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. 11/ 2024** **dicembre 2024**

E' una bella cosa l'automazione!

Qualche tempo fa, dovendo prenotare una visita specialistica, sono andato sul sito della Regione e, dopo essere entrato con lo SPID e aver inserito il numero della tessera sanitaria e il codice della ricetta, il sistema mi ha esposto le strutture dove poter effettuare la visita.
La prima era dopo due giorni – incredibile! - in una struttura sanitaria un po' distante dalla mia zona ma l'alternativa era aspettare sei mesi!!! Ovviamente ho prenotato subito, il sistema mi ha dato la conferma, ho stampato la ricevuta e avrei anche potuto pagare online ma siccome mi avevano fatto un po' di storie qualche tempo prima per essermi presentato ad una visita con un pagamento già effettuato - cosa che evidentemente li aveva disturbati - ho deciso di pagare direttamente in cassa il giorno della visita. Mi è arrivato un sms di conferma sul telefonino e così dopo due giorni mi sono avviato di buon mattino.
Conoscendo il traffico della zona e le difficoltà di parcheggio ed essendo, come dicevo, la struttura un po' lontana, mi sono avviato molto per tempo, partendo due ore prima… ed ho fatto bene!

Preso il numeretto, sono andato in sala di attesa aspettando il mio turno per pagare. Non vi dico la confusione, un sacco di gente, alcuni che si lamentavano, c'era un vecchio che stava dando in escandescenze e un sorvegliante che stava cercando di rabbonirlo.
Al mio turno, mancava mezz'ora alla visita, ho mostrato la ricevuta e ho tirato fuori il portafoglio per il pagamento. Però ho visto che l'addetta allo sportello stava mettendoci un po' troppo tempo, poi ha cominciato ad agitarsi e infine, smoccolando qualcosa tra sé e sé, mi ha quasi gridato:

'Ma lei come l'ha prenotata questa visita???'

'Io? Online…'

'Come, online? Da solo?'

Ho cominciato a sentirmi un po' imbarazzato, anzi quasi offeso:

'Certo che sì, ancora sono capace!'

'E come ha fatto, senza l'operatore?'

'Ma sì, l'ho prenotata sul sito web della Regione'

'NON LO FACCIA MAI PIU', ha quasi gridato, 'mi ha bloccato tutto il sistema, mancano informazioni che avrebbe dovuto inserire!'

A quel punto ho cominciato a impaurirmi, pensavo che forse mi avrebbero cacciato, ho visto con la coda dell'occhio che anche il sorvegliante si era avvicinato.

'Ma io ho inserito tutti i dati che voleva il sistema, non mi ha chiesto altro, tanto che mi ha stampato la ricevuta e mi ha inviato anche la conferma via sms… cosa altro voleva che mi chiedesse…' ho quasi balbettato, ormai rosso di vergogna.

'Macché sistema e sistema, lei ha fatto una cosa che non doveva fare, ci sono le persone pagate apposta per svolgere certi compiti, altro che modernità, sistemi automatici, internet, sms e belle cose di questo genere!'

'E adesso cosa facciamo?' ha proseguito, dopo un prolungato consulto con un collega, scuotendo la testa.

'A me lo domanda?'

'Si proprio a lei! Adesso dovremo cancellare questa prenotazione e poi farne una nuova ma possiamo farlo solo cinque minuti prima dell'appuntamento, altrimenti il sistema potrebbe impazzire… e lei risulterebbe prenotato due volte e magari potrebbe perdere la visita e dover pagare una multa! Vada in quell'angolo e attenda!'

Allora mi sono messo in un angolo dello stanzone, proprio come fossi in punizione e ho atteso con trepidazione che arrivasse il momento giusto.
Proprio cinque minuti prima dell'appuntamento ho richiamato l'attenzione della sportellista, tra gli sguardi inferociti delle altre persone che pensavano volessi saltare la fila, e grazie a Dio – ormai non ci speravo più – tra imprecazioni varie dell'operatore sono riuscito ad ottenere la mia accettazione. Al momento di pagare il ticket ho mostrato la mia carta di credito e dopo un primo tentativo andato a vuoto e vedendo lo sguardo di muto rimprovero, per evitare altri guai e qualche condanna certa, ho preferito pagare in contanti, fino all'ultimo spicciolo.

Sono corso al piano superiore appena in tempo perché era già apparso il mio numero sul tabellone e ho cercato la stanza del dottore. Era chiusa, con un bel cartello 'PROIBITO ENTRARE – NON BUSSARE – VISITA IN CORSO'. Non c'era nessuno a cui chiedere, e rischiavo di fare tardi, allora mi sono fatto coraggio, ho bussato e ho sentito 'AVANTI!' Ho infilato la testa e ho chiesto 'Posso?'

