Cybersecurity Trends

Edizione italiana, N. 4 / 2023

INTERVISTE VIP:

- AGNESE SCAPPINI
- AGOSTINO GHIGLIA
- BRUNO FRATTASI

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Folder centrale: Cybersecurity – eventi del 2023 e prospettive 2024

Cybersecurity Trends

Leggi la rivista **online** quando
e dove vuoi!
Puoi scegliere tra news, articoli,
interviste, nuove sezioni,
approfondimenti,
rubriche e contenuti multimediali.

Scopri anche la nuova sezione
dedicata agli esperti della cyber security!
Al suo interno
Hacking Around e Technical Video.

Nella sezione Rubriche:
Bibliografia
Dalla Redazione
Dalle Aziende
Dalle Università
Eventi
Offerte di Lavoro

www.cybertrends.it

Indice

Editoriale

2 **L'anno che verrà...**
Autore: Nicola Sotira

Folder Centrale – Cybersecurity: eventi del 2023 e prospettive 2024

3 **Evoluzione degli attacchi informatici in Africa ed Europa nel 2023.**
Autore: Corradino Corradi

5 **Digital Operational Resiliance Act (DORA) - Così cambia la cyber security nella finanza europea.**
Autore: Alberto Perini

8 **Trend Cybersecurity 2023 e 2024.**
Autore: Ilaria Buonagurio

11 **Quantum Computing: La più misteriosa tra le teorie scientifiche.**
Autore: Jelena Zelenovic Matone

22 **Il mercato assicurativo italiano sempre più dedicato alla copertura del rischio cyber.**
Autore: Annamaria Damiani

24 **AI, Blockchain e Quantum Computing: una Nuova Ghirlanda Brillante.**
Autore: Giovanni Assolini

27 **Svelare il Shadow Market: esplorare l'allarmante aumento delle acquisizioni di account vendute sulla Darknet.**
Autore: Liran Cohen

31 **Cyber Security, a Jesolo un evento di nuova generazione.**
Autore: Alessandra Pernechele

Interviste VIP

33 **Allargare la visuale: la cyber security ha trovato il giusto metodo. Intervista VIP ad Agnese Scappini.**
Autore: Massimiliano Cannata

36 **L'era digitale? Una rivoluzione epocale paragonabile alla scoperta del fuoco e della ruota. Intervista VIP ad Agostino Ghiglia.**
Autore: Massimiliano Cannata

39 **La sicurezza, un bene comune da tutelare. Intervista VIP a Bruno Frattasi.**
Autore: Massimiliano Cannata

Focus

42 **La Cyber Security incontra La Psicologia.**
Autore: Veronica Patron

Bibliografia

44 **Marcello Fausti, Storie di cybersecurity. Appunti di viaggio nel mondo del rischio cyber.**
Autore: Massimiliano Cannata

44 **Mauro Ceruti, Francesco Bellusci: Umanizzare la modernità. Ed. Raffaello Cortina.**
Autore: Massimiliano Cannata

45 **La sicurezza nel Cyberspazio, Federico Ursi (a cura di). Ed. Franco Angeli.**
Autore: Massimiliano Cannata

46 **57° Rapporto del Censis. Ed. Franco Angeli.**
Autore: Massimiliano Cannata

Filmografia

47 **Neptune Frost, Saul Williams e Anisia Uzeyman (USA, Rwanda 2021).**

47 **Tetris, Jon S. Baird (USA, Gran Bretagna 2023).**

L'anno che verrà...

Autore: Nicola Sotira

"Caro amico, ti scrivo, così mi distraggo un po'", così comincia una delle canzoni più belle di Lucio Dalla. E in questo modo proviamo a farci accompagnare nel nuovo anno da tutti i nostri amici, che insieme a noi hanno una grande passione per la cybersecurity e ci hanno seguito in questo intenso anno scrivendo e condividendo con noi questo spirito; la voglia di condividere cercando di semplificare per tutti una materia spesso incomprensibile. Cosa ci riserveranno i prossimi anni? Quali sfide in un mondo sempre più interconnesso e dipendente dalla tecnologia? In questo numero ci siamo interrogati sulle prossime sfide e sulle possibili soluzioni cercando, come sempre, di fornire risposte concrete a chi lavora in questo settore e anche a chi vuole semplicemente capire di più di questa materia. Sicuramente i temi, oggi molto in voga, sono **Intelligenza Artificiale e Quantum Computing**, che porteranno sicuramente molti cambiamenti, opportunità per le aziende, ma anche strumenti nelle mani di criminali informatici che potranno sviluppare attacchi sempre più sofisticati e adattativi. Pertanto, gli strumenti di difesa dovranno marcare le distanze ed evolversi per poter contrastare minacce altamente avanzate. Una maggiore attenzione sicuramente, dovrà interessare l'integrazione della sicurezza nel processo di sviluppo del software, la sicurezza dovrà sempre più essere integrata fin dall'inizio nello sviluppo del software, adottando approcci come **DevSecOps** al fine di garantire la protezione dei sistemi sin dalla loro progettazione. L'espansione poi, **dell'Internet Of Thing** comporterà una maggiore esposizione ai rischi di sicurezza. Evidenziando in questo modo, che la sicurezza di questi dispostivi dovrà diventare una priorità, poiché la mancanza di standard, insieme alle loro vulnerabilità, possono diventare minacce e rendere possibili attacchi su larga scala. Non vedremo, purtroppo, nemmeno una diminuzione degli **attacchi ransomware**. Anzi, questi ultimi diventeranno sempre più mirati e distruttivi, prendendo a bersaglio grandi aziende, PMI e persino gli utenti singolarmente. Questo scenario richiederà a tutte le organizzazioni maggiori investimenti in strategie di protezione dei dati e continuità operativa allo scopo di aumentare la resilienza a questa tipologia di attacco cyber. Si dovrà insistere ancora sulle tematiche di **sensibilizzazione**, investendo in programmi di formazione che promuovano una maggiore conoscenza delle tecnologie e sull'importanza di pratiche di sicurezza informatica. Le organizzazioni dovranno anche aumentare le loro capacità di **collaborare e condividere minacce**, il tutto in uno scenario dove la richiesta di professionisti in cybersecurity supererà l'offerta. Ci sarà una crescente necessità di formazione e specializzazione in questo settore per fare fronte alla domanda crescente di competenze. In sintesi, la cybersecurity sarà una priorità cruciale nei prossimi anni, richiedendo un approccio proattivo, investimenti in tecnologie e competenze, nonché una cultura di sicurezza diffusa per affrontare sfide sempre più complesse in un mondo digitale in continua evoluzione. Io mi sto preparando è questa la novità… ■

BIO

Nicola Sotira è Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Evoluzione degli attacchi informatici in Africa ed Europa nel 2023.

