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. 01/ 2024** | **gennaio 2024**

Intelligenza artificiale ed imprese: focus sulla tutela dei dati personali

Secondo il rapporto 2023 dell'Osservatorio sulla Trasformazione Digitale dell'Italia, pubblicato da The European House – Ambrosetti, l'utilizzo dell'intelligenza artificiale (IA) nei settori produttivi sarà sempre più capillare, assumendo un valore strategico a livello di sistema-Paese. Le previsioni, incluse nel rapporto, stimano un valore aggiunto annuo potenziale di 312 miliardi di euro, il quale rappresenterebbe il 18,2% del PIL, e liberebbe 5,7 miliardi ore annue lavorate. Nonostante le grandi potenzialità, sussistono importanti sfide e criticità per l'implementazione dell'IA nel tessuto economico, tra queste, emergono quelle legate all'utilizzo dei dati personali sia nella fase di addestramento dei modelli algoritmici su informazioni per cui è difficoltoso disporre della proprietà intellettuale o del consenso informato, sia rispetto all'output, frequentemente inficiato dalla poca trasparenza del processo di elaborazione. Al fine di affrontare e superare tali problematiche, lo studio evidenzia come l'incremento delle competenze digitali, la promozione della gestione del rischio e la digitalizzazione dei vari processi aziendali siano gli strumenti d'elezione.

Appare però evidente che una corretta gestione della complessa interconnessione tra salvaguardia della privacy e Intelligenza Artificiale necessiti di un approccio integrato che consideri tanto gli elementi tecnici quanto quelli di aderenza alle normative vigenti, integrando riflessioni etiche e considerazioni di natura strategica. L'intento principale dovrebbe essere quello di valorizzare le capacità dell'IA per il miglioramento tecnologico, assicurando, al contempo, la tutela dei diritti essenziali legati alla privacy e alla sicurezza dei dati personali.
Nella dinamica e variegata connessione tra protezione della privacy e avanzamento tecnologico, l'impiego degli algoritmi di intelligenza artificiale rappresenta una delle aree più delicate e di rilievo sia per le aziende che per gli organismi di regolamentazione; il punto focale di questa relazione consiste nel trovare un equilibrio tra lo sviluppo tecnologico e la difesa dei diritti basilari degli individui, specialmente il diritto alla privacy. L'intelligenza artificiale, con la sua abilità nell'elaborare e analizzare ampi volumi di dati, ha aperto nuove possibilità nel trattamento e nella generazione di informazioni, apportando significativi vantaggi in termini di efficienza e personalizzazione dei servizi offerti dalle aziende. Questo processo, tuttavia, si fonda sull'uso di estese raccolte di dati che permettono la formazione degli algoritmi e ne affinano l'impiego, per adattarli alle specifiche necessità degli utilizzatori. Si verifica quindi un'interdipendenza strutturale tra IA e dati, inclusi quelli personali, poiché, in ultima analisi, gli algoritmi dell'intelligenza artificiale rappresentano un metodo innovativo e dalle vaste potenzialità per processare e custodire dati.
Sullo sfondo del veloce progresso tecnologico dell'IA, le imprese che vogliano integrare le potenzialità della nuova tecnologia ai propri processi, stanno formulando strategie basate su un utilizzo consapevole dei dati personali e incentrate sulla sicurezza dei procedimenti e dei dataset impiegati nella formazione degli algoritmi, sull'elaborazione di meccanismi di privacy dinamici adattati alle scelte degli utenti, sulla trasparenza delle interazioni con IA.
Tra gli esempi all'avanguardia in queto campo, l'azienda multinazionale Microsoft sta estendendo l'applicazione dell'IA a diversi suoi prodotti: Bing, Copilot, Edge e il sistema operativo Windows, inserendosi in un dialogo costante con gli enti regolatori. Questo permette un rapido adattamento alle

