fvgtech.it

CULTURA DIGITALE

fvgtechmag

OPUSCOLO GRATUITO

PROGRAMMA E APPROFONDIMENTI DEI TEMI DEL DSF

DIGITAL **TRANSFORMATION**
FRA PROCESSI E STRATEGIE

SANITÀ DIGITALE: LA CENTRALITÀ DELL'UOMO TRA TECNOLOGIE PERVASIVE, CYBERSECURITY E NEW SPACE ECONOMY

CYBERSECURITY NELLE PMI: UN CAMBIAMENTO DI MENTALITÀ

Sicurezza e consapevolezza digitale: l'impatto del

DIGITAL SECURITY FESTIVAL

DALLA COPIA FORENSE ALLA "COPIA MEZZO", UN CAMBIO DI PARADIGMA

LA CULTURA DIGITALE: PILASTRO DIFENSIVO

DOVE VANNO I **SOCIAL**
E PERCHÈ FACEBOOK VINCE SEMPRE

Digital Security Festival

FvgTech

FvgTechMag opuscolo informativo e programma del Digital Security Festival 2023

FvgTechMag

www.fvgtech.it

FvgTech

per

Digital Security Festival

Caro lettore...

Benvenuto su questo freebook dedicato alla tecnologia, al digitale e all'information technology. **In questa edizione, il focus è sul Digital Security Festival.** Abbiamo ideato questo strumento alcuni 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 **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 ingranaggio 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 <<

FvgTechMag
Programma e informazioni temi DSF 2023

IDEA
da un'idea di Gabriele Gobbo
www.gabrielegobbo.it
e FvgTech programma TV
www.fvgtech.it
e MacPremium Digital Company
www.macpremium.it.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.

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 © 2023 MacPremium ove possibile

beanTech®
IT moves your business
METTITI
AL "SICURO"
CON I NOSTRI
SERVIZI GESTITI IT
WWW.BEANTECH.IT

Viviamo l'epoca della convergenza di vari elementi. Da un lato, le nuove tecnologie si evolvono ad un ritmo sempre più vertiginoso, quasi esponenziale, e il digitale ha permeato ogni aspetto delle nostre vite, complice anche lo sviluppo dei dispositivi mobili.

Dall'altro lato, le nuove generazioni sono immerse in questo processo; per loro, il digitale non è più un'innovazione, ma qualcosa che fa parte integrante delle loro vite, dato per scontato come l'aria che respiriamo. Di conseguenza, ogni aspetto della nostra società è stato trasformato: il modo in cui instauriamo relazioni sociali, come ci comunichiamo e, in generale, i nostri modelli di comportamento e abitudini. In questo contesto, la comunicazione attraverso l'email, l'instant messaging e le videochiamate è diventata lo standard, tanto che l'app del telefono è stata superata in utilizzo già da molti anni. Tuttavia, nel mondo digitalmente connesso di oggi, la sicurezza informatica non può essere affrontata solo attraverso la tecnologia. È diventato un tema che richiede una forte e consapevole componente umana, oggi più che mai. Questa è la visione del Digital Security Festival, un evento dedicato all'educazione e alla formazione sulla sicurezza digitale.

SICUREZZA E CONSAPEVOLEZZA DIGITALE: L'IMPATTO DEL DIGITAL SECURITY FESTIVAL

di Marco Cozzi, founder del Digital Security Festival

Il festival si propone di creare incontri formativi per educare le persone alla consapevolezza della sicurezza informatica. Ma perché la consapevolezza è così importante? Perché è il fulcro che ci permette di raggiungere il massimo livello di efficacia ed efficienza nella protezione dei dati, degli strumenti tecnologici, delle informazioni aziendali e, soprattutto, delle nostre identità digitali.

La consapevolezza in materia di sicurezza informatica è fondamentale per proteggere ciò che è più prezioso in un mondo sempre più digitalizzato. Non si tratta solo di proteggere i nostri dati o i nostri dispositivi, ma di proteggere le nostre identità digitali, diventate parte integrante della nostra vita quotidiana. Il Digital Security Festival pone particolare enfasi sulle categorie più vulnerabili, spesso le più esposte agli attacchi informatici. Educare queste categorie alla sicurezza digitale può contribuire a proteggere non solo i loro dati personali, ma anche la loro dignità e autonomia nel mondo digitale. Oggi vorrei condividere con voi una riflessione sull'importanza della conoscenza e dell'innovazione nel mondo della tecnologia. In un'epoca in cui le sfide globali si moltiplicano e il progresso tecnologico accelera, è fondamentale "illuminare la strada con la conoscenza" per garantire un futuro sostenibile e prospero. Vi invito quindi a condividere le vostre idee, progetti ed esperienze per contribuire all'illuminazione della strada con la conoscenza. Insieme possiamo costruire un futuro tecnologico più luminoso e sostenibile.

Grazie, quindi, di partecipare al Digital Security Festival!

LA SICUREZZA INFORMATICA COME PARTE INTEGRANTE DEL PROCESSO DI GESTIONE DEL RISCHIO

di Angelo Fragnito

Se è ormai opinione comune che non si tratta di SE ma di QUANDO si paleserà un attacco informatico, forse è arrivato il momento di evolvere il paradigma in QUANTO sarà ampia la sua ricorrenza, tenendo presente la molteplicità e l'eterogeneità delle minacce cyber a cui quotidianamente sono sottoposte le aziende.

È per questo motivo che si rende necessario, per ogni organizzazione, considerare la sicurezza informatica come parte integrante del processo di gestione del rischio che integri una valutazione delle diverse tipologie di rischio informatico, un efficace sistema di protezione attiva e passiva e un adeguato piano di resilienza atto a proteggere l'attività di business aziendale da tutti i tipi di attacco, interruzione o disastro.

La valutazione del rischio informatico è un'analisi indispensabile per poter determinare il livello di maturità della sicurezza dei sistemi informativi; troppo spesso però si tende a considerare il rischio informatico come un pericolo specificatamente attinente al solo ambito tecnologico, tralasciando invece gli aspetti del comportamento umano che, anche inconsapevolmente, sono la causa prima, nonché il vettore principale, degli attacchi informatici. Allo stesso modo diventa di vitale importanza garantire un'adeguata protezione di fronte alla crescente dimensione e complessità degli attacchi informatici.

In ultimo, è mandatorio predisporre un piano di resilienza che permetta all'organizzazione di far fronte agli incidenti informatici, proteggendo le applicazioni e i dati critici e consentendo il ripristino della funzionalità successivamente a una violazione o un malfunzionamento. Axians Italia, grazie ad un team altamente specializzato, è costantemente impegnata a supportare aziende e organizzazioni nell'affrontare le crescenti minacce della sicurezza informatica.

PURPLE TEAM E CULTURA DELLA SICUREZZA

di Alice Mini e Eleonora Ghiani

La cybersecurity è un processo continuo e strutturato con cui vengono controllate e migliorate tecnologie, strumenti informatici, e la gestione vera e propria delle informazioni.
La maggior parte delle aziende, mirando alla compliance, svolge annualmente un'attività di Vulnerability Scan, erroneamente chiamato Assessment. Un approccio più completo, parte del processo di Vulnerability Management (VM), prevederebbe:

1. Asset Management;
2. Risk Assessment;
3. Vulnerability Assessment;
4. Patching.

Queste attività sono svolte da un gruppo di professionisti specializzati nell'implementazione e nel mantenimento della sicurezza interna verso potenziali attacchi e minacce (Blue Team), e dalla sua controparte offensiva (Red Team), esperta nell'attacco simulato che individua i punti deboli nelle difese.
Per elevare il valore del VM, il Red Team testa le vulnerabilità o svolge un'attività di simulazione di attacco per capire quali sono i modi in cui i cybercriminali agirebbero.
Questa attività, se svolta con il Blue Team, migliora la capacità di detection e porta a implementare difese ad hoc. La sinergia tra i due team forma il Purple Team.

Inoltre, bisogna implementare e testare procedure e linee guida, conosciute da tutti gli interessati e seguite correttamente. Questo fa parte della Cultura della Sicurezza, comprensiva non solo della formazione base sull'Awareness (molto spesso sterile), ma tesa alla creazione di un ambiente che permetta di colmare il gap knowledge-intention-behavior.
avorare sulla cultura di sicurezza in azienda porta benefici di diversa natura dal punto di vista economico, comportamentale e di riduzione degli effort e del rischio.

DI GABRIELE GOBBO

MA FACEBOOK È MORTO O NO?

>> Può il social della più potente organizzazione digital mondiale arrivare al capolinea?

Ogni giorno sembra emergere una nuova dichiarazione che proclama la "morte" di Facebook, sostenendo che è obsoleto, che è abbandonato, o che è semplicemente inutile. In parallelo, quotidianamente, assistiamo a proclamazioni di individui che annunciano l'intenzione di lasciare il celebre social in blu alla ricerca di alternative. Ma queste affermazioni sono realmente fondate? Decisamente no!

Non è così poiché, al momento, che ci aggradi o meno, Facebook persiste come la piattaforma social con il maggior numero di utenti attivi, nonché con la più vasta gamma di contenuti consultabili. È, altresì, il social che consente più interazioni e offre maggiori opportunità di diffusione dei nostri post. Ciò nonostante, la piattaforma presenta i suoi difetti e problemi, tra cui un algoritmo capriccioso e la costante impressione di essere un luogo di litigi, nei quali, spesso, siamo noi stessi protagonisti. Facebook rimane un elemento imprescindibile all'interno di qualsiasi strategia di marketing e comunicazione, sia che si tratti di un'azienda, di un creatore di contenuti o di un utente senza scopi precisi. Al giorno d'oggi, è la piattaforma più completa in termini di tipologie di media che è possibile pubblicare, permettendoci di caricare video, reel, stories, gif animate, link, immagini e testo, senza tralasciare tag, hashtag, dirette, luoghi e altre funzioni.

Si estende anche a gruppi, pagine aziendali, profili privati, pubblicità con un solo click, reazioni, traduzioni e sottotitoli automatici, eventi, e molto altro. In pratica, Facebook supporta una varietà di funzioni con pochi click. Un altro aspetto cruciale è la possibilità di condividere contenuti di altri utenti, che a loro volta possono condividere i nostri. Su Facebook sono inoltre presenti contenuti di Instagram, principalmente i reel.

È vero, altri social vantano alcune di queste caratteristiche, ma nessuno possiede un insieme così completo, rendendo le altre piattaforme limitate in alcune funzionalità. Per tali ragioni, chiunque si affacci per la prima volta al mondo dei social media dovrebbe iniziare da Facebook, per godere di un ambiente senza limiti, ricco di informazioni, immagini e suoni. Coloro che cercano un canale crossmediale ad ampio spettro dovrebbero ugualmente concentrarsi sul social in blu, che offre innumerevoli possibilità e tipologie di post ad una platea quasi globale.

È essenziale ricordare che, pur dando grande importanza a Facebook, non si dovrebbe limitare l'uso dei social a questa piattaforma.

È FONDAMENTALE TENERLO IN CONSIDERAZIONE, ANCHE SE MARK ZUCKERBERG NON AVRÀ INTENZIONE DI LASCIARSI SUPERARE FACILMENTE DALLA CONCORRENZA.

ECCO COSA SIGNIFICA DIGITAL TRANSFORMATION

di Andrea Virgilio

Il percorso della Digital Transformation mira a creare soluzioni innovative per assistere persone e organizzazioni nella realizzazione coerente della propria missione. La Digital Transformation non riguarda solo l'adozione di nuove tecnologie ma è una vera e propria strategia che ridefinisce modelli di lavoro, business, comunicazione e abbraccia i paradigmi digitali, compresi l'uso dei dati, nuovi ricavi e valori. Questo processo richiede un'ottimizzazione continua e presenta vari livelli di complessità.

È fondamentale distinguere tra la digitalizzazione dei processi e l'adozione di una vera strategia di Digital Transformation, il che può essere complesso per alcune organizzazioni. L'educazione continua è essenziale offrendo scenari, implicazioni e opportunità. Occorre accelerare la comprensione dei nuovi paradigmi digitali tramite formazione, coaching e design thinking. La soluzione? Un approccio olistico che consenta agli di esplorare scenari di trasformazione e interagire con ecosistemi online. Gli esperti sono essenziali, dai tradizionali agli specialisti, in nuove tecnologie (Digital Scientist) e ai professionisti dei processi core.

Ed è proprio questo quello che cerchiamo di tenere a mente in ogni progetto che curiamo in modo da prendere per mano chi cerca una soluzione digitale adeguata e competitiva.

TECH FEED

Italiamac.it a 130.000

Il social network dedicato agli utenti Mac e Apple raggiunge e supera i 120.000 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.

IOT: QUALI SCENARI DI RISCHIO?

di Anna Vaccarelli

Il termine 'Internet delle cose" (Internet of Things - IoT) ha cominciato a diffondersi negli ambienti tecnici e di ricerca verso la metà degli anni 2000.

Oggi gli oggetti connessi e attivi in Italia sono 110 milioni, poco più di 1,8 per abitante. Nel 2021 in Italia è cresciuto anche il mercato dell'IoT, che vale circa 7,5 miliardi di euro, di cui circa 3 miliardi di euro (pari al 40% del totale) relativi ai soli servizi, con un +25% rispetto al 2020 (dati dell'Osservatorio Internet of Things del Politecnico di Milano, Aprile 2022).

Il PNRR prevede complessivamente 29,78 miliardi di euro dedicati direttamente o indirettamente al settore dell'Internet of Things: possiamo immaginare, quindi, un ulteriore sviluppo nella diffusione di questa tecnologia.

I campi di applicazione sono numerosissimi e molti di essi già oggi sono una realtà: Wereable, Smart agricolture, Smart car, Smart city, Smart mobility, Smart home e Smart building, Smart metering, tutto il settore di Industria 4.0, Smart health. Questa tecnologia è spesso un "facilitatore" anche nella nostra vita quotidiana, ma qual è il risvolto della medaglia? La sicurezza.

In generale, i danni connessi ai rischi cyber dell'IoT possono derivare da una loro sottovalutazione, perché spesso li consideriamo come oggetti di uso comune: chi si preoccupa della sicurezza della lavatrice? Eppure, è connessa in rete al pari di smarphone e PC e, come questi, dovrebbe essere protetta: come vengono controllati gli accessi? Come è garantita l'autenticazione? Posso configurare la lavatrice in modo che sia

su una rete diversa da quella con al quale lavoro? Come posso aggiornare il software che la fa funzionare?

Anche in questo campo, quindi la consapevolezza dei rischi e delle minacce che gli IoT comportano è alla base di qualunque soluzione e contromisura efficace.

infostar
TECNOLOGIE DIGITALI

DSF Telegram

Il canale Telegram del Digital Security Festival è il luogo dove potete trovare tutte le novità, gli aggiornamenti e le informazioni più rilevanti sull'evento e sulla sicurezza digitale e durante tutto l'anno notifiche su fatti e notizie di rilievo. Iscrivetevi per rimanere sempre informati!

https://t.me/digitalsecfest

L'unione fa AXERA

Quattro percorsi che si incontrano in un'**unica grande realtà**: questo è ciò che ci permette di fare la differenza.