Autore: **Corradino Corradi**

Nel 2023 Il numero degli attacchi informatici è aumentato in numero, sofisticazione e persistenza, e il continente africano non è un'eccezione.

Tra gli esempi di attacchi informatici in Africa nel 2023 possiamo citare i seguenti:

- A marzo, un gruppo di hacker si è introdotto nei sistemi del principale Internet Service Provider (ISP) della Nigeria, causando un prolungato disservizio per milioni di utenti. L'attacco, rivendicato da un collettivo chiamato CyberLions, aveva lo scopo di protestare contro il governo nigeriano per la presunta repressione delle manifestazioni democratiche e i diritti umani.

- A luglio, una sofisticata campagna di phishing ha preso di mira le banche centrali di diversi paesi africani, tra cui Egitto, Kenya e Senegal. Gli hacker, sospettati di essere legati alla Corea del Nord, hanno inviato email contraffatte ai dipendenti delle banche, fingendo di essere partner internazionali o autorità di regolamentazione. Le email contenevano "malware" che ha infettato i computer delle vittime, consentendo agli hacker di accedere ai dettagli delle transazioni finanziarie delle banche target dell'attacco. Si stima che gli hacker abbiano rubato circa 50 milioni di dollari dalle riserve valutarie dei paesi colpiti.

- A novembre, una rete di cybercriminali ha lanciato una serie di attacchi "ransomware" contro ospedali e cliniche in Sud Africa, richiedendo il pagamento di un riscatto in criptovaluta per sbloccare i file crittografati. Molti ospedali non avevano copie di backup dei loro dati e hanno dovuto pagare il riscatto per ripristinare la normale operatività. Gli attacchi sono stati attribuiti a un gruppo noto come DarkSide.

Seppur con modalità e forme diverse, attacchi "ransomware" su ospedali e infrastrutture critiche sono una minaccia comune per Africa ed Europa (in particolare Italia) e mostrano come gli hacker spesso adottino un approccio "business oriented"; una volta investito tempo e denaro nella creazione di un malware, gli hacker provano a massimizzare il loro guadagno attaccando "anytime" ed "anywhere".

Nel 2023 abbiamo assistito anche a una generalizzata crisi economica globale; l'Africa è stata colpita in maniera pesante dalla svalutazione monetaria e dall'inflazione. Molte aziende hanno introdotto programmi di contenimento dei costi per evitare un eccessivo impatto sui margini. Spesso il CISO è stato costretto a ridurre il budget di sicurezza (9,1% CAGR 2022-2027 in Africa secondo IDC) con possibile rischio di degrado della capacità di mettere in campo contromisure di sicurezza informatica efficaci e proporzionali alla "risk acceptance", definita dal board o dal comitato di rischio aziendale.

In particolare, a partire da settembre 2023, la svalutazione della moneta locale in Nigeria (naira) e in Sud Africa (rand) ha provocato una forte perdita di potere d'acquisto e un aumento dei prezzi dei beni essenziali. La svalutazione è stata causata da diversi fattori, tra cui la caduta dei prezzi del petrolio, la fuga di capitali internazionali ed errori di politica economica commessi dai governi nazionali. La svalutazione ha anche reso più difficile per i paesi africani importare tecnologie e servizi di sicurezza informatica, esponendosi così a maggiori rischi di attacchi cyber.

BIO

Corradino Corradi è responsabile della funzione ICT Security & Fraud Management di Vodafone Italia e all'interno del Gruppo Vodafone nel mondo ricopre il ruolo di Senior Member del Corporate Security Leadership Team. L'Ing. Corradi ha 10 anni di esperienza nel campo della security e della gestione delle frodi, della sicurezza dei pagamenti e della protezione delle infrastrutture critiche; è responsabile dell'implementazione delle strategie di sicurezza proattive e reattive, del coordinamento delle operazioni antifrode, nonché del coordinamento di grandi team di professionisti della sicurezza. Corradino Corradi è anche responsabile della gestione dei piani di Business Continuity e Crisis Management di Vodafone Italia. Ha inoltre esperienza nei settori di Risk Management, Compliance, Privacy e Data Protection, Awareness & Training di Frodi e Security, Security Operations Center e CERT, Security Audit e Certificazioni (ISO 27001, SOX, BS25999). In precedenza ha maturato più di 5 anni di esperienza come IT & Security Manager per i principali operatori italiani di telecomunicazioni e banche internazionali.

Nel corso dell'anno abbiamo assistito anche a un peggioramento della crisi geo-politica globale, come il protrarsi della guerra in Ucraina e la nuova instabilità nella Africa sub-sahariana. Nelle regioni francofone dell'Africa ci sono stati colpi di Stato che hanno causato, tra le altre cose, un aumento degli attacchi informatici di matrice politica. Anonymous Sudan, un gruppo di hacker sudanese, nell'agosto del 2023 ha preso di mira le aziende nigeriane e le infrastrutture critiche del paese (inclusi operatori telefonici), in risposta alla minaccia del governo nigeriano di un'azione militare in Niger contro i militari che avevano preso il potere.

La crisi energetica del Sudafrica (fenomeno del distacco programmato dell'elettricità denominato localmente "load-shedding") ha comportato un aggravio di costi per tutte le aziende (dal minerario, al retail alle telecomunicazioni) che si sono dovute dotare di batterie e gruppi di continuità per garantire la continuità dei loro servizi a fronte della prolungata indisponibilità della corrente elettrica. Non ci sono stime concordi sull'impatto economico della indisponibilità di elettricità in Sudafrica; tuttavia, molti economisti stimano l'impatto sul valore aggiunto lordo dell'economia nazionale in 725 miliardi di rand e una perdita di posti di lavoro pari a 860.000.