recenti disposizioni legislative e fornisce una base di sperimentazione che mostri l'evoluzione della tecnologia IA e fornisca un banco di prova per eventuali problematiche emergenti. La cooperazione tra imprese e autorità regolative appare infatti fondamentale per aggiornare e migliorare la normativa vigente, fronteggiando un fenomeno in rapida evoluzione come l'intelligenza artificiale.
Ad oggi, né gli Stati Uniti né l'Unione Europea hanno un quadro legislativo definitivo per regolare questo campo: negli USA, un ordine esecutivo del Presidente Biden del 30 ottobre 2023 ha fornito una guida per l'intervento nei vari ambiti di applicazione di questa tecnologia. In Europa, è stato raggiunto un accordo sul nuovo regolamento, denominato Artificial Intelligence Act (AI Act), che sarà pienamente vincolante entro due anni.
Nell'attuale contesto normativo europeo, l'impiego dell'IA nel trattamento dei dati personali è guidato dalle disposizioni del Regolamento Generale sulla Protezione dei Dati (GDPR) che rappresenta un compromesso ritenuto ideale dal legislatore, poiché capace di mediare tra le esigenze spesso contrastanti dell'innovazione tecnologica, del mercato e del rispetto dei diritti personali.
Ad oggi, le imprese che decidano d'integrare l'IA per offrire servizi avanzati ai propri clienti, vedono nell'aderenza al GDPR la guida per indirizzare le loro pratiche aziendali in materia di privacy. Il GDPR stabilisce infatti criteri stringenti e all'avanguardia per il trattamento dei dati personali, particolarmente rilevanti nel contesto dell'IA, dove l'uso dei dati è spesso automatizzato e può impattare significativamente sui diritti e libertà degli individui. Un elemento cruciale del GDPR è la necessità di una Valutazione di Impatto sulla Protezione dei Dati (DPIA) per i trattamenti che presentino un alto rischio per i diritti e le libertà delle persone. Nel caso dell'IA, una DPIA dettagliata aiuta a individuare e mitigare i rischi specifici legati a decisioni automatizzate, come nel caso di discriminazioni non intenzionali o dell'uso inappropriato di dati sensibili ricavati della profilazione. La trasparenza verso gli utenti rappresenta un altro caposaldo del GDPR applicato alla nuova tecnologia: le aziende devono fornire informazioni chiare e comprensibili su come i dati vengono raccolti e trattati dall'IA, iniziando dall'acquisizione esplicita del consenso. Ciò implica la necessità d'informare gli utenti in modo trasparente e dettagliato sulle informazioni raccolte e sulle modalità di utilizzo da parte degli algoritmi, includendo il tipo di logica usata per la categorizzazione, l'ampiezza e le conseguenze del trattamento automatizzato. Il consenso deve essere ottenuto secondo criteri di libera espressione, specificità e chiarezza. Il modello legislativo richiede anche che, nel processo di sviluppo e affinamento del sistema IA, l'azienda integri il concetto di privacy by design, garantendo che la protezione dei dati personali sia un elemento fondamentale e prioritario sin dalla progettazione del dataset e della definizione delle funzioni dell'algoritmo. Questo richiede l'adozione di tecniche di pseudonimizzazione e la limitazione dell'uso dei dati esclusivamente per le necessità del servizio offerto, in modo da incrementare la sicurezza del sistema e prevenire il trasferimento delle informazioni a dataset per l'addestramento o l'uso di IA differenti da quelli originariamente autorizzati. L'azienda deve anche assicurare un alto livello di trasparenza nel trattamento dei dati personali, consentendo agli utenti e ai gestori di accedere alle informazioni raccolte e di comprendere come il sistema IA elabori e utilizzi tali dati per le raccomandazioni personalizzate e i suggerimenti. Gli utenti devono inoltre essere in grado di gestire le richieste di rettifica o cancellazione dei dati in modo semplice e tempestivo, attraverso procedure facilmente identificabili.
Queste disposizioni si configurano come una mappa, certo non ancora definitiva né completa in ogni suo aspetto, ma capace fin da ora d'orientare l'azione di quelle aziende che vogliano porsi all'avanguardia nell'utilizzo della rivoluzionaria tecnologia dell'intelligenza artificiale, iniziando a costruire un ambiente digitale sicuro per la propria operatività e un vantaggio competitivo rispetto a coloro i quali intendano aspettare la creazione di standard affermati e di una legislazione totalmente coerente.

