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 2023 **n. 2/ 2023** **Febbraio 2023**

ECCO LE DIRETTIVE NIS2 E CER*

Il Parlamento europeo ha approvato la nuova normativa Nis2 in materia di cyber-security.
La direttiva Nis2 arricchisce e amplia la portata rispetto alla precedente, allargando qualità e quantità del perimetro di azione e introducendo una serie di attività e vincoli in capo ai destinatari.
La nuova direttiva individua due categorie di settori ai quali si applica: altamente critici e critici.
Nei primi abbiamo energia, trasporti, banche e mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, gestione di servizi Ict, Pubblica amministrazione, spazio. Nei secondi abbiamo: fornitori di servizi postali, compresi i servizi di corriere, gestione dei rifiuti, fabbricazione, produzione e distribuzione di sostanze chimiche, produzione, trasformazione e distribuzione di alimenti, manifatture, fornitori di servizi digitali, ricerca.
In particolare, la Nis2 mira a superare le carenze della differenziazione tra gli operatori di servizi essenziali e i fornitori di servizi digitali, ritenuta obsoleta.
Il testo armonizza i parametri per individuare i soggetti sottoposti agli obblighi della Nis2 introducendo un criterio relativo alle dimensioni aziendali che fissa i criteri per individuare medie e grandi imprese.
Tutte le aziende, a partire dalle medie che operano nei citati settori, sono oggetto di applicazione della direttiva. Le disposizioni potrebbero essere applicate anche alle imprese di piccole dimensioni, qualora siano ritenute essenziali per la vita economico sociale di uno Stato membro.
Il Consiglio ha poi approvato il testo della direttiva Cer (Critical entities resilience) che sostituisce la direttiva 114/08 sulla identificazione e designazione delle Infrastrutture critiche europee.
La Cer va di pari passo con la Nis2, di fatto riconciliando il concetto di sicurezza fisica o cinetica, come si dice oggi, con quello della sicurezza logica o cyber. La Nis2 si occupa infatti della sicurezza cyber delle entità critiche e altamente critiche e la Cer della loro resilienza rispetto a minacce cinetiche sia naturali sia antropiche, volontarie o involontarie, ivi comprese le minacce di stampo terroristico.
I settori delle potenziali entità critiche sono gli stessi della categoria “altamente critici” della Nis2, ai quali si aggiunge anche la produzione, trasformazione e distribuzione di alimenti (la quale rientra invece nella categoria critica della Nis2).
Il concetto di infrastruttura diventa materiale mentre quello di entità è immateriale. L’entità è pubblica o privata, fornisce un servizio essenziale ed è costituita anche da infrastrutture.
Ogni Stato membro adotterà una strategia per la resilienza che conterrà un framework di descrizione delle attività e delle responsabilità, quindi la descrizione della catena di comando e controllo e le misure adottate per la resilienza del sistema-Paese.
Se l’entità critica fornisce il servizio essenziale in sei o più Stati membri è considerata critica a livello europeo e la Commissione potrà designare delle advisory mission per verificare che le contromisure vengano applicate.
Infine, gli Stati membri dovranno basare il risk assessment governativo anche sui rischi legati alle interdipendenze – tema espressamente citato dalla direttiva – quindi serviranno modelli di effetti domino e delle interdipendenze tra settori.

* AirPress, n.140, gennaio 2023

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

Luisa Franchina
presidente dell'Associazione Italiana esperti in Infrastrutture Critiche

Luisa Franchina È stata Direttore Generale della Segreteria per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri 2010-2013). Ha pubblicato numerosi articoli e libri sulla sicurezza e sulla protezione delle infrastrutture critiche.

ATTIVITA' DELL'ASSOCIAZIONE

ATTIVITA' DI EDUCATION

Sono in corso di programmazione le attività di formazione per soci e simpatizzanti che si svolgeranno nell'anno 2023.

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.

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.
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.

VISITA GUIDATA PRESSO LA DIVISIONE AEREA DI SPERIMENTAZIONE AERONAUTICA E SPAZIALE (AEROPORTO DI PRATICA DI MARE) ultimi posti disponibili

Rimane ancora qualche posto disponibile per la visita guidata che si svolgerà **giovedì 2 marzo 2023, dalle ore 9.00 alle ore 13.00** presso il **Reparto Sperimentale di Volo** della **Divisione Aerea di Sperimentazione Aeronautica e Spaziale (D.A.S.A.S.)**, situato presso l'aeroporto militare "Mario de Bernardi" di Pratica di Mare (Roma).