AXERA

interplanet

SET ICT Business Solutions

Telemar

ipcompany Connecting Business

720km	250	95	6	200	25M
di rete in fibra ottica	ripetitori wireless	data center progettati	sedi	dipendenti	di fatturato

Axera S.p.A. - Telecomunicazioni e Soluzioni ICT

www.axera.it

is copy

Il tuo digital partner

Servizi informatici completi e funzionali per ogni tipo di attività ed organizzazione

is copy

SOLUZIONI PER LA STAMPA

is cloud

RETI E SICUREZZA INFORMATICA

is service

ASSISTENZA TECNICA E INFORMATICA

is visual

SISTEMI MULTIMEDIALI E VISUAL COMMUNCATION

is office

CANCELLERIA E ARTICOLI PER L'UFFICIO

is dev

SVILUPPO DI SOLUZIONI SOFTWARE AD HOC

IS Copy Srl Società Benefit

TRIESTE
VIA FLAVIA 23

UDINE
VIA IPPLIS 52

WWW.ISCOPY.IT

040 577626
0432 1698238

ISCOPY@ISCOPY.IT

Connettività e sicurezza: tra evoluzione e privacy

di Alessandro Curioni

È un dato di fatto che tecnologie dell'informazione stanno rendendo il nostro pianeta sempre più piccolo connettendo oggetti e persone che diventano visibili e raggiungibili in tempo reale ovunque si trovino. Uno degli effetti collaterali di questa evoluzione è un apparente incremento della sicurezza. Sistemi di videosorveglianza sempre più diffusi e collegati potrebbero rendere un'impresa sovrumana farla franca dopo un omicidio o un banale scippo. La possibilità di integrare grandi basi dati e di analizzarle attraverso strumenti automatizzati porterà i governi a una capacità predittiva senza precedenti, tanto da fare ritenere che in un prossimo futuro un altro 11 settembre sarà impossibile o quasi.

L'avvento dei wearable medical device potrebbe salvare milioni di vite consentendo ai medici di intervenire sul paziente da remoto e in tempo reale. Tanta pervasività tecnologica ha sollevato il problema del prezzo che l'individuo dovrà pagare in termini di perdita di privacy. Sistemi di sorveglianza massiva, dispositivi che invadono la sfera biologica e strumenti che correlano tra loro anche le più insignificanti azioni di ogni individuo potrebbero diventare i mezzi per l'esercizio di un potere incondizionato e incondizionabile. Sul tema sono già stati riversati fiumi di parole e viene dibattuto continuamente, ma ci sarebbe un'altra questione, molto meno discussa, anzi pressoché ignorata, che si potrebbe riassumere in una domanda: il progredire delle nuove tecnologie ha veramente reso il mondo un posto più sicuro?

Esserci al Digital Security Festival significa cercare delle risposte e nello specifico 'cercare" è più importante del 'trovare", ma di certo meno dello 'sperare".

CONOSCI L'IT CLUB FVG?

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**

di Piero Giacomelli

INTELLIGENZA COLLETTIVA: RIVOLUZIONE SWARM E LLM NEI SISTEMI COMPLESSI COORDINATI

Alla fine degli anni '90 nel mondo della ricerca dell'intelligenza artificiale stava prendendo piede un nuovo settore di studio che considerava la possibilità di usare singoli agenti capaci di operazioni molto elementari che lavorando in maniera coordinata potessero eseguire compiti piuttosto complicati.

La ricerca al tempo era nota come Swarm Intelligence, perché simulava il comportamento biologico degli sciami di api o delle legioni di termiti. Presa singolarmente una formica o una termite è capace di azioni molto elementari, ma, soprattutto la termite africana, è in grado di costruire strutture gigantesche. Se noi esseri umani dovessimo costruire qualcosa di simile dovremmo essere in grado di costruire con sabbia e terra dei grattaceli alti 6 KM. La ricerca aveva poi subito una fase di arresto dovuta al fatto che era molto difficile fornire ad un agente semplice un qualche comportamento decisionale intelligente e soprattutto che poi lavorassero tutti di concerto.

Con l'esplosione del Large Linguistic Models (LLM) che hanno trovato la loro killer application per il grande pubblico in ChatGPT e Bard, si sta cominciando a delineare la possibilità di riprendere la Swarm Intellingence, dotandola di capacità decisionali e memorie basate su LLM. Ricerche molto promettenti stanno esplorando la possibilità di dotare gli agenti swarm di una intelligenza condivisa in modo da eseguire tasks complessi e lavori di concerto molto più complicati. In un promettente lavoro svolto presso la Stanford University un gruppo di ricercatori sono riusciti a dotare degli agenti di una intelligenza base presa da un modello linguistico e di dotarli di ragionamento semplice e memoria che va ad incrementare la base del modello linguistico, per testare il loro sistema hanno usato il noto gioco 'The Sims" dove un gruppo di 25 agenti intelligenti sono stati fatti interagire fra di loro per arrivare ad uno scopo comune. Ad esempio, è stato dato ad un singolo agente il compito di organizzare organizzare una festa di San Valentino, gli agenti hanno creato gli inviti alla festa nei due giorni successivi, fatto nuove conoscenze, e si sono organizzati per uscire insieme per la festa e per presentarsi insieme al momento giusto. Sembra quindi non lontana la possibilità di usare questi agenti generativi come se fossero un intero team formato da umani ognuno specializzato in un compito specifico al fine di raggiungere un obiettivo comune.

"SI STA COMINCIANDO A DELINEARE LA POSSIBILITÀ DI RIPRENDERE LA SWARM INTELLINGENCE"

Cyber Security & Infinityhub

di Massimiliano Braghin

Infinityhub S.p.a. Benefit è la prima Energy Social Company italiana che realizza progetti di riqualificazione energetica con un modello unico, scalabile e innovativo. Il nostro payoff PERSONE ENERGIE FUTURO, che è diventato anche una pubblicazione edita dall'Università Ca' Foscari di Venezia, descrive perfettamente gli elementi determinanti della nostra impresa. Al centro ci sono le Persone, c'è il desiderio di sostenibilità che è capacità di Futuro per tutte e per tutti. E come possiamo pensare al futuro senza cultura, Energia vitale per qualsiasi tipo d'impresa? L'identificativo 'social" ben spiega che la nostra attività tra ingegneria e finanza, economia e sociologia, genera alleanze e connessioni distribuite tra i vari stakeholder nella società anche attraverso i social network. Il nostro lavoro, poi, è reso possibile dall'utilizzo di strumenti fintech che hanno bisogno di un alto livello di guardia rispetto la cyber security.

Partecipare al Digital Security Festival – come sponsor - è un'azione coerente con il nostro modello di business che ha come basi strutturali la cultura, la formazione continua e l'educazione cyber, per un utilizzo consapevole degli strumenti digitali che ci permettono di realizzare tanta parte delle nostre opere e, soprattutto, di comunicare velocemente senza limiti di spazio e di tempo.

PARTECIPARE AL DIGITAL SECURITY FESTIVAL È UN'AZIONE COERENTE CON IL NOSTRO MODELLO DI BUSINESS

Massimiliano Braghin, presidente e fondatore di Infinityhub sottolinea: 'Siamo felici di sostenere questa iniziativa e auguriamo a chi ha desiderato e si prodiga per questo sogno di portare lontano nel tempo e nello spazio questo progetto che realizza la vera condivisione – divisione con – di saperi che aiutano la società a crescere ed evolvere. La tecnologia ha trasformato le nostre vite, ma rimane uno strumento. Tocca a noi farne buon uso. La scienza ci ricorda che il valore delle scoperte scientifiche non sarebbe tale, se non venisse condiviso. Lo stesso vale per l'evoluzione digitale, è determinante educare in famiglia, al lavoro, nel mondo della scuola e nella società tutta per un buon uso delle tecnologie digitali".

Infinityhub nasce nel 2016 da venti azionisti fondatori, oggi conta 2250 socie e investitori.

Utilizza un modello di business innovativo, costituendo insieme all'energivoro una società partecipata per lo sviluppo ad hoc di interventi di riqualificazione edile 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.

Ad oggi, sono quindici i progetti finanziati e monitorati all'interno di settori dalla sanità alla vendita al dettaglio, dal turismo allo sport, distribuiti in tutta Italia. Il modello di business di Infinityhub ha permesso la realizzazione di 18 campagne di equity e lending crowdfunding, concluse con successo, con una raccolta complessiva di 6,1 milioni di euro. I progetti realizzati e in pipeline superano i 20 milioni di euro.

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**.

2815 BATTUTE PER PARLARE DI COSA?

di Max Guadagnoli - Humane Technologist

Del concetto Social di *Moderazione* o della grossa truffa della Consistency che tiene inchiodata la gente alla macchina Social, senza tregua? Del Social Zombing? Delle Echo Chamber? Dei bias cognitivi? Del Sistema Estrattivo e Dopaminergico? Dei comitati etici e degli attivisti per i diritti digitali che non possono parlare? Oppure delle fake-policy asfissianti di FaKEbuk che comunque fa sempre come gli pare, basta copiare e pagare?

Raccontiamo di TikTok (cinese) che ha in pancia un bel tracker che manda dati aggregati a VKontakte (russo) e tutto sotto la coperta calda di una bella sede legale negli Stati Uniti oppure della rapidità di aggregazione di contenuti altamente fuorvianti da parte degli algoritmi? Vogliamo parlare di algoritmocrazia? Di che vogliamo parlare?

Delle piattaforme di web advertising che falsano i numeri, certificati dal Niente & Dintorni e che mettono gli advertiser nella posizione di non poter aggiustare le proprie inserzioni nella modalità più conveniente per loro? O di Google? Di nuovo querelato per posizione predominante e di monopolio sul mercato con la gestione del 90% delle ricerche online, l'88% delle pubblicità testuali e il 74% di quelle generiche e che paga miliardi l'anno per garantirsi di essere sempre il browser di default su qualsiasi device e piattaforma che si piegano a colpi di milioni?

Magari può essere interessante sapere che tutte le app degli smartphone includono tracker di terze parti a cui concedono i nostri dati aggregati e che si ciucciano fino a 35-37 parametri del *nostro* - si fa per dire - smartphone, perfettamente agevolate dal sistema operativo Android? Però potremmo trattare la correlazione tra dismorfismo e alcuni Social Media oppure... tentare di confutare le dichiarazione di chi ci lavorava dentro dove si ammette di aver creato un sistema fisio-psico-economico-induttivo-estrattivo che più disfunzionale non si può e che produce miliardi.

Parliamo della fulgida e splendente capacità deresponsabilizzante delle AI? Siamo tutti figli degli Hype Masters of the Universe? Digitalmente: Sì. Esiste un mondo digitale onesto? Sì ma solo se si elimina la coincidenza di estrema concentrazione di tecnologia e capitale. Avverrà? No, perché è un ossimoro. Semplicemente non è la grande rivoluzione culturale e strutturale del secolo che pensavamo ma una distorsione dei due concetti precedenti e di cui niente è realmente nostro neanche lo smartphone che ripalleggiamo tra le mani tutto il giorno. Lo smartphone, IL FACILITATORE, il tassello mancante che ha convalidato e fatto funzionare questo loophole continuo e infinito.

In conclusione chiedo: Perché Jaron Lanier, padre della realtà virtuale, nel 2018 scriveva il libro: "Ten Arguments for Deleting Your Social Media Accounts Right Now"? Rispondete Voi, Io esco di fuori a fumare.

CYBERSECURITY NELLE PMI: UN CAMBIAMENTO DI MENTALITÀ

di Cristian Feregotto

Negli ultimi anni, la cybersecurity è diventata una priorità non solo per le grandi aziende ma anche per le piccole e medie imprese (PMI). A differenza del passato, quando la sicurezza informatica era spesso considerata un lusso o un'opzione secondaria, oggi le PMI sono sempre più consapevoli dei rischi associati a violazioni e attacchi informatici.

Perché le PMI sono un Target?0 Le PMI sono diventate un target appetibile per i cybercriminali perché rappresentano un "punto debole" nel panorama della sicurezza informatica. Spesso, queste imprese non hanno le risorse per investire in soluzioni di sicurezza avanzate, rendendole vulnerabili. Tuttavia, una violazione può avere conseguenze devastanti, non solo in termini di perdita di dati ma anche di reputazione e fiducia del cliente.

Un Cambiamento Necessario. Fortunatamente, c'è stato un cambiamento di mentalità. Le PMI stanno iniziando a comprendere che la sicurezza non è un costo, ma un investimento. Strumenti come firewall, antivirus e servizi di monitoraggio sono diventati standard, e c'è una crescente attenzione verso la formazione del personale per riconoscere potenziali minacce come phishing o ransomware.

Soluzioni Accessibili. Le soluzioni di sicurezza sono diventate più accessibili, grazie all'avvento del cloud e ai servizi in abbonamento. Questo permette alle PMI di accedere a tecnologie avanzate senza dover sostenere costi proibitivi.

Conclusione. La crescente consapevolezza delle PMI riguardo alla cybersecurity è un segno positivo. Non è più un argomento relegato alle sale riunioni delle grandi corporazioni. Investire in sicurezza è diventato una necessità per tutte le imprese, indipendentemente dalle dimensioni. In un mondo sempre più connesso, la sicurezza informatica non è più un optional, ma un imperativo.

NAVIGANDO LE ACQUE DELL'ECCELLENZA: IL CONTRIBUTO DEL CHAPTER VENICE DI ISACA

di Board ISACA Venice Chapter

La gestione dell'Information Security e della Privacy, l'IT Governance, l'Audit e il Risk Management, insieme alla Cybersecurity, sono temi di crescente rilevanza nell'attuale epoca in cui le aziende dipendono sempre di più dalla tecnologia. L'interesse per tali argomenti è in costante crescita, poiché imprese e individui cercano di navigare in acque sempre più complesse.

La consapevolezza e la competenza nell'utilizzo delle nuove tecnologie e delle tendenze IT che influenzeranno i professionisti italiani in futuro non sono più sufficienti per garantire una carriera in continua crescita. In questo contesto, le certificazioni promosse da ISACA, come CISA, CISM, CRISC, CGEIT, CSX, Cobit, e altre (informazioni disponibili su www.isacavenice.org), sono oggetto di grande interesse da parte di imprese e organizzazioni, sia private che pubbliche.

Il Chapter di ISACA a Venezia svolge un ruolo cruciale nell'accompagnare i professionisti del futuro, preparandoli ad affrontare le sfide poste dalla tecnologia in continua evoluzione e dalle discipline correlate per migliorare le proprie competenze, impegnandosi a mettere a disposizione risorse, formazione e opportunità di networking per coloro che desiderano eccellere.

Organizziamo eventi educativi, workshop e conferenze di alto livello, fornendo conoscenze e competenze di prim'ordine. Inoltre, offriamo opportunità di networking per aiutare i professionisti a svilupparsi e progredire nella loro carriera.

Ogni attività è concepita per promuovere l'eccellenza e l'etica nei settori sopra menzionati, guidata da professionisti con anni di esperienza nel campo. In conclusione, il Chapter ha l'obiettivo di offrire valore ai nostri membri e alla comunità nel suo complesso.