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

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

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2024

Il 31 dicembre 2023 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare con sollecitudine l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2024".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it.
Ricordiamo che **la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2024.** Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione versando anche il contributo per le spese di segreteria.
La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@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.

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

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*

MANIFESTAZIONE DI INTERESSE
VISITA GUIDATA
AL CORPO NAZIONALE DEI VIGILI DEL FUOCO

Riprendendo il nostro programma di visite sul campo, abbiamo la disponibilità di massima ad organizzare una **visita guidata** presso il **Centro Studi ed Esperienze (CSE) del Corpo Nazionale Italiano dei Vigili del Fuoco** situato in Roma, via delle Capannelle.

Il programma di massima prevede:

- presentazione delle principali attività del Centro Sudi ed Esperienze;
- visita ai laboratori di prova dei materiali (Scienza delle costruzioni, Difesa Atomica, Macchine e Termotecnica, Elettrotecnica, Idraulica);
- indicazioni sull'utilizzo dei materiali nella realtà delle costruzioni civili e industriali;
- attività del Nucleo Investigativo Antincendio (NIA).

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 visita potrebbe essere effettuata nel **periodo metà marzo-aprile 2024**, durata prevista 3 ore, luogo di incontro via delle Capannelle – Roma, da raggiungersi con mezzi propri.

Poiché la visita è soggetta ad un numero minimo ed uno massimo di partecipanti, e bisogna prevedere i tempi per i permessi di ingresso, chiediamo di esprimere il proprio interesse – non vincolante – a partecipare, rispondendo via mail a: segreteria@infrastrutturecritiche.it entro il giorno 29 febbraio p.v.
Qualora si raggiunga il numero minimo di interessati, procederemo con l'organizzazione e l'apertura delle iscrizioni.

Attenzione! La visita è riservata ai soli soci AIIC in regola con il pagamento delle quote sociali. 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

Il Centro Studi ed Esperienze (CSE) del Corpo Nazionale Italiano dei Vigili del Fuoco è stato istituito nel 1961 ed è ospitato nelle Scuole Centrali Antincendi di Capannelle a Roma.
Da oltre sessanta anni il contributo del Centro Studi è stato di ricerca applicata attraverso i suoi laboratori di prova dei materiali (Scienza delle costruzioni, Difesa Atomica, Macchine e Termotecnica, Elettrotecnica, Idraulica) con le correlate indicazioni in merito al loro utilizzo nella realtà delle costruzioni civili e industriali del Paese. Nell'ultima legge di riordino del Corpo Nazionale il CSE è stato integrato dalle attività del Nucleo Investigativo Antincendio (NIA).

Un cordiale saluto a tutti.

Silvano Bari
Vice presidente AIIC

NEWS E AVVENIMENTI

Cosa ci insegna l'attacco a Westpole: cloud e ransomware priorità 2024 Una lezione fondamentale sulla sicurezza nel cloud e la minaccia persistente del ransomware, il caso Westpole evidenzia la necessità di prepararsi a fronteggiare questa minaccia persistente con proattività
Nel panorama sempre più complesso della gestione del cloud, l'attacco ransomware a Westpole offre una lezione cruciale sulla sicurezza delle infrastrutture nazionali .
Indice degli argomenti

- Caso Westpole, necessaria una revisione dei fornitori cloud
- Lisi: troppe cose non tornano nell'attacco
- La minaccia ransomware è sempre più preponderante

Caso Westpole, necessaria una revisione dei fornitori cloud

In un momento in cui si progetta un cloud nazionale, è imperativo che un paese come l'Italia eviti la paura dei Big Tech e si concentri sulla scelta oculata dei provider cloud, in particolare per garantire la sicurezza delle proprie infrastrutture. Le strade percorribili in questo senso sono due: o ci fidiamo di chi fa questo lavoro da sempre oppure cerchiamo ad ogni costo di emularli, su tutti i lati positivi, primo fra tutti quello relativo alla sicurezza dell'infrastruttura e di tutta la catena dei dipendenti coinvolti. *(continua…)*
https://www.cybersecurity360.it/cybersecurity-nazionale/cosa-ci-insegna-lattacco-a-westpole-cloud-e-ransomware-priorita-2024/
Cybersecurity360 *-Dario Fadda- 27 Dic 2023*

