

CULTURA DIGITALE

OPUSCOLO GRATUITO

dsfmag

powered by



PROGRAMMA CON APPROFONDIMENTI DEI TEMI DEL DSF

DEEFAKE
LE NUOVE SUPER TRUFFE

.....

INTELLIGENZA ARTIFICIALE:
IL FUTURO DELLA CYBERSICUREZZA
FRA NUOVE SFIDE E OPPORTUNITÀ

.....

LA SICUREZZA DIGITALE
È COME UN VIAGGIO.

.....

DIGITAL SECURITY FESTIVAL 6

Umanocentrico
per natura:

.....

**LE TENDENZE EMERGENTI
DELLA SICUREZZA INFORMATICA**

.....

**LA TECNOLOGIA AL
SERVIZIO DELL'UMANITÀ**

.....

DIRETTIVA NIS2



digitalsecurityfestival.it

FvgTechMag opuscolo informativo e programma del Digital Security Festival 2024





per



FvgTechMag
Programma e informazioni temi DSF 2024

IDEA PROGETTO
da un'idea di Gabriele Gobbo
www.gabrielegobbo.it
e FvgTech programma TV
www.fvgtech.it
e MacPremium Digital Company
www.macpremium.it
in collaborazione con
Digital Security Festival
www.digitalsecurityfestival.it

INFO
In questo opuscolo sono disponibili informazioni sul Digital Security Festival, sul programma del DSF e informazioni sulla sicurezza digitale e la tecnologia. Le informazioni riportate sono a solo scopo illustrativo o di mero esempio. Il programma è stato realizzato dal Digital Security Festival e suoi organizzatori che ne curano la consegna ai partecipanti.

PARTNERSHIP
MacPremium Digital Company
E: fvgtech@macpremium.it

INTERNATIONAL
FvgTech Mag is available for licensing.
Contact the international department to discuss partnership opportunities.

International Licensing
E: licensing@macpremium.it

PROTEZIONE MARCHI E LINEA GRAFICA
Per FvgTech: Marchi, denominazioni e linea grafica protetti e depositati con marcatura e certificati digitali Patamu Registry: fvgtechmag certificato n.108697, FvgTech certificato n.88292, linea grafica e impaginazione certificato n.108698 e altri. Altri nomi o marchi citati sono di proprietà dei rispettivi titolari.

Copyright © 2024 MacPremium e DSF ove possibile

Caro lettore...



■ Benvenuto su questo freebook dedicato alla tecnologia, al digitale e all'information technology. **Questa edizione speciale di chiama DSFMAG, perchè è l'opuscolo del programma con gli approfondimenti del Digital Security Festival 2024.** Abbiamo ideato FvgTech Magazine diversi anni fa perché ci sembrava mancasse un canale di comunicazione che potesse arrivare anche ai meno esperti o a chi non usa la tecnologia o non ha avuto modo di avvicinarsi a questo mondo. Oggi, grazie al Festival, lo abbiamo realizzato ancora una volta **anche per i professionisti** di settore.

FvgTech nasce come programma televisivo ed ora è diventato una **"Piattaforma di divulgazione della cultura digitale"** che opera in modo crossmediale per diffondere conoscenza sui temi tecnologici a più livelli. Sfruttando diversi canali informativi online e offline, si prefigge l'obiettivo di far conoscere e informare i cittadini in tutta Italia sul mondo tecnologico e digitale che li circonda: dai social network all'intelligenza artificiale, dal marketing digitale alla protezione dei dati, dalla fotografia alla sicurezza cibernetica, fino a coprire tutti gli argomenti dell'attualità che corre veloce.

Una mission culturale e sociale per aiutare appassionati ed esperti a costruire un sapere condiviso su argomenti che, soprattutto per i meno giovani, risultano noiosi o a volte inaccessibili. Grazie alla collaborazione fra professionisti di settore, esperti di specifici ambiti, appassionati e conoscitori delle materie tecnologiche, informatiche e digitali, FvgTech porta il "sapere" sui diversi media.

Cuore della divulgazione è l'omonimo programma TV distribuito in molte emittenti private italiane, il programma radio in pillole e la partecipazione agli eventi, come in questo caso in cui siamo un'importante colonna del **Digital Security Festival**.

A rafforzare la diffusione delle informazioni si affiancano tutti gli altri canali: presenza sulla carta stampata come autori per testate, eventi informativi sul territorio nazionale, interventi radiofonici, corsi e seminari per i cittadini, collaborazioni con eventi di terzi e disponibilità a presenziare nelle scuole e nei corsi di realtà esterne.

FvgTech vuole quindi essere una "organizzazione divulgativa" spontanea al servizio dei cittadini, degli organi di stampa, degli eventi e del mondo dell'istruzione.

Oggi partecipiamo e collaboriamo con il Digital Security Festival, e state stringendo fra le mani il frutto di un lungo lavoro di preparazione e molte ore di elaborazione al computer, ma soprattutto di incontri e riunioni per dare vita ad un opuscolo che potesse lasciare il segno ed essere utile anche dopo le giornate del festival.

Per informazioni, collaborazioni, presenze esterne, potete contattarci all'indirizzo email: fvgtech@macpremium.it

Gabriele Gobbo

Ideatore di FvgTech e co-founder del Digital Security Festival

>> HAI QUALCHE COSA DA RACCONTARE?
COLLEGATI A WWW.FVGTECH.IT
E PROPONI IL TUO CONTENUTO <<



NetApp®

Rendiamo l'infrastruttura

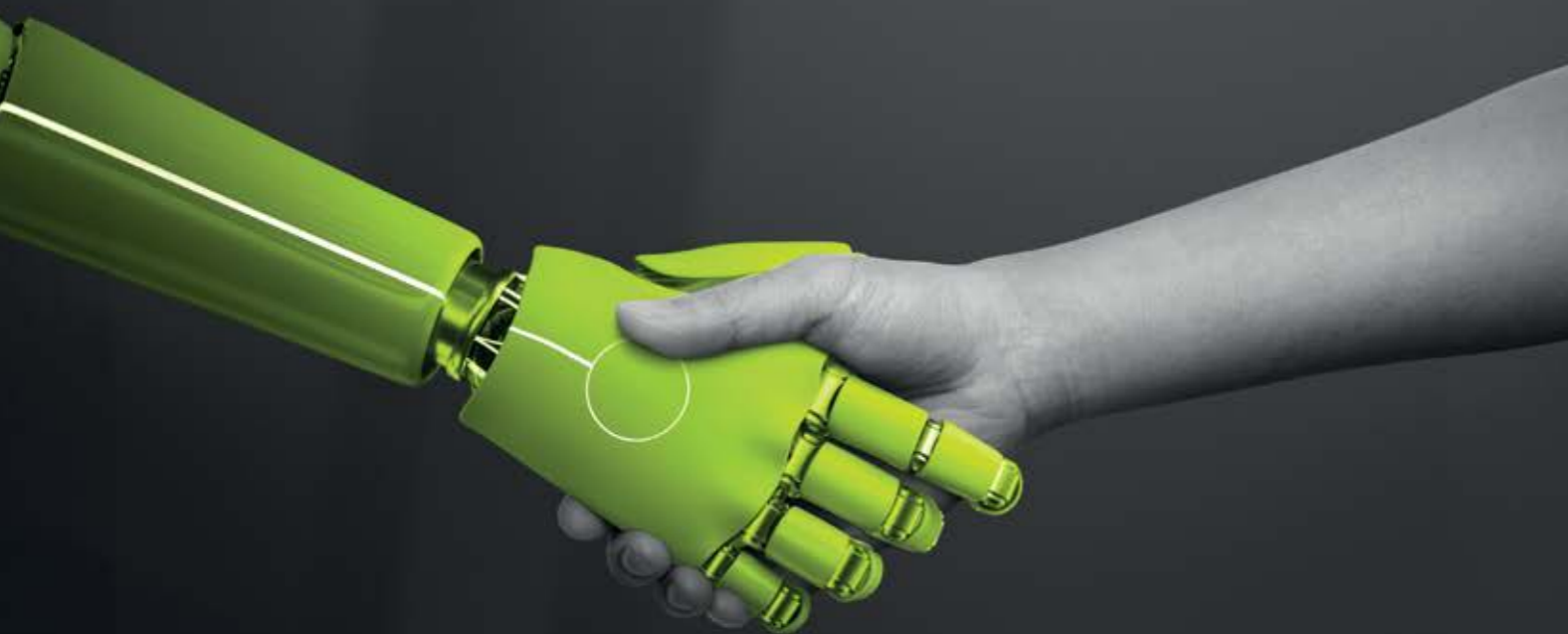
DATI INTELLIGENTE



©2024 NetApp. Tutti i diritti riservati. NETAPP, il logo NETAPP e i marchi riportati alla pagina <http://www.netapp.com/> TM sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.

Affida a noi la gestione della tua **infrastruttura IT.**

“END YOUR WORRIES”



Offriamo soluzioni personalizzate, per grandi e piccole aziende, garantendo **affidabilità e continuità operativa.**

I tuoi sistemi saranno **costantemente monitorati e controllati**, con un servizio che potrai estendere anche attraverso una **reperibilità h24 7x7.**



Digital Security Festival: Un viaggio nella sicurezza digitale

di Marco Cozzi Presidente Digital Security Festival

Benvenuti al Digital Security Festival, un evento che non è solo un'occasione di apprendimento, ma una vera e propria immersione nel mondo della sicurezza digitale, progettato per coinvolgere e sensibilizzare tutti: dai giovani agli adulti, dalle imprese alle istituzioni, coinvolgendo scuole e università.

In un'epoca in cui siamo sempre più connessi, la cultura della sicurezza digitale è diventata fondamentale. Ma cosa significa, esattamente, sicurezza digitale? Potremmo paragonarla alla conoscenza delle regole della strada: così come impariamo a guidare per evitare pericoli, è necessario conoscere e prevenire le minacce online. Si tratta di usare internet e dispositivi in modo consapevole, proteggendo la nostra privacy e i nostri dati personali.

Il Digital Security Festival si propone di rispondere a questa esigenza, fornendo gli strumenti necessari per affrontare il mondo digitale con maggiore consapevolezza. Oggi più che mai, la sicurezza informatica non è solo un tema per esperti, ma una competenza che riguarda tutti. Attraverso una serie di eventi, online e in presenza, affronteremo

argomenti di grande attualità come la cyber security, l'uso sicuro dei social media, la gestione dei rischi online, e l'importanza della protezione dei dati.

Ma la vera forza del Festival è la sua accessibilità. Abbiamo voluto creare un programma che parli a tutti, senza tecnicismi inutili, con l'obiettivo di rendere la sicurezza digitale alla portata di chiunque.

Partecipare al Digital Security Festival è molto più che seguire conferenze o seminari: è investire nella propria sicurezza, imparando a riconoscere i pericoli e a diventare cittadini digitali consapevoli. In un mondo sempre più "Onlife", dove la vita online e offline si fondono, questo evento vi offrirà competenze essenziali per vivere serenamente e in sicurezza.

Vi invitiamo a unirvi a noi, a esplorare, a imparare e a fare della sicurezza digitale una parte integrante della vostra quotidianità. Il futuro è digitale: prepariamoci a viverlo in modo sicuro.

Grazie per essere parte del Digital Security Festival.

DI **GABRIELE GOBBO**, Vicepresidente Digital Security Festival

IL WEB È MORTO, EVVIVA IL WEB!



"NONOSTANTE LA CRESCITA DI PIATTAFORME COME SOCIAL MEDIA E PODCAST, IL SITO WEB RIMANE UNO STRUMENTO FONDAMENTALE PER IL MARKETING E IL PERSONAL BRANDING, OFFRENDO LIBERTÀ, CONTROLLO E FLESSIBILITÀ IMPAREGGIABILI.

sulle nostre aziende e sui nostri prodotti, se non addirittura il nostro negozio con cui vendere.

Il sito web è soprattutto casa nostra, dove possiamo decidere cosa pubblicare, cosa dire senza filtri, senza algoritmi che ci censurino, senza limiti di caratteri, media, lunghezza, durata, formato. Il nostro sito web è

scalabile, ampliabile, implementabile senza limiti, nel senso che possiamo equipaggiarlo di sistemi e servizi su misura per noi e i nostri potenziali clienti: blog, newsletter, moduli, sondaggi, vetrine, cataloghi, file da scaricare, lista dei nostri contatti, player video, file audio, aree riservate, eventi. E poi sulle nostre pagine web, possiamo integrare contenuti provenienti da tutte le altre piattaforme: video di YouTube, post dei social, calendari di Google, prenotazioni di appuntamenti, recensioni.

Solo un nostro spazio web, gestito da noi e di nostra proprietà, permette tanta libertà e si adatta alle nostre necessità. Inoltre le persone si faranno un'idea precisa di noi visitando uno spazio che è nostro e rispecchia il nostro essere, la nostra professionalità, la nostra immagine coordinata.

Ricordiamoci sempre, infine, che i social media e le piattaforme di pubblicazione hanno la possibilità di farci sparire, di chiudere i nostri account senza motivazioni apparenti, di eliminare i nostri follower, di cancellare i nostri post e di cambiare le regole del gioco come e quando vogliono, senza preavviso.

Sono sempre di più le piattaforme per pubblicare contenuti su internet, dai social media ai podcast, dallo streaming video ai piccoli blog. Per questo motivo molti pensano che il "sito web" sia obsoleto o addirittura passato di moda... roba da boomer, direbbero le nuove generazioni.

Attenzione però, è un pensiero basato più su sensazioni che su un reale ragionamento di marketing o personal branding. Perché la verità è che il sito web è lo strumento principe di ogni strategia di comunicazione, è il luogo dove dobbiamo far atterrare le persone che vogliono informazioni su di noi,

SOC E IA

di Angelo Fragnito



L'espansione della minaccia Cyber ha reso necessario, per le aziende, implementare complesse e variegate soluzioni tecnologiche a protezione della propria infrastruttura IT e OT; queste stesse soluzioni generano una significativa mole di dati che è necessario analizzare attentamente per cercare indizi di attacchi sempre più sofisticati e distribuiti.

