,5 per cento del consumo nazionale, e con una transizione energetica verso l'elettrificazione che sta continuando con un ritmo molto importante".. *(Continua…)*

https://www.agenzianova.com/news/inaugurata-a-milano-la-cabina-elettrica-fantasma-in-grado-di-resistere-al-cambiamento-climatico/

Agenzia Nova *– Agenzia Nova – 17 Nov 2023*

Attacchi cyber alle infrastrutture critiche sanitarie: dagli USA i primi provvedimenti normativi.
Per far fronte al problema dell'**aumento dei cyber attacchi nel settore sanitario** nello Stato di New York – considerando che il 77% delle violazioni dei dati sanitari segnalate al Department of Health and Human Services (HHS) sono attribuibili all'hacking – il governatore Kathy Hochul ha proposto un **pacchetto di norme di cyber security** che si applicherebbe agli ospedali di tutto lo Stato, congiuntamente a 500 milioni di dollari di finanziamenti per aiutare le strutture sanitarie ad aggiornare i loro sistemi tecnologici al fine di soddisfare i requisiti delle norme proposte. In particolare, la normativa richiederà agli ospedali di implementare infrastrutture difensive per prevenire gli attacchi informatici e di sviluppare gli **incident response plans**.
Inoltre, viene previsto che gli ospedali di New York debbano istituire il ruolo di Chief Information Security Officer (CISO), utilizzare l'autenticazione a più fattori, stabilire politiche per valutare e testare la sicurezza delle applicazioni di terze parti utilizzate dall'ospedale ed eseguire test dei loro piani di risposta agli incidenti per garantire che l'assistenza ai pazienti continui anche in caso di interruzione.

Indice degli argomenti

Attacchi alle infrastrutture critiche sanitarie: le nuove norme
Questo nuovo pacchetto normativo, oltre a fungere da prima roadmap di mitigazione del rischio informatico a livello statale, rappresenta un "complemento" della **Health Insurance Portability and Accountability Act (HIPAA)**, contenente molti degli stessi requisiti, anche se intenzionalmente meno prescrittivi. *(Continua…)*
https://www.cybersecurity360.it/nuove-minacce/attacchi-cyber-alle-infrastrutture-critiche-sanitarie-dagli-usa-i-primi-provvedimenti-normativi/
Cybersecurity360 *– Gaia D'Ariano – Luca Marchese – 17 Nov 2023*

NCSC highlights threat to UK critical infrastructure
According to the review, the UK's critical sectors, including essential services like water, electricity, communications, transport, financial networks, and internet connectivity, are under 'enduring and significant' threat. This risk is attributed partly to the rise of state-aligned groups and a noticeable increase in aggressive cyber activities.
In the past year, the NCSC has observed the emergence of a new class of cyber adversary in the form of state-aligned actors, often sympathetic to Russia's further invasion of Ukraine. These actors are motivated ideologically rather than financially.
In May, the NCSC issued a joint advisory revealing the details of 'Snake' malware, a core component in Russian espionage operations carried out by Russia's Federal Security Service (FSB) for nearly two decades.
NCSC CEO Lindy Cameron stated, *"The last year has seen a significant evolution in the cyber threat to the UK – not least because of Russia's ongoing invasion of Ukraine but also from the availability and capability of emerging tech."*(Continua…)
https://ukdefencejournal.org.uk/ncsc-highlights-threat-to-uk-critical-infrastructure/
UK Defence Journal *– George Allison – 27 Nov 2023*

AI Act, c'è scontro in Europa: ecco i nodi che ne ostacolano l'approvazione

I governi italiano, francese e tedesco hanno proposto di non regolamentare i modelli di fondazione dell'intelligenza artificiale, fatto che ha creato preoccupazione tra i player tecnologici e organizzazioni della società civile. Il dibattito è acceso: vediamo le diverse posizioni

In un contesto di crescente consapevolezza riguardo all'impatto dell'intelligenza artificiale sulla società, le istituzioni europee si trovano attualmente al centro di un dibattito cruciale sulla regolamentazione dell'IA e, in particolare, dei suoi modelli di base. La discussione, tuttavia, **è permeata da posizioni divergenti e contraddittorie**, come evidenziato dai recenti sviluppi tra Italia, Francia, e Germania.