Cinque pilastri per difendersi: la cyber security secondo gli Stati Uniti. Gli approcci della difesa collaborativa fra le entità che contribuiscono alla sicurezza cyber dai diversi settori istituzionali. Annita Larissa Sciacovelli, docente di diritto internazionale all'Università di Bari e advisor ENISA, ci spiega la strategia Usa
In considerazione della crescente frequenza e sofisticatezza degli attacchi informatici che colpiscono obiettivi statunitensi (USA), l'amministrazione americana ha adottato misure per rafforzare la posizione di sicurezza informatica degli Stati Uniti.
Oltre all'Ordine esecutivo del 2021 del presidente Joe Biden sulla sicurezza informatica e alla legislazione del Congresso del 2022, nel marzo 2023 è stata pubblicata la strategia nazionale statunitense per la sicurezza informatica. In aggiunta anche il Pentagono ha emesso la strategia per la difesa cyber sul fronte della Difesa nazionale.
Ma in generale diverse entità americane come la CISA e il Dipartimento del tesoro hanno avviato azioni per intervenire operativamente in modo collaborativo e coerente con le indicazioni strategiche del governo Biden.
Ne abbiamo analizzato le caratteristiche grazie anche al contributo di Annita Larissa Sciacovelli, professore di diritto Internazionale all'Università di Bari e Advisor ENISA.
Indice degli argomenti

- La strategia americana nella Cyber security
  - Cinque pilastri
  - Così cambia il paradigma Usa
- La strategia del dipartimento della Difesa americana
  - I timori della Casa Bianca
  - Le operazione in corso nel mondo
  - La centralità della cyber security

La strategia americana nella Cyber security
La Strategia nazionale per la sicurezza informatica degli Stati Uniti (marzo 2023) delinea una visione globale per un ecosistema digitale statunitense "difendibile, resiliente e allineato ai valori nazionali". La strategia punta a riequilibrare la responsabilità di difendere il cyberspazio e riallineare gli incentivi per gli investimenti a lungo termine nella sicurezza informatica.
Cinque pilastri
La Strategia nazionale per la sicurezza informatica degli Stati Uniti, pubblicata nel marzo 2023 è strutturata attorno a cinque pilastri: 1) difendere le infrastrutture critiche; 2) smantellare gli attori della minaccia; 3) intervenire sulle aziende per promuovere sicurezza e resilienza; 4) investire in un futuro resiliente; 5) creare partenariati internazionali per perseguire obiettivi condivisi.
(continua…)

https://www.cybersecurity360.it/outlook/cinque-pilastri-per-difendersi-la-cyber-security-secondo-gli-stati-uniti/
Cybersecurity360*- Alessia Valentini- 29 Dic 2023*

Cyberattackers Target Nuclear Waste Company via LinkedIn. The hackers were unsuccessful in their attempt, but this is not the first time.
Last week, a group of hackers targeted Radioactive Waste Management (RWM), a UK government-owned company behind the country's multibllion-dollarGeological Disposal Facility (GDF) nuclear waste-storage project, using social engineering and LinkedIn.
RWM merged last year with two other companies to create Nuclear Waste Services (NWS), which also administers the Low-Level Waste Repository in Cumbria, UK. Corhyn Parr, NWS's chief executive, noted that the attackers have been capitalizing on the business changes stemming from that merger to try to dupe targets into falling for social engineering gambits, largely through LinkedIn. So far, though, none of the attempts have had any "material effect," he added.
"NWS has seen, like many other UK businesses, that LinkedIn has been used as a source to identify the people who work within our business,"a company spokesperson told the Guardian. The attackers, however, were denied through what a company spokesperson referred to as "multi-layered defenses."
(continua)
https://www.darkreading.com/ics-ot-security/cyberattackers-target-nuclear-waste-company-via-linkedin
DarkReading -*Dark Reading Staff- January 2, 2024*