'Che fa lì sulla porta, entri e venga qui!'

'Ma ho letto il cartello, PROIBITO ENTRARE…'

'Ma dove vive, non lo sa che in Italia la parola 'proibito' è quasi un invito? Per essere veramente proibito deve esserci scritto SEVERAMENTE PROIBITO, magari accompagnato da qualche disegno come un teschio o pericolo di morte o di radiazioni… ma venga qui a sedere!'
E ha cominciato a domandare delle mie malattie passate e degli interventi subìti.

Allora, tutto orgoglioso, ho tirato fuori dalla cartellina due fogli con l'elenco di tutte le cose di cui ho sofferto, insomma una anamnesi completa che aggiorno sempre ed esibisco ad ogni visita, perché - non so se ci avete mai fatto caso - tutti quanti i dottori fanno sempre le stesse domande e ogni volta bisogna ricordarsi e ripetere tutto quanto, dalle malattie dell'infanzia, alle operazioni effettuate, all'unghia incarnita. Mah!

'E questo cos'è?', mi ha chiesto un po' sorpreso il medico.

'Mi sono premunito, non sapevo se lei poteva accedere col computer al mio Fascicolo Sanitario Elettronico e allora in questo modo le faccio risparmiare tempo'.

'Ma lei è proprio strano… alla sua età lei crede ancora nelle favole? Non lo sa che quello che lei chiama Fascicolo Sanitario Elettronico è praticamente un contenitore vuoto? Non si è accorto che ci stanno a malapena solo le ricette mediche e niente altro? Senza parlare dei problemi di accesso e di alimentazione? È la solita storia, nel nostro Paese si fanno le cose, dopo tempi biblici, e una volta realizzate, si lasciano perdere! E poi noi medici che ci stiamo a fare se non facciamo l'anamnesi del paziente?'

Comunque, bene o male, dopo aver subito l'ennesimo rimprovero, ha cominciato a scrivere a penna su un foglio tutte le cose che raccontavo e, dopo la visita, devo dire molto accurata, mi ha consegnato il

foglio riempito bello bello con la solita scrittura indecifrabile da medico, raccomandandomi di non perderlo e di portarlo la prossima volta alla visita di controllo.

Quando ho raccontato della mia avventura dell'accettazione, mi ha stretto la mano dicendomi: 'Non se la prenda e non dia retta a certe persone che evidentemente non amano il cambiamento, continui a prenotare online, è una bella cosa l'automazione… quando funziona!'
E mi ha congedato sorridendo.

Silvano Bari
Docente di "Risk Management" presso l'Università Campus Bio-medico di Roma, è vicepresidente di AIIC

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2025

Il 31 dicembre 2024 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 2025".
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 2024, pagando la relativa quota sociale, il nuovo socio avrà diritto a vedere la propria iscrizione valida fino a tutto l'anno 2025.

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.

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

NEWS E AVVENIMENTI

Leaky Cybersecurity Holes Put Water Systems at Risk At least 97 major water systems in the US have serious cybersecurity vulnerabilities and compliance issues, raising concerns that cyberattacks could disrupt businesses, industry, and the lives of millions of citizens.
Despite a spate of recent cyberattacks raising the awareness of water-infrastructure vulnerabilities, nearly 100 large community water systems (CWS) continue to have serious security weaknesses in Internet-facing systems, putting the water supply of nearly 27 million Americans at risk.

The critical and high-severity vulnerabilities affect more than 9% of the 1,062 water systems in the United States that serve at least 50,000 people, according to an Environmental Protection Agency (EPA) report released on Nov. 13. The vulnerabilities were discovered through passive assessments conducted in October that looked at more than 75,000 IP addresses and 14,400 domains.

Overall, millions of citizens — along with businesses, schools, and hospitals — rely on the affected water systems. "If malicious actors exploited the cybersecurity vulnerabilities we identified in our passive assessment, they could disrupt service or cause irreparable physical damage to drinking water infrastructure," the EPA stated.

Over the past three years, water systems have become increasingly targeted by state-sponsored groups, ransomware gangs, and hacktivists. In 2023, Iran-linked cyberattackers compromised programmable logic controllers (PLCs) at a water utility in Pennsylvania, as well as 10 wastewater treatment plants in Israel. In 2021, a hacker targeted a water treatment plant in Florida and even changed the chemical mixture for the water, but did not have the sophistication to evade detection. In September, a water treatment plant in Arkansas City, Kan., switched to manual operation after the facility was the target of a cybersecurity incident.