Il governo italiano, in sintonia con la Francia e la Germania, **ha proposto di non regolamentare i modelli di fondazione dell'IA**, suscitando preoccupazione tra organizzazioni della società civile e attori del settore tecnologico. Questa posizione, osteggiata da diversi esperti e gruppi di interesse, sottolinea **la necessità di un approccio normativo serio e coraggioso** per gestire le potenzialità e le implicazioni dell'IA generativa sulla società, i diritti fondamentali e la democrazia.

Indice degli argomenti

La proposta: l'integrazione dell'AI Act

L'Unione Europea ha risposto a questa sfida proponendo integrazioni al Regolamento sull'Intelligenza Artificiale (AI Act), che include specifiche regole per i fornitori di foundation models. Tra queste regole figurano l'obbligo di **audit indipendenti**, test di sicurezza e cybersecurity, misure di governance dei dati, valutazione dei rischi e sforzi per la loro riduzione. Tuttavia, il processo legislativo è attualmente bloccato, con alcuni paesi, tra cui l'Italia, che stanno facendo marcia indietro sulla regolamentazione dei foundation models.

Il dibattito si è intensificato a seguito del successo di modelli avanzati, come il GPT-4, portando le istituzioni europee a cercare un equilibrio tra regolamentazione e innovazione. Tuttavia, l'opposizione di Francia, Germania e, più recentemente, dell'Italia, riflette le pressioni delle lobby industriali, come la start-up francese Mistral e l'azienda tedesca Aleph Alpha. Queste aziende **sostengono che una regolamentazione troppo stringente** potrebbe danneggiare la competitività delle imprese europee rispetto ai concorrenti statunitensi e cinesi. (continua)

https://www.cybersecurity360.it/legal/privacy-dati-personali/ai-la-lunga-strada-verso-la-regolamentazione-ecco-lo-scenario-europeo/

CYBERSECURITY360- *Luisa Franchina , Tommaso Maria Ruocco- 28 Nov 2023*

Dominio cyber e spaziale sono interdipendenti. L'attacco a Jaxa lo dimostra

Le autorità giapponesi hanno reso noto che Jaxa è stata soggetta ad un cyber-attacco. Nessuna informazione sensibile è stata alterata, ma l'episodio evidenzia la necessità di incrementare gli sforzi nella protezione informatica di assetti critici come quelli spaziali.

Un attacco cyber ha perforato i sistemi di sicurezza dell'agenzia spaziale giapponese (Jaxa) senza che quest'ultima se ne sia resa conto. Anzi, ad avvisare l'ente spaziale sarebbero state le forze di sicurezza nazionali di Tokyo a mesi di distanza. A darne notizia è stato il segretario del Gabinetto giapponese, **Hirokazu Matsuno**, durante una conferenza stampa, confermando come l'Agenzia sia stata soggetta ad un attacco cibernetico, specificando però che gli attaccanti non avrebbero avuto accesso a informazioni sensibili.

La dinamica

L'attacco, come si apprende da fonti giapponesi, è avvenuto quest'estate, ma dalle prime ricostruzioni non avrebbe riguardato informazioni sensibili su razzi o satelliti. Sarebbe stato portato all'attenzione dell'agenzia solo in autunno da parte della polizia giapponese. Una dinamica che evidenzia la necessità di incrementare gli sforzi di controllo delle infrastrutture critiche. Al momento, le autorità giapponesi stanno portando avanti le operazioni di investigazione per identificare l'origine dell'attacco. Uno sforzo, questo, particolarmente complesso se si considera la difficoltà legata al processo di attribuzione di cyber-attacchi. *(Continua…)*
https://formiche.net/2023/11/dominio-cyber-e-spaziale-sono-interdipendenti-lattacco-a-jaxa-lo-dimostra/
***Formiche.net** – Giulia Pascuzzi – 29 Nov 2023*

Uso sicuro dell'intelligenza artificiale, l'ACN aderisce alle linee guida internazionali: punti chiave

L'Agenzia per la Cybersicurezza Nazionale è tra le 23 autorità di 18 Paesi che hanno sottoscritto le linee guida internazionali sull'intelligenza artificiale, proposte dal National Cyber Security Centre del Regno Unito e scaturite durante l'AI Safety Summit. Obiettivo: sostenerne uno sviluppo responsabile, etico e sicuro

Fornire agli sviluppatori una serie di **utili indicazioni per un uso sicuro, responsabile ed etico dell'intelligenza artificiale**: è questo l'obiettivo delle **linee guida internazionali** alle quali ha aderito anche l'**Agenzia per la Cybersicurezza Nazionale (ACN)** insieme ad altre 22 agenzie di 18 paesi in tutto il mondo.