A tale scopo le aziende si affidano a SOC esterni che sono chiamati ad affrontare la sfida di "stare sul mercato" mantenendo una elevata efficacia di rilevamento e risposta alle minacce, in linea con i requisiti dei Clienti.

Chi scrive ritiene che, per affrontare adeguatamente questa sfida, è ormai indispensabile per i SOC adottare metodologie di Detection basate non solo su Regole di Correlazione (seppure ottimizzate) ma anche su Intelligenza Artificiale (AI) con cui i SOC

possono gestire in modo più rapido e accurato l'enorme quantità di dati generati dai sistemi di monitoraggio. Attraverso tecniche di machine learning e analisi predittiva, l'AI è in grado di individuare anomalie e comportamenti sospetti che potrebbero indicare una violazione della sicurezza, anche in contesti di attacco avanzati come l'Advanced Persistent Threat (APT).

Anche in fase di Response, l'AI supporta l'analisi automatica degli alert riducendo drasticamente il numero di falsi positivi che spesso rappresentano una sfida significativa per gli analisti di sicurezza. Questo permette agli analisti di concentrarsi su incidenti reali, migliorando l'efficienza operativa e la rapidità di risposta.

Ovviamente l'esperienza e la competenza degli analisti di sicurezza restano elementi fondamentali. L'AI può fornire strumenti potenti per identificare minacce e automatizzare processi, ma senza la "guida" di esperti qualificati, il suo pieno potenziale non può essere sfruttato. I security analyst, grazie alla loro conoscenza e capacità decisionale, analizzano i risultati forniti dall'AI affinando le strategie di risposta e risolvendo situazioni complesse che richiedono un'intuizione umana.

In conclusione, si ritiene che l'AI sia un alleato cruciale per i SOC nel fornire supporto reattivo e predittivo, andando ad ottimizzare il lavoro degli Analisti a garanzia di maggiore efficienza dei costi e maggiore efficacia nell'incontrare le esigenze dei Clienti.

Italiamac.it a 130.000



Il social network dedicato agli utenti Mac e Apple raggiunge e supera i 130.000 iscritti.

Nato nel 1996 è cresciuto ogni anno e oggi è la comunità Mac riconosciuta da Apple Inc. (AMUG) più grande d'Italia.

FvgTech Podcast



La trasmissione televisiva FvgTech dispone di un podcast in due versioni: video e audio. Entrambi gratuiti e disponibili su Apple Podcast oppure tramite il sito www.FvgTech.it. Inoltre sono reperibili sulla selezione di Spotify oppure su YouTube e Facebook. Disponibili tutte le puntate complete anche via App proprietaria.

Apimac.com



Su Apimac.com si trovano app per Mac e iPhone. Utility e soluzioni per il lavoro quotidiano.

LagunaMag.it

Molto utilizzato il servizio per il download della versione digitale di Laguna Magazine Fvg. Tramite il sito web www.lagunamac.it è possibile ricevere via email in versione PDF l'ultimo numero disponibile e una raccolta delle edizioni precedenti. Il servizio è completamente gratuito.

MacPremium
DIGITAL SOLUTIONS COMPANY
hello@macpremium.it

Sviluppiamo e ottimizziamo la **comunicazione** d'impresa in rete come missione; sfruttiamo tutte le opportunità dell'Information **Technology**.

VERSO UN APPROCCIO TRASVERSALE E CONSAPEVOLE ALLA CYBER SECURITY

di Manuel Valerio

L'Italia si colloca tra i paesi più bersagliati dal cybercrime a livello globale. Le minacce digitali si evolvono costantemente, e sebbene normative come la direttiva NIS2 abbiano aumentato (o hanno l'intenzione di farlo) la consapevolezza, non bastano a fronteggiare un cybercrime sempre più specializzato e industrializzato, anche grazie all'Intelligenza Artificiale.

In un mondo sempre più connesso e dipendente dalla tecnologia, la sicurezza informatica non può più essere considerata una semplice aggiunta alle operazioni aziendali. È diventata una componente essenziale per garantire la certezza e la continuità del business. La crescente sofisticazione delle minacce informatiche e l'aumento della superficie di attacco richiedono un approccio integrato e consapevole alla cybersecurity, che coinvolga non solo figure tecniche, ma l'intera organizzazione, a partire dalla direzione.

Un approccio integrato alla cybersecurity comporta che tutte le misure di sicurezza siano coordinate e interconnesse. Non basta implementare singoli strumenti di protezione senza una strategia complessiva che li unisca in un sistema coeso e completo. Le diverse soluzioni di sicurezza – firewall, antivirus, sistemi di rilevazione delle intrusioni, gestione delle identità, crittografia dei dati e così via – devono lavorare insieme in modo armonioso per fornire una difesa multilivello contro le minacce. Un sistema di gestione delle informazioni e degli eventi di sicurezza (un SIEM per esempio), può raccogliere e analizzare dati da diverse fonti, offrendo una visione d'insieme delle attività sospette e permettendo una risposta più rapida e efficace agli incidenti.

La consapevolezza è un pilastro fondamentale per un approccio efficace alla cybersecurity. La tecnologia da sola non è sufficiente per proteggere un'organizzazione; è necessario che tutto il personale, a tutti i livelli, sia consapevole delle minacce e delle buone pratiche di sicurezza. Gli attacchi di phishing, ad esempio, sfruttano spesso l'ingenuità degli utenti o la poca dimestichezza con gli strumenti tecnologici per raccogliere informazioni o addirittura arrivare a compromettere i sistemi informatici. Formare il personale, insegnando a riconoscere e rispondere correttamente a questo tipo di minacce può ridurre significativamente il rischio di successo di tali attacchi. Programmi di formazione e sensibilizzazione sulla sicurezza informatica dovrebbero essere regolarmente aggiornati e parte integrante della cultura aziendale. La sicurezza aziendale è come una catena, dove è l'anello più debole a determinare la robustezza di tutto il sistema.

La protezione non può e non deve limitarsi solo alle infrastrutture interne. Con l'aumento del lavoro remoto e l'uso di servizi cloud, è importante estendere le misure di sicurezza anche a queste aree. La protezione degli endpoint, delle vulnerabilità, la sicurezza



delle connessioni remote ed un approccio sicuro verso il cloud devono essere previste e/o integrate nel piano di cybersecurity aziendale. La collaborazione e la condivisione delle informazioni, poi, sono fondamentali.

Le minacce informatiche sono in continua evoluzione, motivo per cui nessuna organizzazione può dirsi al sicuro. Collaborare con altre organizzazioni e partecipare ad eventi di condivisione e formazione può aiutare a rimanere aggiornati sugli ultimi sviluppi e ad adottare misure preventive che possano aiutare ad avere un piano di sicurezza aziendale più efficace.

In conclusione, un approccio integrato e consapevole alla cybersecurity è indispensabile per proteggere le risorse digitali di un'organizzazione. Solo attraverso la combinazione di tecnologie avanzate, formazione del personale, gestione delle vulnerabilità, estensione della sicurezza al cloud e alle connessioni remote, e collaborazione si può costruire una difesa efficace contro le minacce informatiche.

Per questi ed altri motivi vi invito a partecipare all'Axera Cyber Security Day il 7 novembre 2024. Un evento ideato e pensato per fornire risposte concrete alle sfide attuali della sicurezza digitale. L'evento vedrà la partecipazione di speaker di rilievo che esploreranno i trend e le soluzioni più avanzate che possono aiutare a costruire la giusta consapevolezza, necessaria per riuscire a mettere in campo un piano cybersecurity efficace.

Vorresti dormire meglio la notte? GESTIAMO NOI I TUOI PROBLEMI IT



 **beanTech**[®]
IT moves your business

Assistenza completa 24/7 ■ Supporto di esperti
Monitoraggio proattivo e continuo

www.beantech.it

Ci sono quattro tendenze che più di altre stanno influenzando il mercato dei prodotti e servizi di cybersecurity per le imprese e sono tutti legati a strategie di "Trasformazione Digitale".

1. Lo sviluppo di applicazioni cloud-native e il suo ecosistema continuano a stimolare cambiamenti nella sicurezza, dalla fase di sviluppo alla produzione, per vari carichi di lavoro.

La natura ibrida e multicloud delle implementazioni basate su cloud richiede un approccio più dinamico e specializzato per abilitarne la sicurezza. Così la fornitura e la gestione dell'accesso alle risorse cloud stanno diventando particolarmente impegnativi, soprattutto se c'è una grande varietà di utenti e di dispositivi che si connettono a questi sistemi. Inoltre, la rapida adozione delle applicazioni SaaS richiede un approccio più completo ed "end-to-end" alla sicurezza. Senza contare il crescente numero di applicazioni "cloud-native" che richiede un'integrazione delle funzioni di sicurezza nel processo di sviluppo delle applicazioni cloud. Tutti questi elementi stanno portando all'emergere di un insieme di nuove tecnologie, come le piattaforme di protezione delle applicazioni cloud-native (cloud-native application protection platforms - CNAPPs), la gestione dei privilegi e credenziali delle infrastrutture cloud (cloud infrastructure entitlement management - CIEM), la gestione della "postura di sicurezza" SaaS (SaaS security posture management SSPM) e la sicurezza degli ecosistemi SaaS.

2. La necessità di avere controlli strettamente integrati che condividano la telemetria, oltre che l'aumento dei costi e delle sfide di gestione dei prodotti derivanti dalla complessità del portafoglio di prodotti di sicurezza, ha spinto un numero crescente di acquirenti a consolidare gli strumenti di sicurezza attorno ad un numero minore di fornitori.

La difficoltà di gestire attacchi sempre più complessi e mirati sta plasmando la necessità di avere una sicurezza più integrata e di sfruttare l'automazione, l'orchestrazione dell'intelligence e la telemetria per fornire un servizio di sicurezza più dinamico. La rilevazione e risposta estesa (Extended detection and response - XDR), la sicurezza basata

sull'IA, l'iperautomazione nella sicurezza e il secure access service edge (SASE), così come la "composable security" sono alcune delle offerte emergenti che si allineano a questo trend.

3. Le iniziative di trasformazione digitale, indirettamente, hanno portato a un aumento delle aree aziendali soggette ad un potenziale attacco. Questo ha comportato l'emergere di un insieme di controlli che offrono una migliore visibilità dei rischi. Le iniziative di trasformazione digitale, l'adozione generalizzata del lavoro remoto e la spinta a connettere tutte le aree gestionali di un'azienda, stanno spingendo verso l'adozione di nuovi strumenti mirati a supportare la gestione dell'esposizione al rischio



MERCATO DELLA CYBERSECURITY AZIENDALE: LE QUATTRO MAGGIORI TENDENZE CHE SPINGONO ALL'INNOVAZIONE

di Ruggero Contu

(exposure management) che si estende anche oltre il perimetro aziendale tradizionale per avere una migliore visibilità delle vulnerabilità.

4. Oggi più che mai è importante proteggere imprese sempre più distribuite e quindi le tecnologie di gestione dell'identità e degli accessi (Identity and access management - IAM) si stanno rapidamente evolvendo. Il segmento dell'offerta IAM è in forte fermento, guidato dalla necessità di adattarsi ai requisiti di nuovi modelli architetturali, dove l'autenticazione "edge computing machine-to-machine authentication" e i requisiti cloud stanno guidando cambiamenti e strumenti emergenti. Da considerare anche la crescente frustrazione nell'uso di fattori di autenticazione più tradizionali, come le password, che sono bersagli sempre più vulnerabili. Per queste ragioni, il settore IAM sta vivendo un periodo di forte fermento creativo (questa frase ripete la frase di apertura).



Figura 1. Le Quattro Principali Tendenze Tecnologiche che Impattano sulla Sicurezza

CYBERSECURITY NELLE PMI: UN CAMBIAMENTO DI MENTALITÀ

di Federica Maria Rita Livelli



Viviamo in contesto digitalizzato ed innovativo, caratterizzato da un crescente aumento di attacchi cyber e da un maggiore utilizzo dell'IA. Ne consegue che le organizzazioni devono sviluppare un framework di cyber resilience, quale intersezione dei principi di risk management, business continuity e cybersecurity.

Le organizzazioni, per garantire una trasformazione digitale efficace, dovranno bilanciare l'uso dell'AI con la competenza umana, investendo in formazione continua e difese adattabili, mirando al bene comune e mantenendo l'essere umano al centro del processo decisionale in modo da sfruttare la tecnologia per affrontare le complessità, senza esserne sopraffatti.

Inoltre, il rapido processo di digitalizzazione e innovazione nelle organizzazioni richiede un maggior coinvolgimento della Leadership che deve trasformarsi, adottando un approccio creativo e reattivo oltre ad esplorare nuove modalità di

comunicazione e relazioni. Ovvero, una "Leadership distributiva", capace di risolvere problemi attraverso reti collaborative e di trasformarsi in "E-Leadership", maggiormente vicino ai lavoratori ed in grado di interpretare i dati, prendere decisioni rapide e promuovere il cambiamento culturale.

In futuro, il rapporto tra uomo e macchina è destinato a diventare sempre più stretto. Ciò non significherà che le macchine sostituiranno gli esseri umani, piuttosto, completeranno le loro capacità, assumendo compiti faticosi o pericolosi, permettendo alle persone di concentrarsi su attività che richiedono abilità manuali e ingegno umano, in modo sicuro.

Indubbiamente si tratta di un cammino pieno di sfide e sine die con cui le organizzazioni si stanno confrontando. Tuttavia, come affermava lo scienziato Lavoisier: "nulla si crea, nulla si distrugge, tutto si trasforma".