Anche l'Europa è stata impattata dalla crisi ucraina con un forte aumento del prezzo del petrolio e soprattutto del gas. Comunque, le utilities in Europa sono riuscite a diversificare le fonti energetiche, grazie anche all'aumento dell'utilizzo del gas liquefatto e piattaforme di rigassificazione (GNL)

Comune sia all'Europa che all'Africa è invece il tema del cyber-supply chain management e la necessità, sancita anche da nuove norme e regolamenti (vedi in europea NIS2 e DIRA), di certificare e testare la catena dei fornitori IT e ICT.

Infine, bisogna considerare l'impatto del Covid sul modo di lavorare, nello specifico l'aumento del "working from home" (tradotto in Italia in "smart working"). Il lavoro cloud e ibrido è qui per restare e rappresenta un cambio permanente nell'organizzazione del lavoro soprattutto per le aziende dei servizi e per i "knowledge workers".

Nelle fasi iniziale della pandemia, molti lavoratori sono stati costretti a isolarsi o a lavorare da remoto (significativa l'indisponibilità di vaccini soprattutto in Africa) senza avere adeguati strumenti e protezioni informatiche (ad esempio accesso da remoto in VPN con MFA) o strumenti di protezione dell'endpoint. Questa situazione ha comportato un notevole aumento delle compromissioni di credenziali aziendali e diffusione di malware.

L'ENISA ha evidenziato come gli attacchi informatici in Europa siano aumentati in modo esponenziale durante la pandemia di Covid-19. Tra le tipologie di attacchi più frequenti ci sono stati gli attacchi ransomware, DDoS, phishing e le intrusioni nei database. La situazione non è stata molto diversa in Africa, dove il continente ha subito un aumento del 300% degli attacchi informatici post 2020 (fonte Trend Micro). Gli attacchi hanno colpito soprattutto le organizzazioni governative, le ONG, le istituzioni accademiche e le imprese.

Cosa aspettarci nel 2024? Sicuramente molte delle attuali crisi continueranno così come resterà significativa l'instabilità geo-politica, molti storici e politici ormai parlano di *"perma-crisis"* o di *"crisis as the new normal"*.

I CISO sia in Africa che in Europa dovranno essere agili e capaci di adottare velocemente nuove contromisure informatiche per far fronte ai nuovi rischi cyber. Dovranno presidiare i "basics" (asset inventory, path management incident manager, IUAM) e al contempo lavorare per la comprensione delle nuove tecnologie. Nel nuovo anno resteranno "hot topics" sia la Generative AI (in ottica di attacco che di difesa) sia l'accelerazione verso la "digital trasformation" con necessità di governo dei dati e protezione delle infrastrutture on-premise e cloud. ■

Digital Operational Resiliance Act (DORA) - Così cambia la cyber security nella finanza europea.

Autore: Alberto Perini

Negli ultimi anni abbiamo assistito a una crescente serie di attacchi informatici contro istituzioni finanziarie, che hanno dimostrato l'urgente necessità di rafforzare la cybersecurity. Ad esempio, il noto attacco informatico al sistema di pagamento SWIFT nel 2016 ha rivelato la vulnerabilità delle istituzioni finanziarie alle minacce cibernetiche.

Il Digital Operational Resilience Act (DORA) dell'Unione Europea è emerso come una risposta chiara a questa sfida. DORA è stato proposto per la prima volta nel 2020 e rappresenta un importante passo avanti nella regolamentazione della cybersecurity nel settore finanziario europeo. Questa legislazione è progettata per garantire che le istituzioni finanziarie siano pronte a far fronte alle minacce informatiche e che possano operare in modo sicuro e continuativo in un ambiente digitale in rapida evoluzione.

Introduzione al DORA Act

Il Digital Operational Resilience Act (DORA) è un quadro normativo dell'Unione Europea progettato per migliorare la resilienza operativa digitale nel settore finanziario. È stato introdotto in risposta all'aumento delle minacce cibernetiche e alla crescente dipendenza delle istituzioni finanziarie dalle infrastrutture digitali. DORA si concentra su tre obiettivi principali:

- **Resilienza Operativa**

DORA mira a garantire che le istituzioni finanziarie siano in grado di resistere e recuperare da eventi che potrebbero interrompere le loro operazioni digitali, come attacchi informatici, guasti tecnici o disastri naturali.

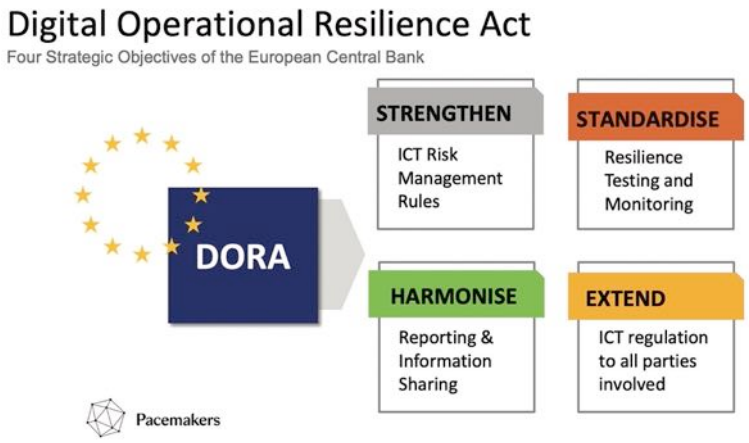
- **Risposta Coordinata**

DORA promuove la collaborazione e la condivisione delle informazioni tra le istituzioni finanziarie e le autorità competenti per garantire una risposta coordinata alle minacce informatiche.

- **Gestione dei Rischi Digitali**

La legislazione richiede alle istituzioni finanziarie di identificare, valutare e mitigare i rischi digitali in modo proattivo.

Questi obiettivi sono fondamentali per garantire la stabilità e la sicurezza del settore finanziario europeo nell'era digitale.