Unisciti a noi in questa straordinaria avventura mentre continuiamo a esplorare le profondità dell'eccellenza in questa era tecnologica.

ISACA Venice Chapter

Infinityhub

PERSONE | ENERGIE | FUTURO

La nuova *dimensione* dell'energia

Realizziamo progetti di riqualificazione energetica, aprendo la partecipazione al capitale sociale a persone e imprese.
Siamo il primo hub di progetti condivisi per una sostenibilità ambientale, economica e sociale.
Utilizziamo strumenti fintech e di finanza etica. Attraverso i social educhiamo alla sostenibilità.
Il nostro è ...

Un nuovo modo di fare impresa
Sostenibile, accessibile, condiviso

con Relazioni di Valore
che accelerano l'Energia

Galassia Infinity*hub*

INVESTITORI PRIVATI

CONSUMATORI DI ENERGIA

PROFESSIONISTI E IMPRESE

BANCHE E FONDI

Infinityhub S.p.A. Benefit - Palazzo Giustinian Lolin, Canal Grande
Sestiere San Marco 2893, 30124 Venezia (VE)
www.infinityhub.it

La componente **umana** nella sicurezza

di Stefano Gabaglio

Uffici IS Copy, il telefono suona all'impazzata, dall'altra parte una voce che non conosco: 'computer fuori uso, rete paralizzata, attività bloccata, ditta sotto attacco hacker". Faccio così conoscenza con un nuovo cliente.

Seguono giorni di lavoro febbrile per rimettere in piedi l'infrastruttura digitale che regge l'attività, puntando a salvare il salvabile, grazie a repository mantenute off-site. Nel frattempo, in attesa che i tecnici risolvano la situazione, produzione ferma e dipendenti a casa in ferie forzate. Dalla direzione fanno poi confidenzialmente sapere di aver ricevuto una richiesta di denaro da parte degli hacker. Un autentico riscatto, ransom in inglese e ransomware sono questi malware capaci di criptare e bloccare i dati aziendali.

Con i livelli di digitalizzazione attuali, è facile capire come una circostanza del genere sia in grado di paralizzare tutto: amministrazione, logistica, magazzino, rete vendite. Come può succedere? La causa è sempre la stessa: Mancanza di percezione del rischio. La componente umana qui gioca un ruolo cruciale, gli attacchi hanno successo quando manca la consapevolezza delle connessioni tra processi aziendali e ambiente esterno, portando a sottovalutare strategie e ruoli, rendendo ognuno meno responsabile delle proprie azioni.

Soluzioni? Zero trust, non fidarsi e poi tecnologia e formazione del personale. Sviluppando un approccio sistematico, anche grazie a specialisti certificati ISO 27001. La norma sui sistemi di gestione della sicurezza delle informazioni svolge un ruolo cruciale, fornendo un metodo strutturato e promuovendo la mentalità corretta, aiutando a comprendere il contesto interno ed esterno all'azienda, rivelando aspetti spesso trascurati.

Ulisse e le sirene del digitale: le nuove sfide della Cyber Security

di Francesco Marchesani

Nell'Odissea di Omero, celebre è la scena descritta nel Canto XII, quando Ulisse si ritrova a fronteggiare la voce ammaliante delle sirene. In quel frangente, il re di Itaca riesce a superare indenne la prova, facendo leva sulla propria arguzia e scongiurando una fine ignobile per sé e per il proprio equipaggio. Nell'epoca attuale, ci troviamo in un mondo digitale che ha le sue proprie 'sirene", minacce cibernetiche che richiedono un ingegno considerevole per evitarle. La sicurezza informatica moderna è una sfida fondamentale del nostro tempo, una battaglia costante per proteggere i nostri dati e la nostra privacy in un oceano di pericoli digitali, amplificata dall'avvento delle tecnologie emergenti.

Le sirene dell'era digitale, che si celano spesso nell'oscurità dei server e dei codici informatici, sono pronte a moltiplicarsi sempre più anche per quello che riguarda le nuove tecnologie: dall'intelligenza artificiale alla blockchain, passando per i servizi cloud e il metaverso. La collaborazione tra organizzazioni, governi e individui è fondamentale per affrontare queste minacce emergenti. Lo stesso Ulisse coinvolgeva pienamente i suoi compagni nei propri piani, che si trattasse di fuggire dalla grotta di Polifemo o di fronteggiare la furia distruttrice di Scilla e Cariddi. La resilienza rimane un valore essenziale: dobbiamo essere pronti a fronteggiare gli inevitabili tentativi di attacco, rafforzando le nostre difese e imparando dalle esperienze passate.

Ulisse, vero e proprio hacker ante litteram, dimostra numerose volte la sua astuzia e determinazione nel suo viaggio; a noi tocca fare lo stesso nell'era moderna, scandita dal ritmo dei bit e dell'incessante progresso tecnologico.

DI VALERIA LAZZAROLI

Sanità digitale: la centralità dell'uomo tra tecnologie pervasive, cybersecurity e new space economy

'Accadde in un teatro che le quinte presero fuoco. Il clown uscì per avvisare il pubblico. Credettero che fosse uno scherzo e applaudirono; egli ripeté l'avviso; la gente esultò ancora di più. Così mi figuro che il mondo perirà fra l'esultanza generale degli spiritosi, che crederanno si tratti di uno scherzo" (Kierkegaard e Fabro, 2013, p.129). È il 1843 quando Kierkegaard scrive queste parole che risultano efficacissime per descrivere uno scenario che impone il consesso di sociologi, tecnocrati e scienziati per produrre quanto più possibile ipotesi di contesto sulle quali canalizzare politiche attive per il futuro dell'essere umano.

La centralità di quest'ultimo sarà, infatti, il leitmotiv dei prossimi decenni. Capacità di adattamento ai cambiamenti climatici, tecnologie pervasive, nuove economie. Un vissuto analogico traghettato su dispositivi digitali che daranno nuovi connotati al vivere di tutti i giorni. Per intuirne la vastità e la trasversalità della portata e dell'impatto del fenomeno nel nostro Paese, sarà utile ipotizzarlo come l'attività di un aereo: se il decollo di ogni evoluzione fosse stato veloce, difficilmente due o più progetti indipendenti sarebbero decollati nello stesso momento: quasi certamente il primo progetto avrebbe completato il proprio decollo prima dell'inizio di qualsiasi altro, consentendo la metabolizzazione e l'adattamento della capacità amministrativa di uno Stato. Ma nella fattispecie il decollo, specie in Paesi come l'Italia, è stato ed è lento ed è quindi plausibile che molti progetti siano e saranno in decollo contemporaneamente. Questo ritardo, in ogni caso, potrebbe portare vantaggi se esprimessimo indipendenza industriale dal resto del mondo, perché, alla fine della transizione, i progetti avrebbero capacità enormemente maggiori e nessuno di essi si troverebbe in posizione di dominio rispetto ad altri. Ma le interconnessioni geopolitiche, economiche e industriali del nostro Paese, lo legano a doppio filo ai progetti di intelligenza digitale di BigTech e grandi Potenze come la Cina e gli USA che si trovano in posizione estremamente avanzata nella competizione mondiale, ottenendo un vantaggio strategico decisivo sia a livello tecnologico che di altri settori, sufficiente per raggiungere il completo dominio del mondo. E quindi non è difficile vedere già nei nostri giorni, progetti (un esempio su tutti, Starlink di Elon Musk) ottenere un vantaggio strategico decisivo, usato per neutralizzare possibili concorrenti e dare forma a singleton laddove a livello globale vi è il rischio di un'unica entità che prende le decisioni e quindi le sorti di intere nuove economie.

La grande novità con cui dovremo condividere, è dunque, la nascita di una superintelligenza per la quale ogni Stato cercherà di nazionalizzare qualunque progetto nell'ambito del proprio territorio che giudica importante per l'evoluzione tecnologica al fine di aumentare la propria capacità economica, amministrativa ed energetica. Solo negli ultimi mesi le autorità nazionali o internazionali si sono accorti dell'imminenza del fenomeno ma in ogni caso, quando tra gli scienziati più autorevoli si diffondesse la convinzione di un avvio, qualunque progetto che iniziasse a mostrare un progresso sufficiente, potrebbe essere rapidamente nazionalizzato, regolamentato o dichiarato illegale.

Fatto questo doveroso preambolo, cruciale sarà il progetto di transizione della sanità da analogica a digitale. Un processo legato a doppio filo con la sostenibilità ambientale, energetica e di sicurezza nazionale delle grandi infrastrutture critiche e quindi del rischio cyber. L' intelligenza artificiale potrebbe assegnare una probabilità notevole all' ipotesi di vivere in una simulazione. Già oggi molto intelligenze artificiali risiedono in mondi simulati; i miglioramenti delle tecniche di programmazione e l'aumento della potenza di calcolo consentiranno di realizzare mondi virtuali più ricchi e complessi che troveranno nella sanità digitale, l'habitat ottimale. Dunque, una Digital Healthcare

che, matura, creerà contesti virtuali plurimi, ottimizzando la medesima simulazione molte volte e con piccole variazioni. Pur rendendoci conto di quanto sia difficile immaginare cosi tanta evoluzione, quest'ultima è scritta nella tecnologia già presente sul mercato che, comunque, dovrà scontrarsi con la forte connotazione etica del mondo occidentale di cui, per fortuna, siamo parte e che vorrebbe l'esercizio costante di forze centripete per mantenere l'uomo al centro. Ma come saggiamente riportato da Massimo Chiriatti nel suo libro 'Incoscienza artificiale", difficile che questo possa avvenire, 'per tre motivi: il primo è che non sempre ne abbiamo le abilità; il secondo è che introduciamo tempi di latenza troppo alti; il terzo riguarda i costi del nostro intervento. Ogni intervento dell'essere umano nelle operazioni porterebbe a un drastico rialzo del costo marginale, che nell'economia digitale è prossimo allo zero: pertanto il modello di business salterebbe." Non sarà difficile, dunque, assistere ad una comunicazione che, nell'interesse del market System e dei Governi, convincerà l'utente ad abbassare le difese verso la nuova tecnologia a fronte di una maggiore efficienza in termine di tempistica, qualità delle diagnosi ed una relazione medico-paziente a più livelli ma meno problematica di quella in essere con la medicina di prossimità. A tal fine, un utile strumento per misurare il polso della transizione digitale della sanità, è il Future Health Index, l'indagine più estesa a livello globale che analizza le priorità e le prospettive dei leader della sanità dei professionisti più giovani. Giunto alla sua ottava edizione, si basa su ricerche proprietarie condotte in 14 paesi.

Quest'anno (2023), lo studio ha esplorato i nuovi modelli di erogazione dell 'assistenza, con integrazione di quella fisica e virtuale, all'interno e all'esterno delle strutture sanitarie: emerge una chiara necessità a mantenere alta la qualità dell'assistenza, nonostante la carenza di personale e le continue pressioni finanziarie. Nel frattempo, anche le esigenze dei pazienti sono cambiate: la trasformazione digitale, diventata sempre più pervasiva in ogni aspetto della nostra vita, ha infatti innalzato le loro aspettative, sempre più orientate a un'esperienza di cura più integrata ed efficiente. Il Report ha fornito indicazioni interessanti su come sarà il nuovo paradigma dell'assistenza, che racconta di un futuro in cui i pazienti beneficeranno di una gamma sempre più ampia di punti di accesso alla cura, virtuali e fisici, tra cui poter scegliere e a costi inferiori. In linea con il disegno del PNRR di potenziare l'assistenza a livello territoriale, i leader della sanità in Italia stanno già lavorando per costruire un sistema sanitario connesso e integrato che fornisca assistenza sia all'interno che all'esterno delle mura ospedaliere. Parallelamente, gli investimenti in intelligenza artificiale continuano ad aumentare, con l'Italia, sorprendentemente, al di sopra della media globale: tre leader su quattro (74%) stanno attualmente investendo in IA, contro il 59% a livello globale. Gli intervistati italiani ne riconoscono infatti il potenziale e sono impegnati a sfruttarlo nel loro lavoro quotidiano, per automatizzare i processi, migliorare l'efficienza, l'esperienza di staff e pazienti, oltre che i risultati clinici. É chiaro che per vincere la sfida della medicina territoriale abilitata dalle tecnologie digitali, sia necessaria una collaborazione sempre più stretta con i player del settore dell'health technology. Ed in tal senso, le partnership saranno un punto chiave: le aziende IT, i system integrator e le aziende che forniscono tecnologie sanitarie avranno un ruolo sempre più strategico nell'aiutare le strutture sanitarie a liberare i dati, a renderli interoperabili e a trasformarli in informazioni quando e dove servono. Infine, i partner saranno centrali per contribuire a migliorare la sostenibilità, area in cui l'assistenza sanitaria avrà ampi spazi di crescita.

È importante aggiungere che il trend demografico conferma l'Italia tra i paesi più longevi dell'Unione Europea, con un'aspettativa di vita (prima della pandemia) pari a 81,2 anni per gli uomini e 85,6 per le donne e la percentuale di over 65enni pari al 21,1 e come già detto, la qualità delle prestazioni sanitarie percepita bassa e in declino, soprattutto per quanto riguarda l'assistenza territoriale, la cura delle cronicità, la prevenzione e l'assistenza farmaceutica territoriale. Su scala europea e nazionale siamo quindi a un crocevia che richiede capacità di innovare radicalmente i servizi di cura e assistenza, oltre che una maggior efficacia ed efficienza nell'utilizzo delle risorse. Occorre quindi individuare percorsi di innovazione che sappiano conciliare qualità del servizio e controllo della spesa e la telemedicina può esserne un driver fondamentale, abilitando assistenza diffusa e capillare sul territorio, integrazione delle informazioni nei percorsi di cura e deospedalizzazione, con benefici diretti e indiretti sia per i pazienti sia per il SSN. Il mercato mondiale della telemedicina è già una realtà, in continua e rapida crescita anche a causa dell'epidemia Covid-19, e BCC Research stima raggiungerà i 104 miliardi di dollari nel 2024, con un tasso di crescita annuale del 19,1%. La maggior parte dei servizi di telemedicina prevede la trasmissione di informazioni e dati di carattere medico nella forma di testi, suoni, immagini o altre forme. Essa è basata su un'infrastruttura di telecomunicazione che deve garantirne la trasmissione sicura a determinati livelli di servizio a seconda dell'ambito di intervento In un'ottica di sviluppo imminente, lo Spazio rappresenterà una valida risposta alle sfide della medicina del futuro. Secondo un rapporto di UNOOSA, redatto in collaborazione con l'Organizzazione Mondiale della Sanità, le tecnologie satellitari di telecomunicazione possono migliorare la fruizione di servizi legati alla telemedicina, alla tele-salute, alla tele-epidemiologia e alla gestione delle emergenze. Le tecnologie di navigazione (quali ad esempio il GPS) potranno migliorare il tracciamento delle vie di soccorso, ottimizzare i servizi di assistenza sul territorio e contribuire alla localizzazione e al tracciamento delle infezioni sul territorio. I satelliti di Osservazione della Terra, attraverso il continuo monitoraggio dell'ambiente e dell'atmosfera, favoriranno l'individuazione di fattori di rischio che possono essere legati all'insorgenza di malattie nelle aree geografiche prese in analisi. Da ultimo, lo spazio è sempre stato e sarà sempre il luogo privilegiato per approfondire la conoscenza del corpo umano e degli effetti di protocolli o tecnologie per curarlo, si pensi ad esempio allo studio sull'osteoporosi degli astronauti. In questo senso, le applicazioni spaziali forniscono già oggi importanti strumenti per migliorare la salute e la vita delle persone:

- le telecomunicazioni satellitari permettono di superare il digital divide cui sono soggetti servizi di telemedicina erogati solo da antenne a terra, garantendo così maggior qualità e uguali condizioni di accessibilità ai servizi di cura territoriale per tutti i cittadini.