WE ARE
HUMAN
EXPERT
IN HUMAN
RESOURCES
DIGITALIZATION

Alveria
www.alveria.it | www.hcms.it



Il Gruppo Quid e la pesca sportiva

di Federico Passeri e Maurizio Astarita

La responsabilità nella gestione di soluzioni IT per i nostri Clienti bancari ci porta a investire nei migliori framework di sicurezza, come quello dei Financial Services di IBM, e a rispondere alle prescrizioni ISO27001. Tuttavia, anche in questo scenario, il collega che clicca sul link per firmare digitalmente un documento urgente inviato da una fantomatica segreteria resta uno dei timori maggiori in capo al responsabile della sicurezza aziendale.

«Prima di cliccare pensa»: lo diciamo da metà anni 90. All'epoca i phishing in stile "il tuo premio da un milione di lire da ritirare" ci facevano sorridere, ora propongono un buono sconto per le scarpe n. 43 di colore bianco della mia marca preferita. Hanno visto sui social le mie foto, come vesto.

I nostri sistemi di difesa si avvalgono di IA per la valutazione dei comportamenti anomali nelle comunicazioni in entrata e in uscita, bloccando circa il 90% degli attacchi. Il comportamento umano, però, non rientra in un framework e il confine tra vita privata e professionale è pressoché ridotto a un formalismo da citare nelle policy aziendali.

Nel Gruppo Quid alleniamo i dipendenti con oltre 2000 campagne di phishing al mese e raccogliamo periodicamente le reti per capire che tipologie di "pesci" ci sono finiti dentro. Discutiamo le condizioni

che hanno portato il "pesce" a non vedere la rete e impariamo che, in caso di forte tensione, è meglio non gestire le mail in treno; che le mail dell'HR sono quelle in cui (erroneamente) riponiamo maggior fiducia. La nostra resilienza agli attacchi di phishing è cresciuta del 400% nel corso del 2023. Il miglior risultato? Il collega che, con naturalezza, ti sottopone una mail privata per capire se è autentica.

Nessun pesce è stato maltrattato durante le nostre campagne... o quasi!



IT CLUB FVG, partner DSF



Una associazione fondata NEL 2018, con le seguenti finalità:
Porsi come promotore di una cultura associativa tra coloro che ricoprono ruoli di responsabilità in ambito informatico all'interno delle Aziende e degli Enti pubblici; **Promuovere la conoscenza, la formazione e la collaborazione** tra gli aderenti, obbiettivi finalizzati al raggiungimento di una rinnovata interpretazione della funzione informatica aziendale; **Sviluppare una struttura informativa** preferenziale capace di offrire ai Soci un canale d'accesso ad informazioni e nuove tecnologie applicate in campo informatico; **Promuovere la collaborazione** con enti e associazioni, italiane ed estere, che perseguono finalità analoghe; **Stipulare convenzioni** per conseguire migliori condizioni contrattuali in tutti i settori di attività di interesse dell'Associazione e dei Soci; **Promuovere, organizzare e gestire** attività e corsi di formazione volti a facilitare e assistere lo sviluppo della professionalità, l'avviamento al lavoro e/o la riqualificazione dei lavori del settore. Tutte le informazioni e lo statuto su: www.itclubfvg.org

SECURE YOUR DATA

Always and everywhere



cabel.it

di Veronica Leonardi

CYBERSECURITY E INNOVAZIONE: LA SFIDA DEL NOSTRO TEMPO



"LE TECNICHE DI ATTACCO EVOLVONO CONTINUAMENTE, SFRUTTANDO ORA ANCHE L'INTELLIGENZA ARTIFICIALE"

degli attacchi informatici in Italia, con l'11% di essi riusciti, evidenziando la professionalizzazione dei criminal hacker.

Le tecniche di attacco evolvono continuamente, sfruttando ora anche l'intelligenza artificiale per generare, ad esempio, phishing più convincenti, eludere sistemi di difesa tradizionali e sfruttare vulnerabilità tramite analisi predittive. Affrontare tali minacce richiede un approccio evoluto alla cybersecurity che coinvolga aziende, persone e processi, oltre a soluzioni tecnologiche. Creare un ambiente digitale sicuro necessita di monitoraggio costante, specialisti dedicati, piani di risposta agli incidenti e gestione delle crisi informatiche, un compito arduo per molte organizzazioni.

In questo contesto, i servizi di Managed Detection and Response (MDR) offrono supporto vitale, garantendo monitoraggio in tempo reale e interventi proattivi, con vantaggi in termini di costi e conformità. Gartner raccomanda l'adozione dell'MDR come strategia per i Chief Information Security Officer. L'MDR fornisce funzioni SOC da remoto, gestite da personale umano, che monitorano e rispondono a intrusioni e comportamenti sospetti.

Cyberoo si distingue come Representative Vendor nella Market Guide di Gartner per i servizi MDR, offrendo un servizio completo di Detection e Response con una dedizione Above The Rest. La sua Cybersecurity Suite offre protezione continua basata su monitoraggio 24/7 e Threat Intelligence, ottimizzando i costi e rispettando le normative. Un passo avanti per un ambiente digitale sicuro e resiliente per tutti.

Crescente complessità: queste le prime due parole che mi vengono in mente per descrivere l'attuale contesto della cybersecurity. Un contesto legato all'innovazione digitale iniziata con ARPANET nel 1969. Sebbene l'evoluzione digitale abbia portato benefici in termini di efficienza, ha anche aumentato i rischi, creando una situazione di cyber-insicurezza. Nel 2024, il rapporto Clusit ha registrato un aumento del 65%

Dalle caverne allo spazio: Come adattarsi al progresso tecnologico



di **Davide Bazzan**
Segretario Digital Security Festival

novembre, la scrittura viene inventata il 25 dicembre, le piramidi costruite il 26 dicembre, la Divina Commedia di Dante scritta 20 ore fa e 5 ore fa realizzata la prima locomotiva.

E i più recenti successi tecnologici? L'uomo scende sulla luna 1,6 ore fa e l'iPhone realizzato 29 minuti fa. Da questa prospettiva è più facile comprendere l'enorme accelerazione che l'evoluzione umana ha subito. Siamo pronti ad affrontare le sfide e le opportunità che la rivoluzione digitale ci pone davanti? In un mondo sempre più virtuale, connesso e digitalizzato, l'educazione digitale non è più un'opzione,

SIAMO PRONTI AD AFFRONTARE LE SFIDE E LE OPPORTUNITÀ CHE LA RIVOLUZIONE DIGITALE CI PONE DAVANTI?

ma una necessità. Solo sapendo maneggiare con cura gli strumenti che utilizziamo ogni giorno, potremo utilizzare al meglio le potenzialità, proteggendoci dai rischi.

La digitalizzazione ha reso il mondo più connesso, ma ha anche aumentato i rischi per la privacy, la sicurezza e l'eventuale superficie di attacco. È fondamentale sviluppare una cultura della sicurezza informatica, insegnando alle persone a riconoscere eventuali attacchi, a proteggere i propri dati e a navigare in rete in modo consapevole.

Abbiamo bisogno di un nuovo modello educativo che promuova la curiosità, la creatività e la capacità di adattarsi a un mondo in continuo cambiamento. Da questi concetti è partita l'avventura del Digital Security Festival, trasferire le conoscenze degli esperti al numero maggiore di persone, nel modo più semplice possibile.

AXERA

7 NOVEMBRE 2024

MONTRESOR HOTEL TOWER (VR)

www.axera.it

CYBER SECURITY DAY

LA SICUREZZA DEL FUTURO: AI E CYBERCRIME INDUSTRIALIZZATO

di Federico Rosso

IoC Rendere accessibile l'intelligence a tutti nella sicurezza

In un contesto globale sempre più complesso, caratterizzato da minacce informatiche, instabilità geopolitiche e rapidi cambiamenti nei mercati, disporre di informazioni accurate e tempestive è essenziale per il successo aziendale. Tuttavia, per molte piccole e medie imprese, i costi elevati dei servizi di sicurezza e analisi di settore rappresentano una barriera importante.

Un Intelligence Operation Center (IOC) offre una visione completa delle minacce informatiche, spinte da cambiamenti geopolitici o dal mercato stesso, che possono colpire le aziende. Tuttavia, non tutte le imprese possono permettersi di sviluppare costosi sistemi interni o acquistare servizi esterni che siano accessibili e, allo stesso tempo, in grado di offrire solo le informazioni veramente utili.

Quello che serve è un approccio su misura, dove le aziende ricevono solo le informazioni rilevanti per il loro contesto, mantenendo i costi sotto controllo. In questo modo si riduce il "rumore" dei dati superflui e si risparmiano risorse, evitando l'investimento in infrastrutture o personale per gestire informazioni in eccesso.

HTS, con il suo Intelligence Operation Center, offre un servizio su misura che non solo protegge le aziende, ma consente loro di guardare al futuro con fiducia, basandosi su informazioni precise e pertinenti. Anche le PMI possono così accedere a un sistema di intelligence efficace e sostenibile, proteggendo il loro business in modo semplice e conveniente.



NETAPP: LEADER GLOBALE NELLA SICUREZZA DEI DATI E INNOVAZIONE NEL CLOUD IBRIDO

di Massimo Mondiani

NetApp è l'azienda di infrastruttura dati intelligente che, attraverso lo storage unificato, i servizi di dati integrati e le soluzioni CloudOps, trasforma le sfide di ogni cliente in opportunità. Come leader globale nella gestione dei dati, ci distinguiamo per il nostro impegno nella sicurezza del dato, un aspetto cruciale nell'era digitale. Anche quest'anno, partecipando come sponsor al Digital Security Festival 2024, ribadiamo la nostra missione di aiutare le organizzazioni a proteggere i loro dati. Continuiamo a essere un partner affidabile per le aziende che navigano nel complesso panorama della sicurezza digitale.

Le nostre soluzioni di sicurezza includono tecnologie di crittografia avanzata, sistemi di rilevamento delle intrusioni e soluzioni di backup e ripristino, tutte integrate

nelle piattaforme di gestione dei dati. La resilienza informatica è al centro della nostra strategia, utilizzando l'automazione e l'IA per migliorare la prevenzione e la risposta alle minacce. Offriamo soluzioni multi-cloud per garantire flessibilità e sicurezza dei dati e continuiamo a investire in tecnologie emergenti come la blockchain e l'edge computing per migliorare la resilienza e offrire una protezione end-to-end integrata.

Gartner ci ha riconosciuto come Leader del settore per 12 anni consecutivi e, con la recente nomina a Leader nel Magic Quadrant 2024 per le Piattaforme di Storage Primario, confermiamo il nostro continuo impegno verso i clienti, offrendo innovazione e soluzioni all'avanguardia nel settore a livello globale.



DI MARCO COZZI

L'intelligenza artificiale e il futuro del banking: Opportunità e sfide

Immaginate di entrare in banca e trovare un assistente virtuale pronto a rispondere a ogni vostra domanda, 24 ore su 24. O di ricevere un prestito in pochi minuti, grazie a un'analisi del rischio di credito quasi istantanea. Fantascienza? No, è il presente che sta prendendo forma grazie all'intelligenza artificiale applicata nel settore bancario.

L'IA sta ristrutturando dalle fondamenta un mondo tradizionalmente conservatore come quello delle banche, trasformandolo in un vivace ecosistema dinamico, laboratorio di innovazione che punta all'efficacia e all'efficienza del sistema economico, creditizio e finanziario. Ma cosa significa realmente tutto questo per i clienti e per chi lavora nel settore?

Pensiamo ai vantaggi: servizi bancari su misura, come un abito cucito dal miglior sarto, grazie all'analisi dei nostri dati. Assistenti virtuali pronti a darci una mano in tempo reale. E, ultima ma non per importanza, la sicurezza: algoritmi instancabili che setacciano le transazioni alla ricerca di attività sospette, proteggendoci dalle frodi, meglio di qualsiasi guardia del corpo.

Il termine che meglio rappresenta l'effetto dell'AI nel mondo si chiama "tempo".

Le performance dell'IA accelerano la valutazione del rischio di credito, perché enormi mole di dati, analizzate in pochissimi minuti, danno un risultato che per qualsiasi persona o impresa determina l'evoluzione, la competitività e la sostenibilità finanziaria. D'altra parte, un istituto bancario che riesce a gestire il rischio in tempo reale, usando modelli predittivi, riesce a gestire le risorse finanziarie con maggior sicurezza, efficacia e solidità.

Ma una moneta, usando la metafora della medaglia, ha sempre il suo rovescio. Come in ogni grande rivoluzione, ci sono anche sfide da affrontare. E una delle sfide dell'IA è il suo addestramento. Se i dati usati per addestrare l'AI sono viziati da pregiudizi, i cosiddetti bias algoritmici, potremmo trovarci di fronte a decisioni discriminatorie nell'assegnazione dei prestiti. Questa tema va affrontato

con trasparenza, rigore e intelligenza "umana", che rimane sempre la capacità di leggere dentro alle situazioni.

E poi, il tema dei temi del momento, la privacy dei dati, che non si risolve firmando tomi di carta, ma prendendo sul serio la questione della mercificazione delle nostre preziose informazioni, che sono parte determinante del nostro vissuto. L'IA è basata sulla raccolta massiva di informazioni personali e le banche devono garantire la protezione dei dati dei clienti, rispettando normative come il GDPR e prevenendo possibili violazioni.

C'è poi la questione lavoro. L'automazione potrebbe far sparire alcuni ruoli tradizionali in banca. Ma come è successo da sempre nell'innovazione, pensiamo al passaggio dalle lanterne da accendere nelle strade alla luce elettrica, la maestria dell'uomo è cogliere nuove opportunità, magari più stimolanti e creative. Alle macchine possiamo demandare la parte meccanica del lavoro, lasciando alle persone quella parte creativa che l'IA non ha. Dal canto loro, le banche dovranno investire nella formazione e riqualificazione dei propri collaboratori, preparandoli a ruoli più strategici e abilitandoli all'uso di nuove tecnologie.