Da un punto di vista pratico poniamo che una grande banca europea stia cercando di implementare DORA per migliorare la sua resilienza

BIO

Alberto Perini è il fondatore di Cyber Ducks, un network specializzato in cyber security, e di Dynamo, un progetto di startup studio per lo sviluppo e il lancio di startup tecnologiche. Attualmente, ricopre il ruolo di CISO presso STIM tech group che Azimut Holding, dove è anche responsabile del gruppo GRC e degli standard NIST, ISO27001, e ISA/IEC 62443, applicati anche ai sistemi di controllo industriale (ICS). In precedenza, presso DI.GI International, ha contribuito allo sviluppo delle strategie e dei processi iniziali di Competence Center e SOC durante l'integrazione nel gruppo Softlab. Ha inoltre lavorato per Alascom Italia come responsabile della Business Unit per la sicurezza delle informazioni e come responsabile della sicurezza informatica per IT/OT/IoT/ICS, concentrandosi sull'analisi di nuove minacce cyber e sulla ricerca di soluzioni innovative. Perini è stato un consulente tecnologico chiave nel progetto BI-REX, focalizzato sull'innovazione nei big data e sull'eccellenza nella ricerca in Cybersecurity OT, collaborando con le Università di Bologna, Imola, Reggio e Ferrara. Ha inoltre assunto ruoli di leadership nella sicurezza informatica e come ricercatore per Sphere Soc in Germania, sviluppando progetti SOC e lavorando con diverse società di sicurezza informatica in Italia, Regno Unito e Svizzera, nonché con fornitori israeliani e statunitensi.

operativa digitale e garantire una risposta coordinata alle minacce informatiche: la sequenza che seguirà sarà accompagnata da una valutazione approfondita dei suoi rischi digitali. Questo processo coinvolge l'identificazione di potenziali vulnerabilità nei sistemi informatici, nelle applicazioni e nei processi operativi.

Sulla base dei risultati della valutazione dei rischi, la banca svilupperà piani di continuità operativa dettagliati. Questi piani definiscono procedure specifiche per affrontare scenari di interruzione, come attacchi informatici, guasti tecnici o disastri naturali.

In questo senso sarà fondamentale investire in misure di sicurezza avanzate per proteggere i suoi dati e le sue operazioni. Questo potrebbe includere l'implementazione di firewall avanzati, sistemi di rilevamento delle intrusioni, autenticazione a due fattori per l'accesso ai sistemi critici e cifratura dei dati sensibili.

Non dovrà, inoltre, mancare un piano adeguato di formazione del personale che verrà sottoposto a programmi di formazione intensivi sulla sicurezza informatica. Questo include la sensibilizzazione sulle minacce cibernetiche, l'istruzione su come riconoscere gli schemi di attacco e la formazione sulla gestione degli incidenti.

Ma la vera mission sarà implementare un sistema di monitoraggio continuo per rilevare e rispondere rapidamente alle minacce informatiche. I team di sicurezza informatica monitoreranno costantemente l'attività dei sistemi e analizzando i dati per individuare comportamenti anomali.

In conformità con i requisiti di DORA, la banca stabilirà un processo di segnalazione degli incidenti ben definito.

Inoltre, fondamentale sarà la collaborazione con i fornitori di servizi IT per garantire che anche loro rispettino gli standard di sicurezza richiesti da DORA.

Implementare DORA richiede un impegno significativo da parte dell'organizzazione finanziaria, ma fornisce una solida base per una maggiore resilienza operativa digitale e una migliore protezione contro le minacce informatiche. Per comprendere meglio gli obiettivi principali di DORA, è importante sapere che le istituzioni finanziarie devono sviluppare piani di continuità operativa robusti che includano misure per la prevenzione, la mitigazione e il ripristino delle operazioni in caso di incidenti cibernetici o altre interruzioni digitali.

Inoltre, DORA promuove la condivisione di informazioni sugli incidenti tra le istituzioni finanziarie e le autorità competenti. Ciò consente una risposta più rapida e coordinata alle minacce informatiche, riducendo l'impatto negativo degli attacchi.

Le istituzioni finanziarie devono condurre valutazioni periodiche dei rischi digitali e adottare misure preventive per proteggere i propri sistemi e dati. Questo implica l'identificazione dei punti deboli e la messa in atto di soluzioni per mitigare i rischi.

Queste considerazioni pongono le basi per un settore finanziario più sicuro e resiliente alle minacce cibernetiche sempre più sofisticate.

Le implicazioni di DORA per le organizzazioni finanziarie e bancarie sono significative e richiedono un approfondimento dettagliato.

Con l'implementazione di DORA, le organizzazioni finanziarie devono assumersi nuove responsabilità nella gestione dei rischi digitali. Queste responsabilità comprendono la valutazione periodica dei rischi, la pianificazione di emergenza e la notifica delle violazioni.

DORA introduce una serie di requisiti normativi specifici che le organizzazioni finanziarie devono rispettare. Questi requisiti spaziano dalla protezione dei dati sensibili alla segnalazione tempestiva degli incidenti.

Le organizzazioni finanziarie devono affrontare sfide come il costo dell'implementazione di misure di sicurezza avanzate e la complessità di conformarsi ai nuovi requisiti. Tuttavia, c'è anche l'opportunità di migliorare la sicurezza operativa e la reputazione aziendale.

L'adeguamento a queste nuove normative richiede un impegno significativo da parte delle organizzazioni finanziarie, ma è essenziale per garantire la sicurezza e la resilienza dell'intero settore.

Il framework di DORA è il cuore della legislazione e definisce le linee guida e i requisiti che le organizzazioni finanziarie devono seguire per essere conformi. Questo framework si compone di diversi pilastri chiave.

Le organizzazioni, in questo senso, devono sviluppare una solida strategia di gestione dei rischi digitali, identificando le vulnerabilità, valutando i rischi e adottando misure di mitigazione.

DORA, inoltre, richiede alle organizzazioni di notificare tempestivamente le violazioni dei dati e gli incidenti cibernetici alle autorità competenti.

Questo contribuisce a una risposta più rapida e coordinata alle minacce informatiche.

Si è tenuti, dunque, a dimostrare di essere in grado di resistere agli eventi digitali disruptivi attraverso esercitazioni di resilienza e test.

DORA pone anche l'accento sulla valutazione dei fornitori di servizi IT, garantendo che anche i partner esterni rispettino gli standard di sicurezza richiesti.

Questi pilastri forniscono un quadro completo per la protezione dei dati e la gestione dei rischi digitali nell'ambito del settore finanziario.