Il programma prevede:

- presentazione delle principali attività del Reparto Sperimentale di Volo e dei Gruppi componenti, in particolare il Gruppo Gestione Software ed il Gruppo Ingegneria per l'Aerospazio;
- illustrazione delle attività per il biocontenimento dei velivoli per l'emergenza Covid-19;

- le caratteristiche dei velivoli presenti;
- la funzione di Entry Point sanitario nazionale per la gestione delle emergenze epidemiologiche.

Il luogo di incontro è l'Aeroporto di Pratica di Mare (Roma) da raggiungersi con mezzi propri.

Chi fosse interessato a partecipare è pregato di contattare la segreteria AIIC (segreteria@infrastrutturecritiche.it) con urgenza, e comunque entro e non oltre il giorno 17 febbraio p.v., fornendo al contempo i seguenti dati necessari per ottenere il "passi" per l'ingresso in zona aeroportuale:
nome
cognome,
luogo e data di nascita
recapito telefonico
targa dell'auto

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

RINNOVO ASSOCIATIVO ANNO 2023

Il 31 dicembre 2022 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La partecipazione associativa inalterata da anni, pari ad euro 40, con delibera del Consiglio Direttivo del 19.9.2022 è stata aumentata di una modesta quota pari ad euro 10 per l'aumento generale dei costi di gestione.
La nuova quota per il rinnovo individuale è quindi adesso 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.
Ricordiamo che la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2023. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione versando anche il contributo per le spese di segreteria.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

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

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*

NEWS E AVVENIMENTI

A Widespread Logic Controller Flaw Raises the Specter of Stuxnet

More than 120 models of Siemens' S7-1500 PLCs contain a serious vulnerability—and no fix is on the way.

In 2009, the computer worm Stuxnet crippled hundreds of centrifuges inside Iran's Natanz uranium enrichment plant by targeting the software running on the facility's industrial computers, known as programmable logic controllers. The exploited PLCs were made by the automation giant Siemens and were all models from the company's ubiquitous, long-running SIMATIC S7 product series. Now, more than a decade later, Siemens disclosed today that a vulnerability in its S7-1500 series could be exploited by an attacker to silently install malicious firmware on the devices and take full control of them.

The vulnerability was discovered by researchers at the embedded device security firm Red Balloon Security after they spent more than a year developing a methodology to evaluate the S7-1500's firmware, which Siemens has encrypted for added protection since 2013. Firmware is the low-level code that coordinates hardware and software on a computer. The vulnerability stems from a basic error in how the cryptography is implemented, but Siemens can't fix it through a software patch because the scheme is physically burned onto a dedicated ATECC CryptoAuthentication chip. As a result, Siemens says it has no fix planned for any of the 122 S7-1500 PLC models that the company lists as being vulnerable.

Siemens says that because the vulnerability requires physical access to exploit on its own, customers should mitigate the threat by assessing "the risk of physical access to the device in the target deployment" and implementing "measures to make sure that only trusted personnel have access to the physical hardware." The researchers point out, though, that the vulnerability could potentially be chained with other remote access vulnerabilities on the same network as the vulnerable S7-1500 PLCs to deliver the malicious firmware without in-person contact. The Stuxnet attackers famously used tainted USB thumb drives as a creative vector to introduce their malware into "air-gapped" networks and ultimately infect then-current S7-300 and 400 series PLCs.

"Siemens PLCs are used in very important industrial capacities around the world, many of which are potentially very attractive targets of attacks, as with Stuxnet and the nuclear centrifuges," says Grant Skipper, a Red Balloon Security research scientist.

The ubiquity and criticality of S7-1500 PLCs are the two traits that motivated the researchers to do a deep dive into the security of the devices. To a motivated and well-resourced attacker, any flaws could be worth exploiting. (continua….)

https://www.wired.com/story/siemens-s7-1500-logic-controller-flaw/

***Wired** -Lily Hay Newman- Jan 10, 2023*

Una app israeliana sta destando molti timori fra gli esperti di security - Alcune riviste specializzate hanno dato notizia di una applicazione israeliana, messa a disposizione di specifiche utenze pubbliche, in grado di modificare in tempo reale le immagini video, catturati da impianti di videosorveglianza. Di cosa si tratta?