Il futuro del banking sarà caratterizzato da una crescente collaborazione tra uomo e macchina. L'IA non sostituirà completamente l'intervento umano, ma lo affiancherà, fornendo strumenti per prendere decisioni più informate, dettagliate, riducendo al massimo il margine d'errore.

Le banche del futuro saranno sempre più digitali, accessibili ovunque e in qualsiasi momento, e in grado di adattarsi rapidamente ai cambiamenti del mercato e delle esigenze dei clienti.

Inoltre, potremo avere nuovi modelli di business, dove le banche si trasformeranno in piattaforme flessibili, capaci di offrire servizi su misura che usano al massimo le potenzialità dell'AI per rispondere a un mercato sempre più complesso, competitivo e veloce.

La collaborazione del DSF con Radio Studio Nord

www.studionord.news



Noi del Digital Security Festival siamo entusiasti di rinnovare la storica collaborazione con Radio Studio Nord. Abbiamo scelto di collaborare anche quest'anno perché riconosciamo che la radio è un mezzo di comunicazione potente e inclusivo, capace di raggiungere anche coloro che sono meno avvezzi al mondo digitale. Ogni mattina, Radio Studio Nord ha condotto un'intervista con un protagonista del festival. Queste interviste sono state trasmesse in diretta FM e sono anche disponibili in streaming sui social network. L'obiettivo è di rendere i temi della sicurezza digitale accessibili a tutti, spiegando concetti complessi in modo semplice e diretto. Riteniamo che la nostra partnership con Radio Studio Nord sia fondamentale per espandere la portata del nostro festival. La radio ha il potere di arrivare ovunque (anche grazie allo streaming

online), portando conoscenza e consapevolezza su temi cruciali come la sicurezza digitale.

La condivisione di molti dei nostri eventi fisici in diretta sui social network ci permetterà inoltre di raggiungere un pubblico ancora più ampio e variegato, proprio grazie al supporto tecnico e alla regia dello staff di RSN. Desideriamo che chiunque abbia l'opportunità di apprendere, di farsi un'idea sullo stato attuale della sicurezza digitale e di comprendere l'importanza di proteggere le proprie informazioni online. Siamo convinti che, unendo le forze con Radio Studio Nord, facciamo un passo significativo verso la realizzazione di questo obiettivo, rendendo il Digital Security Festival un evento inclusivo e istruttivo per tutti.

ABOVE THE REST

Abbiamo dato vita alla nuova campagna ABOVE THE REST.

Cyberoo si racconta in una veste nuova con nuovo spot e una serie di 10 podcast, con la voce di Federico Buffa.

Visita la pagina dedicata alla nostra campagna.

Le tendenze emergenti della cybersecurity nel 2024

Nel 2024, il panorama della cybersecurity continua a evolversi rapidamente, spinto dall'innovazione tecnologica e dall'aumento delle minacce informatiche. Le organizzazioni devono rimanere all'avanguardia per proteggere i loro dati e infrastrutture. Ecco una panoramica delle tendenze emergenti e delle sfide principali che plasmeranno il settore della cybersecurity nei prossimi anni.

1. Generative AI: promesse e sfide.

La tecnologia generativa AI, come ChatGPT e Gemini, sta rivoluzionando vari settori, inclusa la cybersecurity. Sebbene ci sia un certo scetticismo a breve termine, le potenzialità a lungo termine sono significative. Le applicazioni di AI promettono di aumentare la produttività, colmare le lacune di competenze e migliorare le operazioni di sicurezza. Tuttavia, la gestione delle aspettative e l'adozione etica della tecnologia sono cruciali per evitare la "prompt fatigue" e garantire che queste soluzioni siano utilizzate in modo sicuro ed efficace.

2. Metrics Outcome-Driven: colmare il gap comunicativo con il Board.

La crescente frequenza degli incidenti di cybersecurity ha messo in evidenza la necessità di metriche basate sui risultati (ODMs) per dimostrare l'efficacia degli investimenti in sicurezza. Queste metriche aiutano a tradurre gli investimenti in termini comprensibili per i dirigenti non IT, migliorando così la fiducia del board nelle strategie di sicurezza. ODMs forniscono un'espressione credibile del rischio, supportando decisioni di investimento mirate a migliorare i livelli di protezione.

3. Continuous Threat Exposure Management (CTEM).

Il CTEM è un approccio sistematico che consente alle organizzazioni di valutare continuamente l'accessibilità, l'esposizione e la sfruttabilità delle loro risorse digitali e fisiche. Questo metodo aiuta a identificare e prioritizzare le vulnerabilità, riducendo significativamente le possibilità di violazioni. Le organizzazioni che adottano il CTEM possono aspettarsi una riduzione delle violazioni fino a due terzi entro il 2026.

4. Aumento delle minacce AI.

L'AI non è solo una risorsa per le difese informatiche, ma anche una nuova frontiera per i criminali informatici. Gli attacchi basati su AI stanno diventando più sofisticati, richiedendo difese altrettanto avanzate. Le organizzazioni devono sviluppare nuove strategie di difesa che integrino l'AI per contrastare queste minacce emergenti e mantenere la sicurezza delle loro infrastrutture.

5. Crescita delle minacce malware e ransomware.

Il 2024 ha visto un aumento del 30% nel volume di malware



e un incremento significativo degli attacchi ransomware, in particolare nelle aree geografiche meno preparate. Questa tendenza sottolinea la necessità di difese più robuste e di una preparazione adeguata per rispondere a queste minacce in modo efficace. I ransomware, in particolare, sono diventati più sofisticati, con i criminali informatici che utilizzano strategie mirate per massimizzare l'impatto.

6. Attacchi DDoS in aumento.

Gli attacchi DDoS sono aumentati del 109% tra il 2022 e il 2023, creando una domanda crescente per servizi di mitigazione più sofisticati. Questi attacchi sovraccaricano i server, interrompendo i servizi e richiedendo soluzioni di mitigazione durature. Le organizzazioni devono investire in tecnologie e personale capaci di identificare e implementare le migliori soluzioni per mitigare questi attacchi.

7. Protezione delle informazioni affidabili.

Con l'aumento dell'uso dell'AI, la fiducia nelle informazioni diventa cruciale. Gli utenti cercheranno sempre più fonti che garantiscano informazioni affidabili e sicure. Questo sposta l'attenzione dalla sola privacy dei dati alla protezione dell'integrità delle informazioni. Le organizzazioni devono garantire che le loro informazioni siano accurate e affidabili per mantenere la fiducia degli utenti.

Conclusioni.

Le tendenze del 2024 nella cybersecurity indicano un panorama in rapida evoluzione che richiede adattabilità e proattività. Le organizzazioni dovranno investire non solo in tecnologie avanzate ma anche in formazione continua e consapevolezza culturale per proteggere efficacemente le loro risorse digitali. Con queste strategie, sarà possibile affrontare le sfide emergenti e garantire una maggiore resilienza contro le minacce informatiche future. La cybersecurity nel 2024 richiederà un approccio integrato che combini tecnologia, formazione e una cultura della sicurezza robusta. Solo così sarà possibile proteggere efficacemente le infrastrutture digitali e garantire un ambiente sicuro per le operazioni aziendali e personali.

di Michele Laurelli

Negli ultimi anni, l'intelligenza artificiale (AI) ha rivoluzionato numerosi settori, dall'assistenza sanitaria alla finanza, passando per la mobilità e l'industria manifatturiera. Questa tecnologia ha permesso di automatizzare processi complessi, migliorare l'analisi dei dati e offrire servizi innovativi. La rapida adozione dell'AI ha però sollevato nuove sfide in termini di sicurezza informatica. I modelli di AI sono diventati bersagli di attacchi sofisticati che mirano a manipolare, ingannare o compromettere i sistemi. In questo articolo, esploreremo i principali tipi di attacchi informatici specifici per i modelli di AI e le difese più avanzate attualmente disponibili, fornendo esempi pratici per una migliore comprensione.

Attacchi adversariali: il nemico invisibile. Gli attacchi adversariali coinvolgono l'introduzione di perturbazioni minime nei dati di input per ingannare i modelli di AI. Queste perturbazioni sono spesso impercettibili all'occhio umano ma possono causare errori significativi nel modello. Ad esempio, un'immagine



AI e sicurezza informatica: a che punto siamo?

di un gatto potrebbe essere leggermente alterata aggiungendo un "rumore" specifico. Per un osservatore umano, l'immagine appare invariata, ma un sistema di riconoscimento potrebbe classificarla erroneamente come un cane. Un caso celebre riguarda la manipolazione di segnali stradali. Ricercatori hanno dimostrato che aggiungendo piccoli adesivi su un segnale di stop, un'auto a guida autonoma potrebbe interpretarlo come un limite di velocità, ignorando l'obbligo di fermarsi. Questo tipo di attacco potrebbe avere conseguenze pericolose nel mondo reale. Per difendersi dagli attacchi adversariali, una delle strategie più efficaci è l'addestramento adversarial. Questo metodo prevede l'allenamento del modello con esempi di attacchi, in modo che possa riconoscerli e resistervi. Ad esempio, durante la fase di addestramento, al modello vengono presentate sia immagini normali che immagini con perturbazioni adversariali, insegnandogli a fare la distinzione. Un'altra difesa consiste nell'implementare tecniche di rilevamento che identificano input sospetti prima che raggiungano il modello principale. Questo può essere fatto analizzando le caratteristiche statistiche dell'input o utilizzando modelli separati dedicati al rilevamento di anomalie. Ad esempio, un sistema di sicurezza potrebbe analizzare le immagini in arrivo e segnalare quelle che presentano pattern insoliti. Infine, la certificazione di robustezza mira a sviluppare modelli con garanzie matematiche contro specifici tipi di perturbazioni. Questo approccio fornisce una sicurezza formale che il modello non sarà ingannato da perturbazioni entro certi limiti. Ad esempio, potrebbe essere garantito che qualsiasi modifica all'immagine inferiore a una certa soglia non altererà la classificazione.

Data poisoning: contaminazione alla fonte. Il data poisoning implica l'inserimento di dati malevoli nel set di addestramento del modello. Questo può portare il modello a comportarsi in modo imprevisto o a creare backdoor utilizzabili dagli attaccanti. Un esempio classico è l'inserimento di immagini etichettate in modo errato nel set di addestramento. Se un numero sufficiente di immagini di cani viene etichettato come "gatto", il modello potrebbe iniziare a confondere le due categorie. Un altro scenario riguarda i sistemi di raccomandazione. Un attaccante potrebbe aggiungere false recensioni o valutazioni per manipolare il modello a favorire o penalizzare certi prodotti. Questo non solo distorce i risultati per gli utenti, ma può anche avere implicazioni economiche significative per le aziende coinvolte. Per prevenire il data poisoning, è essenziale implementare validazioni rigorose dei dati. Ciò significa verificare l'integrità e la provenienza dei dati di addestramento, utilizzando tecniche come il controllo delle firme digitali o la tracciabilità delle fonti. Ad esempio, le piattaforme di raccolta dati possono richiedere l'autenticazione degli utenti e monitorare attività sospette. L'apprendimento robusto è un'altra difesa chiave. Si tratta di sviluppare algoritmi che siano meno sensibili ai dati anomali o corrotti. Questi algoritmi possono identificare e ignorare automaticamente gli outlier nel set di addestramento. Ad esempio, utilizzando metodi statistici per rilevare e rimuovere dati che deviano significativamente dalla media. Il monitoraggio continuo delle prestazioni del

modello aiuta a identificare comportamenti anomali che potrebbero indicare un avvelenamento dei dati. Se il modello inizia improvvisamente a fornire risultati inaspettati, può essere segno che qualcosa è andato storto durante l'addestramento. Ad esempio, un sistema di rilevamento delle frodi che inizia a classificare transazioni legittime come fraudolente richiederebbe un'indagine immediata.

Model stealing: furto di intelligenza. Il model stealing si verifica quando un attaccante riesce a replicare un modello di AI proprietario interrogandolo ripetutamente. Questo può portare alla perdita di proprietà intellettuale e a violazioni di sicurezza. Ad esempio, un concorrente potrebbe utilizzare questo metodo per copiare un modello di previsione finanziaria avanzato, ottenendo un vantaggio competitivo senza aver investito nelle risorse necessarie per svilupparlo. Gli attaccanti possono inviare una serie di input al modello e registrare le risposte. Con abbastanza dati, possono addestrare un nuovo modello che imita il comportamento dell'originale. Questo non solo rappresenta una perdita economica, ma il modello rubato potrebbe essere utilizzato in modi non etici o illegali, danneggiando la reputazione dell'azienda originale. Per difendersi dal model stealing, le aziende possono implementare limitazioni delle query. Questo significa impostare restrizioni sul numero di richieste che un utente può fare al modello in un determinato periodo. Ad esempio, limitando le query per indirizzo IP o richiedendo l'autenticazione per accedere al servizio. Un'altra difesa è fornire risposte limitate. Invece di restituire informazioni dettagliate o probabilità precise, il modello può offrire solo le informazioni strettamente necessarie. Ad esempio, un servizio potrebbe indicare solo se un'immagine contiene un volto umano, senza fornire ulteriori dettagli. Il watermarking dei modelli è una tecnica avanzata che prevede l'inserimento di segnali unici nel modello per dimostrarne la proprietà in caso di furto. Questo può essere fatto incorporando pattern specifici nel comportamento del modello che possono essere rilevati successivamente. Ad esempio, il modello potrebbe rispondere in modo specifico a input particolari, funzionando come una sorta di "firma digitale".