Piano Adattamento ai Cambiamenti Climatici, approvato il PNACC - Il via libera è arrivato con il Decreto del MASE n. 434 del 21 dicembre 2023. Previste 274 azioni “soft” su un totale di 361 misure individuate dagli esperti
L’Italia si trova un’area estremamente vulnerabile al climate change, inserita nella lista degli hotspot più importanti ed esposti a livelli mondiale. Eppure redigere un programma difensivo non è stato semplice. Dalla prima strategia italiana in materia all’adozione del Piano Nazionale di Adattamento ai Cambiamenti Climatici (PNACC) sono passati oltre sette anni. Un lungo periodo di tempo durante il quale si è registrato un incremento di fenomeni quali alluvioni, ondate di calore, frane e siccità. Basti pensare che nel solo 2023, il moltiplicarsi di eventi estremi quali grandinate, trombe d’aria, bombe d’acqua e alte temperature, ha provocato nel Paese oltre 6 miliardi di euro di danni all’agricoltura italiana.
Piano di Adattamento ai Cambiamenti Climatici, cosa è?
Il PNACC costituisce lo strumento di indirizzo nazionale per “l’implementazione di azioni finalizzate a ridurre al minimo possibile i rischi derivanti dai cambiamenti climatici, a migliorare la capacità di adattamento dei sistemi socioeconomici e naturali”.
Il via libera ufficiale è arrivato alla fine del 2023 con il Decreto del Ministero dell’Ambiente e della Sicurezza Energetica n. 434 del 21 dicembre 2023. A darne notizia è lo stesso Dicastero in una rapida nota stampa del 2 gennaio 2024, in cui è tuttavia allegato oltre allo stesso documento di Piano anche il database delle azioni di adattamento. Di cosa si tratta? Del catalogo degli interventi settoriali individuati dal gruppo multidisciplinare di esperti che ha collaborato alla elaborazione PNACC del 2018. Parliamo di 361 misure di carattere nazionale e/o regionale in grado di incidere su uno o più settori tra: acquacoltura; agricoltura; energia; turismo; foreste; dissesto idrogeologico;

desertificazione; ecosistemi acquatici e terrestri; zone costiere; industrie; insediamenti urbani; patrimonio culturale; risorse idriche; pesca; salute; trasporti.

Per ognuna di queste 361 azioni esiste un'ulteriore classificazione in "soft", "green" o "grey" nel caso in cui, rispettivamente: non richiedono interventi strutturali e materiali diretti, siano interventi materiali identificati come soluzioni basate sulla natura, siano azioni materiali su impianti, materiali e tecnologie, infrastrutture o reti.
(continua)
https://www.rinnovabili.it/ambiente/cambiamenti-climatici/piano-adattamento-cambiamenti-climatici-pnacc/
Rinnovabili.it *– 3 gennaio 2024*

Cambiamento climatico e superfici urbane: il ruolo chiave delle pavimentazioni nel mitigare gli effetti - In un momento in cui gli eventi climatici estremi sono sempre più frequenti è importante comprendere quale risposta possono dare le superfici urbane. Comprendere questi fenomeni è essenziale per affrontare i rischi associati e per sviluppare città più resilienti e sostenibili per garantire il benessere delle comunità anche durante le condizioni climatiche più avverse.
Oggi circa il 75% della popolazione europea risiede nelle aree urbane, una percentuale destinata a crescere, superando l'80% entro il 2050, secondo le stime del World Urbanization Prospects (2018) delle Nazioni Unite.
Il fenomeno dell'urbanizzazione è di cruciale importanza quando si tratta di cambiamenti climatici. Da un lato, le città sono tra le principali fonti di emissioni di gas serra e contribuiscono in modo significativo all'origine del problema. Dall'altro, le aree urbane si rivelano particolarmente suscettibili agli impatti di un clima in continuo mutamento. Gli impatti dovuti al clima possono includere fenomeni come l'aumento delle temperature, le precipitazioni intense (le cosiddette "bombe d'acqua"), l'innalzamento del livello del mare, le inondazioni e la siccità.
Sulla vulnerabilità degli insediamenti urbani italiani si consiglia la lettura del paragrafo 3.14 del Piano Nazionale di Adattamento ai Cambiamenti Climatici (Dicembre 2022) del MASE.
Una città resiliente ai cambiamenti climatici è in grado di affrontare gli impatti climatici in modo proattivo, mitigando i danni e preservando la qualità della vita dei suoi cittadini anche di fronte alle sfide complesse poste del clima. La resilienza di una città si misura in base alla sua capacità di pianificazione, preparazione, adattamento e collaborazione tra i vari attori e settori coinvolti.
Quale contributo può dare il settore delle pavimentazioni nel mitigare gli effetti dovuti ai cambiamenti climatici in città? Quali strategie possiamo adottare? Quale tipologia di materiali da costruzione scegliere?
(continua)
https://www.ingenio-web.it/articoli/cambiamento-climatico-e-superfici-urbane-il-ruolo-chiave-delle-pavimentazioni-nel-mitigare-gli-effetti
INGENIO *- Dalila Cuoghi*