Alcune software house israeliane sono ormai diventate famose nel mondo per avere sviluppato degli applicativi particolarmente invasivi. Certamente il più conosciuto è l'applicativo Pegasus, grazie al quale è possibile inserirsi negli apparati cellulari di personaggi politici e industriali, catturando preziose informazioni, che vengono messe a disposizione del gestore dell'applicativo.

È di pochi giorni fa la notizia, pubblicata su un quotidiano israeliano, che una software house specializzata ha messo a disposizione dei clienti, esclusivamente soggetti governativi coinvolti nella sicurezza nazionale, una app, chiamata TOKA.
L'azienda è elencata sul sito web della direzione internazionale per la cooperazione nella difesa (SIBAT), il che significa che è riconosciuta come esportatrice ufficiale di sistemi di difesa.
Sempre secondo le notizie di stampa, questa app sarebbe in grado di modificare in tempo reale l'immagini video, sia in diretta, sia registrate, cambiando ad esempio il volto delle persone che vi appaiono, oppure cancellando la presenza di soggetti, ripresi dalle telecamere.
Che fosse possibile manipolare immagini video è fatto ormai ben noto, ma l'invasività di questa applicazione supera certamente il livello di conoscenze sino ad oggi disponibili. Ecco perché, nell'interesse dei lettori e mio, ho cercato di approfondire questo tema, prendendo contatto con soggetti, operanti soprattutto in Medioriente, che certamente hanno di questa situazione una conoscenza più approfondita, rispetto agli esperti occidentali.
(*continua*….)
https://www.puntosicuro.it/security-C-125/una-app-israeliana-sta-destando-molti-timori-fra-gli-esperti-di-security-AR-22966/
PuntoSicuro - *Adalberto Biasiotti , 11/01/2023*

Royal Mail halts international services after cyberattack
The Royal Mail, UK's leading mail delivery service, has stopped its international shipping services due to "severe service disruption" caused by what it described as a "cyber incident."
While delivery and collection services across the UK have been unaffected by the incident, the company advised customers to hold export times while the issues are resolved, as they cannot be dispatched to overseas destinations.
"Incident was detected yesterday, UK/ domestic mail remains unaffected," a Royal Mail spokesperson told BleepingComputer when we reached out for more details earlier today.
In a separate statement, Royal Mail said items that have already been delivered might be subject to delays and added that Parcelforce Worldwide services haven't been disrupted.
"Our import operations continue to perform a full service, with some minor delays. Parcelforce Worldwide export services are still operating to all international destinations though customers should expect delays of one to two days." Royal Mail said.
Even though Royal Mail is yet to reveal the actual nature of this incident, it did say that it hired outside experts for an ongoing investigation and reported it to UK security agencies.
"We immediately launched an investigation into the incident and we are working with external experts. We have reported the incident to our regulators and the relevant security authorities."
A UK National Cyber Security Centre (NCSC) spokesperson said that the NCSC is "aware of an incident affecting Royal Mail Group Ltd and are working with the company, alongside the National Crime Agency, to fully understand the impact."
"Our teams are working around the clock to resolve this disruption and we will update you as soon as we have more information," Royal Mail also said on Wednesday.
Today's incident follows a November 2022 outage that led to the Royal Mail's tracking services being unavailable for more than 24 hours.
The outage affected Track and Trace website, with British residents only able to track their parcels, letters, and mail deliveries through the Royal Mail app. (continua…)
https://www.bleepingcomputer.com/news/security/royal-mail-halts-international-services-after-cyberattack/
BleepingComputer- *Sergiu Gatlan-January 11, 2023*

FAA preliminary investigation traces NOTAMS outage to damaged database file

An initial investigation into the outage that hit the Federal Aviation Administration's Notice to Air Missions system has found that the error may have been caused by a damaged database file.

In a statement issued at 6:30 p.m. EST Wednesday, the agency said it was continuing a "thorough review to determine the root case of the Notice to Air Missions (NOTAM) system outage."

"At this time, there is no evidence of a cyber attack," it said. "The FAA is working diligently to further pinpoint the causes of this issue and take all needed steps to prevent this kind of disruption from happening again."

The Federal Aviation Administration took the decision to ground aircraft between 7:30 a.m. and 9:00 a.m. EST Wednesday after an attempted reboot of the notification system was unable to rectify a system error.