Il documento congiunto, promosso dal National Cyber Security Centre del Regno Unito ed elaborato con la collaborazione della Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti, è stato realizzato da esperti governativi e del settore privato che hanno partecipato ai lavori del primo "AI Safety Summit".

I Paesi che hanno contribuito alle linee guida sono: Australia, Canada, Cile, Corea del Sud, Estonia, Francia, Germania, Giappone, Israele, Italia, Nigeria, Norvegia, Nuova Zelanda, Polonia, Regno Unito, Repubblica Ceca, Singapore e Stati Uniti.

Indice degli argomenti

Innalzare i livelli di cyber security dell'intelligenza artificiale

Le linee guida internazionali offrono, dunque, alcune utili indicazioni generali destinate, in particolare, agli sviluppatori di qualunque sistema basato sulle tecnologie di intelligenza artificiale. Tali sistemi, infatti, sono soggetti a **nuovi rischi di sicurezza** che devono essere considerati insieme alle minacce standard alla sicurezza informatica.

La cyber sicurezza, grazie ai principi essenziali di correttezza, affidabilità, privacy e resilienza diventa condizione pre-essenziale dell'intelligenza artificiale, garantendo così un cyberspazio più sicuro. Pertanto, gli sviluppatori che utilizzano modelli ospitati da un'organizzazione terza o interfacce di programmazione di applicazioni esterne (API), sono invitati a seguire tali direttive al fine di contribuire a creare un'IA responsabile, sicura ed etica. (continua)
https://www.cybersecurity360.it/cybersecurity-nazionale/uso-sicuro-dellintelligenza-artificiale-lacn-aderisce-alle-linee-guida-internazionali-punti-chiave/

CYBERSECURITY360- *Alessandro D'Ascenzo- 29 Nov 2023*

L'attacco cyber al distretto idrico del Texas si sta rivelando un disastro. Ecco il perché sono importanti le Infrastrutture Critiche Nazionali.
Un paio di giorni fa si è saputo di un attacco informatico al **North Texas Municipal Water District (NTMWD)** da parte **del gruppo ransomware Daixin**. Ciò è accaduto poco dopo l'attacco alla **Aliquippa Water Authority in Pennsylvania,** presumibilmente dietro il **gruppo iraniano Cyber Av3ngers.**
Nel caso di NTMWD, gli hacker criminali di Daixin affermano di aver bloccato dai **300 ai 400 server della contea l'11 novembre,** come confermato da un corrispondente rapporto di interruzione telefonica emesso da NTMWD il giorno successivo. Inoltre, **ancora oggi si osservano interruzioni, a giudicare dalla tabella rossa sul sito web NTMWD.**
Il sito di leak di Daixin afferma che gli aggressori hanno avuto accesso a **33.844 file NTMWD, sostenendo inoltre che nel prossimo futuro si verificherà una fuga completa di questi dati**. I funzionari di Daixin hanno affermato di non aver disabilitato le apparecchiature tecniche NTMWD né di aver interrotto le forniture idriche.
NTMWD serve circa **2 milioni di residenti in 10 contee del Texas settentrionale,** fornendo **servizi essenziali per l'acqua, le acque reflue e i rifiuti solidi.** *(Continua…)*
https://www.redhotcyber.com/post/lattacco-cyber-al-distretto-idrico-del-texas-si-sta-rivelando-un-disastro-ecco-il-perche-sono-importanti-le-infrastrutture-critiche-nazionali/
Red Hot Cyber *- Redazione RHC – 30 Nov 2023*