Water system vulnerabilities are a critical issue that could impact businesses, especially power-generation systems and data centers, but especially have the potential to cause human harm, says Vinod D'Souza, head of manufacturing and industry in the Office of the CISO at Google Cloud.

"Water utilities are unique in the [operational technology] OT world because they directly impact public health, requiring stringent security to prevent catastrophic consequences like contaminated water supplies," he says. "Their geographical spread and complex systems pose distinct cybersecurity challenges not found in other sectors."

Water, Water, Everywhere ... Nary a Drop of Security?

The United States has nearly 150,000 water systems, consisting of three types of public infrastructure. Community water systems (CWS) provide water to residents living in a town or city year-round and account for approximately a third (33.7%) of water systems. Transient noncommunity water systems (TNCWS) supply water to travelers and visitors to a specific location — such as a campground or gas station — but not on a permanent basis. These make up 54.3% of public water systems. The final 12% of systems consist of nontransient noncommunity water systems (NTNCWS), which provide water to people in nonresidential locations — such as schools, businesses, and hospitals. (continua…)

https://www.darkreading.com/vulnerabilities-threats/leaky-cybersecurity-holes-water-systems-risk

Darkreading -*Robert Lemos - November 22, 2024*

Cyber Resilience Act, cosa cambia per la sicurezza dei prodotti digitali e IoT - Il Cyber Resilience Act è stato pubblicato in Gazzetta Ufficiale dell'Unione Europea: un passaggio importante per l'incremento della sicurezza in tutti i prodotti IoT, connessi tra loro e/o alla Rete. Il regolamento entrerà in vigore il 10 dicembre 2024 e sarà pienamente applicabile dall'11 dicembre 2027. Ecco i punti cardine

Cyber Resilience Act pubblicato in GU UE

Il nuovo Regolamento Europeo 2024/2847 relativo a requisiti orizzontali (ovvero generali) di cybersecurity per i prodotti con elementi digitali (cosiddetto "Cyber Resilience Act" – "CRA") è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea lo scorso 20 novembre. Un passo sostanziale per l'incremento della sicurezza in tutti i prodotti IoT, connessi tra loro e/o alla Rete.

Di seguito cerchiamo di ripercorrere le principali disposizioni del CRA partendo, ovviamente, da quali sono i suoi obiettivi, il suo oggetto, il suo ambito applicativo e le sue peculiarità.
Inoltre, non è possibile compiere un'analisi esaustiva del CRA senza considerare l'intero ecosistema normativo riguardante la cyber security emanato, pubblicato o già entrato in vigore nel corso di questi ultimi anni da parte dell'Unione Europea.
In ultimo, vedremo quali sono le tappe applicative di questo nuovo Regolamento: informazione fondamentale per le aziende che dovranno prepararsi alla compliance.

Indice degli argomenti

Perché il Cyber Resilience Act: ce n'era bisogno?
Quando applicare il CRA; il supporto alle PMI
Le eccezioni di applicabilità del Cyber Resilience Act
Le PMI non sono esentate dall'applicazione del regolamento
Cosa cambia per i prodotti con elementi digitali
Attenzione ai prodotti con elementi digitali "importanti" e "critici"
IA e prodotti con elementi digitali: i casi ad alto rischio (dell'AI Act)
Il CRA nel nuovo contesto europeo di cyber security
Spinta all'enforcement: sanzioni rilevanti
Quando il Cyber Resilience Act andrà applicato
Conclusioni *(continua…)*

https://www.cybersecurity360.it/legal/cyber-resilience-act-cosa-cambia-per-la-sicurezza-dei-prodotti-digitali-e-iot-luci-e-ombre/

Cybersecurity360 - *Michele Pellerzi, Andrea Michinelli - 25 nov 2024*

NIS2, al via il censimento dei soggetti interessati: tutto quello che c'è da sapere - Dal primo dicembre i soggetti impattati dalla NIS2 potranno cominciare a registrarsi sulla piattaforma digitale dell'ACN, pena l'applicazione di sanzioni. Si rende quindi necessario comprendere quali siano le organizzazioni potenzialmente coinvolte dai nuovi obblighi e gli elementi centrali della normativa
A partire dal prossimo primo dicembre, i soggetti impattati dalla NIS2 in Italia potranno cominciare a registrarsi sulla piattaforma digitale dell'Agenzia per la Cybersicurezza Nazionale: l'Autorità ha rilasciato utili chiarimenti in proposito tramite una determinazione del Direttore.
In vista di tale adempimento, il cui mancato rispetto determina anche l'applicazione di sanzioni, è utile comprendere quali siano le organizzazioni potenzialmente coinvolte dai nuovi obblighi e quali siano gli elementi centrali della normativa in materia di cybersecurity di derivazione europea.