- garantiscono stabilità, continuità, velocità di trasmissione e qualità del segnale oltre a standard di sicurezza e privacy della trasmissione dei dati non altrimenti replicabili.

- l'elaborazione di dati satellitari derivanti dall'osservazione della Terra, del suolo e dell'aria, consente misurazioni omogenee e capillari con una conseguente più efficiente pianificazione dei servizi sanitari, soprattutto per l'individuazione e la previsione di malattie legate al territorio.

Dunque il trasferimento tecnologico dallo Spazio alla Sanità è un processo già consolidato che porterà sempre più valore alla collettività anche attraverso l'innovazione in ambito medico. Resta un punto fermo da sdoganare la Sicurezza Nazionale Cibernetica. Se oggi annoveriamo attacchi hacker 'uomo – macchina", con l'affermazione della new space economy, assisteremo ad attacchi 'macchina – macchina" e quindi, con l'utilizzo pervasivo della telemedicina attraverso indossabili, la possibilità di esporre al rischio i pazienti, pregiudicandone sicurezza ed incolumità. Ma la certezza che il nostro Paese saprà far bene, non è messa in discussione.

>> DI MARCO COZZI

Ridurre l'analfabetismo digitale

Una delle principali missioni del Digital Security Festival è ridurre l'analfabetismo digitale. Nel tempo in cui la connessione digitale è diventata la norma, è cruciale che tutte e tutti abbiano le competenze necessarie per navigare in sicurezza nel mondo digitale. Gettare solide basi per una società connessa e digitalizzata non solo aiuta a proteggere i dati personali e le identità digitali, ma ha anche benefici dirompenti per le famiglie, le imprese e la società nel suo complesso. Le competenze digitali possono aprire nuove opportunità di lavoro, migliorare la produttività e rendere la vita quotidiana più comoda e sicura.

Il Digital Security Festival è un passo importante verso la creazione di una società digitalizzata più sicura. Attraverso l'educazione e la formazione, può aiutare a creare una cultura della sicurezza digitale che protegge non solo i nostri dati, ma anche le nostre identità digitali. Tutto questo perché educare è sinonimo di cura, per illuminare menti e cuore nel vivere quotidiano, per un domani capace di futuro.

Illuminare la strada con la conoscenza: Tecnologia e Innovazione come guide per il futuro.

Ho il piacere di condividere con voi una riflessione sull'importanza della conoscenza e dell'innovazione nel mondo della tecnologia. In un'epoca in cui le sfide globali si moltiplicano e il progresso tecnologico accelera, è fondamentale 'illuminare la strada con la conoscenza" per garantire un futuro sostenibile e prospero.

#Globalizzazione e sfide: Viviamo in un mondo interconnesso e globale, in cui le sfide ambientali, sociali ed economiche riguardano tutti noi. La conoscenza e la tecnologia giocano un ruolo cruciale nel permetterci di affrontare queste sfide e trovare soluzioni innovative e sostenibili.

#Innovazione come motore di cambiamento: L'innovazione è il motore principale del progresso e del cambiamento. Grazie a nuove idee, processi e tecnologie, possiamo migliorare e ottimizzare la nostra società. La conoscenza è la chiave per alimentare questa innovazione, permettendoci di comprendere meglio il mondo che ci circonda e di sviluppare soluzioni adatte alle esigenze del nostro tempo.

#Tecnologia come guida: La tecnologia è una guida preziosa che ci permette di esplorare nuovi orizzonti e di superare i limiti del nostro sapere. Con l'aiuto delle più recenti scoperte e innovazioni, possiamo affrontare le sfide del futuro e illuminare la strada con la conoscenza. Ad esempio, l'intelligenza artificiale, la blockchain e l'Internet of Things stanno rivoluzionando la nostra vita quotidiana e il modo in cui interagiamo con il mondo.

#Collaborazione e condivisione: Per poter illuminare la strada con la conoscenza, è fondamentale anche promuovere la collaborazione e la condivisione tra individui e organizzazioni. Insieme, possiamo unire le nostre competenze, le nostre esperienze e la nostra creatività per creare un futuro migliore.

Vi invito quindi a condividere le vostre idee, i vostri progetti e le vostre esperienze per contribuire all'illuminazione della strada con la conoscenza. Insieme, possiamo costruire un futuro tecnologico più luminoso e sostenibile.

di Michele Laurelli

A.I. E CYBER SECURITY

L'intelligenza artificiale alla conquista della cyber security: tra sfide e prospettive

Viviamo in un'era in cui la nostra dipendenza dalla tecnologia e dai dati è cresciuta a ritmi vertiginosi, aprendo nuove frontiere ma contemporaneamente esponendoci a rischi e minacce sempre più sofisticate nel mondo della cyber security. L'intelligenza artificiale (AI) si presenta come un faro nel buio, una risorsa indispensabile per difenderci dalle ombre della rete e garantire la sicurezza delle nostre informazioni.

Ma in che modo l'AI può essere applicata alla cyber security e quali sono le sue potenzialità nello sviluppo dei prodotti per la difesa informatica?

Per rispondere a queste domande, è necessario comprendere quale sia il cuore pulsante dell'AI. L'apprendimento automatico (Machine Learning), ossia la capacità degli algoritmi di migliorare le proprie prestazioni attraverso l'esperienza accumulata nel tempo, costituisce il cardine su cui la tecnologia AI si basa. Proprio questa peculiarità permette all'AI di affinare le proprie capacità e adattarsi alle nuove sfide poste dall'universo della cyber security.

La natura dinamica delle minacce informatiche necessita di sistemi di difesa altrettanto dinamici e proattivi. Ecco allora che l'AI può profondere il proprio valore aggiunto sull'intero panorama, dotando i software di protezione di una notevole efficacia, sia nella prevenzione che nel riconoscimento e nella risoluzione delle intrusioni.

Uno degli strumenti più evoluti offerti dall'AI è quello della "anomaly detection", la capacità di identificare comportamenti anomali e potenzialmente pericolosi nel traffico di dati. Grazie all'AI, i sistemi di cyber security possono elaborare ed analizzare enormi quantità di dati in tempo reale, rilevando schemi irregolari e bloccandoli prima che possano provocare danni. È come se i nostri guardiani digitali fossero dotati di superpoteri per prevedere e neutralizzare le malefatte dei cybercriminali. L'intelligenza artificiale può inoltre contribuire alla lotta contro il fenomeno dei ransomware, uno dei flagelli più in voga nel panorama criminale. L'AI è in grado di creare algoritmi in grado di decifrare le chiavi di cifratura utilizzate dai ransomware, permettendo agli utenti di recuperare i propri dati senza cedere alle richieste di riscatto. Tuttavia, come ogni arma, anche l'AI può essere usata in maniera impropria e finire nelle mani sbagliate. I cybercriminali stessi possono avvalersi dell'intelligenza artificiale per creare attacchi più sofisticati e difficili da contrastare. È quindi fondamentale promuovere l'implementazione etica dell'AI e garantire che i suoi benefici siano sempre orientati al bene comune.

Il cammino dell'AI nella cyber security è appena cominciato, e le sfide che attendono i nostri eroi digitali si fanno sempre più complesse. Tuttavia, le prospettive di una tecnologia in continua evoluzione ci permettono di guardare al futuro con la consapevolezza che, anche di fronte alle minacce più impervie, l'intelligenza artificiale sarà al nostro fianco, pronta a difendere l'integrità delle nostre informazioni e della nostra vita digitale.

beliven / HAPPY CODERS

BUILDING RELIABLE DIGITAL ASSETS

{ Scopri di più su beliven.com }

>> di Roberto Murenec

Dalla copia forense alla "copia mezzo", un cambio di paradigma

Negli ultimi anni, la rapida diffusione di dispositivi capaci di immagazzinare, con estrema facilità, una quantità considerevole di dati e informazioni - che prendono il nome di digital evidence - potenzialmente rilevanti nel corso di un accertamento giudiziario, amplificata e complicata dalla possibilità di archiviare sempre più big data su piattaforme cloud residenti in ordinamenti giuridici diversi dal nostro, non ha fatto altro che contribuire ad aumentare significativamente la quantità di dati - espressi in Gigabyte e/o Terabyte - che entravano in gioco nel procedimento giudiziario; dati che spesso rischiavano di risultare estranei al procedimento per cui si procedeva senza considerare tutte le problematiche connesse al loro trattamento.

Ormai da anni si discute degli effetti della rivoluzione tecnologica e della globalizzazione anche sulle tecniche investigative e, in particolare, sull'esigenza di disporre di nuovi mezzi di ricerca della prova, proprio perché di per sé l'adozione degli stessi non è tassativa ai sensi e per gli effetti di cui all'art. 189 c.p.p., tanto che il giudice anche quando si trova di fronte ad una 'prova atipica" la può assumere liberamente purché l'accertamento dei fatti non sia pregiudizievole per la libertà morale della persona. In realtà, proprio il trattamento della prova informatica nell'ordinamento giuridico italiano, argomento approfondito in una mia recente monografia dal titolo 'Digital Forensics: Aspetti tecnico-giuridici ed operativi sul trattamento dei dati digitali" - di cui si riporta un estratto – edito da Egaf Edizioni S.r.l., sin dal suo riconoscimento nel processo quale 'nuovo" mezzo di ricerca della prova, per effetto dell'intervento della Legge n. 48/2008, ha sollevato numerose questioni di estremo interesse, pratico e scientifico, alle quali recentemente tanto la giurisprudenza di legittimità quanto la dottrina hanno tentato di fornire una soluzione adeguata che cercasse di contemperare la tutela degli interessi delle differenti esigenze processuali.

Non più di venti anni fa, gli atti investigativi a sorpresa, in primis le perquisizioni, senza tralasciare anche gli altri mezzi di ricerca della prova indicati dal legislatore, rappresentavano un indispensabile e straordinario strumento di 'discovery" per ricercare - sfruttando l'effetto sorpresa - in luoghi fisici (domicili, uffici, casseforti, autovetture, persone, ecc..), potenziali prove per l'accertamento di responsabilità penali e per comprendere la dinamica dei fatti. In tale contesto, l'adozione di quella pratica investigativa, che allora era prettamente indirizzata su ciò che era visibile e tangibile, ha consentito per diverso tempo e, ancora continua in parte tutt'oggi, di sviluppare un modus procedendi che prevedesse, a fronte di un provvedimento adeguatamente motivato, il sequestro erga omnes ed indiscriminato di tutti i devices che venivano rinvenuti nel corso di quell'attività operativa senza tener conto delle reali esigenze probatorie e comportando, come conseguenza, un elevato sacrificio dei diritti in capo al e/o ai destinatari della misura ablativa. Questa prassi veniva adottata in barba a qualsiasi esigenza temporale per la mancanza di una cultura-digitale e soprattutto per

ragioni di opportunità, perché la logica delle 'esigenze di giustizia" dietro cui si trincerava l'Autorità Giudiziaria, e di conseguenza anche la Polizia Giudiziaria delegata all'esecuzione della misura emessa, considerava ogni supporto rinvenuto la potenziale prova processuale e, di conseguenza, di quest'ultimo doveva essere fatta la 'copia forense" o la 'copia bit a bit " senza porre la dovuta distinzione tra ciò che era il 'contenuto" da ciò che era il suo 'contenitore". Quest'ultima logica associativa trovava fondamento non solo nella prassi investigativa-operativa, ma veniva avvalorata anche in punta di diritto trovando il proprio appiglio nella vecchia formulazione dell'art. 491-bis c.p. 'Documenti informatici" che originariamente al co. 2 sembrava esprimere una certa connessione inscindibile tra dato e/o informazione processuale e supporto informatico che li conteneva, facendo maturare l'idea tra coloro che svolgevano un ruolo operativo che avere l'intero dispositivo significava avere in mano anche tutti i dati digitali, tra cui anche quelli d'interesse per il procedimento.

Tale ideologia ha iniziato a 'vacillare" a seguito della ratifica della Convenzione di Budapest sul Cybercrime per effetto della Legge 48/2008 , la quale tra le numerose modifiche ed integrazioni apportate al Codice di Procedura Penale e al Codice Penale ha inciso profondamente proprio su quell'art. 491-bis, comportando l'abrogazione di quel co. 2. e decretando la scissione tra ciò che è il 'contenuto" (i dati/informazioni) e il suo 'contenitore" (supporto di archiviazione), generando di conseguenza non pochi problemi di applicazione pratica. Tali problemi sono stati in parte risolti con un successivo intervento legislativo il quale nel riformare anche il co. 1 dell'art. 491-bis ha posto fine definitivamente alla dicotomia 'contenuto-contenitore" affermando il valore probatorio della prova informatica quale elemento autonomo e dematerializzato indipendentemente dal supporto che lo incorpora.

Alla luce di quanto sin qui affermato, la prova informatica - fragile per natura - entra a tutti gli effetti all'interno dell'ordinamento giuridico nazionale, anche se, sin dal suo ingresso, quest'ultima ha sollevato numerose problematiche di estremo interesse pratico e scientifico, alle quali la giurisprudenza e la dottrina hanno cercato di fornire una soluzione adeguata nel rispetto della tutela delle diverse ed eterogenee esigenze investigative e processuali. La Corte di Cassazione nelle sue diverse sentenze - per taluni versi innovative –, in tema di sequestro di dati informatici, è intervenuta a tutela degli interessi in gioco ponendosi proprio a garanzia di quell'esigenza di 'giusto processo" tutelata dalla Costituzione in genere e dai suoi corollari ad essa collegati e lo ha fatto fondando le proprie ragioni sul necessario rispetto del rapporto di proporzionalità tra res appresa e finalità investigative. La spinta propulsiva riformatrice, sospinta dalla diffusione a livello nazionale degli orientamenti espressi dalla Circolare emanata dalla Procura Generale presso la Corte di Appello di Trento del 21.10.2021 e, in ultimo, dal tentativo di normazione della procedura di sequestro di dispositivi informatici di cui al DDL n. 806 presentato in data 19.07.2023, in Seconda Commissione permanente (giustizia), sta si sta andando a sviluppare negli ambienti consolidati della Digital Forensics consiste infatti nella comprensione che la copia forense qualunque essa sia, copia fisica dell'intero reperto digitale o semplice copia logica di taluni dati e/o informazioni del medesimo supporto di archiviazione, raccolti in un file immagine, è divenuta la cd. 'copia mezzo", ovvero rappresenta l'unico mezzo (e non il fine!) per la selezione, l'estrazione e il successivo sequestro del solo materiale pertinente e rilevante alla finalità probatoria perseguita nel processo. Secondo i recenti orientamenti una volta effettuata la copia forense, il device originario dev'essere restituito immediatamente all'avente diritto (ecco la temporaneità!), la copia dev'essere utilizzata per l'analisi ai fini della ricerca e della selezione dell'esclusivo materiale probatorio pertinente ed al termine di questa fase la 'copia mezzo" dev'essere distrutta o restituita all'avente diritto, unico legittimo titolare del trattamento di quei dati. Nel dare attuazione agli orientamenti richiamati , non ultimo in ordine di tempo quello espresso dalla Cassazione nella sentenza n. 17604 del 23/03/2023, l'Autorità Giudiziaria procedente deve fare ricorso alle competenze specialistiche degli esperti di informatica forense affinché, in modo trasparente, facciano uso di quegli strumenti tecnici adeguati all'esecuzione di accertamenti a carattere informatico nel rispetto delle garanzie processuali riconosciute dall'ordinamento in termini di genuinità, integrità ed immodificabilità del contenuto acquisito.