Conclusioni. La sicurezza informatica nell'era dell'AI è una sfida complessa e in continua evoluzione. Gli attacchi stanno diventando sempre più sofisticati, sfruttando le stesse tecnologie avanzate che alimentano i modelli di AI. È fondamentale che sviluppatori, ricercatori e professionisti della sicurezza lavorino insieme per sviluppare difese efficaci. Investire nella sicurezza dei modelli di AI non è solo una necessità tecnica, ma anche un imperativo etico per proteggere gli utenti e garantire la fiducia nel progresso tecnologico. Ad esempio, garantire che un sistema di diagnosi medica non possa essere manipolato significa salvaguardare la salute dei pazienti. Solo attraverso uno sforzo congiunto possiamo assicurare che l'AI continui a servire come forza positiva nella società, mantenendo al contempo alti standard di sicurezza e privacy.

1. Nel panorama attuale della cybersicurezza, quali considerate le principali minacce emergenti e come NetApp si sta adattando per affrontarle?

Ad oggi, le aziende sono costantemente esposte a attacchi ransomware, phishing di natura sofisticata, vulnerabilità zero-day e attacchi basati su intelligenza artificiale. NetApp affronta queste minacce implementando soluzioni avanzate di protezione dei dati e sicurezza informatica. Le soluzioni di NetApp includono la crittografia dei dati, il backup e il ripristino rapido, e l'integrazione di tecnologie di rilevamento delle minacce basate su AI per identificare e mitigare le minacce in tempo reale.

2. La cybersicurezza è un campo in rapida evoluzione. Come fa NetApp a rimanere all'avanguardia e a garantire che le soluzioni proposte siano sempre aggiornate rispetto alle nuove minacce?

Non smettiamo mai di investire nella ricerca e sviluppo, incluse le collaborazioni con leader del settore e l'adozione di standard di sicurezza all'avanguardia. NetApp aggiorna regolarmente le sue soluzioni per affrontare le nuove minacce e utilizza l'intelligenza artificiale per migliorare continuamente le capacità di rilevamento e risposta agli attacchi. NetApp possiede diverse certificazioni che dimostrano il suo impegno verso

la sicurezza e la conformità. Queste certificazioni, molte delle quali sono riconosciute dal governo americano, aiutano NetApp a garantire ai clienti che i loro dati sono gestiti in modo sicuro e conforme alle normative internazionali.

3. L'intelligenza artificiale ormai permea quasi ogni settore, come NetApp sta affrontando questo cambiamento, quali sono i maggiori rischi e quali i maggiori benefici?

NetApp è l'infrastruttura dati intelligente, che sfrutta difatto l'intelligenza artificiale per migliorare le proprie soluzioni di gestione e protezione dei dati. I maggiori benefici includono l'automazione dei processi di sicurezza, il miglioramento della precisione nel rilevamento delle minacce e l'ottimizzazione delle operazioni IT. Tuttavia, i rischi includono la possibilità che gli attaccanti utilizzino l'AI per sviluppare attacchi più sofisticati. Per mitigare questi rischi, NetApp implementa rigorosi controlli di sicurezza e monitora continuamente le sue soluzioni AI per garantire la loro integrità e sicurezza.

4. L'errore umano è uno dei principali fattori di rischio nella cybersicurezza. Come affronta NetApp la questione della formazione e della sensibilizzazione degli utenti e dei clienti?

NetApp è sempre attiva in questo ambito

proponendo programmi di formazione e sensibilizzazione continui per i propri dipendenti e clienti. L'azienda offre corsi di formazione sulla sicurezza informatica, workshop e materiali didattici per educare gli utenti sulle migliori pratiche di sicurezza. Questo avviene anche attraverso l'ecosistema di canale formato da partner ovvero da una rete di distributori e rivenditori che NetApp supporta con attività di enablement, dunque formazione e assistenza. Inoltre, NetApp promuove una cultura della sicurezza all'interno dell'organizzazione, incoraggiando la segnalazione di incidenti e il miglioramento continuo delle competenze di sicurezza.

5. Dove vedete il settore della cybersicurezza tra 5/10 anni? E come NetApp si sta preparando per quel futuro?

Il settore della cybersicurezza vedrà un aumento dell'uso di tecnologie avanzate come l'intelligenza artificiale, il machine learning e la blockchain per migliorare la protezione dei dati. NetApp si sta preparando per questo futuro investendo in queste tecnologie e sviluppando soluzioni innovative che possono adattarsi rapidamente alle nuove minacce. Inoltre, NetApp continua a collaborare con partner strategici e a partecipare a iniziative di sicurezza globale per rimanere all'avanguardia nel settore.

Il lato oscuro dell'IA

di Ettore Guarnaccia

Internet, Web, social e smartphone hanno trasformato la società. Oggi siamo entrati nell'era dell'intelligenza artificiale, con il metaverso all'orizzonte. Molti manager sono entusiasti dell'IA per la sua efficienza, ma con oltre il 90% dei dipendenti che già ne fa uso, non stiamo forse sottovalutando i rischi per la sicurezza?

L'IA non è infallibile: è fatta di hardware, software, dati e logiche matematiche, vulnerabili a manipolazioni e attacchi. Ragiona per probabilità, la sua accuratezza dipende dall'addestramento ricevuto, e può produrre errori o allucinazioni. Inoltre, le sue logiche possono riflettere pregiudizi e resta aperto il tema della responsabilità morale e legale per i suoi errori. Molti ne parlano, ma pochi la conoscono veramente.

Quante aziende hanno adottato policy di uso sicuro dell'IA? Quanti dati e documenti aziendali sono stati esposti a terze parti tramite l'uso di app IA? Quanti dipendenti hanno ingenuamente permesso a queste app di monitorare riunioni e chat? Quanti team di sicurezza sono pronti a fronteggiare attacchi molto più sofisticati grazie all'IA? E quanti CEO hanno considerato l'impatto sociale dell'IA sui dipendenti?

Consideriamo le situazioni in cui le decisioni dell'IA possono mettere a rischio vite umane, come nei trasporti autonomi, sistemi medici o armamenti. In circostanze impreviste, l'IA agirebbe solo secondo la sua programmazione, senza coscienza, emozioni, sentimenti, intuito, creatività, etica o questioni morali. Non crediamo all'illusione di un'IA superiore in tutto all'essere umano, piuttosto prepariamoci a gestire questa nuova ondata tecnologica e uscirne indenni.



postpickr
Your Social Media Assistant
Gestisci tutti i social da un'unica app e risparmi il 70% del tempo.
www.postpickr.com
PROVALO GRATIS!

infostar
TECNOLOGIE DIGITALI

DI ELEONORA GHIANI

SICUREZZA INFORMATICA E MENTE UMANA: QUANDO I PREGIUDIZI SABOTANO LA DIFESA

In ambito della cybersecurity aziendale, soprattutto nelle PMI e nelle PA, si tende a focalizzarsi su minacce come cybercriminali e malware, trascurando i bias cognitivi, che influenzano le decisioni e possono compromettere la sicurezza. Questi pregiudizi mentali sono responsabili di molti errori umani, spesso causa di gravi violazioni.

Tra i bias più comuni c'è il bias della familiarità, che porta le persone a fidarsi di ciò che appare conosciuto. Un esempio tipico è l'apertura di e-mail di phishing perché il mittente sembra un collega o un fornitore abituale. C'è poi il bias dell'ottimismo, che spinge a credere che certi eventi negativi non capiteranno a noi, riducendo così la vigilanza e aumentando il rischio di cadere in trappole come il phishing. Il bias di conferma porta invece le persone a cercare solo informazioni che confermano le loro convinzioni preesistenti, ignorando segnali di allarme. Infine, il bias dell'autorità fa sì che ci si fidi ciecamente di figure autorevoli o di messaggi apparentemente provenienti da fonti elevate, sfruttato ad esempio dagli attacchi di pretexting.

Per contrastare l'impatto dei bias cognitivi, è essenziale investire nella formazione continua per sensibilizzare i dipendenti e condurre simulazioni di phishing per migliorare la consapevolezza dei segnali di allarme. Utilizzare strumenti di verifica automatica aiuta a confermare l'autenticità delle comunicazioni, mentre una cultura del dubbio costruttivo incoraggia i dipendenti a verificare anche le richieste provenienti da fonti autorevoli. Infine, fornire feedback immediato dopo gli errori permette di correggere comportamenti errati e migliorare la consapevolezza collettiva.



La velocità è tutto quando si parla di proteggersi dagli attacchi informatici

di Bruno Trani



Lo sentiamo dire ogni giorno, la sicurezza informatica è diventata una vera e propria corsa contro il tempo. Le minacce digitali si evolvono a un ritmo impressionante e i cybercriminali affinano costantemente le loro tecniche per penetrare anche nei sistemi più protetti. Nel corso del 2023, i sistemi di monitoraggio del Security Operation Center di Yarix (YSOC) hanno rilevato circa 311 mila eventi di sicurezza (+87% rispetto al 2022), occorrenze che indicano possibili

violazioni di un sistema, un servizio o una rete informatica: quasi il doppio rispetto all'anno precedente. Sempre più veloci e complessi: gli attacchi sono tra le principali sfide che le imprese devono e dovranno affrontare anche in futuro. Ciononostante, le aziende difficilmente scelgono di prevenire questi problemi di sicurezza e si ritrovano a doverli affrontare solo ad attacco avvenuto. Yarix, business unit di Var Group - operatore leader nel settore dei servizi e delle soluzioni digitali, con un fatturato di 823 milioni di Euro al 30 aprile 2024 - è una delle aziende italiane più innovative nel comparto della sicurezza informatica. Da oltre 20 anni fornisce servizi e soluzioni a industrie, enti governativi e militari, aziende del comparto sanitario e università. Con sedi in Italia e in Europa, dispone di un Cognitive Security Operation Center tra i più evoluti, si avvale di team specializzati in defensive e offensive security, Cyber Threat Intelligence, Incident Response, assicurando una difesa avanzata in ambito cyber security, network & edge security, cloud security.

La Sicurezza Digitale Spiegata Semplice

I tre punti del DSF

01

Divulgazione della cultura digitale e della sicurezza applicata ad aziende, scuole, istituzioni, ragazzi e genitori.

02

Verranno creati eventi online e offline per tutte le età, per coprire tutta la gamma di fruitori del web e del mondo digital in genere.

03

Onlife è quanto accade e si fa mentre la vita scorre, restando collegati a dispositivi interattivi (on + life) [Treccani].



La Cooperativa numero 1 in Italia nella gestione amministrativa e previdenziale per i lavoratori dello spettacolo. Dal 2002 abbiamo iscritto oltre 13.000 Soci e regolarizzato oltre 360.000 esibizioni. La soluzione completa, professionale ed economica per mettere in regola Band, Musicisti, Deejay, Prestigiatore, Attori, Presentatori, Comici, etc....

www.esibirsi.it



ACARA

La piattaforma semplice e sicura per la segnalazione di condotte illecite.

whistleblowing platform



è un servizio



Chi nella vita ha ricevuto questa domanda? Penso tutti. Questa potrebbe essere una delle domande che meglio potrebbe adattarsi al contesto tecnologico in corso. Un contesto caratterizzato da un'impennata inflazionistica di parole quali: Digital Transformation, efficienza, flessibilità etc... Parole che generalmente sono accostate a uno dei temi più trattati del momento, ahimè, più delle guerre in corso ovvero il fenomeno dell'Intelligenza Artificiale. I social media e le stampa non fanno altro che scrivere articoli sul tema dell'IA. L'argomento è così appealing che sono entrati in campo i notissimi tuttologi, i famosi allenatori di calcio al tempo dei mondiali piuttosto che gli skipper ai tempi, tra l'altro attuali, di Luna rossa. L'effetto è che si sta diffondendo il concetto secondo cui l'IA è una sorta di evolutiva tecnica, con un impatto esclusivamente tecnologico e soprattutto con un processo implementativo plug & play. Spesso sembra che venga percepita, ma potrei sbagliarmi, come una semplicistica equazione del tipo: IA = riduzione lavori ripetitivi = risparmio di manodopera. E purtroppo, sono queste correnti a creare le aspettative più pericolose. Sebbene si parli di IA da pochi anni, le radici del fenomeno risalgono agli anni '50 con il lavoro pionieristico di Alan Turing, da cui prende il nome del famoso test di Turing. Le evoluzioni successive (machine learning, deep learning) hanno portato alla nascita, nel 2021, dell'ultima frontiera, la più evoluta al momento e la più impattante ovvero la generative AI. Quest'ultima rappresenta il fenomeno che impatterà in maniera stravolgente (nel bene e nel male) i prossimi 5 - 10 anni. Tornando al tema dell'appeal, proprio Gartner, in una pubblicazione risalente all'estate 2023, ha collocato, per la prima volta, l'IA generativa all'interno del Gartner Hype Cycle nel "picco delle aspettative gonfiate". Gli esperti, mi riferisco a coloro che sponsorizzano l'evoluzione con consapevolezza, scrivono che l'impatto non sarà solo industriale ed economico ma soprattutto etico - sociale. E aumenterà significativamente nei prossimi 5 - 10 anni con conseguenze che potrebbero essere drammatiche se non saremo preparati. Tra l'altro, seppur in piccolo e

COSA VUOI FARE DA GRANDE?