Indice degli argomenti

L'approccio corretto per il rispetto dei requisiti NIS2
Ampliamento del campo di applicazione della normativa
Rafforzamento degli obblighi per imprese e PA
La designazione del punto di contatto
Obblighi in materia di gestione del rischio cyber e notifica degli incidenti
Notifica degli incidenti
Adeguatezza e proporzionalità della sicurezza
Sanzioni
Conclusioni
(continua)

https://www.cybersecurity360.it/legal/nis2-pronti-per-la-registrazione-sul-portale-acn-quale-approccio-alla-compliance-cyber/
Cybersecurity360 - *Pietro Boccaccini - 29 nov 2024*

Fascicolo Sanitario Elettronico, cos'è, a che serve e come attivarlo
Che cos'è il Fascicolo Sanitario Elettronico, come funziona, come attivarlo. Quali gli obiettivi, i livelli di diffusione, la normativa di riferimento, le criticità ancora aperte all'apertura del nuovo anno scolastico 2024. Tutto quello che c'è da sapere.
Il **Fascicolo Sanitario Elettronico** (FSE) è uno degli strumenti in cui si concretizza la **Sanità Digitale**, insieme alle **ricette elettroniche**, alla **telemedicina** , le app e a tutti quegli interventi, che si basano sull'impiego delle tecnologie e strumenti ICT, compreso l'impiego dell'IA e dei Big Data, in ambito sanitario per riorganizzare e potenziare i servizi, coordinare l'attività dei diversi operatori, garantire una migliore e più semplice comunicazione e interazione con utenti e aziende potenzialmente coinvolte come fornitori a livello centrale, regionale e locale. Recentemente, per la necessità di dare più completa applicazione di numerosi progetti legati al PNRR, si sta provando a realizzare un salto di qualità per il FSE quanto a uniformizzazione dei documenti e dei servizi messi a disposizione nei diversi FSE delle regioni italiane.
Indice degli argomenti

Cos'è il Fascicolo sanitario elettronico
Il Fascicolo Sanitario Elettronico (FSE) è lo strumento attraverso il quale **il cittadino può tracciare e consultare tutta la storia della propria vita sanitaria**, condividendola sulla base di una opportuna autorizzazione con i professionisti sanitari di propria fiducia, per provare a garantire un servizio più efficace ed efficiente. Esso è in effetti definito come uno strumento che raccoglie "l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito" (DPCM n.179/2015) e si colloca in una ampia gamma di attività relative all'erogazione di servizi sanitari, dalla prevenzione alla verifica della qualità delle cure.
Il FSE è concepito per avere un orizzonte temporale che copre l'intera vita del paziente, in quanto è alimentato in maniera continuativa dai soggetti che lo prendono in cura nell'ambito del SSN e dei servizi socio-sanitari regionali. In esso, dunque, dovrebbe confluire l'intera storia clinica di una persona generata da più strutture sanitarie, e se possibile anche arricchita da ulteriori documenti caricati online

nel FSE dall'utente/assistito stesso, nonché dal cosiddetto "taccuino personale dell'assistito". (vedi § successivo).

Come funziona il Fascicolo sanitario elettronico e cosa contiene

L'FSE è istituito, previo consenso dell'assistito, dalle Regioni e Province Autonome, nel rispetto della normativa vigente in materia di protezione dei dati personali, per le finalità di prevenzione, diagnosi, cura e riabilitazione perseguite dai soggetti del SSN e dei servizi sociosanitari regionali che prendono in cura l'assistito. Tali soggetti, nel caso in cui il cittadino lo desideri e li autorizzi esplicitamente, possono consultare online i documenti sanitari digitali contenuti nel FSE per finalità di cura. Nelle intenzioni del legislatore, **il nucleo minimo dei dati e documenti del Fascicolo doveva essere è costituito sin da subito da**: dati identificativi e amministrativi dell'assistito; referti; verbali pronto soccorso; lettere di dimissione; profilo sanitario sintetico; dossier farmaceutico; consenso o diniego alla donazione degli organi e tessuti. Ma i contenuti dei FSE regionali sono stati a lungo abbastanza differenziati, per cui non è detto che tutto ciò fosse effettivamente disponibile e funzionante ovunque in Italia esattamente in tutti gli ambiti. (continua…)

https://www.agendadigitale.eu/sanita/fascicolo-sanitario-elettronico-cose-e-a-che-punto-e-la-guida/