"L'Ue deve difendersi dagli attacchi informatici e saper rispondere"
Lo ha detto il presidente del Consiglio europer, Charles Michel a una conferenza sulle debolezze dell'Ue nel settore della Difesa, che i 27 Stati membri faticano a risolvere
Il presidente del Consiglio europeo **Charles Michel** ha proposto una "forza cibernetica europea" contro gli attacchi informatici dotata di "capacità offensive".
Da tempo si parla delle difficoltà dell'Ue nel settore della Difesa e in quello della risposta agli **attacchi informatici**, ma l'idea che Michel ha lanciato a una Conferenza annuale dell'Agenzia europea per la difesa (EDA) suggerisce un approccio più assertivo rispetto ai termini in cui si parla della questione ai vertici delle istituzioni europee.
Il capo del Consiglio europeo, che contribuisce all'indirizzo politico dei 27 capi di Stato e di governo dell'Ue, ha insistito sulla necessità "di assumere una posizione di leadership nelle operazioni di risposta informatica acquisendo anche una condizione di **superiorità** nella raccolta delle informazioni".
Alla stessa conferenza la presidente della Commissione europea **Ursula von der Leyen** ha suggerito ai governi europei di trasferire le competenze di difesa cibernetica dal livello nazionale a quello europeo. "Dobbiamo identificare le nostre capacità di punta, come la forza dell'industria spaziale".*(Continua…)*
https://it.euronews.com/my-europe/2023/11/30/lue-deve-difendersi-dagli-attacchi-informatici-e-saper-rispondere
Euronews *- Mared Gwyn Jones & Gianluca Martucci – 30 Nov 2023*

Siemens PLCs Still Vulnerable to Stuxnet-like Cyberattacks

Security updates are tedious and difficult, so users continue to use a weak version of a core protocol and remain exposed to major attacks on critical infrastructure. Programmable logic controllers (PLCs) that were vulnerable to the Stuxnet attack are still in use globally and rarely have security controls deployed — meaning they're still at risk.
More than 10 years after Stuxnet, new research shows users rarely switch on security controls such as using passwords, and feel updates are too cumbersome to be applied.
Colin Finck, tech lead of reverse engineering and connectivity at Enlyze, says the Siemens proprietary protocol which is used to read and write data as well as to program the S7 PLC. However, this is only protected by obfuscation, which the researchers were able to bypass.
Finck and his colleague Tom Dohrmann, software engineer, reverse engineering and connectivity, will present their findings at Black Hat Europe in London next week, in a talk titled "A Decade After Stuxnet: How Siemens S7 Is Still an Attacker's Heaven."
Still Feeling the Stuxnet Effects
In the 2010 attack, the Stuxnet attackers exploited several zero-day vulnerabilities in Microsoft Windows to ultimately gain access to Siemens software and the PLCs. This was done to gain access to and effectively damage high-speed centrifuges at the Iranian Bushehr nuclear power plant.
The impact of Stuxnet was huge, as it remotely damaged around a thousand centrifuges, and the worm's controllers were also able to analyze communication protocols between the PLCs to exploit further technological weaknesses. It also paved the way for things to come: After Stuxnet, a number of industrial control-related attacks were detected over the years, including BlackEnergy and Colonial Pipeline. (continua)
https://www.darkreading.com/ics-ot-security/siemens-plcs-still-vulnerable-stuxnet-like-cyberattacks
Dark Reading *-Dan Raywood -November 30, 2023*

Pro-Iran Attackers Access Multiple Water Facility Controllers
Multiple agencies warn that attackers have been active since Nov. 22, targeting operational technology (OT) across the US. Critical infrastructure in multiple US states may have been compromised by Iran-affiliated attackers targeting programmable logic controllers (PLCs).
A warning from the FBI, Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), the Environmental Protection Agency (EPA), and the Israel National Cyber Directorate comes after an attack was detected on a Pennsylvania water authority last week, where the CyberAv3ngers threat group hacked Unitronics Vision Series PLCs.
Researchers believe that the CyberAv3ngers are affiliated with Iranian Government Islamic Revolutionary Guard Corps (IRGC), and are politically motivated to go after the Unitronics PLCs, which have components that are Israeli-owned.
The national intelligence and security agencies are now warning that the attacks extend beyond the Keystone State; beginning on Nov. 22, the cyber actors accessed multiple US-based facilities that utilize Unitronic PLCs with human machine interfaces (including water and wastewater installations), likely by compromising Internet-accessible devices with default passwords. Worse, the attackers may have had access for more than 10 days. (continua)
https://www.darkreading.com/ics-ot-security/Pro-Iran-Attackers-Access-Multiple-Water-Facility-Controllers
Dark Reading *-Dan Raywood- December 4, 2023*

Cyber security delle infrastrutture critiche, una priorità: il governo definisce le strategie di difesa

Nella recente riunione del Comitato interministeriale per la cybersicurezza, presieduto dal Presidente del Consiglio Giorgia Meloni, sono state analizzate le sfide che attendono il nostro Paese, alla luce dei conflitti in Ucraina e Medio Oriente, e definite le necessarie strategie difensive per proteggere le infrastrutture critiche. Facciamo il punto

La **delicata situazione geopolitica internazionale** relativa ai **conflitti in Ucraina e Medio Oriente** sta notevolmente **influenzando lo stato nazionale di sicurezza cibernetica**: in questo contesto, diventa **prioritario adottare le migliori strategie difensive** per garantire la protezione delle nostre infrastrutture critiche.