Russian Agents Hack Webcams to Guide Missile Attacks on Kyiv. Incident prompts Ukraine's security service to ask webcam operators in country to stop live broadcasts.
The Security Service of Ukraine (SSU) has asked owners and operators of webcams in the country to stop broadcasts from their devices over concerns about Russia's intelligence services using the feeds to conduct military reconnaissance against strategic targets.

The SSU's move follows a recent incident where Russian agents hacked into two residential webcams in Kyiv to gather information on the city's air defense systems prior to launching a missile attack on the Ukrainian capital.
In a statement, the SSU described one of the webcams as being located on top of a Kyiv apartment building — apparently near a critical infrastructure facility — and being used by the condo association to monitor the surrounding area. Russian intelligence services hacked into the camera, changed its viewing angle, and streamed its live feed to YouTube from which they monitored everything within the camera's range.
The second camera too was located at a residential complex in Kyiv, this one for monitoring the building's parking facility. Russian agents took control of the webcam the same way they did with the first and used it to gather information on an adjacent critical infrastructure facility. "The aggressor used these cameras to collect data to prepare and adjust strikes on Kyiv," the SSU said. "Based on the uncovered facts, the SSU is acting to neutralize new attempts by the invaders to conduct reconnaissance and sabotage through online cameras." (continua…)
https://www.darkreading.com/ics-ot-security/russian-agents-use-residential-webcams-to-gather-info-for-missile-attack-on-kyiv
DarkReading *-Jai Vijayan, Contributing Writer - January 3, 2024*

Getting Started With Passkeys, One Service at a Time. Passkeys help do away with passwords for logging into websites and cloud services. This Tech Tip outlines ways to get started.
Passkeys gained momentum in 2023.
In addition to the major three technology firms supporting passkeys — Apple, Google, and Microsoft third-party password providers, such as 1Password and Bitwarden, implemented their own support for managing the credentials. Dozens, and likely hundreds, of major websites have followed suit, implementing the necessary support for passkey authentication.
Overall, more than 7 billion accounts could be using passkeys, according to the FIDO Alliance, whose technical specifications power the authentication standard. Left unsaid: The vast majority of users are not.
The whole point of passkeys is to make passwordless authentication as convenient and secure as passwords, says Andrew Shikiar, executive director of the FIDO Alliance.
"Passwords are a clear and present danger to everything we do online right now," he says. "To take on passwords, you need to be able to prove the same characteristics as passwords ubiquity and convenience."
For those who want an easier and more secure way to sign into cloud services and websites, this Tech Tip is for you. (continua…)
https://www.darkreading.com/identity-access-management-security/how-to-get-started-using-passkeys
Dark Reading -*Robert Lemos -January 4, 2024*

US, Israel Used Dutch Spy to Launch Stuxnet Malware Against Iran. Report says US and Israel spent $1 billion to develop the infamous Stuxnet virus, built to sabotage Iran's nuclear program in 2008. After a two-year investigation into the details surrounding the Stuxnet virus, unleashed in 2008 against the Iranian nuclear program, journalists with Dutch newspaper Volkskrant have released a report saying the malware cost $1 billion to develop.