Agenda Digitale -*Anna Francesca Pattaro- 2 dic 2024*

Intelligenza artificiale a servizio dei territori: al via progetti in tutte le regioni - Toscana, Liguria, Lombardia e Puglia a capo delle iniziative che si sono aggiudicate i 20 milioni messi a disposizione dal Fondo Innovazione. Callari: "La Commissione è riuscita a trovare la quadra sui progetti ritenuti maggiormente validi"

Le regioni italiane stanno avviando una serie di progetti innovativi che sfruttano l'intelligenza artificiale (AI) per risolvere problemi critici e migliorare i servizi. Toscana, Liguria, Lombardia e Puglia sono in testa a queste iniziative, assicurandosi i 20 milioni di euro stanziati dal Fondo Innovazione.

Indice degli argomenti

Toscana: AI per la sicurezza del territorio
Liguria: AI per la salute e il turismo
Lombardia: AI per l'efficienza energetica
Puglia: AI nella pubblica amministrazione
Il fil rouge: applicare l'AI nei diversi ambiti della PA
(continua)

https://www.corrierecomunicazioni.it/pa-digitale/intelligenza-artificiale-a-servizio-dei-territori-al-via-progetti-in-tutte-le-regioni/

Corriere delle Comunicazioni - *Veronica Balocco, 3 dic 2024*

NIS 2: quali obblighi per le aziende sanitarie? - La NIS 2 è la Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio, che aggiorna la precedente direttiva NIS (Network and Information Security) del 2016. Ha l'obiettivo di rafforzare la sicurezza informatica nell'Unione Europea, soprattutto nei settori critici, a fronte dell'aumento e della complessità degli attacchi informatici, introducendo una serie di obblighi e misure per migliorare la resilienza e la risposta agli attacchi subiti dagli Stati membri e dalle organizzazioni operanti in settori essenziali.

La Direttiva, rispetto alla previgente, si applica a un maggior numero di soggetti considerati essenziali e importanti, come il sanitario, l'energia, il trasporto, le finanze, le infrastrutture digitali, i servizi

pubblici, le industrie chimiche e la fornitura di acqua potabile, e introduce criteri dimensionali (sono incluse anche realtà di medie dimensioni).
Le aziende devono adottare misure di sicurezza più stringenti per prevenire e mitigare i rischi informatici. Devono anche implementare un sistema di gestione della sicurezza delle informazioni, valutare regolarmente i rischi e adottare pratiche di gestione della continuità operativa.
Le organizzazioni devono segnalare entro 24 ore all'ACN (Agenzia per la Cybersicurezza Nazionale) eventuali incidenti rilevanti per la sicurezza, seguendo un processo di notifica diviso in fasi. Questo include un rapporto iniziale, un rapporto intermedio e una relazione finale sull'incidente. L'ACN è designata come Autorità nazionale competente NIS e punto di contatto unico, con il compito di coordinare l'attuazione del decreto che recepisce la Direttiva e collaborare con le autorità di settore per garantire la sicurezza informatica. Sono ovviamente previste sanzioni per le organizzazioni che non rispettano gli obblighi stabiliti, al fine di incentivare l'adozione di adeguate misure di sicurezza.
(*continua…)*
https://www.snewsonline.com/saccone-nis-2-obblighi-aziende-sanitarie/
SNews - *Umberto Saccone - 3 Dicembre 2024*

L'intelligenza artificiale per il futuro sostenibile - Promuovere lo sviluppo di modelli di IA rispondenti ai principi di responsabilità sociale e sostenibilità: le nuove tecnologie possono ottimizzare l'uso dell'energia, definire azioni per ridurre l'inquinamento e prevedere eventi climatici estremi.
L'intelligenza artificiale (IA) è una delle principali tecnologie in grado di cambiare in modo drastico la nostra società.
La capacità dei sistemi di IA di analizzare in modo rapido enormi quantità di dati e di automatizzare diversi processi umani mostra caratteristiche potenzialmente rivoluzionarie in diversi ambiti nel settore pubblico e privato.
Per quanto riguarda l'Italia, che ha una lunga tradizione industriale e manifatturiera, l'integrazione delle tecniche principali di IA rappresenta una sfida fondamentale per rafforzare la competitività economica e migliorare la qualità della vita.
Tuttavia, questi obiettivi devono essere raggiunti attraverso una visione human-centered dell'IA, che sia al servizio del benessere delle persone e della società e che rivolga una particolare attenzione agli aspetti etici. Infatti, la tecnologia non deve essere neutra, ma espressamente orientata verso un miglioramento delle condizioni sociali e ambientali, nel rispetto della privacy e dei diritti delle persone.
Per queste ragioni è cruciale promuovere lo sviluppo e l'adozione di modelli di IA che siano affidabili e trasparenti e che rispondano ai principi europei di responsabilità sociale e sostenibilità.
(continua…)
https://www.puntosicuro.it/sostenibilita-C-149/l-intelligenza-artificiale-per-il-futuro-sostenibile-AR-24898
Punto Sicuro - *Redazione, 5.12.2024*