Giova ricordare, in questo stato di cose, che nulla vieta che se su quei dati e/o informazioni acquisite, che non hanno valenza processuale per cui si procede, dovessero emergere altre ipotesi di reità in capo allo stesso soggetto o a terzi, la Polizia Giudiziaria potrà sempre redigere una nuova informativa preliminare di reato ex art. 347 c.p.p. e depositarla alla Procura della Repubblica competente per territorio.

Note e informazioni sull'articolo si possono reperire sul sito del Digital Security Festival.

ALERT

>> PERICOLI SOCIAL
>> ATTACCHI ALLA REPUTAZIONE

DI GABRIELE GOBBO

SOCIAL ZOMBING: NON È TUTTO ORO QUELLO CHE LUCCICA

I social network sono croce e delizia dei tempi moderni, ormai considerati imprescindibili per persone e aziende, li usiamo in continuazione, spesso senza nemmeno farci caso, passandoci diverse ore a settimana, se non al giorno. Emozionanti e divertenti per le persone, grandi occasioni di crescita e acceleratori di business per imprese ed aziende. Nella quotidianità considerati abbastanza sicuri e agevoli da utilizzare, in poche occasioni ci ricordiamo che possono avere dei risvolti negativi o creare dei danni, a partire dagli ormai frequenti furti di account con relativo abuso dei nostri profili per perpetrare truffe online. Ebbene oggi vi racconto un altro pericolo che si cela su queste piattaforme e dà la possibilità a persone senza scrupoli di danneggiare la nostra credibilità o la nostra azienda semplicemente piegando al proprio volere i sistemi di protezione dei social stessi, ad esempio quelli che cercano di combattere gli account falsi e la compravendita di like fasulli. Io e Max Guadagnoli abbiamo denominato queste strategie dannose col termine 'Social Zombing" e ruotano principalmente attorno ad un semplice concetto: se compro migliaia di falsi follower (zombie, appunto) per il profilo del mio concorrente, prima o poi la piattaforma lo limita oppure addirittura lo chiude, con buona pace dell'ignara vittima, che magari ha lavorato anni per avere un account molto seguito e ottimo per la sua attività Ovviamente si possono comprare a poco prezzo follower, reazioni, visualizzazioni di video e ascolti di brani musicali fasulli. Tutti possono portare gli algoritmi di protezione dei social network a limitare gli account in quanto pieni di account e reaction false; un disastro per la presenza online aziendale. L'unico modo per difendersi è monitorare le statistiche e i numeri dei propri account e non essere mai subito felici se crescono a dismisura senza motivo, quindi se notiamo aumenti sospetti dobbiamo correre ai ripari, ad esempio rendendo privato il profilo Instagram o limitando l'accesso da stati esteri alla pagina Facebook.

L'importanza dell'ITCLUBFVG e del Digital Security Festival per gli IT Manager e Professionisti IT

di Luigi Gregori

In un mondo digitalmente interconnesso, la sicurezza informatica non è solo una priorità, ma una necessità vitale. Come presidente di ITCLUBFVG, desidero sottolineare la rilevanza dell'adesione al nostro club e la promozione del Digital Security Festival. L'ITCLUBFVG non è solo un club, ma una comunità di menti brillanti, di professionisti IT e IT manager. Entrare in questo ambiente significa diventare parte di una rete di esperti, pronti a collaborare e a crescere insieme in un settore in continua evoluzione. Ogni IT manager rappresenta un pilastro nel panorama digitale contemporaneo. La capacità di unire una solida base tecnica a competenze trasversali, come la comunicazione, il problem-solving e il pensiero critico, rende questi professionisti fondamentali nel mercato del lavoro attuale. Non è un caso che vi sia una crescente domanda di tali figure: sono individui capaci di navigare nella complessità tecnologica, interpretando le esigenze del business e costruendo ponti tra mondi apparentemente distanti.

L'informatica di oggi passa per 3 punti chiave

di Massimo Della Vedova e Giuseppe Mazzoli

Le complessità dei sistemi informatici e della cybersecurity in continua evoluzione hanno rivoluzionato il mondo ICT per sempre. Le esigenze tecnologiche di aziende e Pubblica Amministrazione oggi passano per 3 punti cardine:

1. Approccio olistico. La protezione dei dati e l'innovazione tecnologica della propria organizzazione non possono più essere pensati per singoli elementi, ma devono essere approcciati con uno sguardo più ampio, 'olistico", che li integri e consideri come un unico e grande organismo.

2. Pochi e affidabili interlocutori. Scegliere tanti fornitori per diverse soluzioni significa essere costretti ad adottare anche tanti approcci, metodi di fatturazione e punti di contatto. Alla complessità dei sistemi si aggiunge quindi la complessità dei rapporti con i partner che può essere notevolmente semplificata scegliendo pochi interlocutori, esperti in maniera trasversale per diverse soluzioni tecnologiche.

3. Soluzioni a servizio. Scegliere un prodotto o un software validi ormai non è più sufficiente. Servono tempo e competenze capillari e verticali per gestire tutto al meglio. Ecco perché l'informatica e la cybersecurity vengono ora sempre più considerate in un'ottica as a service. I prodotti hanno pregi e difetti, ma sono le persone e le loro capacità a fare tutta la differenza.

Per far fronte a tutte queste nuove esigenze, a maggio 2021 è nato il Gruppo MEET IT dalle aziende NT Nuove Tecnologie di Udine e 3CiME Technology di Bologna. Una realtà composta da oltre 35 donne e uomini esperti nel settore ICT e con un catalogo unificato di soluzioni informatiche gestite.

esibirsi

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, Prestigiatori, Attori, Presentatori, Comici, etc....

www.esibirsi.it

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].

Il Digital Security Festival ha come desiderio primario creare incontri formativi per educare alla consapevolezza sul tema della cyber security. Cyber security che non si risolve più solo con la tecnologia, ma che necessita, oggi più che mai, della componente umana, per avvicinarci al 100% di efficacia ed efficienza, in termini di protezione di dati, di strumenti tecnologici, di informazioni aziendali, ma più di tutto, delle nostre identità digitali, con un occhio di riguardo per le categorie più fragili Ridurre l'analfabetismo digitale getta solide basi per una società connessa e digitalizzata, con benefici dirompenti per le famiglie, le imprese e la società tutta.

Vision

>> di Marco Ramilli

RIVOLUZIONE NELL'ATTRIBUZIONE DEGLI ATTACCHI INFORMATICI: VERSO UN FUTURO DI SICUREZZA DIGITALE GLOBALE

Il conflitto informatico che ha accompagnato la guerra in Ucraina ha segnato un cambiamento nella risposta degli Stati nazionali agli attacchi informatici.

I governi dei 'Five Eyes" (Stati Uniti, Regno Unito, Australia, Nuova Zelanda e Canada) hanno congiuntamente attribuito AcidRain, il malware wiper che ha messo fuori servizio migliaia di satelliti KA-SAT di Viasat in Ucraina e nell'Europa occidentale, all'agenzia di intelligence militare russa (GRU) nel maggio 2022. Successivamente, più di una dozzina di Stati membri dell'UE si sono allineati a tale attribuzione.

Questa è stata una delle più grandi accuse pubbliche formali di un'operazione di cyber-offensive contro un paese specifico (nominato) nella storia della rete. Alcuni paesi membri della NATO, tra cui gli Stati Uniti e il Regno Unito, hanno collegato questo attacco anche a diverse famiglie di malware wiper, tra cui WhisperGate, che hanno colpito organizzazioni ucraine a metà gennaio dello stesso anno.

Potenziare l'Attribuzione per Combattere i Criminali

La pratica adottata dai principali stati denominata in lingua inglese 'name-and-shame" (ovvero attribuire una minaccia o un attacco ad una specifica nazione) è destinata a diventare comune, poiché l'Ucraina cosi' come diverse nazioni occidentali hanno confermato di potenziare le proprie capacità di attribuzione in terreno di 'Cybercrime" e 'CyberWarfare".

Il 1 marzo 2023, il Ministro delle Forze Armate francese Sebastien Lecornu ha ammesso che la Francia doveva progredire in tre aree informatiche: attribuzione degli attacchi cibernetici, capacità di difese avanzate e contro-offensiva applicata alla legittima difesa digitale.

Sempre nel marzo 2023, nell'ambito dell'aggiornamento del governo britannico alla Revisione Integrata, il Regno Unito ha lanciato l'Autorità Nazionale per la Sicurezza Protettiva (NPSA), che è ora parte dell'MI5 ed è incaricata di affrontare minacce cibernetiche ponendo particolare attenzione a tematiche inerenti all'attribuzione.

Secondo Clara Assumpção, ricercatrice delle relazioni internazionali presso l'Università Charles di Praga, il motivo principale per cui gli Stati nazionali attribuiscono pubblicamente gli attacchi informatici è quello di mostrare le loro ampie capacità agendo di conseguenza come elemento di deterrenza. Infatti la principale finalità dell'attribuzione pubblica di un attacco informatico è la deterrenza: ovvero la vittima dimostra di essere in grado di identificare i responsabili attraverso alte competenze e quindi, enfatizza la sua capacità di punire e reagire.

Un buon esempio di ciò che è possibile raggiungere in ambito di attribuzione è il lavoro effettuato da Mandiant nel 2021 quando, con dovizia di causa, è riuscita ad attribuire il famoso attacco al produttore informatico SolarWinds ad APT29. Sebbene all'inizio non fosse ancora cosi' estremamente chiara l'attribuzione, Mandiant ha rilasciato il proprio report

aperto alla comunità affinché tutti i ricercatori di threat intelligence potessero beneficiarne. Infine, grazie al contributo di numerosi ricercatori è stato possibile rimuovere la preliminare attribuzione all'attacco ad UNC2452 assegnandola per via definitiva ad APT29.

E' infatti doveroso mantenere "piedi di piombo" quando si parla di attribuzione sopratutto se si vuole accusare un gruppo appartenente ad uno stato o ad una organizzazione governativa. Vi sono dinamiche geo-politiche rilevanti e molto complesse da dover rispettare. Per esempio la politica in Yoroi è molto chiara: non riteniamo sia nostro compito attribuire una minaccia ad uno stato. Possiamo attribuire una minaccia ad un gruppo criminale oppure ad un gruppo APT già noto, ma non vogliamo associare nuovi attori ad un'area geo-politica senza espressa richiesta dagli organi competenti.

Le agenzie governative hanno numerosi elementi in più rispetto ad organizzazioni private come per esempio: informazioni provenienti da human intelligence, collaborazioni Nazionali ed internazionali decennali, segnalazioni di reati non squisitamente cibernetici ma con impronte digitali e report classificati provenienti da agenzie del territorio. Queste informazioni se unite a quelle tecniche di OSINT ed CLOSINT provenienti da organizzazioni private, pone tali organi in una condizione privilegiata per effettuare nuove attribuzioni di scenari geo-politici.

Una ulteriore differenza tra organizzazioni private ed agenzie governative nell'attribuzione degli attacchi è il "movente". Nell'attribuzione informatica tra gli Stati, la domanda fondamentale non è 'Chi l'ha fatto?' ma piuttosto 'Chi è il responsabile?'. Queste domande sono profondamente differenti: la prima è principalmente rivolta ad individuare chi ha effettivamente compiuto l'attacco mentre la seconda domanda è orientata a comprendere chi è il vero mandante, spesso figura giuridica (o fisica) separata dall'esecutore. Gli obiettivi sono differenti in quanto le organizzazioni private hanno come mandato quello di ripristinare lo stato prima dell'attacco e di bloccarlo sul nascere, quindi informazioni tecniche come per esempio (ma non limitato a): IP, hash, domini, url, wallets, sono fondamentali per la veloce identificazione di un attaccante, il suo blocco ed eventualmente la sua eradicazione da un sistema vittima. Contemporaneamente le agenzie governative usano l'attribuzione per diverse ragioni; in primo luogo, vogliono scoraggiare i loro avversari, cioè cercano di impedire che gli altri Stati compiano attacchi informatici. Inoltre, vogliono apportare modifiche alle loro strategie difensive ed offensive per migliorare la loro sicurezza interna. Infine, quando possibile, cercano di portare i colpevoli davanti alla giustizia.

L'attribuzione è fondamentale in una epoca digitale come quella in cui stiamo vivendo perché aiuta gli Stati a comprendere chi è il reale mandante di un attacco informatico. Questo processo consente loro di prendere misure per proteggersi e per rispondere alle minacce digitali interne ed esterne in modo adeguato seguendo le linee politiche e le regole imposte dalle normative vigenti.

Tuttavia, il diritto internazionale fornisce ancora poche indicazioni specifiche su come dovrebbe avvenire l'attribuzione degli attacchi informatici da parte degli Stati. Ciò significa che non esiste una regola univoca o un quadro definito su come dovrebbe avvenire l'attribuzione e quanto dovrebbe essere dettagliata. In breve, l'attribuzione aiuta gli Stati a identificare i responsabili e a prendere le misure necessarie per proteggersi e rispondere, anche se manca un quadro ufficiale di riferimento. Allo stesso tempo, aiuta le aziende a individuare tempestivamente la minaccia, a bloccarla e a ripristinare il più rapidamente possibile lo stato originale della loro rete.

Sono chiamate "false flag" (bandiere false) le tecniche che utilizzano attaccanti strutturati per depistare analisi ed attribuzioni. Una serie di operazioni al modus-operandi, al codice sorgente, ai template sociali utilizzati che simulano altri attaccanti per indurre in errore anche analisti esperti. L'intelligenza artificiale che oggi viene utilizzata per la realizzazione di codice funzionante si pone come grande intermediario tra il reale attaccante e lo stile di codice realizzato. Le collaborazioni tra gruppi che rendono sempre più complesso il "tracking", ovvero il tracciamento delle operazioni che spesso finiscono in differenti parti del globo senza una apparente relazione. La differenziazione del mercato nero, ovvero la differenziazione di intenti dei gruppi coinvolti in un attacco. Chi produce software difficilmente è colui che lo utilizza che difficilmente è colui che si procura il primo accesso alla vittima. Se sommiamo tali sfide al fatto che non vi è ancora uno standard riconosciuto e nemmeno un framework legale chiaro su questa tematica è facile a vedere quali potranno essere le principali sfide per il futuro della cybersecurity.