Besides the enormous price tag, the outlet said a Dutch spy was used to release the Stuxnet virus into the Iranian nuclear infrastructure. The Dutch government told Volkskrant that the government understood the then-36-year-old Erik van Sabben was working to sabotage the Iranian nuclear project, however there was no knowledge of a cyber weapon of Stuxnet's consequence being used as part of the proceedings. (continua…)
https://www.darkreading.com/ics-ot-security/us-israel-dutch-spy-stuxnet-malware-against-
Dark Reading *-Becky Bracken, - January 9, 2024*

Move Over, APTs: Cybercriminals Now Target Critical Infrastructure Too. Danish energy sector attacks attributed to Russia's Sandworm APT turn out to be the work of a new concern: cyber opportunists.
A "crimewave" of mass exploitation of Zyxel firewall devices has been washing over critical infrastructure in Europe — and Sandworm, the Russian state-sponsored advanced persistent threat (APT) that specializes in such attacks, is behind only part of it.
According to an analysis from Forescout Research, Vedere Labs this week, one of two previously reported attacks against the Danish energy sector in May was mistakenly attributed to Sandworm.
Mass Exploitation of CVE-2023-27881 in Zyxel Firewalls
At the time, Danish critical infrastructure security nonprofit SektorCERT noted that attackers were leveraging multiple, critical vulnerabilities in Zyxel gear, including two zero-days, to isolate targets from the national grid, and that command-and-control (C2) servers known to be associated with Sandworm were involved, across two different campaigns.
Further analysis however shows that "the second wave of attacks took advantage of unpatched firewalls using a newly 'popular' CVE-2023-27881, and additional (C2) addresses that went unreported," according to the firm. "Forescout evidence suggests the second wave was part of a separate mass exploitation campaign."
Forescout researchers noted that the perpetrators are targeting firewalls indiscriminately and only changing staging servers periodically — a very different M.O. from that of the infamous APT.
"Distinguishing between a state-sponsored campaign aimed at disrupting critical infrastructure and a crimewave of mass exploitation campaigns, while also accounting for potential overlaps between the two, is more manageable in hindsight than in the heat of the moment," notes Elisa Costante, vice president of research at Forescout Research. (continua…) "
https://www.darkreading.com/ics-ot-security/common-cybercriminals-begin-critical-infrastructure-targeting
Dark Reading *- Tara Seals -January 11, 2024*

In quattro miliardi chiamati al voto nel 2024, il rischio diventa planetario. Si parte con Taiwan, poi Ue, Russia e Stati Uniti per un anno in cui si va alle urne in 76 Paesi e nel quale potrebbero votare più persone di sempre. E cresce esponenzialmente il rischio misinformation, deep fake e interferenze sui vari candidati. Ma qualcosa si può fare
“Di recente ho letto una statistica che mi ha lasciato di stucco: nel 2024 potrebbero votare più persone che in qualsiasi altro anno della storia”. A parlare è **Bill Gates**, nelle previsioni per i prossimi dodici mesi condivise, come ogni anno, sul proprio blog.
Indice degli argomenti

- Il voto riguarderà metà della popolazione mondiale
- La preoccupazione è palese tra gli osservatori

- E la tecnologia complica il quadro
- I rischi per i candidati
- Manipolazione sempre più sofisticata
- Allenarsi a comprendere i rischi
- Una guida per rimuovere i contenuti "tossici"
- Il ruolo di Big Tech (e del giornalismo)
- Così la tecnologia può aiutarci

Il voto riguarderà metà della popolazione mondiale

Si voterà (comprese le elezioni UE, come da rapporto dell'**Economist**) in 76 paesi. Alle urne più di metà della popolazione globale, quasi 4 miliardi di persone. Certo, in molti casi non si tratterà di consultazioni del tutto libere: ma l'impatto della cifra rimane. Apre **Taiwan**, dove la popolazione sarà chiamata a decidere fra pochi giorni, il 13 gennaio. Ma nell'elenco degli Stati o entità territoriali in cui si terranno elezioni nel 2024 figurano anche **India, Regno Unito, Stati Uniti, El Salvador, Unione Europea, Russia, Bielorussia, Messico, Sudafrica, Egitto, Iran, Indonesia e Corea del Sud**.