Vulnerability Management Challenges in IoT & OT Environments
By understanding the unique challenges of protecting IoT and OT devices, organizations can safeguard these critical assets against evolving cyber threats.
COMMENTARY

As Internet of Things (IoT) and operational technology (OT) devices proliferate across critical infrastructure, manufacturing, healthcare, and other sectors, they bring with them unique and significant security challenges. These devices are increasingly woven into the fabric of everyday business operations, making them essential, yet difficult to secure. While vulnerability management is a well-understood practice in traditional IT environments, IoT and OT introduce complexities that render many of these traditional practices less effective, if not completely obsolete. Here are some of the key challenges, along with strategies for tackling them.

1. Device Diversity and Legacy Systems

IoT and OT environments consist of an eclectic mix of devices that vary greatly in age, functionality, and design. For example, a manufacturing plant might have sensors and controllers that are 20 years old sitting alongside cutting-edge IoT devices. Each device often has a unique operating system and set of protocols, which complicates vulnerability assessments and patch management. Furthermore, many of these legacy systems were designed without security in mind, and their manufacturers may no longer support them.

Solution: Given the heterogeneous nature of these devices, it's crucial to take a risk-based approach. Prioritize the most critical systems and those with the highest vulnerability impact. In some cases, implementing compensating controls, such as network segmentation or increased monitoring, can mitigate risks when patching is not an option.

2. Resource Constraints and Limited Patching Options

Unlike IT systems, many IoT and OT devices have limited processing power, memory, and storage, which makes it challenging to run security software or apply frequent updates. Additionally, many OT devices can't be easily patched or updated without downtime, which can be costly in critical industries like healthcare or manufacturing.

Solution: To mitigate the limitations of patching, consider adopting lightweight vulnerability scanning tools that are specifically designed for IoT and OT environments. Moreover, focus on securing device access by implementing strict authentication controls and isolating critical devices in dedicated network segments.

3. Operational Disruption and Downtime

The need to keep OT systems operational 24/7 is often at odds with the requirements of effective vulnerability management. For instance, in a power plant or factory, even a brief downtime for patching could result in significant financial losses and potential safety risks.

Solution: Careful planning and collaboration between IT and OT teams are essential to manage these trade-offs. Schedule updates and vulnerability scans during maintenance windows and consider redundancy strategies to minimize impact. Additionally, organizations can implement patch-testing in lab environments to ensure compatibility before deploying to production.

4. Inadequate Security Protocols and Access Controls

Many IoT and OT devices lack robust security protocols, making them prime targets for attackers. For example, default passwords and insecure network protocols are common in legacy OT systems, and many IoT devices lack strong encryption or authentication mechanisms. This lack of security leads to increased risk of unauthorized access and exploitation.

Solution: Start by enforcing strict access control policies, such as unique credentials and multifactor authentication. Implementing network segmentation to isolate vulnerable devices from other parts of the network can further limit exposure. Adopting a zero-trust model for IoT and OT environments can also help mitigate the risks associated with inadequate authentication and access controls. (continua….)

https://www.darkreading.com/vulnerabilities-threats/vulnerability-management-challenges-iot-ot-environments

Dark Reading -*Malleswar Reddy Yerabolu - December 5, 2024*

"Unprecedented cyberattack" sparks warning to US citizens to switch to encryption

The attack by Salt Typhoon has reignited calls for people to switch to more secure services

US authorities are urging Americans to use encrypted messaging apps to secure their sensitive data against foreign attackers.

The security call comes in the wake of an "unprecedented cyberattack" on the country's telecom companies, NBC News reported. The attack is considered among the largest intelligence compromises in US history and isn't yet fully fixed.

The China-linked Salt Typhoon group was first spotted targeting US telecoms with a new backdoor malware a few months ago. It has reportedly hacked the likes of AT&T, Verizon, and Lumen Technologies to spy on their customers' activities.