Speaking to reporters on Wednesday, Transportation Secretary Pete Buttigieg shared additional details about the timeline of the outage, noting that it first began at 3:28 p.m. on Tuesday, Jan. 10.

A backup system went into effect and the main system resumed before which problems reappeared, according to the secretary's comments, which were reported by the Washington Post.

Buttigieg also shared that the FAA conducted a "complete reboot" of the NOTAMS system at about 5 a.m. EST Wednesday morning before making the decision to temporarily ground U.S. domestic air traffic because of concerns that the alerts were not populating correctly.

If the diagnosis is correct, NOTAMS will be the latest example of a major federal IT system outage caused by a damaged database file. (continua…)

https://www.fedscoop.com/faa-preliminary-investigation-traces-notams-outage-to-damaged-database-file/

FEDSCOOP- *John Hewitt Jones- JAN 12, 2023*

"Grazie a Musk ho costruito una molotov"

«Voglio lanciare un messaggio: occhio all'intelligenza artificiale, ci vuole un controllo. E serve spiegare quali siano i vantaggi e i pericoli. Prima che sfugga di mano». Marco Camisani Calzolari è uno dei massimi esperti del mondo digitale: vive a Londra, è docente all'Università Europea di Roma e molti lo conoscono come di esperto per Striscia la Notizia. Il suo allarme arriva dopo aver convinto ChatGPT, il programma di OpenAI di (chi se no?) Elon Musk, a dargli le istruzioni per costruire una bomba molotov.

Com'è possibile?

«È stato semplice: ho girato la domanda. Sono partito chiedendo come produrre un virus sul web, poi fatto lo stesso con la molotov. Ho confuso il sistema, passando da scrivi punto per punto come fare una bomba, e lì il software ha rifiutato di rispondere, a cosa bisogna fare per non far esplodere una bottiglia. Ed ecco le istruzioni».

Dunque è vero: l'intelligenza artificiale è stupida.

«È che noi sbagliamo a chiamarla intelligenza. In realtà è un sistema statistico che mette insieme pezzi di linguaggio e di informazioni. Lontano da essere senziente. Lavora per sentito dire, è come un Bar Sport».

Però, dicono, ci toglierà il lavoro.

«Solo quelli automatizzabili. Pensi a un cacciavite: all'elettricista è utile, piuttosto che togliere le viti a mano. Però bisogna saperlo usare. Ci vuole competenza: pensare di sostituirla con uno strumento così è sbagliato».

Un aiutante, in pratica.

«Certo, più veloce di noi. Ma serve un controllo. Se io chiedo a GPT3 una ricerca sulle dieci cose più usate nel mio lavoro, di sicuro lo fa meglio di un redattore. E con strumenti aggiuntivi può anche scrivere come me. Però non sa se ciò che scrive sia corretto».

Ecco il Bar Sport.

«Appunto. E può essere pericoloso. OpenAI, per carità, non vuole certo essere uno strumento negativo. Eppure pensi per esempio alle informazioni sui vaccini: poteva cambiare tutto».

In che senso?

«L'intelligenza artificiale è un associatore di frasi trovate in giro. Non sa giudicare che siano corrette. E se qualcuno gliele fa trovare sbagliate...» .(continua…)

https://www.msn.com/it-it/notizie/tecnologiaescienza/grazie-a-musk-ho-costruito-una-molotov/ar-AA16sZwf?ocid=msedgntp&cvid=3f1822902e29444b92574efd6b1b3d04

***MSN**-Marco Lombardo- 18 gennaio 2023*

Critical Manufacturing Sector in the Bull's-eye

Serious security flaws go unpatched, and ransomware attacks increase against manufacturers. More than three-quarters of manufacturing organizations harbor unpatched high-severity vulnerabilities in their systems, a study of the sector found.

New telemetry from SecurityScorecard shows a year-over-year increase in high-severity vulns in those organizations.

In 2022, some "76% of manufacturing organizations, SecurityScorecard observed unpatched CVEs on IP addresses our platform attributes to those organizations," says Aleksandr Yampolskiy, co-founder and CEO of SecurityScorecard.

Nearly 40% of these organizations — which include metals, machinery, appliance, electrical equipment, and transportation manufacturing — suffered malware infections in 2022.