Conclusioni

Il cambiamento di paradigma nell'attribuzione degli attacchi informatici, evidenziato dalla risposta degli Stati nazionali durante il conflitto informatico legato alla guerra in Ucraina, rappresenta un passo significativo verso la creazione di un ambiente digitale più sicuro. L'adozione della pratica "name-and-shame" e l'attribuzione pubblica degli attacchi dimostrano la determinazione delle nazioni nel rendere gli aggressori responsabili delle loro azioni.

L'esempio dei "Five Eyes" e di altri Stati membri dell'UE che hanno attribuito l'attacco con AcidRain alla GRU russa è stato un momento cruciale nella storia della cybersecurity. Questa trasparenza e chiarezza nell'identificazione degli autori di attacchi informatici rappresenta un passo avanti nel contrastare il cybercrime e la cyberwarfare.

L'investimento nel potenziamento delle capacità di attribuzione e nella difesa cibernetica da parte di diverse nazioni è un segnale di speranza per il futuro. La deterrenza attraverso l'attribuzione pubblica diventa sempre più efficace, mostrando agli aggressori che saranno identificati e che ci saranno conseguenze per le loro azioni.

Tuttavia, ci aspettano sfide significative, come le "false flag" e la complessità delle operazioni di attacco. La collaborazione tra gruppi criminali e l'evoluzione del mercato nero rappresentano ulteriori ostacoli da affrontare. Nonostante ciò, il progresso nell'attribuzione e la consapevolezza dell'importanza di questa pratica sono ulteriori segnali verso una nuova collaborazione tra pubblico e privato.

In un'epoca digitale in continua evoluzione, mantenere un impegno costante nell'identificare e affrontare gli autori degli attacchi informatici sarà fondamentale per garantire la sicurezza digitale globale. Con determinazione e collaborazione, possiamo guardare al futuro della cybersecurity con speranza e fiducia.

NetApp: Soluzioni avanzate per la sicurezza digitale e la protezione dei dati contro i ransomware

di Gianluca Coppola

NetApp è un'azienda leader nel settore delle soluzioni di storage e gestione dei dati, che presta grande attenzione alla sicurezza digitale. Con l'aumento delle minacce cibernetiche e dei ransomware, NetApp si impegna a fornire soluzioni avanzate per proteggere i dati dei clienti e garantire la sicurezza dei loro ambienti digitali.

La minaccia dei ransomware è diventata sempre più pervasiva e dannosa negli ultimi anni. I criminali informatici utilizzano sofisticate tecniche di attacco per crittografare i dati delle aziende e richiedere un riscatto per il ripristino dell'accesso. NetApp riconosce l'importanza di mitigare questa minaccia e offre soluzioni di sicurezza avanzate per proteggere i dati dagli attacchi ransomware.

Una delle soluzioni chiave di NetApp in ambito di sicurezza digitale è la funzionalità di "immutabilità dei dati". Questa funzionalità impedisce la modifica o la cancellazione dei dati per un periodo di tempo specificato, creando una barriera contro gli attacchi ransomware. In caso di tentativo di modifica o cancellazione dei dati, NetApp rileva l'attività sospetta e impedisce l'azione, proteggendo così i dati critici dell'azienda.

NetApp integra anche funzionalità di rilevamento delle minacce e di prevenzione delle intrusioni nei suoi sistemi di storage. Queste funzionalità utilizzano algoritmi avanzati per monitorare costantemente l'ambiente di storage alla ricerca di attività sospette o comportamenti anomali. In caso di rilevamento di una minaccia, NetApp attiva meccanismi di blocco automatici per isolare l'attacco e prevenire la diffusione all'interno del sistema.

Inoltre, NetApp offre soluzioni di backup e ripristino dei dati avanzate per aiutare le aziende a recuperare rapidamente da un attacco ransomware. Le funzionalità di snapshot e replicazione consentono di creare copie dei dati in modo che, in caso di attacco, sia possibile ripristinare i dati non compromessi a uno stato precedente all'attacco.

NetApp sta anche investendo nella ricerca e nello sviluppo di nuove tecnologie per affrontare le minacce future. Sta esplorando l'uso dell'intelligenza artificiale e dell'apprendimento automatico per migliorare la capacità di rilevamento del rischio e per identificare modelli di attacco emergenti. Questo approccio proattivo alla sicurezza digitale aiuta NetApp a stare al passo con le minacce in continua evoluzione e a fornire soluzioni di sicurezza digitale affidabili e innovative, sempre più avanzate per i propri clienti, garantendo che i loro dati siano al sicuro e protetti.

Inoltre recentemente NetApp ha annunciato il programm Ransomware Recovery Guarantee: NetApp sfrutta la combinazione unica delle funzionalità di sicurezza integrate e di protezione da ransomware di ONTAP, bloccando automaticamente tipi di file maligni noti, bloccando amministratori fraudolenti e utenti malintenzionati con la verifica multi-amministratore e creando snapshot inviolabili che non possono essere eliminate, nemmeno dall'amministratore di storage. Con la protezione da ransomware di ONTAP, gli attacchi possono essere rilevati, vengono immediatamente eseguiti ulteriori snapshot e il ripristino può avvenire in pochi minuti.

WHISTLEBLOWING: QUANDO LA TECNOLOGIA NON BASTA.

di Alberto Di Noia

Con l'entrata in vigore del D.Lgs. 24/2023, diverse tipologie di aziende sono tenute ad adottare strumenti e procedure per consentire la denuncia di comportamenti illeciti (Whistleblowing) dando 'giuste garanzie, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante..." Ad una prima lettura, si recepisce l'ennesima complicazione di una procedura semplice prima gestita con una e-mail. L'ulteriore punto che salta agli occhi è ovviamente la menzione degli 'strumenti di crittografia", il che riporta tutto in un contesto meramente tecnologico.

Con una lettura più approfondita, diventa necessario il coinvolgimento di giuristi in grado di comprendere alcune specifiche istruzioni, con particolare riferimento alla necessità di dividere l'identità del segnalante dalla segnalazione, piuttosto che l'attenzione più volte sollecitata sulle notifiche. A quel punto diventa impossibile non scontrarsi con le Linee guida ANAC, con i pareri del Garante per la Protezione dei Dati Personali o con i provvedimenti dello stesso Garante nei confronti di aziende e PA.

È proprio l'analisi delle contestazioni mosse dal Garante (con relative sanzioni da 40.000,00 Euro) che impone approfondimento e comprensione del fatto che la piattaforma di whistleblowing non è solo questione di crittografia, informative e DPIA ma che è necessario utilizzare procedure a supporto alla tecnologia. In sintesi è necessario ragionare di security e privacy (by design), non solo di codice, conoscere le norme di riferimento e supportare i clienti con tutte le informazioni necessarie, come abbiamo fatto con Acara, il servizio di whistleblowing di Net Patrol, perché un software da solo non basta.

Digital Security Festival: il mio perché

di Davide Bazzan

Nel mondo della sicurezza informatica, il vero punto debole non è la tecnologia. Con il Digital Security Festival, noi puntiamo ad accrescere la consapevolezza tra i giovani, gli anziani, gli insegnanti e i genitori, tutti attori fondamentali nel plasmare il futuro digitale. Vogliamo costruire una comunità più solida e consapevole dei rischi online, valorizzando l'importanza dell'elemento umano nella difesa dei dati. Questo festival è un momento chiave per comprendere meglio i rischi del digitale e l'importanza di navigare in rete in modo sicuro e informato. Sappiamo che l'informazione e la formazione sono essenziali per fortificare le difese contro le minacce sempre più sofisticate. Il nostro obiettivo è fare in modo che ogni persona diventi il primo baluardo nella protezione dei propri dati. È fondamentale che ognuno sviluppi le abilità necessarie per esplorare il mondo digitale in modo sicuro. Noi, con il Digital Security Festival, vogliamo essere il motore di questo cambiamento, contribuendo a creare un ambiente digitale più sicuro per tutti.

di Ferdinando Femiano

TECNOLOGIE AVANZATE: RISCHI E SICUREZZA

>> Sistemi di protezione avanzati contro le crescenti minacce del mondo digitale.

Le nuove tecnologie, come l'IoT e l'IA, stanno generando una grande quantità di dati di elevata qualità, consentendo di migliorare l'efficienza complessiva dei processi. Tuttavia, questo progresso presenta un lato oscuro, poiché l'incremento di dati e di automazione espone l'infrastruttura a rischi di sicurezza sempre maggiori. In particolare, i settori vitali dell'economia, quali trasporti, manifattura, energia e utilities, stanno affrontando un serio problema riguardante la sicurezza dei loro sistemi di automazione e controllo industriale. Attualmente, questi sistemi non sono adeguatamente protetti e costituiscono un obiettivo primario per gli attacchi informatici da parte di hacker. Le conseguenze di tali attacchi possono essere devastanti. Per le aziende, possono tradursi in danni economici di portata esponenziale a causa di malfunzionamenti, interruzioni dei servizi o della linea di produzione, e persino la compromissione della proprietà intellettuale e della perdita di dati personali sensibili. Pertanto, è fondamentale adottare misure di sicurezza adeguate per proteggere queste infrastrutture critiche dall'evolversi delle minacce informatiche. Solo così potremo garantire il corretto funzionamento delle nuove tecnologie e trarne vantaggi senza mettere a repentaglio la nostra economia, la nostra sicurezza e la nostra incolumità.

Sp-Cybertec: sistemi integrati di sicurezza informatica. Sp-Cybertec progetta e installa sistemi integrati di sicurezza fisica e logica con esperienza e creatività, per offrire servizi innovativi e personalizzati. L'azienda opera sul territorio italiano ed europeo. SP-Cybertec ha avviato il suo percorso strategico nel 2019 e a distanza di poco più che un triennio, è riuscita a conquistare una

È FONDAMENTALE ADOTTARE MISURE DI SICUREZZA ADEGUATE PER PROTEGGERE LE INFRASTRUTTURE CRITICHE.

posizione di leadership nel contesto italiano. Il team è formato da persone con grande esperienza nel settore della Sicurezza Informatica, con un background caratterizzato da esperienze maturate all'estero in ambienti altamente stimolanti, insieme a giovani capaci di realizzare idee con approcci ancora parzialmente inesplorati. SP-Cybertec completa l'offerta con servizi di assistenza H24 e manutenzione degli impianti. SP-Cybertec è il partner ideale per le aziende, enti pubblici, istituti bancari, centri di raccolta, retail & GDO, aziende ospedaliere, centri logistici e centrali elettriche che desiderano una maggiore sicurezza delle aree interne ed esterne.

"Il mercato italiano relativo alle pmi è ancora poco esplorato in tal senso, la definizione di protezione e digitalizzazione nel comparto è ancora visto come un centro di costo puro, la sfida da parte di 'Sp-Cybertec ' è quella di cambiare la visione dei nostri interlocutori, attraverso una formazione costante, facendo percepire loro il valore aggiunto di tali attività, ed il vantaggio competitivo che potrebbero acquisire sul mercato' queste le parole dell'amministratore unico di Sp- Cybertec, dott Ferdinando Femiano.

TRE FATTORI CHIAVE PER SOPRAVVIVERE AL MODERNO SCENARIO DI MINACCIA CYBER

di Ettore Guarnaccia

Nello scenario sempre più interconnesso e digitalizzato in cui viviamo e operiamo, il rischio cyber è diventato indubbiamente uno dei principali fattori di preoccupazione, nonché un fattore determinante per la sopravvivenza di aziende di ogni dimensione e settore. Il panorama delle minacce, cybercrime in testa, si è evoluto notevolmente ed è in costante mutamento, con attacchi sempre più sofisticati e dannosi. Gli attaccanti sfruttano soprattutto il fattore umano, attraverso tecniche di phishing e social engineering sempre più sofisticate ed efficaci, e le vulnerabilità che affliggono i servizi online e i sistemi informatici. Il malware viene introdotto nella rete della vittima per compromettere i dati e abilitare varie tipologie di attacco.

Il ransomware la fa ancora da padrone, con gruppi di criminali che prendono in ostaggio i dati delle aziende chiedendo un riscatto in valuta digitale non tracciabile. Spesso il panico induce a pagare, alimentando la minaccia senza garanzie di ripristino. Il wiper ha modalità di esecuzione analoghe ma con l'obiettivo di cancellare per sempre tutti i dati aziendali, senza possibilità di recupero. Violazioni della rete aziendale e fughe di dati (cd. data leakage) comportano cause legali e sanzioni regolamentari di elevata entità, mentre aziende che svolgono il proprio business online sono esposte ad attacchi di tipo DDoS, che sovraccaricano reti e sistemi informatici e rendono inaccessibili i servizi pubblicati (siti web e app mobile), spesso con motivazioni ideologiche o legate a conflitti geopolitici in corso. Nessuna azienda può né deve sentirsi al sicuro, soprattutto se inclusa nella supply chain di realtà molto appetibili. Si rischia l'arresto totale e improvviso del business, cioè cassa integrazione per il personale, elevatissimi costi di ripristino di dati e sistemi informatici, ingenti danni di immagine e reputazione, reclami di clienti e fornitori, cause legali e perdita di importanti posizioni di mercato, fino al fallimento. Le tecniche di attacco sono ben conosciute, ma l'aumento degli incidenti dimostra l'incapacità cronica di difendersi. Per garantire la resilienza urge delineare strategie preventive e proattive che contemplino i seguenti fattori.

Il primo fattore è il business aziendale, da conoscere a fondo nei suoi aspetti cruciali e sottoporre alla gestione strutturata del rischio, che determini ciò che va assolutamente protetto per garantirne la sopravvivenza. La cybersecurity intelligence consente di delineare scenari realistici di minaccia e attacco, basati sull'effettivo contesto operativo dell'azienda, abilitando l'ottimizzazione degli investimenti in misure di sicurezza. Non puoi proteggere qualcosa che non conosci da ciò che non conosci.

Il secondo fattore è quello umano, cui indirizzare campagne strutturate di consapevolezza basate su scenari realistici, affinché tutti i dipendenti dell'azienda (dall'usciere al CEO), siano perfettamente coscienti delle minacce e degli attacchi applicabili al contesto, quali comportamenti proattivi adottare e come agire a fronte di eventi negativi. Saper riconoscere i segnali di un attacco consente efficacia e tempestività, limitando gli impatti. Affinché una campagna sia efficace, i concetti devono risultare semplici, riconoscibili, fruibili, pervasivi e persistenti, sfruttando tecniche moderne di fruizione.