È stato questo il tema affrontato nel corso della riunione, tenutasi il 28 novembre 2023, del Comitato interministeriale per la cybersicurezza (CIC), presieduta dal Presidente del Consiglio dei ministri, Giorgia Meloni, che ha visto la partecipazione del Sottosegretario Alfredo Mantovano, Autorità delegata per la sicurezza della Repubblica (ASSM), e delle Amministrazioni di governo centrale con competenze in ambito cyber.

Durante la riunione del Comitato interministeriale è stata focalizzata l'attenzione sull'incremento degli attacchi informatici e dell'attivismo hacker registrato a seguito dei conflitti e indirizzato anche verso siti istituzionali.

Inoltre, ai lavori del CIC hanno presenziato, su invito del Presidente Meloni, anche il Governatore della Banca d'Italia, Fabio Panetta, il Procuratore nazionale antimafia e antiterrorismo, Giovanni Melillo, e il Direttore del Dipartimento Informazioni per la Sicurezza, Elisabetta Belloni.

Indice degli argomenti

Impegno concreto nel fronteggiare le cyber minacce

Il Comitato interministeriale per la cybersicurezza (CIC), lo ricordiamo, ha funzioni di consulenza, proposta e vigilanza in materia di politiche di cyber security, suggerendo al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale. (continua)

https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-security-delle-infrastrutture-critiche-una-priorita-il-governo-definisce-le-strategie-di-difesa/

CYBERSECURITY360 - *Luca Marchese, Gaia D'Ariano- 05 Dic 2023*

Israele, finita la tregua riprende anche la guerra cyber. L'analisi di Iezzi

Gli hacktivisti pro Hamas, protagonisti digitali nei primi giorni del conflitto, hanno rialzato la testa dopo il fallimento delle trattative in Qatar e l'improvvisa interruzione della tregua sul terreno, finalizzata allo scambio di ostaggi e prigionieri. Secondo l'osservatorio Cyber war di Swascan – parte del polo italiano per la cybersicurezza di Tinexta Group – già dalle prime ore di venerdì, poche ore dopo alcuni attentati a Gerusalemme, sono riprese le attività offensive della quinta dimensione e due collettivi in particolare hanno rivendicato attacchi contro Israele: Hacktivist of Garuda, un gruppo di origine indonesiana, attivo dal luglio 2022 e specializzato in *web defacement*; e VulzSec, attivo invece da fine aprile 2023 – anch'esso apparentemente indonesiano – che oltre alla pubblicazione di data leak ha anche effettuato attacchi DDoS.

Inoltre, VulzSec ha annunciato la pubblicazione di un presunto *data breach* in queste ore del ministero della Difesa israeliano. A queste due realtà si aggiunge il gruppo Anonymous Arabia, che è riuscito a mettere offline il sito di una delle prime 20 compagnie israeliane produttrice di semiconduttori.
La fine della tregua tra le due parti ha quindi riacceso la polveriera: non è da escludere che i movimenti di questi collettivi, apparentemente indipendenti o spontanei, siano in realtà in qualche modo influenzati e sostenuti da organismi statali, vista la precisione nell'agire in concomitanza con quanto accade su diversi piani: dal campo di battaglia all'ambiente cittadino dove si compiono attentati terroristici. (continua)
https://formiche.net/2023/12/israele-cyber-finita-tregua-iezzi/
Formiche - *Di Pierguido Iezzi - 05/12/2023 -*

Questa è l'ultima newsletter del 2023.
Come ogni anno, cogliamo l'occasione per augurare a tutti i nostri soci e simpatizzanti un Natale sereno e un buon inizio di Anno Nuovo.
Arrivederci al 2024!

NOTIZIE D'INTERESSE:

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

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 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 Andrea Agostino Fumagalli Marco Raul Massoni *ai quali potete inviare suggerimenti e quesiti scrivendo a:* *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

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.