Il Digital Operational Resilience Act (DORA) rappresenta un importante passo avanti nella protezione e nella resilienza delle istituzioni finanziarie nell'era digitale. Questa legislazione mette l'accento sulla necessità di una gestione dei rischi digitali più rigorosa, su una risposta coordinata alle minacce informatiche e su una maggiore resilienza operativa digitale.

Tuttavia, il mondo della cybersecurity è in costante evoluzione, e il DORA Act è destinato a seguire questa tendenza. In futuro, potremmo vedere ulteriori aggiornamenti normativi per affrontare nuove minacce emergenti, come l'uso sempre più sofisticato dell'intelligenza artificiale da parte degli attaccanti o le minacce alla catena di approvvigionamento digitale.

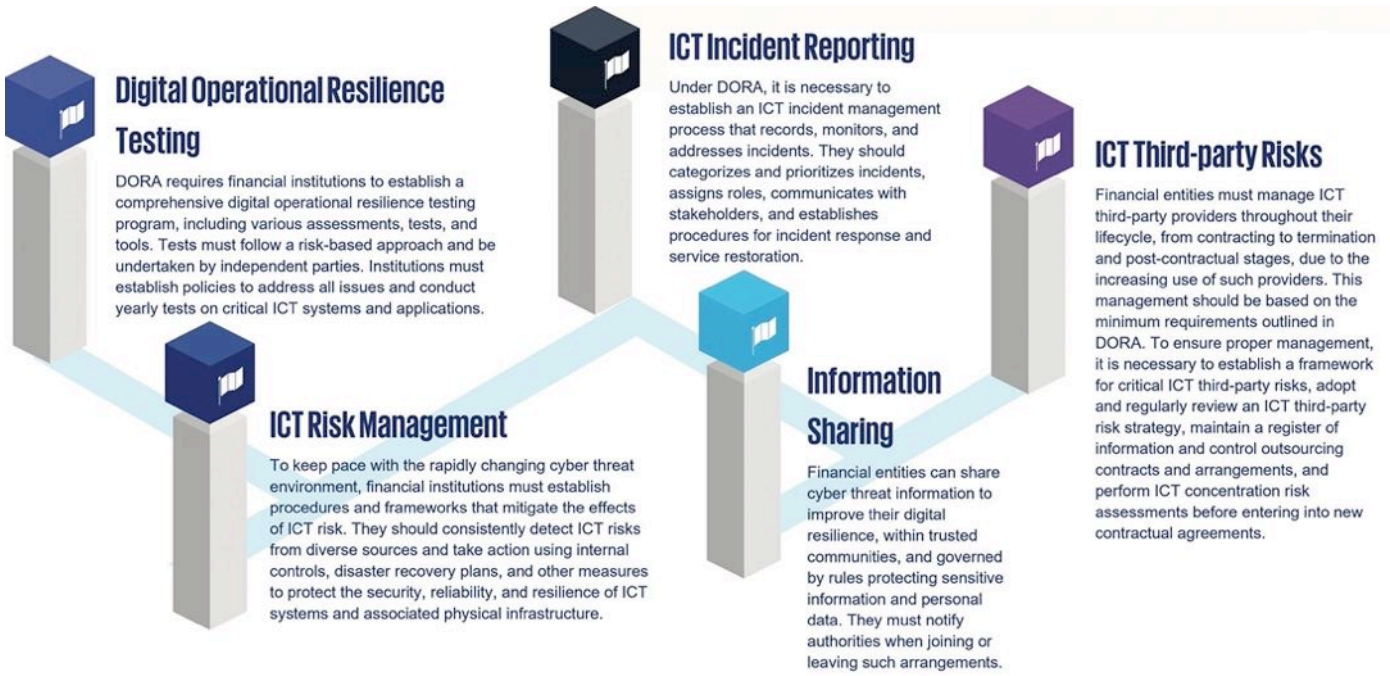
Inoltre, le organizzazioni finanziarie e bancarie dovranno adattarsi continuamente alle sfide della cybersecurity, investendo in tecnologie avanzate, migliorando la formazione del personale e mantenendo una cultura di sicurezza informatica forte. Il DORA Act fornisce una base solida per affrontare queste sfide, ma è essenziale per le organizzazioni rimanere agili e pronte a evolversi con il cambiamento delle minacce digitali.

Ad esempio, l'uso sempre più sofisticato dell'intelligenza artificiale da parte degli attaccanti potrebbe rappresentare una sfida significativa. Gli attaccanti potrebbero utilizzare algoritmi di machine learning per identificare vulnerabilità nei sistemi o per condurre attacchi più mirati. Di conseguenza, le organizzazioni finanziarie dovranno sviluppare difese avanzate basate sull'IA e sull'apprendimento automatico per rilevare e mitigare queste minacce emergenti.

Un altro potenziale scenario futuro riguarda le minacce alla catena di approvvigionamento digitale. Gli attaccanti potrebbero cercare di compromettere i fornitori di servizi IT o i partner commerciali delle istituzioni finanziarie per accedere indirettamente ai loro sistemi. Per mitigare questa minaccia, le organizzazioni finanziarie dovranno rafforzare la sicurezza dei loro fornitori e implementare rigorosi controlli nella catena di approvvigionamento digitale.

Il DORA Act è solo l'inizio della regolamentazione della cybersecurity nel settore finanziario europeo. È probabile che nel futuro si vedano ulteriori aggiornamenti normativi per affrontare nuove sfide e vulnerabilità. Le organizzazioni finanziarie dovranno rimanere aggiornate sulle nuove norme e adattarsi di conseguenza, assicurandosi di essere conformi a tutte le nuove disposizioni legislative. Le minacce cibernetiche non conoscono confini nazionali, e la collaborazione internazionale sarà sempre più importante. Le organizzazioni finanziarie dovranno lavorare a stretto contatto con altre istituzioni finanziarie e agenzie governative in tutto il mondo per condividere informazioni e risorse riguardo alle minacce informatiche. Questa collaborazione globale sarà essenziale per affrontare minacce sofisticate che possono provenire da attaccanti internazionali.