The need for strong encryption

"Encryption is your friend, whether it's on text messaging or if you have the capacity to use encrypted voice communication. Even if the adversary is able to intercept the data, if it is encrypted, it will make it impossible," said Jeff Greene, executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday – as per NBC News.

Encryption refers to scrambling the data into an unreadable form to prevent third-party access. From messaging apps like WhatsApp, Signal, and Session to secure email services like ProtonMail and Tuta, online communications are expected to remain private from the sender to the receiver (end to end) thanks to this technology.

Besides encrypting chats and calls leaving your device, FBI officials also suggest keeping your smartphone up-to-date and enabling two-factor authentication whenever possible to protect your accounts against phishing attacks.

Do you know?

The US Cybersecurity and Infrastructure Security Agency (CISA) has also published new guidance for helping enterprises defend against Salt Typhoon's threats, which includes a series of best practices and other security tips to stay protected. (continua…)

https://www.techradar.com/vpn/vpn-privacy-security/unprecedented-cyberattack-sparks-warning-to-us-citizens-to-switch-to-encryption?utm_term=BE399376-883B-4F0A-B0F5-0EF281E9D4C0&lrh=9b8172938b69372afc2de4d1954e1c5a313105adf4497971eee4ea4dbc37c72a&utm_campaign=79B375AA-AA0B-4881-99A1-64F0F9BDBE17&utm_medium=email&utm_content=AA8CDC97-C840-45A1-BA04-CE53C23A0CE1&utm_source=SmartBrief

TECHRadar - *Chiara Castro - December 5, 2024*

La guerra dei chip tra Stati Uniti e Cina: un conflitto tecnologico e commerciale

La "guerra dei chip" tra USA e Cina non riguarda solo i semiconduttori, ma rappresenta una lotta per il dominio tecnologico globale. Gli sviluppi futuri avranno implicazioni di vasta portata per tutto l'equilibrio economico globale, data la centralità dei chip nelle moderne infrastrutture tecnologiche. Il punto

Negli ultimi anni, la **competizione tecnologica e commerciale tra Stati Uniti e Cina** ha raggiunto un nuovo punto critico, focalizzandosi sul **settore strategico dei semiconduttori**. Il recente ampliamento

della “Entity list” da parte del Dipartimento del Commercio degli Stati Uniti rappresenta l’ultimo sviluppo di questa disputa.

La decisione mira a **limitare l’accesso della Cina a tecnologie avanzate**, considerate cruciali per la sicurezza nazionale americana. La Cina replica bloccando le vendite di materie prime agli USA.

Indice degli argomenti

Le nuove restrizioni nella guerra dei chip

Il 2 dicembre 2024, il Dipartimento del Commercio degli Stati Uniti ha aggiunto 140 aziende cinesi, comprese filiali in Giappone, Corea del Sud e Singapore, alla “Entity List”. Questa misura si aggiunge a provvedimenti simili del 2022 e 2023, consolidando una strategia mirata a rallentare i progressi tecnologici della Cina.

Tra le aziende incluse nella lista spiccano Semiconductor Manufacturing International Corp., Beijing Naura, Acm Research e Piotech, oltre a realtà legate a Huawei.

L’obiettivo dichiarato è impedire che tali organizzazioni utilizzino tecnologie statunitensi per avanzare nei settori dei semiconduttori e dell’intelligenza artificiale, settori ritenuti fondamentali per il potenziale militare e di sorveglianza della Cina.

“Stiamo direttamente impedendo la modernizzazione militare della RPC, i programmi sulle armi di distruzione di massa e la capacità di reprimere i diritti umani” ha dichiarato Matthew S. Axelrod, assistente segretario per l’applicazione delle esportazioni.

Le nuove restrizioni colpiscono anche i chip di memoria a larghezza di banda elevata (HBM), che sono componenti fondamentali per supportare i rapidi trasferimenti di dati tra processori e consentire calcoli avanzati utilizzati in applicazioni di intelligenza artificiale e machine learning.

Questi chip, grazie alla loro capacità di gestire grandi volumi di dati in tempo reale, sono indispensabili per alimentare piattaforme come supercomputer, sistemi di analisi predittiva e tecnologie di guida autonoma.

Le restrizioni riguardano, inoltre, venti tipi di attrezzature per la produzione di semiconduttori, tra cui apparecchiature utilizzate per la litografia avanzata, e tre strumenti software essenziali per lo sviluppo e la progettazione di semiconduttori complessi.