Molte di queste consultazioni avranno un impatto politico ed economico che travalica la dimensione locale: su tutte, le parlamentari continentali di giugno e le presidenziali americane di novembre. Ma è difficile sottovalutare anche il peso dell'India (1,4 miliardi di persone), con i seggi che apriranno tra aprile e maggio.

La preoccupazione è palese tra gli osservatori

Il decennio inaugurato dalla pandemia rischia di essere ricordato come quello della crisi delle democrazie. L'ordine unipolare seguito alla caduta del Muro di Berlino può dirsi definitivamente tramontato, assieme, forse, alla globalizzazione e al sogno di un governo mondiale in grado di assicurare stabilità. (continua…)

https://www.cybersecurity360.it/outlook/quattro-miliardi-chiamati-al-voto-nel-2024-il-rischio-diventa-planetario/

Cibersecurity360 - *Antonio Piemontese- 12 Gen 2024*

Rischio NaTech: come valutare e affrontare il rischio idrogeologico? - Come fare una valutazione quantitativa del rischio di eventi idrogeologici? Quali sono le misure di mitigazione degli eventi alluvionali? Sono utili i sistemi di allerta preventivi? Ne parliamo con Alessandra Marino del Dipartimento DIT dell'Inail.

Per aumentare l'attenzione alla valutazione e mitigazione dei tanti eventi naturali (alluvioni, terremoti, frane, …) che hanno gravi ripercussioni anche sulla sicurezza delle strutture produttive e dei lavoratori, abbiamo intervistato, ad Ambiente Lavoro 2023 a Bologna, Alessandra Marino (Inail, Dipartimento innovazioni tecnologiche e sicurezza degli impianti, prodotti e insediamenti antropici).

Alessandra Marino a Bologna era responsabile scientifica del convegno "Tecnologie 'SMART' per la prevenzione e la gestione del Rischio NaTech da Sisma e Idrogeologico" e allo stesso convegno presentava una relazione sulla prevenzione e gestione del Rischio NaTech da eventi idrogeologici.

L'avevamo, in realtà, già intervistata nel 2017, sempre sull'interazione fra rischio industriale e rischi naturali (" Valutazione dei rischi: come si valutano i rischi naturali?"), ma con particolare attenzione al rischio sismico. Tuttavia dopo le tante alluvioni, dipendenti da fenomeni meteorologici estremi connessi al riscaldamento globale, ci è parso necessario ritornare a parlare con lei di eventi naturali, di pericolosità idrogeologica e di quanto le aziende devono e possono fare per ridurre i pericoli per i lavoratori e i danni alle strutture e all'ambiente.

Queste le domande fatte ad Alessandra Marino sul tema del rischio NaTech, del rischio idrobiologico e sugli strumenti di mitigazione e prevenzione:

Cosa si intende per rischio NaTech?
Il rischio NaTech riguarda solo gli stabilimenti con pericolo di incidente rilevante o può riguardare tutti gli stabilimenti e aziende?
Cosa si intende con pericolosità idrogeologica e dissesto idrogeologico?
Come si può analizzare la pericolosità idrogeologica correlata ad alluvioni e frane?
Con riferimento anche alle recenti alluvioni, quali possono essere le azioni dell'alluvione sugli impianti?
Cosa si intende con valutazione e mitigazione del rischio NaTech?
Come fare una valutazione quantitativa del rischio NaTech?
Quali sono delle possibili misure di mitigazione delle conseguenze di eventi alluvionali?
Esistono delle mappature che possono favorire la valutazione?
I sistemi di allerta preventivi possono essere importanti per prevenire o ridurre il rischio Natech?
Il rischio NaTech relativo ad alluvioni e frane può essere connesso al rischio sismico?
Come aiutare le aziende, le industrie ad implementare idonee misure di prevenzione/mitigazione tecniche e gestionali?
(continua)
https://www.puntosicuro.it/gestione-emergenza-ed-evacuazione-C-84/rischio-natech-come-valutare-affrontare-il-rischio-idrogeologico-AR-23954
Punto Sicuro *- Tiziano Menduto, 12/01/2024*

NOTIZIE D'INTERESSE:

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

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

RIFERIMENTI DELL'ASSOCIAZIONE

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

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

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

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

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*

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.