Almost half (48%) of critical manufacturing organizations received a ranking between "C" and "F" on SecurityScorecard's security ratings platform.

The platform includes ten groups of risk factors, including DNS health, IP reputation, Web application security, network security, leaked information, hacker chatter, endpoint security, and patching cadence.

The severity of cyberattacks against manufacturers is noteworthy, Yampolskiy says.

"Many of these incidents have involved ransomware where the threat actor, usually in the form of a criminal group, sets out to make money through extortion," he says. "While the ransomware problem is global, we've seen a rising number of attacks on critical infrastructure come from nation-state actors in pursuit of various geopolitical objectives."

Meanwhile, incident response investigations by teams at Dragos and IBM X-Force overwhelmingly showed that the hottest operations technology (OT) target is the manufacturing sector, and the main weapon attacking these organizations is now ransomware.

"Democratized" Cybersecurity

Sophisticated state-sponsored actors such as Russia target several different critical infrastructure organizations across the US, from healthcare to energy to telecommunications, Yampolskiy says.

The good news? "Globally, governments are already taking steps to strengthen cybersecurity," he notes.

Take the US Cyber Incident Reporting for Critical Infrastructure Act of 2022, requiring critical infrastructure to report certain cyber incidents to DHS's Cybersecurity and Infrastructure Security Agency (CISA).(continua…)

https://www.darkreading.com/ics-ot/critical-manufacturing-sector-in-the-bulls-eye

DARK READING -*Nathan Eddy -January 20, 2023*

Rafforzare la cybersicurezza e la resilienza a livello dell'UE - L'accordo provvisorio del Consiglio e del Parlamento europeo in grado di garantire un elevato livello di cybersicurezza in tutta l'Unione, al fine di migliorare la resilienza e le capacità di risposta agli incidenti nell'UE nel suo complesso.
Si chiama NIS 2 la nuova direttiva, che sostituirà l'attuale direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS). Ecco come tale direttiva garantirà una migliore gestione e cooperazione dei rischi e degli incidenti informatici. Essa si applicherà in tutti i settori contemplati dalla direttiva, come l'energia, i trasporti, la sanità e le infrastrutture digitali.
La direttiva aggiornata mira a eliminare le divergenze nei requisiti di cybersicurezza e nell'attuazione delle misure di cybersicurezza nei diversi Stati membri. A tal fine, essa stabilisce norme minime per il quadro normativo e stabilisce meccanismi per una cooperazione efficace tra le autorità competenti in ciascuno Stato membro.
Essa aggiorna l'elenco dei settori e delle attività soggetti agli obblighi di cybersicurezza e prevede mezzi di ricorso e sanzioni per garantirne l'applicazione.
La direttiva istituirà formalmente la rete europea di organizzazioni di collegamento per le crisi informatiche, chiamata EU-CyCLONe, che sosterrà la gestione coordinata degli incidenti di cybersicurezza su larga scala.
(continua…)
https://www.puntosicuro.it/sicurezza-informatica-C-90/rafforzare-la-cybersicurezza-la-resilienza-a-livello-dell-ue-AR-22955/
PuntoSicuro *- Adalberto Biasiotti, 20/01/2023*

10 previsioni per il 2023 sul fronte sicurezza e tecnologia - Dopo un 2022 turbolento, caratterizzato da prezzi dell'energia alle stelle, crisi delle materie prime, sconvolgimenti politici e geopolitici, e un'economia che ha subito diversi colpi di scena, quali le previsioni nei settori sicurezza e tecnologia per il 2023, già iniziato? Nel settore tecnologico, nel 2022 le aziende hanno continuato a cercare di trasformare le proprie operazioni per massimizzare i guadagni derivanti dall'automazione e dalla digitalizzazione e rimanere competitive. Cosa ci riserverà quindi il 2023? Ecco le 10 principali previsioni secondo Zscaler.
Le 10 previsioni per il 2023 di Zscaler, sul fronte sicurezza e tecnologia
1. L'ottimizzazione dei costi guiderà la trasformazione. Le strategie per migliorare il rapporto costo/benefici, sulla scia dell'aumento dei tassi di interesse, della recessione economica e della crisi energetica, guideranno la trasformazione dell'architettura e della sicurezza con un'attenzione particolare alla semplificazione dell'infrastruttura e alla riduzione dei costi. Aumenteranno le misure a sostegno della riduzione dei costi e della trasformazione, come la riduzione dell'hardware di vecchia generazione, la scalabilità e la rivalutazione dei progetti. Le aziende prenderanno decisioni più orientate agli aspetti economici che alla sicurezza, investendo in assicurazioni per coprire la differenza e abbandonando l'hardware a favore di modelli di servizio o di abbonamento per ridurre i costi.
(continua…)
https://www.snewsonline.com/10-previsioni-2023-fronte-sicurezza-tecnologia/
SNews *- di Redazione - 24 Gennaio 2023*