Ricadute sullo sviluppo delle tecnologie di punta

I principali produttori di chip HBM, tra cui colossi come SK Hynix, Samsung Electronics e Micron, sono leader di mercato nella fornitura di queste tecnologie critiche. Questi componenti, oltre a essere utilizzati in dispositivi consumer, trovano applicazione in settori strategici come la difesa e la ricerca scientifica.

Il blocco delle esportazioni verso la Cina potrebbe **influire** non solo sulle operazioni dei produttori cinesi, ma anche sullo sviluppo delle tecnologie di punta che richiedono semiconduttori ad alte prestazioni.

Il Dipartimento del Commercio degli Stati Uniti ha sottolineato come queste misure rientrino in un approccio coordinato con alleati e partner per ridurre la capacità della Cina di auto-produrre tecnologie avanzate. (continua…)

https://www.cybersecurity360.it/cybersecurity-nazionale/la-guerra-dei-chip-tra-stati-uniti-e-cina-un-conflitto-tecnologico-e-commerciale/

Cybersecurity360 -*Luisa Franchina, Tommaso Diddi - 6 dic 2024*

Strutture idriche nel mirino: strategie e tecnologie per difenderle

Gli attacchi informatici alle infrastrutture idriche aumentano in maniera allarmante. Sistemi obsoleti, reti poco sicure e mancanza di formazione espongono le infrastrutture critiche a rischi crescenti di penetrazione digitale

L**a protezione delle infrastrutture critiche** rappresenta sempre più una priorità strategica per governi, istituzioni pubbliche e imprese. **Tra i target principali, insieme al settore sanitario, manifatturiero e dei trasporti, vi è il settore Energy & Utilities,** che comprende la produzione, distribuzione e stoccaggio di energia, la gestione dei rifiuti e la manutenzione delle aree verdi, ma anche l'approvvigionamento idrico, l**a gestione del ciclo dell'acqua e il trattamento delle acque reflue.**

Indice degli argomenti

Garantire la sicurezza e la continuità operativa nel settore Energy & Utilities

Garantire la sicurezza e la continuità operativa di questi sistemi è essenziale non solo per preservare la stabilità economica e il benessere della popolazione, ma anche per rafforzare la resilienza del sistema-Paese di fronte a minacce cyber sempre più sofisticate.

Le infrastrutture critiche, tra cui anche quelle idriche, rappresentano, infatti, uno degli obiettivi principali di cyber criminali, hacktivisti e di gruppi hacker cosiddetti "State-sponsored", che agiscono a supporto di enti governativi per il raggiungimento di obiettivi strategici precisi.

Attacchi alle utilities in vertiginosa crescita: i dati Usa

Secondo quanto rilevato dai ricercatori di Check Point Research, nel 2024 si è assistito a un aumento di circa il **70% di attacchi informatici** ai danni di aziende statunitensi del settore Utility. L'utilizzo di tecnologie sempre più avanzate e una maggiore connettività digitale ha permesso alle aziende di migliorare l'efficienza e la gestione delle risorse. Al tempo stesso però, ha ampliato significativamente la superficie d'attacco, rendendo i sistemi utilizzati sempre più vulnerabili.

La situazione in Italia certificata dal Clusit

Questa tendenza è confermata anche a livello nazionale dal Rapporto Clusit 2024 sulla sicurezza ICT, il quale, in relazione al **settore "Energy & Utilities"**, riporta una crescita improvvisa di attacchi nel primo trimestre del 2024 rispetto all'anno precedente. Nel periodo indicato sono infatti stati registrati più della metà del numero di incidenti verificatisi nel corso del 2023.

Le vulnerabilità del settore idrico

A tal proposito, merita particolare attenzione il settore idrico, il quale sta vivendo una forte trasformazione verso una maggiore connettività e automazione, diventando sempre più spesso oggetto di interesse per i criminali informatici.

Criticità delle infrastrutture idriche

Andrea Saturnino, Cybersecurity Specialist di HWG Sababa, ha esaminato le principali criticità che caratterizzano le infrastrutture idriche rilevando che: "La presenza di sistemi obsoleti, la scarsa segmentazione delle reti, i rischi legati alla supply chain e la mancanza di formazione del personale sono i fattori principali che a oggi rendono l'infrastruttura più vulnerabile ad attacchi informatici". (continua…)

https://www.agendadigitale.eu/sicurezza/strutture-idriche-nel-mirino-strategie-e-tecnologie-per-difenderle/

Agenda Digitale - *Martina Rossi - 9 dic 2024*

Il Comitato di Redazione e il Consiglio Direttivo AIIC augurano a tutti Buon Natale e un sereno Anno Nuovo

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

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.