Il terzo fattore è costituito dai processi, che devono essere strutturati, attuabili e disegnati per il contesto operativo e gli scenari di minaccia e attacco determinati da gestione del rischio e intelligence, che contribuiscono anche a determinare le priorità degli investimenti di sicurezza. Non si può prescindere da piani di gestione e risposta, da testare con simulazioni regolari basate su contesto operativo e scenari realistici, per allenare il personale-chiave ad attuare con rapidità ed efficacia le azioni richieste. Importantissima la comunicazione interna ed esterna.

Tre fattori troppo spesso sottovalutati ma relativamente semplici da indirizzare, soprattutto se ci si affida a professionisti di cybersecurity esperti e preparati. Per saperne di più, partecipa al Digital Security Festival 2023, dove la sicurezza è spiegata in maniera semplice e fruibile.

La Cybersecurity aziendale: Un Approccio Imprescindibile per la Protezione Digitale

di Gian Maria Masiero

Nell'era digitale, la cybersecurity aziendale è diventata un elemento fondamentale per garantire il successo, la reputazione e la sopravvivenza delle imprese. L'innovazione porta con sé opportunità straordinarie, ma anche minacce cibernetiche sempre più sofisticate. In Axera cerchiamo di affrontare questi temi con un approccio metodologico che prenda sempre in considerazione alcuni pilastri fondamentali. Vediamoli insieme.

Leadership
Il primo elemento critico è l'impegno della leadership aziendale. La dirigenza dovrebbe essere costantemente informata sui rischi cibernetici e coinvolta nelle decisioni strategiche

Valutazione dei Rischi
Le aziende devono identificare e valutare i punti deboli nella loro infrastruttura. Una volta identificati, è importante assegnare loro una priorità e sviluppare piani per mitigarli

Formazione
Gli utenti finali sono spesso il punto più debole nella catena della sicurezza. Le aziende dovrebbero investire nella formazione e nella sensibilizzazione dei dipendenti fin dalla loro assunzione

Accesso e Protezione dei Dati
L'accesso ai dati o all'infrastruttura aziendale deve essere protetto da password robuste e da sistemi di autenticazione a più fattori. Andrebbero implementate tecnologie di crittografia per proteggere i dati sensibili. La gestione dei dati dovrebbe includere anche procedure di backup regolari e piani di ripristino in caso di perdita di dati.

Monitoraggio
Il monitoraggio costante della rete e dei sistemi è essenziale per rilevare tempestivamente intrusioni o comportamenti sospetti. La raccolta e l'analisi dei log possono aiutare a identificare comportamenti anomali

Aggiornamenti
I software e i sistemi obsoleti o non aggiornati sono spesso vulnerabili agli attacchi. L'utilizzo di sistemi di management possono dare un aiuto prezioso in questo processo per garantire che nessuna patch venga trascurata.

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

IL VIAGGIO DELLA CONOSCENZA

di Sonia Gastaldi

Mi piace associare il viaggio alla straordinaria esperienza che sto vivendo da tre anni a questa parte con Il Digital Security Festival. Perché proprio il viaggio? Perché quando decidi di andare in un luogo diverso da dove vivi, smetti gli abiti del quotidiano e ti immergi in una nuova realtà. Una realtà che spesso è diversa dal nostro essere ordinario, uno spaziotempo che ha bisogno però di una significativa e adeguata preparazione per il nuovo 'vivere", seppur temporaneo.

Gli ingredienti fondamentali del viaggiare sono la conoscenza, la consapevolezza e il controllo, esattamente gli stessi ingredienti per una efficace ed efficiente educazione alla cyber security.

Ho iniziato il mio viaggio con il Digital Security Festival tre anni fa, quando Marco Cozzi mi ha invitata all'evento di apertura e ho spiegato l'innovazione tecnologica con i film. Lì si è aperta quella dimensione creativa che mi aiuta, giorno dopo giorno, a spiegare la cyber security in modo semplice, con l'arte dei film e dei libri, con metafore che ci permettano di riconoscere le situazioni di pericolo, per proteggere e proteggerci.

L'incontro con il Digital Security Festival ha dato una nuova forma alla mia attività di divulgazione ed educazione alla cyber security. Esattamente quello che succede quando faccio un viaggio, breve o lungo che sia, vicino o lontano, se ti è entrato nel cuore, ti fa tornare cambiato e diverso da come eri quando sei partito.

Il Digital Security Festival è uno spaziotempo d'eccellenza, perché nasce dalla gratuità, dalla generosità e dalla gratitudine di professionisti/e che dedicano tempo per fare il bene fatto bene.

Oggi più che mai abbiamo bisogno di educare la componente umana che usa gli strumenti digitali, perché è il fattore H_Human quello più vulnerabile, basta un click distratto perché qualcuno entri – senza autorizzazione – in uno dei nostri profili social, nella posta elettronica o peggio, nel conto corrente. E non dimentichiamo i temi del cyberbullismo, delle estorsioni economiche a imprese e privati. È un grande privilegio esserci e sono grata ai miei compagni di avventura Marco Cozzi, Gabriele Gobbo, Luigi Gregori e Davide Bazzan, perché so che questo viaggio mi renderà migliore anche grazie a loro.

Chi sono gli Evangelist del Digital Security Festival

Parafrasando Forrest Gump potremmo dire che 'evangelist è, chi evangelist fa". Se entriamo dentro la parola scopriamo che evangelista è il 'portatore di buona novella". Bellissima accezione che, se estesa alla nostra domanda, ci aiuta a formulare la dimensione del DSF Evangelist, quale portatore/portatrice di buona novella del/nel mondo digitale. E qual è la buona novella? La buona novella è che costruendo una rete di professionisti/e che spiegano in modo semplice la sicurezza informatica trasformiamo il mondo digitale in un luogo sicuro, sostenibile e abitabile per tutte e per tutti. Cosa fa il DSF Evangelist? Promuove il Digital Security Festival attraverso relazioni di valore che alimentano valori. Supporta l'evento, con la promozione degli obiettivi del Festival, mettendo a disposizione emozioni, competenze tecniche e organizzative e, la cosa più preziosa, il proprio tempo. Essere un DSF Evangelist è incarnare uno stile di vita: significa amare ciò che si promuove e saper trasmettere questa passione attraverso le emozioni. Questa essenza nasce da un'esperienza positiva con il Digital Security Festival, che a sua volta nomina i propri evangelist. **Gli evangelist oggi sono:** Ettore Guarnaccia, Ivano Di Santo, Alberto Fedalto, Luca Moroni, Antonio Piva, Fabrizio Biscotti, Andrea Del Vecchio, Alessandro Franchi

axians

Be **prepared** with Axians

Programma del Festival 2023

17-18-23-25 OTTOBRE ONLINE
SOCIAL ARENA. LE CONFERENZE ONLINE APERTE AL PUBBLICO IN DIRETTA STREAMING

18-19 OTTOBRE ONLINE
WEBINAR PRO. I SEMINARI VERTICALI ONLINE DEDICATI AI PROFESSIONISTI

20 OTTOBRE UDINE
INAUGURAZIONE EVENTI FISICI DEL FESTIVAL. 08:30/13:30 AUDITORIUM COMELLI DEL PALAZZO DELLA REGIONE FRIULI VENEZIA GIULIA. 14:30/19:00 PRESSO PALAZZO TORRIANI

21 OTTOBRE PADOVA
CYBER SECURITY COME VALORE. 09:00/13:30 PRESSO LE VILLAGE BY CA TRIVENETO

22 OTTOBRE SAN DANIELE DEL FRIULI (UD)
LA STORIA INCONTRA IL FUTURO. 09:30/13:00 PRESSO SCRIPTORIUM FOROIULIENSE

23 OTTOBRE TAVAGNACCO (UD)
CYBERSECUIRTY: FRA MEET(O) E REALTÀ. 15:00/19:00 PRESSO DITEDI

24 OTTOBRE TREVISO
ILLUMINARE IL FUTURO. 14:30/19:00 PRESSO PALAZZO DELLA LUCE

25 OTTOBRE TRIESTE
QUANDO SICUREZZA FA RIMA CON BUSINESS. 15:00/19:00 PRESSO ACCADEMIA NAUTICA DELL'ADRIATICO

26 OTTOBRE VICENZA
CLICK CLICK, URRÀ. 15:00/19.00 PRESSO ELEVATOR INNOVATION HUB

27 OTTOBRE VENEZIA
EVENTO DI CHIUSURA DEL FESTIVAL. 13:30/19:00 PRESSO PALAZZO QUERINI DUBOIS

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 / FOUNDER - PRESIDENT
GABRIELE GOBBO / CO-FOUNDER - ADVISOR
LUIGI GREGORI / ADVISOR
SONIA GASTALDI / CONTENT ADVISOR
DAVIDE BAZZAN / PUBLIC RELATION

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

www.digitalsecurityfestival.it

NetApp®

Con la Ransomware Recovery Guarantee di NetApp, i ***tuoi dati non si sono mai sentiti più al sicuro***. Ovunque essi siano.

NetApp.com

© 2023 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.

NOTE E APPUNTI

NOTE E APPUNTI

DSF SUPPORTER

La Cricca

CYBER RESILIENCE: SEMPRE PIÙ NECESSARIA

di Federica Maria Rita Livelli

Le aziende, oggigiorno, devono sviluppare un framework di cyber resilience - quale calibrata sintesi dell'implementazione dei principi di business continuity, risk management e cybersecurity - per affrontare gli attacchi cyber sempre più diffusi a livello globale e che possono avere conseguenze negative sui sistemi aziendali.
La cyber resilience richiede una pianificazione preventiva, l'adattamento continuo delle strategie di gestione del rischio e la capacità di ripristinare tempestivamente le operazioni in caso di incidente. È importante comprendere il contesto dei propri asset hardware e software, delle operazioni dipendenti dalla tecnologia e dei dati critici archiviati, valutare gli impatti potenziali e adottare le misure necessarie per ridurli al minimo. Inoltre, la cyber resilience prepara le organizzazioni ad affrontare le sfide future derivanti dall'uso sempre più diffuso di tecnologie avanzate. Di fatto si tratta di garantire una gestione proattiva dei rischi, sistemi di rilevamento efficaci, piani di risposta e recovery, e procedure di autovalutazione e miglioramento. Inoltre, la progettazione di un framework di cyber resilience richiede il coinvolgimento e il supporto del top management per fornire le risorse necessarie e assicurare la presenza di personale con competenze tecniche di cybersecurity.
Conclusione. Le nostre organizzazioni sono sempre più 'bioniche", i.e. caratterizzate dalla combinazione di tecnologia e personale, con un'enfasi sull'importanza dei dipendenti. Pertanto, l'approccio olistico diventa sempre più importante, con un top management che agisce in modo appassionato e razionale, guidando l'implementazione di una cultura forte, agile e flessibile, la promozione dell'apprendimento tra pari, la discussione aperta e la formazione continua. L'obiettivo è strutturare un framework efficace ed efficiente per prevedere e affrontare l'imprevedibile certezza dei rischi cyber, garantendo così la cyber resilience.

Collaborazione fra Digital Security Festival e Scriptorium Foroiuliense

È nata una nuova collaborazione fra il Digital Security Festival e lo Scriptorium Foroiuliense. Un sodalizio che unisce passato e futuro in una infinita via dell'informazione e della formazione. Lo Scriptorium Foroiuliense è una poliedrica realtà, dove troviamo la Scuola Italiana Amanuensi, il museo vivente Opificium Librorum e dove possiamo trovare proprio degli antichi codici di cifratura e tomi sulla crittografia e le scritture segrete. Un filo rosso perfetto che unisce passato, presente e futuro. La partnership tra il Digital Security Festival e lo Scriptorium Foroiuliense è un luogo di significati importanti, per costruire un futuro di valore, a partire dalla conoscenza, dalla condivisione e dalla consapevolezza che 'più conosci e meglio è".

scriptoriumforoiuliense.it

Perchè abbiamo voluto questo strumento cartaceo

Forse non tutti sanno che:
- il primo giornale italiano è stata la Gazzetta di Mantova uscita la prima volta nel 1664;
- lo "strillone" era il venditore ambulante di giornali che in passato gridava ad alta voce le notizie più importanti e di maggior clamore del giornale;
- la Gazzetta dello Sport in origine era verde, ma dopo due anni dalla sua prima pubblicazione diventa rosa, esattamente il 2 gennaio 1899. I ciclisti vengono premiati con la maglia rosa, perché è il colore del giornale dedicato allo sport.

Potremmo andare avanti con tanti altri aneddoti collegati alla 'carta stampata" e all'intramontabile fascino di entrare in edicola, prendere un giornale e sfogliarlo, magari davanti a un buon caffè.

Nel bel mezzo della rivoluzione digitale, consapevoli dell'importanza della notizia online, ben alimentata dal nostro sito www.digitalsecurityfestival.it, dalla nostra app e dai vari social, noi del Digital Security Festival abbiamo deciso di divulgare la cultura della sicurezza informatica con la carta. Con un magazine che verrà distribuito durante il Festival.

Perché?

Perché la carta ci permette di avere un'esperienza sensoriale più completa rispetto al digitale. Un giornale può essere toccato e sfogliato e viene attivato il tatto. E poi, vogliamo mettere il profumo della carta che mette in azione l'olfatto.

Nell'informazione cartacea abbiamo vista, tatto e olfatto che ci aiutano a vivere la lettura, la comprensione e l'apprendimento in modo più esteso ed efficace, perché se abbini l'esperienza cognitiva alle emozioni, il successo è garantito.

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 tenico 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.

RSN studio nord

interview

>> 5 domande a Massimo Mondiani

Nel panorama attuale della cybersicurezza, quali considerate le principali minacce emergenti e come vi state adattando per affrontarle?

Nel panorama attuale della cibersicurezza, ci sono diverse minacce emergenti che richiedono attenzione e adattamento costante. Alcune delle principali minacce emergenti includono:

1. Attacchi di phishing avanzati: Gli attacchi di phishing sono diventati sempre più sofisticati e mirati. I criminali informatici utilizzano tecniche come l'ingegneria sociale per ottenere informazioni personali sensibili o indurre le persone a rivelare credenziali di accesso. NetApp si adatta a queste minacce fornendo soluzioni di sicurezza avanzate che includono ad esempio il rilevamento automatico e la mitigazione degli attacchi di phishing.

2. Ransomware: Il ransomware è una minaccia sempre più diffusa, in cui i criminali informatici crittografano i dati delle vittime e richiedono un riscatto per rilasciarli. NetApp affronta questa minaccia offrendo soluzioni di backup e ripristino dei dati che consentono di recuperare rapidamente i dati crittografati senza pagare il riscatto.

3. Minacce basate sull'intelligenza artificiale (AI): L'uso dell'intelligenza artificiale da parte dei criminali informatici sta aumentando. Possono utilizzare l'AI per automatizzare gli attacchi, individuare vulnerabilità o eludere i sistemi di sicurezza. NetApp si sta adattando a questa minaccia incorporando funzionalità di AI e machine learning nelle sue soluzioni di sicurezza per rilevare e mitigare le minacce basate sull'AI.

4. Internet delle cose (IoT): L'espansione dell'IoT ha introdotto nuovi punti di accesso per gli attacchi informatici. Dispositivi IoT non sicuri possono essere compromessi e utilizzati come trampolini per attaccare reti e sistemi aziendali. NetApp si impegna a fornire soluzioni di sicurezza IoT che proteggono i dispositivi e le reti IoT da attacchi esterni.