Costruire ponti: guardare indietro per guardare avanti - Cosa insegna l'Ingegneria dei ponti di ieri agli ingegneri di oggi e di domani? Ce lo spiega Mario De Miranda, attraverso una interessante riflessione, dove mette in evidenza cosa sia realmente essenziale per un buon progetto: la corretta visione strutturale e la corretta applicazione delle fondamentali equazioni dell'equilibrio statico.
Due eventi per certi aspetti inconsueti si sono svolti nei mesi recenti "Le straordinarie realizzazioni in ca e cap nell'Ingegneria Italiana dei ponti degli anni 60", è stato il tema del riuscito convegno svolto a Milano ed organizzato con AICAP, e "Analogico v/s Digitale: i ponti del 900. Scienza, tecnica e tecnologia spiegata dagli allievi dei grandi maestri di ieri agli ingegneri digitali di oggi" è stato il tema del workshop svolto a Roma ed organizzato da CSPFEA. In entrambi la partecipazione è stata notevole e l'interesse dei convenuti davvero elevato.
In realtà molti sono i motivi per cui è opportuno, interessante ed anche piacevole rileggere l'Ingegneria del passato, e proprio da questi motivi possiamo ben comprendere il discreto successo dei due eventi citati in apertura.
Proviamo a richiamarli.
Ponti di ieri da curare oggi
Una prima ragione risiede nel fatto che oggi, anche a seguito dell'evidenza della necessità – troppo spesso e troppo a lungo disattesa – della manutenzione delle opere d'arte, ci troviamo ad affrontare il tema della conoscenza delle opere realizzate nel passato al fine di controllarne la sicurezza a seguito del possibile degrado dovuto all'età.
Conoscenza dell'opera, il punto di partenza
La conoscenza dell'opera è il primo passo, indispensabile e fondamentale, per ogni azione di verifica e controllo. E si tratta di una conoscenza che può essere adeguata solo se comprende il modo di costruire e progettare di quelle epoche, dei metodi costruttivi allora adottati, delle prescrizioni normative allora vigenti.
Questa conoscenza oggi è spesso poco accessibile in quanto formalizzata in testi, libri e articoli pubblicati prima dell'avvento dei data-base e quindi non inseriti nelle banche di dati che oggi indirizzano le ricerche nei "search engines".
E tuttavia può essere ricostruita, anche attraverso, almeno per ora, il racconto diretto come avvenuto nei due eventi citati, o, soprattutto, attraverso una azione di ripubblicazione, come alcune riviste tecniche stanno lodevolmente e utilmente cominciando a fare.
Ponti di ieri che resistono anche oggi
Ai miei studenti di Venezia avevo piacere di raccontare come era stato ideato e costruito, tra mille difficoltà, un grande ponte di fine 800, il ponte sul Firth of Forth, ed il racconto era occasione di numerosi spunti tecnici perché altrettanto numerose erano e sono le particolarità di questo ponte, e riscuoteva un bell'interesse.
(continua)
https://www.ingenio-web.it/articoli/costruire-ponti-guardare-indietro-per-guardare-avanti/
Ingenio - *Mario de Miranda- 25.01.2023*

German Government, Airports, Banks Hit With Killnet DDoS Attacks
After Berlin pledged tanks for Ukraine, some German websites were knocked offline temporarily by Killnet DDoS attacks.
After Berlin agreed to send its advanced Leopard 2 tanks to Ukraine, Russia-backed threat group Killnet retaliated with DDoS attacks aimed at Germany's government, banking, and airport sites.
Germany's BSI federal agency, which oversees information security, said the attacks caused some small outages, but otherwise did little damage.