neanche tanto, abbiamo tutti sotto gli occhi l'impatto sociale derivante dall'introduzione dello smartphone: dipendenza e tecnofobia con una riduzione della capacità creativa, problemi di autostima e ansia e sovraccarico cognitivo. Dal momento che errare è umano ma perseverare è diabolico, è arrivato il momento di affrontare gli impatti della generative AI con un approccio strategico integrato. I primi segnali non sono incoraggianti. Nell'interesse del profitto del singolo, i grandi colossi Tech continuano a innovare senza sosta e a seguire le numerose start up. Inoltre, solo l'Europa ha da poco varato una regolamentazione in materia che l'altro pone un tema di vantaggio competitivo verso gli altri continenti che procedono senza regole, un po' come il tema della sostenibilità. Da qui la domanda che mi sono posto da qualche tempo. Come l'uomo vuole gestire tale evoluzione? E quindi, cosa vuole fare da grande? Subire passivamente l'utilizzo massivo di questa tecnologia o cercare di governarla provando mitigando gli impatti sociali ed etici che ne derivano? Nel primo caso, l'ultimo dei problemi forse sarà una società totalmente trasformata. Il vero punto di attenzione è che la generative AI rappresenterà, con un impatto molto più rilevante, il nuovo smartphone. Vi è mai capitato nel corso di un viaggio in auto di dover decidere se seguire i consigli del navigatore o meno? Questo sarà uno degli snodi decisionali che l'uomo sarà chiamato ad affrontare: subire o governare le scelte dell'IA? Applicate questo esempio ad ambiti come la sanità, i processi industriali, l'istruzione, la gestione delle infrastrutture e proviamo a immaginare le conseguenze che



potrebbero generarsi nell'esserci o non esserci affidati all'IA. Quando citavo il termine strategia integrata intendevo riferirmi ad un approccio coordinato al tema da parte delle Istituzioni e di chi crea l'IA. Serve una profonda sensibilizzazione e formazione a tutti i livelli a partire delle generazioni più giovani, le più esposte. Un significativo aumento della consapevolezza circa il valore che l'IA potrebbe apportare e i conseguenti temi etici che sarà necessario affrontare e disciplinare. I più anziani si ricorderanno la nota saga Terminator risalente agli anni '80 dove il regista James Cameron ha praticamente rappresentato in modo visionario il rapporto conflittuale tra uomo e macchina. A differenza delle precedenti rivoluzioni industriali, l'avvento dell'IA ha dei connotati molto più impattanti perché mette fortemente in gioco il ruolo del genere umano. Non possiamo "svendere" l'elemento più prezioso e sofisticato ad oggi presente ovvero il cervello umano. La macchina più complessa e sofisticata, autrice delle invenzioni più importanti ad oggi esistenti al mondo. E l'IA mira proprio ad emulare il comportamento dell'uomo. Quindi, sarebbe davvero imprudente continuare a inventare algoritmi per agevolare e velocizzare tale percorso di emulazione per poi subirne passivamente le decisioni. Credo che l'obiettivo più importante dei prossimi anni debba essere la collaborazione tra digitale e umanesimo in un contesto che richiederà al genere umano una forte azione da protagonista. Credo che debba essere questo il senso di "Umanocentrico".

>> BIZ

CYBERSICUREZZA NEL SETTORE INDUSTRIALE

di Aleandro Agarinis

La cybersicurezza è un argomento molto dibattuto ultimamente, le discussioni sono prevalentemente basate sulla protezione di PC e Server da attacchi informatici che possano limitarne la funzionalità con annessi costi, pochi però pensano che c'è un altro settore, di cui poco si parla ma che, a livello di numero è ordini di grandezza superiore è cioè il settore industriale. I cosiddetti PC mbedded sono dappertutto, dalla macchina del caffè evoluta fino al tornio a controllo numerico, dall'unità di controllo di bordo treno al sistema di comunicazione di un aereo: sono totalmente pervasivi. Cleverynext, startup innovativa con sede in provincia di Udine si occupa di cybersicurezza nel settore industriale. L'azienda propone una soluzione trasversale per tutti i mercati embedded che richiedono un controllo puntuale di tutte le problematiche relative alla sicurezza dei prodotti elettronici, indipendentemente dal loro uso, tutti le fasi, dalla produzione

fino all'utilizzo, vengono coperti. I problemi che l'azienda indirizza sono essenzialmente due: la sicurezza del comportamento dei dispositivi elettronici e la sicurezza del software installato intesa come protezione dalla copiatura e/o sostituzione. L'impatto può essere molto diverso a seconda del settore in cui tale dispositivo elettronico opera, ad esempio nel settore della difesa più che l'aspetto economico è importante garantire l'operatività, mentre nel settore commerciale di fondamentale importanza è la protezione da pirateria. La soluzione è un approccio olistico che garantisce la cosiddetta completa "Chain of Trust" e cioè una protezione che parte dall'hardware ed arriva, livello dopo livello, fino all'applicazione del cliente. Inoltre, viene garantita anche la "Production Chain of Trust" e cioè che anche il fornitore terzo dei prodotti, non sia in grado di minacciare i prodotti che egli stesso produce.



VARGROUP

Accompagniamo le imprese nel loro percorso di evoluzione digitale e lo facciamo con la nostra più grande risorsa: le persone.

Seguici



www.vargroup.it - Numero Verde 800646543

Virus Informatici e Intelligenza Artificiale: La Nuova Minaccia della Sicurezza Digitale

L'integrazione tra intelligenza artificiale e virus informatici sta aprendo scenari inquietanti nel mondo della sicurezza informatica. Sebbene un virus completamente autonomo non sia ancora realtà, già esistono malware sofisticati come i virus polimorfici e i rootkit. Questi mutano continuamente il loro codice per sfuggire alla rilevazione, rappresentando uno step evolutivo verso minacce più avanzate. I virus polimorfici, ad esempio, cambiano costantemente la loro struttura, rendendo difficile il lavoro degli antivirus tradizionali.

Un esempio di tecnologia avanzata in questo campo è DeepLocker, sviluppato da IBM Research. Questo malware rimane inattivo fino a quando non raggiunge il suo target, attivandosi solo quando riconosce obiettivi specifici, come volti o posizioni geografiche. Questa capacità di mascherarsi lo rende quasi impossibile da rilevare fino a quando il danno non è già fatto.

La paura è che l'IA possa permettere ai virus di evolversi autonomamente, utilizzando tecniche come il reinforcement learning e le GAN (Generative Adversarial Networks), consentendo loro di imparare dai propri errori e migliorare costantemente la capacità di eludere le difese.


Per difendersi, anche gli antivirus dovranno evolversi parallelamente, utilizzando l'IA per rilevare comportamenti sospetti in tempo reale. Queste soluzioni sono ancora agli inizi e, a causa dei costi elevati, non accessibili a tutti. L'IA è una risorsa per proteggere i sistemi ma anche un'arma nelle mani dei cybercriminali. In questo contesto, la collaborazione con specialisti del settore come IS Copy S.r.l. SB diventa fondamentale. Aziende con esperienza consolidata e competenze avanzate nel campo della sicurezza informatica sono in grado di fornire le migliori soluzioni per monitorare, prevenire e combattere minacce emergenti. Collaborare con partner qualificati garantisce un livello di protezione elevato, salvaguardando i dati e le infrastrutture aziendali da attacchi complessi e pericolosi.

di Stefano Gabaglio




HTS


HI-TECH SERVICES



Sviluppo Software




IoC




Karmasec

Cyber Security



I AM



Log Management

scopri di più su www.hts-italy.com

L'IMPORTANZA DELL'APPROCCIO UMANOCENTRICO PER UNA CYBERSECURITY EFFICACE E SOSTENIBILE

di Matteo Navacci



La Direttiva NIS2 rappresenta un importante passo avanti per la sicurezza delle reti e dei sistemi informatici in Europa. Tuttavia, spesso è il fattore umano, oltre alle risorse economiche, a ostacolare la piena adozione delle misure di sicurezza richieste. La Direttiva richiama best practices di sicurezza delle informazioni, come quelle della ISO 27001. Tra le misure previste dall'articolo 21 vi sono politiche di analisi dei rischi, gestione degli incidenti, continuità operativa e sicurezza della catena di approvvigionamento. La tecnologia è però solo un mezzo: le persone, con le loro competenze e attitudini, sono il cuore dei processi aziendali. L'approccio umano-centrico alla Governance, Risk & Compliance (GRC) nel contesto della cybersecurity è quindi essenziale per garantire il successo dell'integrazione dei nuovi requisiti della

NIS2. Un approccio umano-centrico alla cybersecurity necessita la collaborazione attiva tra consulenti e personale interno, che devono lavorare insieme per creare sinergie efficaci e sviluppare un sistema di sicurezza sostenibile e adattato alle esigenze reali dell'organizzazione. La formazione, in particolare, dovrebbe essere un processo di accrescimento reciproco, dinamico e interattivo, che coinvolge i dipendenti e permette loro di comprendere e applicare efficacemente le misure di sicurezza. In parallelo, come sottolineato anche dalla ISO 27001, la Leadership aziendale dovrebbe sostenere i processi GRC e incentivare e agevolare le relazioni tra consulenti e dipendenti. Solo con un buon livello di coinvolgimento e con un approccio umano-centrico è possibile costruire un sistema di cybersecurity efficace e sostenibile.

Il Valore dei System Integrator e i Servizi Gestiti

di Enrico Zocca

Nel panorama tecnologico odierno, i System Integrator svolgono un ruolo cruciale nell'aiutare le aziende a navigare la complessità delle soluzioni tecnologiche disponibili. Un system integrator è un'azienda specializzata nell'integrazione di diverse tecnologie e sistemi per creare soluzioni complete e funzionali.

La trasformazione digitale e i servizi IT sono elementi chiave per il successo delle aziende nel mondo moderno. Investire in queste tecnologie e adottare una mentalità aperta al cambiamento può portare a significativi miglioramenti in termini di efficienza, competitività e soddisfazione del cliente.

Quale è il ruolo dei Servizi Gestiti?

Un esempio è la gestione continuativa con monitoraggio delle infrastrutture IT. Lo scopo è che i sistemi siano efficienti e

funzionino in modo sicuro. Questo approccio proattivo consente alle aziende di concentrarsi sulle loro attività principali, lasciando la gestione tecnica agli esperti.

Quali sono i benefici per i Clienti finali?

Riduzione dei Costi: I servizi gestiti permettono di ridurre i costi operativi, eliminando la necessità di un team IT interno dedicato.

Accesso a Competenze Specializzate: I clienti beneficiano dell'esperienza e delle competenze avanzate dei system integrator, che possono risolvere problemi complessi e implementare soluzioni innovative.

Scalabilità e Flessibilità: I servizi gestiti offrono la possibilità di scalare le risorse IT in base alle esigenze aziendali, garantendo una maggiore flessibilità.



Sicurezza Informatica persistente: Con un monitoraggio continuo e aggiornamenti regolari, i servizi gestiti migliorano la sicurezza delle infrastrutture IT, proteggendo i dati sensibili delle aziende.

di **Sonia Gastaldi**, consigliera Digital Security Festival

LA TECNOLOGIA AL SERVIZIO DELL'UMANITÀ



fortemente in una tipologia di progresso tecnologico realizzato per favorire il progresso sociale e culturale.

La preziosa, sapiente e lungimirante visione olivettiana oggi riconoscerebbe nell'evoluzione digitale lo strumento perfetto per liberare l'essere umano dalla schiavitù del lavoro alienante, di qualsiasi tipo, a favore della creatività e dell'utilizzo del tempo libero per la cultura, nelle sue innumerevoli espressioni.

Ma la prospettiva olivettiana, più di tutto, considererebbe la formazione di donne e uomini per abilitarli al buon uso della tecnologia, perché la conoscenza è, da sempre e per sempre, il vero motore della crescita in ogni dove.

Sapienti tecnologie devono considerare i valori etici, perché nessuno venga escluso dal progresso, ma soprattutto perché nessuno subisca danno dalle macchine, che difficilmente saranno capaci di raggiungere quella coscienza che ci rende esseri straordinari, capaci di opere straordinarie.

La vera innovazione non è creare nuovi strumenti, ma trovare nuovi modi di fare le cose, sempre più sostenibili, equi e di valore. La spinta vera dell'innovazione tecnologica è educare, formare e addestrare l'umanità, a favore di una qualità della vita che ci permetta di gustare la natura, la bellezza e la cultura, con una tecnologia a servizio dell'umanità.

Noi del Digital Security Festival ci prodighiamo per questo.

C'era una volta un imprenditore visionario che aveva sognato, agli inizi del '900, un'impresa a servizio dell'umanità. Stiamo parlando di Adriano Olivetti, industriale-innovatore che, oggi più che mai, ispira il mondo imprenditoriale moderno, ma più di tutto il settore tecnologico.

Adriano Olivetti, alla guida dell'azienda di famiglia, vedeva la tecnologia come uno strumento per migliorare la vita delle persone e della società. La sua filosofia si rifletteva non solo in prodotti pionieristici, ma anche nel modo in cui gestiva l'impresa. Olivetti credeva

di **Gabriele Gobbo**



Sempre più potente e sempre più economica per gli utenti, è l'intelligenza artificiale generativa, da ChatGPT in giù. Quindi, più si abbassano i costi e più il rischio che sia inserita nel flusso di "lavoro" dei criminali è alto, anzi, è sicuro. Se mettiamo assieme generazione di

testi, immagini, video e audio, capiamo che la produzione di fake è praticamente già qui. Ora, immaginate che la tecnologia deepfake, cioè la falsificazione di video per far dire a una persona quello che vogliamo, sia diventata talmente a portata di mano da essere applicata in diretta durante una videochiamata di lavoro. Passate ad immaginare un'impiegata che trasferisce milioni di Euro su un conto sconosciuto, perché a chiederlo è stato in diretta un suo superiore. Ora, fate scorrere la mente a una madre che riceve una videochiamata dalla figlia che, in lacrime, dice di essere stata rapita. Ora basta immaginare, perché sono due casi già accaduti, trovate le storie con i dettagli sul web. Il problema non è "se" ci trufferanno con l'intelligenza artificiale generativa, ma "quando" ci trufferanno. Perché la guerra delle piattaforme sta accelerando sempre di più lo sviluppo delle black box che contengono gli algoritmi di ogni

azienda produttrice, e di pari passo i criminali si adeguano e spingono sulla creatività, piegando algoritmi e modelli a loro uso, per migliorare sempre di più i propri sistemi malevoli. Se prima venivano usati i sistemi di AI per generare testi e traduzioni credibili o magari per inscenare una chat testuale dal vivo, ora si punta a video deepfake, che purtroppo molte persone ancora non conoscono. Siamo su un nuovo livello, siamo in un nuovo campionato della truffa, qui si sta giocando duro, molto duro! Messaggi audio credibili e quasi irriconoscibili che giungono ai telefoni di migliaia di cittadini con le robocall, conoscenti o colleghi in tempo reale in una videochiamata, parenti che ci mandano un vocale, video di noi stessi... sono tutti prodotti già realizzabili mettendo assieme le varie intelligenze artificiali odierne. Come finirà? Non lo so, nel frattempo alzate le antenne e dubitate di quello che vedete e sentite.