Per affrontare queste minacce emergenti, NetApp adotta un approccio olistico alla sicurezza, integrando funzionalità di sicurezza avanzate nelle sue soluzioni di storage e gestione dei dati. Queste soluzioni includono crittografia dei dati, autenticazione multi-fattore, rilevamento delle minacce in tempo reale, gestione degli accessi e controlli di conformità. NetApp collabora anche con partner e organizzazioni di sicurezza per rimanere aggiornata sulle ultime minacce e sviluppare soluzioni efficaci per proteggere i dati dei clienti.

Recentemente NetApp ha annunciato il programm Ransomware Recovery Guarantee: NetApp sfrutta la combinazione unica delle funzionalità di sicurezza integrate e di protezione da ransomware di ONTAP, bloccando automaticamente tipi di file maligni noti, bloccando amministratori fraudolenti e utenti malintenzionati con la verifica multi-amministratore e creando snapshot inviolabili che non possono essere eliminate, nemmeno dall'amministratore di storage. Con la protezione da ransomware di ONTAP, gli attacchi possono essere rilevati, vengono immediatamente eseguiti ulteriori snapshot e il ripristino può avvenire in pochi minuti.

La cybersicurezza è un campo in rapida evoluzione. Come fate a

rimanere all'avanguardia e a garantire che le soluzioni proposte siano sempre aggiornate rispetto alle nuove minacce?

NetApp è un'azienda leader nel settore della gestione dei dati e della cybersicurezza. Per rimanere all'avanguardia e garantire soluzioni aggiornate alle nuove minacce, NetApp adotta diverse strategie:

1. Collaborazione con esperti di sicurezza: NetApp lavora a stretto contatto con esperti di sicurezza, consulenti e partner per comprendere le nuove minacce emergenti e le migliori pratiche di sicurezza. Questa collaborazione consente a NetApp di acquisire conoscenze approfondite sulle nuove minacce e di sviluppare soluzioni efficaci per affrontarle.

2. Monitoraggio costante delle minacce: NetApp mantiene un costante monitoraggio delle minacce informatiche attraverso l'analisi di intelligence sulle minacce provenienti da fonti affidabili. Questo monitoraggio consente a NetApp di identificare rapidamente nuove minacce e sviluppare contromisure adeguate.

3. Ricerca e sviluppo: NetApp investe in ricerca e sviluppo per migliorare continuamente le sue soluzioni di sicurezza. Questo include lo studio delle nuove tecniche di attacco, lo sviluppo di algoritmi avanzati di rilevamento delle minacce e l'implementazione di funzionalità di sicurezza avanzate nelle proprie soluzioni.

4. Aggiornamenti regolari del software: NetApp rilascia regolarmente aggiornamenti del software per le sue soluzioni di sicurezza, inclusi patch di sicurezza per affrontare le vulnerabilità note. Questi aggiornamenti garantiscono che le soluzioni NetApp siano sempre allineate alle ultime minacce e siano in grado di fornire una protezione efficace.

5. Formazione e consapevolezza: NetApp investe nella formazione dei propri dipendenti e dei clienti per garantire una corretta comprensione delle minacce informatiche e delle migliori pratiche di sicurezza. Questa formazione aiuta a creare una cultura di sicurezza all'interno dell'azienda e dei clienti, migliorando la capacità di rilevare e rispondere alle minacce.

Attraverso queste strategie, NetApp si impegna a rimanere all'avanguardia nel campo della cybersicurezza e a fornire soluzioni aggiornate per affrontare le nuove minacce informatiche.

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

NetApp è un'azienda leader nel settore della gestione dei dati e offre soluzioni di storage e cloud che consentono alle organizzazioni di sfruttare al meglio i vantaggi dell'intelligenza artificiale (IA) e dell'apprendimento automatico (ML). NetApp affronta il cambiamento portato dall'IA in diversi modi:

1. Soluzioni di storage per i dati dell'IA: NetApp sviluppa e fornisce soluzioni di storage all'avanguardia che soddisfano le esigenze delle applicazioni di IA e ML. Queste soluzioni consentono di gestire, archiviare e analizzare grandi quantità di dati necessari per l'addestramento e l'esecuzione di modelli di intelligenza artificiale.

2. Gestione dei dati: NetApp offre strumenti e tecnologie per la gestione dei dati che aiutano le organizzazioni a organizzare, proteggere e ottimizzare i dati utilizzati nell'IA. Questo include la gestione dei dati non strutturati, la riduzione dei tempi di accesso ai dati e la garanzia della disponibilità e dell'integrità dei dati.

3. Collaborazione con partner: NetApp collabora con partner tecnologici, università e centri di ricerca per sviluppare nuove soluzioni e promuovere l'innovazione nel campo dell'IA. Queste collaborazioni consentono a NetApp di rimanere all'avanguardia delle ultime tendenze e tecnologie dell'IA.

I maggiori benefici dell'IA per NetApp includono:

1. Miglioramento delle prestazioni: L'IA può essere utilizzata per ottimizzare l'efficienza operativa e migliorare le prestazioni dei sistemi di storage e cloud di NetApp. L'IA può analizzare i modelli di utilizzo dei dati, identificare le aree di miglioramento e suggerire ottimizzazioni per massimizzare le prestazioni complessive.

2. Automazione dei processi: L'IA può automatizzare processi complessi di gestione dei dati, consentendo alle organizzazioni di ridurre i tempi di lavoro e migliorare l'efficienza operativa. Ad esempio, l'IA può automatizzare il provisioning dei dati, la gestione delle politiche di conservazione dei dati e la risoluzione dei problemi di storage.

3. Miglioramento delle analisi dei dati: L'IA può aiutare NetApp e i suoi clienti a estrarre informazioni significative dai dati. L'IA può identificare modelli, tendenze e correlazioni nascoste all'interno dei dati, consentendo di prendere decisioni più informate e migliorare la pianificazione e l'ottimizzazione delle risorse.

I maggiori rischi associati all'IA per NetApp includono:

1. Sicurezza dei dati: Con l'aumento dell'uso dell'IA, la sicurezza dei dati diventa una preoccupazione importante. NetApp deve garantire che i dati dei clienti siano adeguatamente protetti da accessi non autorizzati e violazioni della privacy.

2. Bias e discriminazione: L'IA può essere influenzata da bias e discriminazione se i dati utilizzati per l'addestramento contengono pregiudizi o sono rappresentativi solo di determinate categorie di persone. NetApp deve affrontare questa sfida garantendo che i modelli di IA siano equi, inclusivi e non discriminatori.

3. Impatto'occupazione: L'automazione resa possibile dall'IA potrebbe comportare la riduzione di alcuni posti di lavoro tradizionali. NetApp deve affrontare questa sfida collaborando con i dipendenti per sviluppare nuove competenze e opportunità di lavoro nell'ambito dell'IA.

NetApp riconosce sia i benefici che i rischi associati all'IA e si impegna auppare soluzioni innovative e responsabili che

massimizzano i vantaggi e mitigano i rischi per i propri clienti.

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

NetApp affronta la questione della formazione e della sensibilizzazione degli utenti e dei clienti sulla cybersicurezza attraverso una serie di iniziative e programmi. Ecco alcuni dei modi in cui NetApp affronta questo problema:

1. Programmi di formazione interna: NetApp offre programmi di formazione interna per sensibilizzare i dipendenti sulla cybersicurezza. Questi programmi includono sessioni di formazione interattive, corsi online e materiali educativi per aiutare i dipendenti a comprendere i rischi e le migliori pratiche per prevenire le minacce informatiche.

2. Consapevolezza della sicurezza: NetApp promuove una cultura di sicurezza attraverso la sensibilizzazione dei dipendenti su questioni di sicurezza informatica. Ciò include la condivisione di informazioni su nuove minacce e vulnerabilità, l'invio di avvisi di sicurezza regolari e l'organizzazione di campagne di sensibilizzazione sulla sicurezza.

3. Soluzioni di sicurezza integrate: NetApp sviluppa soluzioni di sicurezza integrate per aiutare i clienti a proteggere i loro dati e le loro infrastrutture. Queste soluzioni includono funzionalità di crittografia, autenticazione multi-fattore, gestione delle identità e degli accessi, rilevamento delle minacce e altre funzionalità di sicurezza avanzate.

4. Best practice e consulenza: NetApp fornisce consulenza ai clienti sulle migliori pratiche di sicurezza informatica. Questo include la valutazione dei rischi, la progettazione di architetture sicure, l'implementazione di politiche di sicurezza e la gestione delle minacce. NetApp lavora a stretto contatto con i clienti per garantire che abbiano una comprensione approfondita delle minacce e delle soluzioni disponibili per proteggere i loro dati.

In generale, NetApp riconosce l'importanza della formazione e della sensibilizzazione degli utenti e dei clienti per affrontare l'errore umano come fattore di rischio nella cybersicurezza. L'azienda si impegna a fornire risorse, strumenti e consulenza per aiutare le persone a comprendere e mitigare i rischi associati alla sicurezza informatica.

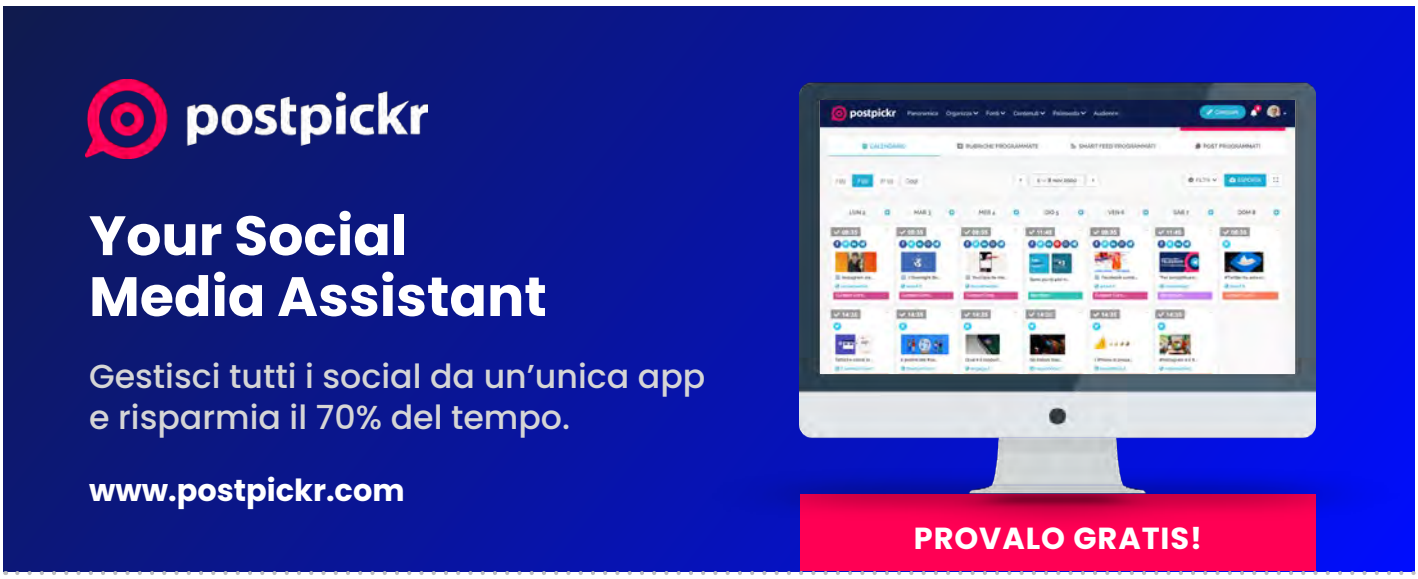
Dove vedete il settore della cybersicurezza tra 5/10 anni? E come vi state preparando per quel futuro?

La cibersicurezza è un settore in rapida evoluzione e di crescente importanza. Con l'aumento delle minacce informatiche, delle violazioni dei dati e delle normative sulla privacy, è probabile che la domanda di soluzioni di cibersicurezza continui a crescere negli anni a venire.

NetApp è un'azienda leader nel settore dello storage e delle soluzioni cloud, e offre anche soluzioni di sicurezza per i dati. Nel corso degli anni, NetApp ha sviluppato una serie di tecnologie e prodotti per proteggere i dati dei clienti, come la crittografia, l'accesso basato sui ruoli, la gestione delle chiavi e la protezione dalle minacce informatiche.

Per prepararsi per il futuro della cibersicurezza, NetApp potrebbe continuare a investire nella ricerca e nello sviluppo di soluzioni innovative per proteggere i dati dei clienti. Potrebbe anche collaborare con esperti di sicurezza informatica, partecipare a standard di sicurezza e adottare le migliori pratiche del settore per garantire la protezione dei dati dei clienti.

Tuttavia, per informazioni più precise sulle prospettive future di NetApp nel settore della cibersicurezza, ti consiglio di consultare le fonti ufficiali di NetApp, come il loro sito web o le comunicazioni pubbliche.



Palazzo della Luce: un luogo che abbraccia il futuro, rispettando il passato

Ci sono luoghi che sono molto di più di semplici spazi. Hanno un'anima, sono in grado di trasferire delle emozioni. È per questo che il **Digital Security Festival** non poteva che trovare naturale dimora qui.

Palazzo della Luce è un edificio storico risalente al 1500 ristrutturato e rinnovato che mette a disposizione uffici, ambienti di condivisione e strumenti innovativi in un contesto in cui **la bellezza del classico incontra il design made in Italy e si fonde con la tecnologia.**

Il nome "Palazzo della Luce" non è solo testimonianza di un edificio costruito per rinnegare il buio, ma rappresenta **la migliore espressione simbolica del risorgimento** di questa nobile dimora.

La luce è un elemento che illumina la nostra vita, la nostra anima e il nostro futuro, alimentando passioni e sogni.

Qui, i professionisti possono sentirsi come a casa e arricchirsi attraverso lo scambio di idee e competenze. **Le sale riunioni ed eventi** offrono a ogni ospite un'esperienza unica e indimenticabile.

Le tecnologie impiegate sono state accuratamente selezionate per offrire **un livello di esperienza** senza precedenti in un edificio in cui storia, innovazione ed emozione si fondono in un unico luogo.

Palazzo della Luce è un progetto di **Infinite Area**, realtà che oltre a fornire spazi e servizi chiavi in mano per **eventi e coworking** dedicati ad aziende e professionisti, si avvale di un gruppo di esperti specializzati nella **progettazione di servizi digitali** (come design sprint e agile) e nella **gestione dell'innovazione** (compresi scouting e trasferimento tecnologico).

Questo permette di accelerare lo sviluppo collaborativo, anche a livello internazionale, di **soluzioni altamente innovative** e favorisce la nascita di **nuove opportunità di business** nella logica dello Startup Studio.

Palazzo della Luce, Via San Nicolò 42 Treviso

www.palazzodellaluce.com

www.infinitearea.com

Entra nel futuro con la flash

Tutta la tecnologia flash
disponibile per ogni budget.

Semplice, sicura e sostenibile.

© 2023 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.

NetApp®