"Currently, some websites are not accessible," the BSI said in a statement to Reuters. "There are currently no indications of direct effects on the respective service and, according to the BSI's assessment, these are not to be expected if the usual protective measures are taken."
Last fall Killnet was behind similar DDoS attacks against US airports last fall and has been escalating its nefarious cyber activities throughout Russia's invasion of Ukraine.
https://www.darkreading.com/ics-ot/german-government-airports-banks-hit-killnet-ddos-attacks
DARK READING -*Dark reading staff -January 26, 2023*

L'uso dei dati nella Sanità: difficoltà procedurali e legislative - Nonostante sia ricca di dati, la Sanità stenta a farne un uso ottimale anche causa del quadro normativo di non facile ricostruzione. Limiti da superare per sfruttare questo enorme potenziale e trasformarli in conoscenze al servizio dei cittadini.
Il benessere e la vita dei cittadini, la prosperità e la stabilità delle società e delle economie, e lo sviluppo sostenibile in generale, sono strettamente correlati al livello di salute della popolazione. Nella pratica quotidiana numerosi sono i trattamenti che vedono coinvolti i dati personali e quelli appartenenti alle categorie particolari (prevalentemente di natura sanitaria) per i quali gli addetti ai lavori si trovano di fronte alla necessità di porsi numerose domande e molto spesso sorgono dubbi operativi, di solito forieri di approfondimenti e confronti.
Indice degli argomenti
I dati e le norme
L'applicazione del Gdpr
La posizione dell'Unione europea
Dati, uso primario e uso secondario
Un cortocircuito normativo
La condivisione dei dati
I ruoli e le responsabilità
Dubbi funzionali
Possibili soluzioni
La costituzionalità
Conclusioni *(continua...)*
https://www.agendadigitale.eu/sanita/dati-sanita-difficolta-procedurali-legislative/
AgendaDIGITALE *- Giovanni Maglio, 26 Gen 2023*

Leaders anticipate cyber-catastrophe in 2023, report World Economic Forum, Accenture
2022 was a difficult year for enterprise security, with the Russia-Ukraine war emboldening cybercriminals and ransomware-as-a-service beginning to thrive. Unfortunately, the Global Cyber Security Outlook 2023 from the World Economic Forum (WEF) and Accenture anticipates that the threat landscape could be getting worse.
WEF's and Accenture's research found that 86% of business leaders and 93% of cyberleaders believe that global geopolitical instability is likely to lead to a catastrophic cyberevent in the next two years.
In addition, the report found that geopolitical uncertainty was forcing organizations to adjust where they invest, with 49% of business leaders and cyberleaders claiming they would "re-evaluate the countries in which their organization does business" in response to geopolitical risk.
On a more positive note, the study also found that organizations that embed cyber-risk into the decision-making process are more confident in their cyber-resilience and better able to recover from cyberattacks.

Geopolitical conflict will provide an opportunity to start the conversation about risk
While it remains to be seen whether these predictions of a catastrophic cyberattack will come to fruition, there have been a number of high-profile breaches over the past few years with enough momentum to be considered catastrophic.
One of the most notorious occurred in 2020. The SolarWinds supply chain attack resulted in the compromise of 100 companies and nine federal agencies. Likewise, in 2021, the Colonial Pipeline ransomware attack forced the organization to shut down 5,500 miles of pipelines.
With the Russia-Ukraine war continuing, the report finds that geopolitical risk "is an entry point for the wider conversation between security leaders and business leaders on how cyberthreats are changing," and how risk can impact business continuity planning.
Having that conversation is critical for mitigating the risk created by emerging cyberthreats. How those threats will manifest is up to debate, but Jon France, CISO of (ISC)2, argues ICS/OT compromise is the most likely avenue for a large cyberevent.
"I think we may see a significant event in the next year, and it will be one in the ICS/OT technologies space. Due to long life, lack of security by design (due in many cases to age) and difficulty to patch, in mission critical areas — an attack in this space would have immense effects that will be felt," France said.
"So I somewhat agree with the hypothesis of the report and the contributors to the survey. You could already argue that we have seen a moderate attack with UK Royal Mail, where ransomware stopped the sending of international parcels for a week or more," France said. (continua….)
https://venturebeat.com/security/leaders-anticipate-cyber-catastrophe-in-2023-report-world-economic-forum-and-accenture/
VENTURE BEAT-*Tim Keary* -January 27, 2023