Il DORA Act rappresenta un passo nella giusta direzione per garantire la sicurezza e la resilienza delle istituzioni finanziarie europee. Tuttavia, il futuro richiede una vigilanza costante e un impegno continuo per mantenere il passo con l'evoluzione del panorama della cybersecurity e proteggere efficacemente i dati finanziari sensibili e le operazioni digitali. ■

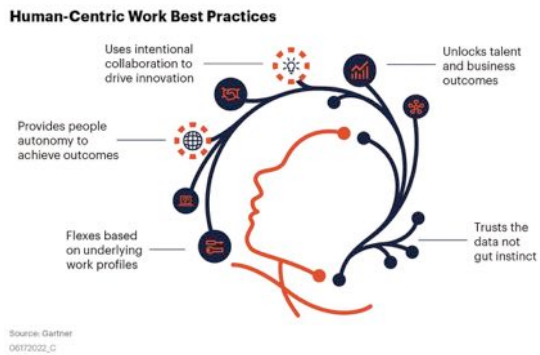


Trend Cybersecurity 2023 e 2024.

Autore: Ilaria Buonagurio

Il panorama digitale è in continua evoluzione e con esso il mondo della cybersecurity. Mentre volgiamo alla fine del 2023 e guardiamo al 2024, stanno emergendo diverse tendenze principali che influenzeranno il futuro della cybersecurity.

2023: Un Approccio Human-Centric



Una delle tendenze più significative del 2023 è il passaggio a un approccio human-centric della cybersecurity. Secondo Gartner, i responsabili della sicurezza e della gestione del rischio (SRM) devono ripensare il bilanciamento degli investimenti tra elementi tecnologici e umani quando creano e implementano programmi di cybersecurity[1].

Il design della sicurezza incentrata sulle persone dà priorità al ruolo dell'esperienza dei dipendenti nel ciclo di vita della gestione dei controlli. Entro il 2027, si prevede che il 50% dei CISO (Chief Information Security Officer) delle grandi imprese adotterà pratiche di design della sicurezza human-centric per ridurre al minimo gli attriti indotti dalla cybersicurezza e incrementare l'adozione dei controlli.

Solitamente, lo sviluppo della cybersecurity si è concentrato sul miglioramento (rafforzamento) della tecnologia e dei processi che supportano i programmi di sicurezza delle aziende, con scarsa attenzione alle persone che creano questi cambiamenti. Nel 2023 questa tendenza ha iniziato a cambiare, evidenziando e concentrandosi sul fattore umano.

L'ascesa dell'intelligenza artificiale

Il 2023 è stato anche l'anno che ha visto l'affermarsi e la diffusione dell'intelligenza artificiale (AI). Quest'anno ha visto l'integrazione delle tecnologie AI in diversi settori, dalla sanità alla finanza, all'istruzione e, naturalmente, alla cybersicurezza. I progressi negli algoritmi di apprendimento automatico (ML) e la disponibilità di grandi quantità di dati hanno portato i sistemi di IA a diventare più efficienti e capaci. Inoltre,

l'aumento degli investimenti nella ricerca e nello sviluppo dell'IA ha portato a innovazioni rivoluzionarie. Questi sviluppi non solo hanno migliorato la funzionalità dei sistemi esistenti, ma hanno anche aperto la strada alla nascita di nuove applicazioni di IA. Di conseguenza, l'IA è diventata uno strumento indispensabile per risolvere problemi complessi e prendere decisioni consapevoli.

L'intelligenza artificiale (AI) svolge un ruolo determinante nella cybersecurity, offrendo una moltitudine di vantaggi e trasformando il modo in cui affrontiamo la cyberdifesa.

L'IA consente alle macchine di svolgere compiti che di solito richiedono l'intelligenza umana, come prendere decisioni, riconoscere il parlato umano, percepire elementi visivi e tradurre le lingue[2]. Nel contesto della cybersecurity, l'IA può essere addestrata per consentire il rilevamento automatico delle minacce informatiche, generare avvisi, identificare nuove categorie di malware e proteggere i dati sensibili delle aziende.

Le tecniche di intelligenza artificiale, come il deep learning, il machine learning, la rappresentazione della conoscenza e il ragionamento e l'elaborazione del linguaggio naturale, vengono sfruttate per una cyberdifesa più automatizzata e intelligente[3].

Il binomio cybersecurity e IA si traduce in una più rapida raccolta dei dati, rendendo la risposta alla gestione degli incidenti più dinamica ed efficiente. Inoltre, elimina la necessità per i responsabili della sicurezza di svolgere attività manuali e dispendiose in termini di tempo, in modo che possano concentrarsi su attività più strategiche che aggiungono valore all'azienda. Infatti, un punto debole comune delle difese di sicurezza tradizionali è la necessità dell'intervento umano, che può portare a costosi errori umani. L'intelligenza artificiale nella cybersecurity elimina l'elemento umano dalla maggior parte dei processi di sicurezza, consentendo di riallocare le risorse umane dove sono più necessarie e riducendo al minimo il fattore dell'errore umano.

Man mano che le soluzioni di IA continuano a svilupparsi, si prevede che porteranno benefici sostanziali alle attività di cyberdifesa in una vasta gamma di organizzazioni e professioni. Automatizzando componenti essenziali di processi fondamentali che richiedono molto lavoro, l'IA può trasformare i flussi di lavoro informatici in processi snelli, autonomi e continui che accelerano la remediation e massimizzano la protezione[4]. L'IA può aiutare a riconoscere modelli di dati complessi, fornire raccomandazioni attuabili e consentire una protezione in autonomia. Migliora il rilevamento delle minacce, supporta il processo decisionale e accelera la risposta agli incidenti[5].

In sintesi, l'IA sta diventando sempre più parte integrante della cybersecurity, offrendo vantaggi significativi in termini di efficienza dei costi, riduzione degli errori e processo decisionale. Con il passare del tempo, il ruolo dell'IA nella cybersecurity è destinato a crescere, trasformando il modo in cui affrontiamo e gestiamo le minacce informatiche.

2024: Previsioni e preparazione

Nel 2024 si prevede che il consolidamento dell'intelligenza artificiale nella cybersecurity raggiungerà nuovi traguardi. Poiché le minacce informatiche diventano sempre più sofisticate, la necessità di meccanismi di difesa avanzati non è mai stata così importante. L'intelligenza artificiale, con la sua capacità di apprendimento e adattamento, è pronta a svolgere un ruolo fondamentale in questo panorama. Gli algoritmi di apprendimento automatico vengono perfezionati per rilevare anomalie e potenziali minacce in tempo reale, garantendo un livello di sicurezza senza precedenti. Inoltre, si prevede che l'analisi predittiva alimentata dall'IA possa prevedere gli attacchi informatici prima che si verifichino, consentendo strategie di difesa proattive e preventive. L'integrazione dell'IA nella cybersecurity non solo migliora la protezione delle risorse digitali, ma trasforma anche il modo in cui le organizzazioni approcciano la cybersecurity. Nel 2024 si prevede un consolidamento significativo dell'IA nel campo della cybersecurity.