Be prepared with Axians

Un approccio olistico alla Cybersecurity e alla Compliance NIS2



Un approccio olistico alla cybersecurity è ormai necessario per affrontare le minacce sempre più sofisticate di oggi.

Adottare un approccio olistico ai rischi informatici significa scegliere una strategia di integrazione fra tecnologie, persone e processi, integrando la sicurezza in ogni ambito dell'azienda, dalla formazione dei dipendenti alla gestione delle vulnerabilità di ogni risorsa, in una continua evoluzione in cui tutti i dipendenti e sistemi sono coinvolti.

La compliance alla recentissima Direttiva europea NIS2 è un altro elemento cruciale che impone alle organizzazioni una visione olistica e proattiva della sicurezza informatica, sia dal punto di vista delle minacce che delle strategie difensive. La NIS2, infatti, richiede alle società europee di adottare misure di sicurezza adeguate per prevenire gli attacchi, proteggere le infrastrutture critiche e i servizi essenziali e reagire in caso di attacco, ponendo l'attenzione anche in questo caso su tutti gli aspetti organizzativi, umani e tecnologici.

Non è più possibile pensare di adottare singole soluzioni o di delegare le responsabilità a pochi, la cybersecurity di oggi è un panorama globale.

È per questo che noi del Team NT (azienda udinese del Gruppo MEET IT) da anni applichiamo un approccio olistico per offrire ai nostri Clienti strategie e soluzioni personalizzate di Cybersecurity e Compliance alla NIS2, basate sulle seguenti fasi:

- Consulenza e Risk Analysis
- Assessment
- Soluzioni e servizi per il raggiungimento del target
- Gestione e monitoraggio

Visita il sito per saperne di più.

#CYBER_RESILIENCE

Servizi integrati per la **Sicurezza Informatica** e la **Compliance NIS2**

www.meetit.cloud

fa parte del Gruppo **MEET IT**

L'INTELLIGENZA ARTIFICIALE NEI PROCESSI HR: OPPORTUNITÀ E SFIDE TRA INNOVAZIONE E SICUREZZA

di Massimo Genova



L'avvento dell'Intelligenza Artificiale nei processi di digitalizzazione HR rappresenta una rivoluzione sia in termini di efficientamento operativo che di cultura aziendale. Sfruttare le opportunità offerte dall'AI, come l'automazione dei processi e la valorizzazione delle competenze strategiche, è fondamentale. Tuttavia, è altrettanto cruciale considerare le implicazioni del suo utilizzo in relazione alla privacy delle risorse e alla sicurezza dei dati sensibili.

Le organizzazioni devono attuare azioni preventive per proteggere sia l'azienda che i dipendenti dai rischi connessi alle nuove tecnologie digitali. Ecco alcune misure fondamentali per non farsi trovare impreparati:

1. Crittografare i dati: proteggere i dati sensibili e prevenire accessi non autorizzati attraverso la crittografia è essenziale per garantire la sicurezza delle informazioni aziendali.
2. Educare l'AI: effettuare audit regolari sui dati utilizzati dall'AI per evitare pregiudizi

nei processi di selezione e valutazione delle competenze.

3. Investire e sensibilizzare sulla sicurezza informatica: le minacce legate al phishing e ai deepfake sono in crescita; per questo è necessario adottare misure di autenticazione a più fattori e formare i dipendenti sui potenziali rischi.

4. Implementare pratiche di monitoraggio strutturate: monitorare correttamente i processi senza violare la privacy è cruciale per promuovere un ambiente di lavoro basato sulla fiducia.

In conclusione, affrontare le sfide poste dall'intelligenza artificiale richiede non solo investimenti nelle tecnologie più adeguate, ma anche un forte impegno per garantire sicurezza e fiducia. Le persone restano al centro del successo di ogni impresa. Per questo motivo, Alveria (link: www.alveria.it) si impegna a garantire che il suo software proprietario, HCMS (link: www.hcms.it), sia costantemente testato e aggiornato, riducendo al minimo i rischi derivanti da vulnerabilità applicative.



ISACA®

Venice Chapter

Programma del Festival 2024

25 OTTOBRE, 4 E 5 NOVEMBRE ONLINE

SOCIAL ARENA. LE CONFERENZE ONLINE APERTE AL PUBBLICO IN DIRETTA STREAMING

18 OTTOBRE UDINE

INAUGURAZIONE IN PRESENZA DEL FESTIVAL. 08:15/13:00 AUDITORIUM COMELLI DEL PALAZZO DELLA REGIONE FRIULI VENEZIA GIULIA. 14:30/19:00 PRESSO PALAZZO TORRIANI

19 OTTOBRE TAVAGNACCO (UD)

AI & CYBER SECURITY. 10:00/11:30 SESSIONE NELL'AMBITO DI ARTIFICIAL INTELLIGENCE FORUM PRESSO TEATRO IMMERSIVO P. MAURENSIG

22 OTTOBRE RONCADE (TV)

PRIVACY, AI & CYBERSECURITY. 14:30/18:30 PRESSO H-FARM

23 OTTOBRE (TV)

NEWGEN CYBER SKILLS. 10:00/13:00 TO BE ANNOUNCED

23 OTTOBRE MONTEBELLUNA (TV)

NIS2. 15:30/19:00 PRESSO INFINITE AREA

28 OTTOBRE TRIESTE

DIGITALIZZAZIONE E CYBERSICUREZZA, DALLA P.A. ALLE AZIENDE. 09:00/19:00 PRESSO SALA PREDONZANI DEL PALAZZO DELLA REGIONE FRIULI VENEZIA GIULIA

30 OTTOBRE PADOVA

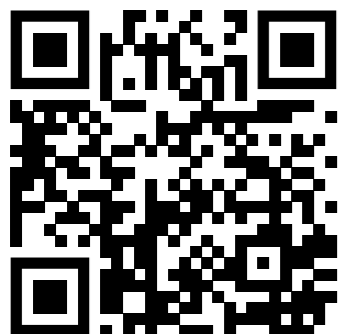
STAY SECURE. 14:30/19.30 PRESSO PALAZZO DEL BO ARCHIVIO ANTICO

4 NOVEMBRE ONLINE

WEBINAR PRO. I SEMINARI VERTICALI ONLINE IN DIRETTA DEDICATI AI PROFESSIONISTI

8 NOVEMBRE VICENZA

EVENTO DI CHIUSURA DEL FESTIVAL. 16:00/19:00 PRESSO VILLA VALMARANA AI NANI



PROGRAMMA DEI CONVEGNI, INFORMAZIONI E RELATORI SONO DISPONIBILI SUL SITO WEB DEL FESTIVAL O SULLA APP PER SMARTPHONE DEDICATA DISPONIBILE PER IOS E ANDROID.

DIRETTIVO DEL DSF:

MARCO COZZI / PRESIDENTE
GABRIELE GOBBO / VICEPRESIDENTE
DAVIDE BAZZAN / SEGRETARIO
LUIGI GREGORI / TESORIERE
SONIA GASTALDI / CONSIGLIERA

Date, informazioni e location possono variare senza preavviso, si invita a consultare il sito web ufficiale per le informazioni aggiornate.

www.digitalsecurityfestival.it

KARMASEC: SICUREZZA INFORMATICA A PROVA DI FUTURO

In un mondo sempre più connesso, la sicurezza informatica è diventata una priorità imprescindibile per aziende di ogni settore. Karmasec, con sede in Italia, si pone come partner di fiducia per chi desidera proteggere i propri dati e infrastrutture digitali, garantendo soluzioni su misura per affrontare le sfide del cyber-crimine.

Fondata da esperti del settore, Karmasec ha l'obiettivo di prevenire, rilevare e rispondere alle minacce informatiche in modo rapido ed efficace. L'azienda offre una vasta gamma di servizi, che spaziano dall'analisi delle vulnerabilità, alla gestione degli incidenti, fino a soluzioni di compliance e governance dei dati. Tutti i servizi sono personalizzabili in base alle specifiche esigenze del cliente, permettendo alle aziende di focalizzarsi sul proprio business, mentre Karmasec si occupa di tenere al sicuro le informazioni.

Il team di Karmasec è composto da specialisti altamente qualificati, costantemente aggiornati sulle ultime metodologie di attacco.

Grazie a una combinazione di competenze tecniche e una profonda conoscenza delle normative in vigore, l'azienda è in grado di supportare le imprese nella conformità a standard internazionali come ISO 27001, fornendo consulenze mirate per garantire una gestione ottimale dei dati.

L'innovazione è il cuore di Karmasec: l'azienda investe continuamente in ricerca e sviluppo per offrire servizi all'avanguardia, come l'intelligenza artificiale applicata alla sicurezza informatica e tecniche di monitoraggio avanzato, capaci di rilevare problemi e minacce.

Affidarsi a Karmasec significa scegliere un approccio proattivo e consapevole alla cybersecurity, assicurando protezione, efficienza e tranquillità.



il sito del festival è utile tutto l'anno con gli articoli del direttivo e dei partner www.digitalsecurityfestival.it

>> SPECIAL THANKS



SDPS

Secure by Design Porting Solution

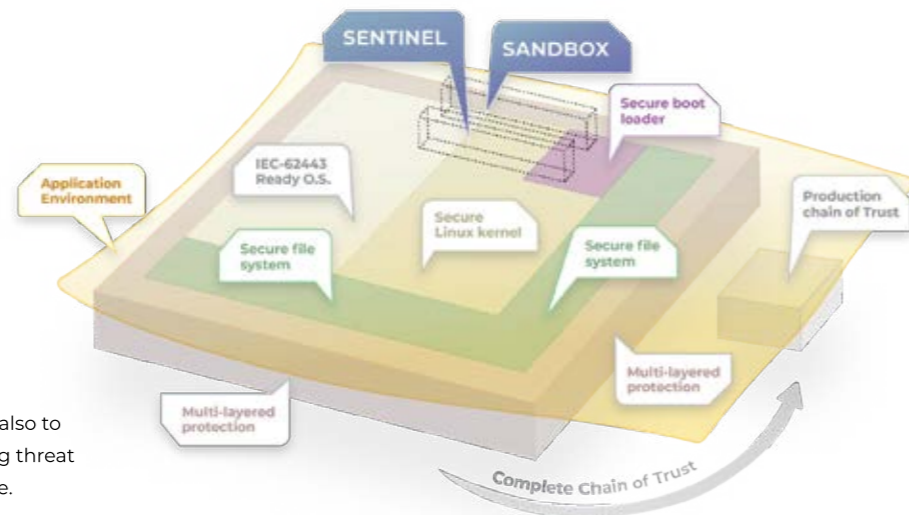
The SDPS solves the cyber security problems of industry operators, builders and integrators.

As such, the solution itself needs to be cyber security resilient throughout its entire lifetime.

In this proposal, several components are integrated to work together as a system to not only meet the IEC 62443-4-2.

Security Level 2 requirements but also to protect against the SDPS's evolving threat environment over its entire lifetime.

With the increased distribution of Ethernet-connectivity also in the so-called embedded environment, as well industrial equipment like machines, robots and other electronic equipment may become subject to cyber attacks. These network elements may be protected with other equipment, hence often much more cost-efficient and reliable is having implemented a modern security architecture in the phase of product development. SDPS is an aggregation of methods, tools and mechanisms in which all the individual elements work hand in hand to ensure defense in depth.



With SDPS your product becomes actively protected against cyber attacks and, at the same time, is passively supervised to ensure the detection of a potential threat.

SDPS can be implemented progressively to obtain stricter and stricter security protection and, if needed, an environment to develop final applications. An extension of security methods including third parties production phase is also available.

- Secure boot loader** - Adaptation and industrialization of the initial line of defense.
- Secure Linux kernel** - Specifically configured kernel to limit potential risks.
- IEC-62443 ready OS** - GNU-Linux Operating System built from scratch, crafted in the wake of the IEC-62443 norm to minimize the attack surface.
- Secure file-system protection** - choice, deployment and tuning of the right file-system and flash-related activities to further increase the solution security. Choices are among encrypted, read-only, redundant and some other possibilities.
- Multi-layered protection** - The 360° security belt proposed is an approach that deploys multiple security controls to protect all the vulnerable areas.
- Execution Sandbox** - An item aimed mainly at protecting the OS from user application misbehaving. An additional line of defense versus external threats.
- SENTINEL Application** - component to analyze, check and filter Ethernet traffic in order to avoid and detect out-of-context and/or malicious frames.
- Application Environment** - to users who want to develop their own solution. It is a middleware with all the ancillary tasks needed around the specific product application, like the CLI engine, installation and upgrade procedures, logging, maintenance tools, etc.
- Production Oriented Chain of Trust** - an extension of security procedures to cover the production phase with its critical handling of keys and secrets.



Cleverlynext srl
 Via J. Linussio, 1 - 33020 Amaro (UD) - ITALY
 administration@cleverlynext.com

cleverlynext.com

Unicorn Trainers Club: Cloud e AI Stanno Rivoluzionando il Settore delle Startup della Cybersecurity



Nell'era digitale, la sicurezza informatica è una priorità assoluta per aziende di ogni dimensione. Con l'aumento delle minacce cibernetiche, le startup nel campo della cybersecurity stanno emergendo come protagonisti fondamentali. Il panorama della cybersecurity è in continua evoluzione, guidato da nuove tecnologie e minacce emergenti. Una delle tendenze più significative è l'adozione dell'intelligenza artificiale (AI) e del machine learning (ML) per rilevare e mitigare le minacce in tempo reale. Infatti, molte startup stanno sviluppando soluzioni avanzate che utilizzano AI e ML per analizzare grandi volumi di dati e identificare comportamenti anomali.