Ahimè: tornano di "moda" i rifugi blindati! - Alla luce dell'attuale crisi mondiale, non deve stupire il lettore il fatto che il comitato tecnico ISO / TC 292, che si occupa di analisi di rischio, abbia dato il via allo sviluppo di linee guida, mirate alla progettazione di rifugi blindati.
I lettori con una buona memoria ricorderanno certamente che, ai tempi della guerra fredda, in diversi paesi del mondo si sostenne l'opportunità, per non dire la necessità, di progettare rifugi blindati, soprattutto in grado di resistere a esplosioni atomiche. In Svizzera per decenni le nuove costruzioni sono state equipaggiate con questi rifugi. Alla luce dell'attuale crisi mondiale, non deve stupire il lettore il fatto che il comitato tecnico ISO / TC 292, che si occupa di analisi di rischio, abbia dato il via allo sviluppo di linee guida, mirate proprio alla progettazione di questi rifugi.
Il nome provvisorio che è stato dato a queste linee guida è il seguente:
ISO/CD 22359 -Security and resilience — Hardened protective shelters — Guidelines.
Questa proposta normativa vuole mettere a punto delle linee guida per la progettazione di rifugi blindati, facendo riferimento agli interventi di pianificazione, costruzione, gestione operativa e manutenzione.
La norma vuole prendere in considerazione qualsiasi attività legata a questi rifugi ed offrirà preziose indicazioni a tutti i soggetti coinvolti, che desiderano proteggere cittadini, beni ed importanti funzioni sociali, contro gli effetti dannosi di tutt'una serie di rischi, che potrebbero essere sia di origine antropica, sia accidentale, o in conseguenza di eventi atmosferici avversi. (continua…)
https://www.puntosicuro.it/security-C-125/ahime-tornano-di-moda-i-rifugi-blindati!-AR-23014/
PuntoSicuro *- Adalberto Biasiotti, 01/02/2023*

Il Garante della Privacy blocca l'app 'Replika': viola il GDPR
Il Garante della privacy ferma "Replika". Il chatbot, dotato di una interfaccia scritta e vocale che basandosi sull'intelligenza artificiale genera un "amico virtuale", per il momento non potrà usare i dati personali degli utenti italiani. L'Autorità ha infatti disposto con effetto immediato, nei confronti della società statunitense che sviluppa e gestisce l'applicazione, la limitazione provvisoria del trattamento dei dati.
(*continua*)
https://www.federprivacy.org/informazione/garante-privacy/il-garante-della-privacy-blocca-l-app-replika-viola-il-gdpr
Federprivacy – *dal garante per la Privacy – 03/02/2023*

Anche Google rimane vittima di un attacco in supply-chain. Oggi nessuno è escluso!
Google Fi, precedentemente Project Fi, è un servizio di telecomunicazioni MVNO (Mobile Virtual Network Operator) di Google che fornisce chiamate telefoniche, SMS e banda larga mobile utilizzando reti cellulari e Wi-Fi. Google Fi si appoggia a reti gestite da T-Mobile e US Cellular. I clienti di Google Fi hanno ricevuto delle notifiche questa settimana che i loro numeri di telefono, i numeri di serie della carta SIM, lo stato dell'account (attivo o inattivo), la data di attivazione dell'account e le informazioni sui piani di servizi mobili erano stati compromessi.
(*continua*)
https://www.redhotcyber.com/post/anche-google-rimane-vittima-di-un-attacco-in-supply-chain-oggi-nessuno-e-escluso/
Red Hot Cyber *– Redazione RHC – 06/02/2023*

Alla scoperta di ESXiArgs. Il malware che sfrutta l'incuria degli amministratori IT alle patch di sicurezza
Come abbiamo riportato in precedenza, il provider di hosting OVH e il CERT francese hanno avvertito che più di 2100 server VMware ESXi sono stati compromessi dal nuovo ransomware ESXiArgs lo scorso fine settimana come parte di una massiccia campagna di hacking. Gli aggressori sfruttano una vulnerabilità vecchia di due anni (CVE-2021-21974) che consente loro di eseguire comandi remoti su server vulnerabili tramite **OpenSLP (porta 427).**
(*continua*)
https://www.redhotcyber.com/post/alla-scoperta-di-esxiargs-il-malware-che-sfrutta-lincuria-degli-amministratori-it-alle-patch-di-sicurezza/
Red Hot Cyber *– Redazione RHC – 06/02/2023*

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.

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

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