Oltre al potenziamento dell'Intelligenza Artificiale, guardando al 2024, un'altra tendenza importante da tenere in considerazione è la crescita degli investimenti nel cybercrime e quindi nella cybersecurity.

I fattori economici e le tattiche sempre più avanzate degli attori delle minacce spingeranno all'ottimizzazione e al consolidamento degli investimenti in sicurezza nel

BIO

Ilaria Buonagurio è un ingegnere con la passione per la cybersecurity, con un forte interesse per la sicurezza industriale e l'automazione. È spinta dall'amore per la soluzione di problemi logici e dalla curiosità di capire come funzionano le cose, come possono essere migliorate e perché funzionano nel modo in cui funzionano. Professionalmente, ricopre il ruolo di coordinatore globale per Offensive Security, in una delle principali aziende italiane di moda e retail. Si occupa di selezionare e implementare nuove soluzioni tecniche e processi per proteggere i perimetri IT e OT. Fornisce inoltre servizi di consulenza ad altre funzioni interne sulla Security By Design per progetti aziendali critici. Il suo mix unico di competenze tecniche, capacità di risolvere i problemi e curiosità culturale la rendono una risorsa preziosa nel campo in continua evoluzione della cybersecurity.

2024. Il tempo di ritorno degli investimenti (ROI) nella tecnologia di cybersecurity è una metrica critica da considerare per le aziende e le organizzazioni[6].

Il concetto di tempo di ritorno dell'investimento (ROI) nella cybersecurity è una metrica critica per le aziende e le organizzazioni. Si riferisce al periodo necessario affinché i benefici derivanti dall'investimento nella cybersecurity superino i costi iniziali e quelli costanti relativi alla sua implementazione.

Questa metrica è fondamentale perché aiuta le organizzazioni a valutare l'efficienza e i profitti dei loro investimenti nel campo della cybersecurity. Un tempo di ROI più breve indica che la tecnologia è efficace nel prevenire le minacce informatiche, proteggendo così l'organizzazione da potenziali perdite dovute a data breach o arresto del sistema.

Tuttavia, il calcolo del tempo di ROI nella cybersecurity può essere complesso. Si tratta di quantificare i vantaggi tangibili e intangibili, come i risparmi sui costi derivanti dalla prevenzione degli attacchi, la maggiore fiducia dei clienti e la conformità alle normative. Questo calcolo deve considerare le spese potenziali che un'azienda potrebbe affrontare in caso di incidente informatico, come la perdita di proprietà intellettuale, la perdita di reputazione, l'interruzione dell'attività e i costi associati alla risoluzione di questi problemi.

Inoltre, è importante notare che un tempo di ritorno dell'investimento più lungo non significa necessariamente che l'investimento non sia conveniente. Date le conseguenze potenzialmente devastanti degli attacchi informatici, il valore di solide misure di cybersecurity non può essere sottovalutato. Pertanto, le organizzazioni dovrebbero considerare il tempo di ROI come uno dei tanti fattori nelle loro decisioni di investimento in cybersecurity.

Il concetto di ritorno sull'investimento (ROI) è molto importante nel contesto della criminalità informatica. Poiché la criminalità informatica è in continuo aumento, con danni che si prevede raggiungeranno i 10.000 miliardi di dollari entro il 2025[7], sempre più aziende stanno aumentando i loro investimenti in cybersecurity.

Si prevede che il crypto crime ovvero l'attività criminale che coinvolge le criptovalute, continuerà ad aumentare nel 2024[8]. Ciò evidenzia la necessità di rafforzare le misure di sicurezza nel settore delle valute digitali.

Nel 2024 si prevede un aumento significativo del cybercrime, con un incremento previsto del 70% degli incidenti[9]. Si prevede che questa crescita sia guidata dai progressi della tecnologia, in particolare dall'intelligenza artificiale (AI), che dovrebbe essere utilizzata dagli attori delle minacce per lanciare attacchi informatici avanzati[10]. Si attente, inoltre, che il costo complessivo dei data breach raggiungerà i 5.000 miliardi di dollari[11], un aumento sostanziale rispetto agli anni precedenti. Questo aumento dei costi non è dovuto solo all'aumento degli incidenti di criminalità informatica, ma anche all'aumento delle sanzioni pecuniarie imposte da normative come il Regolamento generale sulla protezione dei dati (GDPR) e il California Consumer Privacy Act (CCPA). Man mano che l'intelligenza artificiale e altre tecnologie diventano più diffuse, è probabile che vengano attaccate e utilizzate come armi, dando vita a una guerra digitale degli algoritmi[12]. Pertanto, il panorama della criminalità informatica nel 2024 sarà probabilmente caratterizzato da attacchi più sofisticati e costosi, che richiederanno misure di cybersecurity più robuste e avanzate.

In conclusione, il panorama della cybersecurity si è evoluto nel 2023 ed è destinato ad evolversi in modo significativo nel 2024, con uno spostamento verso un approccio più human-centric, l'adozione massiccia dell'intelligenza artificiale a supporto delle operazioni quotidiane e l'emergere di nuove minacce e sfide, con l'aumento dei fondi destinati sia alla criminalità informatica che alla cybersecurity. ■

1 https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023
2 https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity
3 https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity
4 https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024
5 https://www.eccu.edu/blog/technology/the-role-of-ai-in-cyber-security/
6 https://research.g2.com/insights/cybersecurity-trends-2024
7 https://eventura.com/cyber-security/cybersecurity-predictions-and-trends-for-2024/
8 https://eventura.com/cyber-security/cybersecurity-predictions-and-trends-for-2024/
9 https://eventura.com/cyber-security/cybersecurity-predictions-and-trends-for-2024/
10 https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023
11 https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
12 https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Quantum Computing: La più misteriosa tra le teorie scientifiche.