Un'altra tendenza importante è la crescente attenzione alla sicurezza del cloud. Con sempre più aziende che migrano le loro operazioni nel cloud, la necessità di proteggere questi ambienti è cruciale. Anche in questo caso, molte startup stanno rispondendo a questa esigenza sviluppando soluzioni di sicurezza specifiche, che offrono visibilità e controllo sui dati e le applicazioni ospitate nel cloud.

Va ricordato che le startup di cybersecurity, come tutte le startup, devono lavorare duramente per ottenere la fiducia dei clienti, ma allo stesso tempo affrontano la sfida specifica di dover stare puntualmente al passo con le minacce in continua evoluzione, come il ransomware, il phishing, il cryptojacking,

la SQL Injection e gli attacchi a dispositivi IoT. Tuttavia, queste sfide rappresentano anche opportunità significative e lo spazio di mercato disponibile per gli startupper è potenzialmente molto ampio e in continua ridefinizione. Per questo motivo, gli investitori, dai business angels ai venture capitalist e al private equity, mantengono un alto interesse nel sostenere startup che offrono soluzioni innovative e scalabili per la sicurezza informatica.

Lo Unicorn Trainers Club è un'associazione con sede a Udine che mira a creare un ambiente collaborativo tra i vari attori dell'ecosistema delle startup. Organizziamo eventi, workshop e incontri di networking per mettere in contatto startup promettenti con potenziali investitori e partner strategici. Per quanto riguarda l'ambito della cybersecurity, prevediamo che continuerà a essere un'area di investimento prioritario, considerando che le minacce cibernetiche diventeranno sempre più sofisticate, richiedendo soluzioni innovative e avanzate. Per questo supportiamo con entusiasmo le startup tecnologiche che ambiscono a creare soluzioni che vadano a colmare le numerose esigenze di un mercato in continuo cambiamento.

Per ulteriori informazioni sulle nostre attività, visitate il nostro sito web all'indirizzo unicorntrainers.it

NOTE E APPUNTI



Governance IT e Trasformazione Digitale: equilibrio tra tecnologia, dati e talento

di **Luigi Gregori**, Tesoriere Digital Security Festival

Negli ultimi mesi, ho avuto il privilegio di lavorare con diverse organizzazioni nel cuore della loro trasformazione digitale. Oggi vorrei riflettere su alcuni temi fondamentali che emergono dal dibattito attuale su come migliorare questi processi, ispirato da alcune letture recenti.

Uno degli aspetti che ritengo sempre più centrale è l'importanza di un inventario preciso e completo degli asset IT. Ho trovato molto interessante l'articolo "5 Ways an Asset Inventory Improves Your Digital Transformation Project" pubblicato recentemente. Mantenere una mappatura accurata degli asset tecnologici non è solo una pratica di buon governo IT, ma rappresenta la base su cui costruire qualsiasi iniziativa di trasformazione digitale. Quando parliamo di inventario degli asset, non si tratta solo di tenere traccia dell'hardware o dei software. Parliamo di una visione a 360 gradi che include infrastruttura, applicazioni, dati e perfino le competenze umane associate. Un inventario ben gestito permette di identificare in maniera proattiva le aree di rischio, ottimizzare l'utilizzo delle risorse e facilitare l'allineamento delle iniziative tecnologiche con gli obiettivi strategici dell'azienda.

Questo tema si collega perfettamente a un altro spunto che emerge in modo molto chiaro nell'articolo del World Economic Forum "Unlocking the full potential of digital transformation through technology and talent". Il vero potenziale della trasformazione digitale non risiede solo nella tecnologia, ma nella capacità di coniugare l'innovazione tecnologica con il capitale umano. È facile concentrarsi esclusivamente sull'acquisto di nuovi strumenti o piattaforme, ma spesso si dimentica che senza una forza lavoro adeguatamente formata e motivata, la tecnologia da sola non è sufficiente. È fondamentale investire in talenti, dotarli delle competenze giuste, e soprattutto, creare un contesto dove i dati e la tecnologia siano accessibili e utilizzabili da tutti i livelli dell'organizzazione.

Questo concetto di 'democratizzazione dei dati', come viene esplorato nell'articolo di ITWeb "Democratising Data: Empowering IT for a Data-Driven Future", mi sembra essenziale. Viviamo in un'epoca in cui i dati sono diventati la risorsa più preziosa, ma il loro vero valore emerge solo se riusciamo a renderli facilmente accessibili e comprensibili a chiunque ne abbia bisogno, senza barriere tecnologiche o culturali. Un'IT governance moderna deve favorire l'accesso ai dati e la capacità di interpretarli, non limitarli. Inoltre, dobbiamo creare processi in cui le decisioni siano guidate dai dati, promuovendo una cultura aziendale che ne riconosca l'importanza in ogni fase operativa e strategica.

Come IT Governance Advisor, riconosco che la sfida della trasformazione digitale non è solo tecnologica, ma soprattutto culturale. L'integrazione di nuove piattaforme e strumenti richiede un contesto in cui le persone possano sfruttarne appieno le potenzialità. È quindi fondamentale investire sia in



tecnologie innovative che in formazione continua, creando una cultura aziendale che valorizzi l'innovazione.

Il successo si basa sull'equilibrio tra asset tecnologici, dati e talenti. I progetti di trasformazione digitale vincenti integrano sapientemente questi tre elementi, adottando una visione olistica. Le aziende che riusciranno a bilanciare tecnologia e capitale umano saranno quelle più capaci di affrontare le sfide future.

I temi discussi, come l'inventario degli asset IT, la democratizzazione dei dati e la gestione del talento, si allineano con la filosofia del Digital Security Festival 2024. Questo evento, focalizzato su una tecnologia umanocentrica, sottolinea come l'evoluzione digitale debba essere guidata dall'uomo e per l'uomo.

Il festival mira a trasformare l'anello debole umano in un punto di forza attraverso conoscenza e consapevolezza. La sicurezza informatica deve proteggere non solo dati e sistemi, ma soprattutto ciò che ci rende umani. Questa visione si allinea con l'obiettivo di coniugare tecnologia e umanità, promuovendo una cultura della sicurezza digitale etica e resiliente.

Infinityhub

«Quale sarebbe oggi lo scenario socio-economico globale se l'economia prendesse ad esempio i modelli scientifici di apprendimento, dialogo e certificazione congiunta dell'astrofisica?». Iniziamo qui, assieme, con una domanda, un viaggio spazio-tempo, condividendo gli elementi esperienziali che anticipano il futuro al quale tutte e tutti tendiamo. Perché? Perché siamo nati dall'Unità e il nostro destino è quello di riconvergerci proprio nello spazio-tempo, esattamente come accade alle singole gocce di acqua nelle onde del mare.

Inizia così il nostro libro "Persone Energie Futuro", edito da Edizioni Ca' Foscari. Lo studio della fisica, il metodo scientifico applicato al fare impresa e un approccio interdisciplinare, o meglio antidisciplinare, per lo sviluppo del modello "Y" sono gli strumenti che hanno permesso a Massimiliano Braghin di pensare, realizzare e far crescere, alla velocità della luce, Infinityhub SpA benefit. Azienda che ha le fondamenta in "acqua", per ricordare la stretta connessione con la città più bella, fragile e resiliente del mondo "Venezia", dove c'è l'Headquarter della Energy Social Company che punta alle stelle, seguendo l'indicazione del sommo profeta Dante, agire con "l'amor che move il sole e l'altre stelle".

Il tema del Digital Security Festival - sottolinea Massimiliano - ci coinvolge, perché noi possiamo fare quello che facciamo anche attraverso strumenti digitali e software che utilizzano l'intelligenza artificiale. Abbiamo la piena consapevolezza che l'AI può supportare la nostra opera, velocizzando i processi algoritmici, strategici e decisionali. Non sostituirà il nostro ingegno, ma più di tutto non farà la parte che fa la nostra coscienza, che prende decisioni ragionevoli. Quindi, aderire al Festival è fare la nostra parte nel divulgare il buon uso di strumenti software e hardware, che non sono una minaccia in sé, ma dipendono dalla naturale evoluzione

di **Massimiliano Braghin**



verso una sempre maggior cooperazione, che è cultura del fare insieme, e dalle intenzioni del nostro agire. Perché come ci ricorda Federico Faggin nel suo ultimo libro Oltre l'invisibile: «È arrivato il tempo di riconoscere la nostra vera natura e di unirici per creare un mondo migliore.»

Infinityhub nasce nel 2016 da venti azionisti fondatori, oggi conta 2250 soci ed investitori. Utilizza un modello di business innovativo, costituendo insieme all'energivoro una società partecipata per lo sviluppo ad hoc di interventi di riqualificazione ed efficienza energetica. Le società partecipate raccolgono i finanziamenti anche grazie a strumenti di finanza innovativa, come il crowdfunding, con la partecipazione al capitale sociale di cittadini, privati e aziende.



LA NUOVA *DIMENSIONE* DELL'ENERGIA

Infinityhub Spa Benefit finanzia progetti di riqualificazione energetica, coinvolgendo attivamente persone, imprese e comunità che cooperano nel presente per un futuro di unione. Creiamo soluzioni innovative, sostenibili e accessibili che promuovono una transizione energetica partecipata, attraverso impianti di produzione di energie rinnovabili, riqualificazione termica ed edile di immobili, finanza etica e strumenti fintech. Crediamo in un futuro in cui l'energia viene condivisa, con un effetto positivo, duraturo e sostenibile per tutte e per tutti.

Il nostro obiettivo

Un futuro in cui la sostenibilità ambientale, economica e sociale si integrano, dando vita a un modello d'impresa responsabile, quindi capace di dare risposte nel presente, per custodire il futuro.

La bellezza è la vita quando la vita si rivela. La bellezza è l'eternità che si contempla allo specchio, e noi siamo l'eternità e lo specchio.

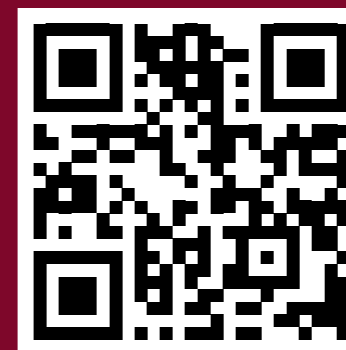
Khalil Gibran



WE MAKE DATA INFRASTRUCTURE INTELLIGENT



Discover more



Digital Security Festival numero 6. Umanocentrico per natura.

«Un robot non può recare danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno»

Per il Digital Security Festival 2024, edizione numero 6, partiamo dalla prima legge della robotica di Isaac Asimov.

L'evoluzione tecnologica deve essere guidata dall'essere umano, per l'umanità intera.

La tecnologia per la persona e non la persona per la tecnologia. Oggi è possibile trasporre la celebre frase di Adriano Olivetti che si riferiva alla fabbrica, ma che nel suo cuore esprimeva il desiderio di accelerare l'evoluzione tecnologica per lasciare il tempo alle persone di vivere e arricchirsi con la bellezza, l'arte e la cultura.

Riprendere il controllo della tecnologia e renderla umanocentrica per natura significa:

- imparare ad usare bene gli strumenti digitali per ridurre quello sforzo e quella ripetizione umana, che è stata ben rappresentata da Charlie Chaplin in Tempi Moderni. L'intelligenza artificiale non è il male, dipende solo dall'uso che se ne fa e da chi la utilizza;
- considerare la sicurezza umana, trasformando il fattore umano da anello debole a punto di forza e resilienza, attraverso la conoscenza, la consapevolezza e il controllo;
- pensare all'uomo come parte integrante della natura, che va protetta e tutelata anche grazie alle nuove tecnologie e all'intelligenza artificiale;
- costruire efficacemente la cultura della cyber security, con attività progettate, realizzate e diffuse su



misura, in base all'età, al livello di conoscenza e alla posizione lavorativa delle persone.

Perché dsf 6.

La tecnologia è uno strumento, non un fine: rappresenta un mezzo per far evolvere la società nelle varie situazioni di vita quotidiana. Per risolvere la complessità di questi tempi dobbiamo semplificare, seguendo il principio per cui less is more. Con questo intento possiamo creare una nuova alleanza tra la tecnologia e l'umanità, lasciando alla prima il lavoro metodico e ripetitivo e consentendo alla seconda di esprimere la creatività.

Uniamoci!

DSF è un laboratorio diffuso per il futuro della sicurezza digitale. È un'opportunità

unica per unire le menti più brillanti e trasversali del settore tech con interventi di filosofi, sociologi, esperti, professionisti, operatori e istituzioni, tutti impegnati a creare un ecosistema digitale più sicuro, etico e profondamente umano. Che siate esperti di cybersecurity, innovatori tech, o semplicemente cittadini interessati al vostro futuro digitale, l'esperienza di questo festival ha moltissimo da offrirvi fuori dall'ordinario. Unitevi a noi per diversi giorni di dialogo, innovazione e co-creazione.

Oggi, insieme, ispirandoci alle visioni dei giganti del passato come Olivetti e Asimov, possiamo ridefinire il concetto di sicurezza per l'era digitale del futuro. Non si tratta solo di proteggere dati o sistemi, ma di salvaguardare e potenziare ciò che ci rende e mantiene umani all'interno di un mondo sempre più digitale.

L' IT nelle nostre mani, "il tuo business al centro."

Non esistono percorsi universali, ma soluzioni su misura. Con i nostri clienti realizziamo un percorso personalizzato, nato studiando le esigenze e gli obiettivi di ciascuna azienda.

Le sfide dei nostri clienti, il motore del nostro miglioramento.

Netx64.com

RSN studio nord



WWW.RSN.IT

Media Partner Ufficiale



Radio Studio Nord

si sente, si vede, si legge