Autore: Jelena Zelenovic Matone

"Information is physical".

– Rolf Landauer

Peggio dell'attacco alla Colonial Pipeline?

Nel maggio 2021, l'attacco ransomware alla Colonial Pipeline ha causato una significativa interruzione dell'infrastruttura energetica sulla Costa Orientale degli Stati Uniti. L'attacco ha compromesso le reti informatiche di Colonial Pipeline, che fornisce quasi la metà del carburante consumato nella regione. Le conseguenze dell'attacco sono state significative e diffuse, con carenze di carburante che hanno provocato ritardi e cancellazioni di voli, acquisti di panico presso le stazioni di rifornimento e la dichiarazione dello Stato di Emergenza da parte del Governo Federale.

L'incidente ha evidenziato le vulnerabilità delle nostre infrastrutture energetiche agli attacchi informatici e la necessità di investimenti più significativi in misure di cybersecurity. Una preoccupazione crescente è la potenziale minaccia rappresentata dai Cryptographically Relevant Quantum Computers (CRQC). Si tratta di un tipo di computer quantistico in grado di violare la nostra attuale infrastruttura a chiave pubblica (PKI), utilizzata per proteggere oltre il 90% di tutti i dati sensibili e le comunicazioni elettroniche.

Man mano che i CRQC continuano ad aumentare potenza e a diventare più ampiamente disponibili, il rischio di un attacco informatico diventa ancora più significativo. Gli hacker stanno già raccogliendo dati criptati, che possono essere decifrati retroattivamente una volta che i CRQC saranno disponibili. Ciò rappresenta una minaccia significativa per la sicurezza e la privacy dei dati sensibili e sottolinea l'urgente necessità di sviluppare nuovi

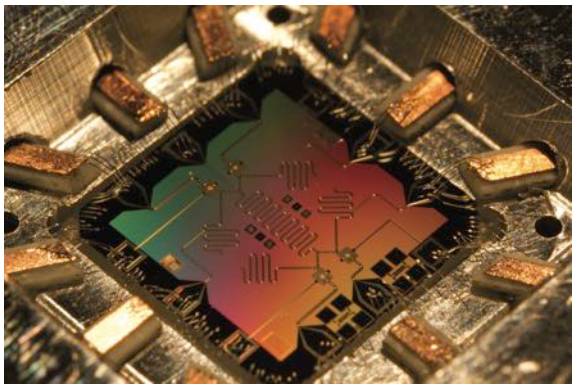
BIO

Rispettata leader CISO, insignita del CISO dell'anno per il 2019 in Lussemburgo, Sentinel CISO Global 2020, EU CISO 2020 e Ambasciatore dell'anno 2021 in Lussemburgo, Jelena è esperta di Cybersecurity versatile e innovativa con enfasi sulla gestione del rischio di sicurezza informatica/ risk management, creazione di policy e procedure, sicurezza IT/ IS, operazioni IT, audit, mitigazione del rischio, miglioramento dei processi aziendali, governance IT, business process improvement, IT governance. Appassionata di partecipazione e incoraggiamento delle donne alla cybersecurity e ai programmi STEM. Prima del ruolo attuale, ha ricoperto il ruolo di Senior Operational Risk e ISO manager per un'altra istituzione dell'UE. All'inizio della carriera, ha gestito IT Audit and Compliance per Sobey's, uno dei due rivenditori nazionali di generi alimentari in Canada e Audit, Corporate Development, M&A e strategie di crescita e IT Audit per George Weston, una delle più grandi società di trasformazione e distribuzione degli alimenti in Canada quotata in borsa.

metodi di crittografia quantum-resistant per proteggere le nostre infrastrutture critiche.

Introduzione

Negli ultimi anni, lo sviluppo del quantum computing ha rappresentato una pietra miliare significativa nel progresso tecnologico. L'immensa potenza di calcolo dei computer quantistici può rivoluzionare diversi settori, dallo sviluppo di nuovi farmaci alla modellazione finanziaria. Tuttavia, questo salto in avanti pone una sfida significativa alla cybersecurity, in quanto può potenzialmente compromettere la privacy e la sicurezza delle informazioni sensibili.



Il quantum computing può risolvere problemi complessi molto più rapidamente rispetto ai computer tradizionali, grazie all'elaborazione in parallelo delle informazioni. Questa potenza potrebbe rompere molti degli attuali algoritmi crittografici, utilizzati per la sicurezza della trasmissione e della conservazione dei dati. La sicurezza dei dati personali, come informazioni finanziarie e documentazioni sanitarie, può essere significativamente compromessa se soggetta ad attacchi da parte di computer quantistici. Le implicazioni sono vaste, dalla privacy personale alla sicurezza nazionale.

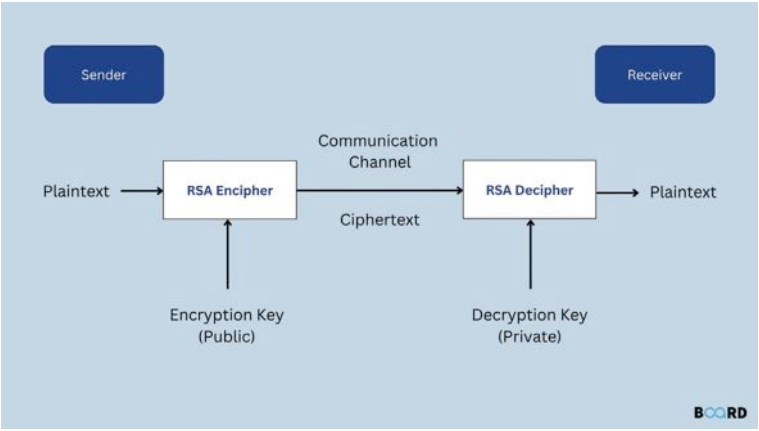
La crittografia quantistica è un campo emergente che offre una soluzione a queste sfide. Utilizza i principi della meccanica quantistica per proteggere i dati in modo che siano teoricamente impenetrabili agli attacchi, anche a quelli dei computer quantistici. La crittografia quantistica usa la proprietà fondamentale della meccanica quantistica secondo cui la misurazione di un sistema disturba il sistema stesso, e qualsiasi tentativo di intercettare una comunicazione quantistica lascerà inevitabilmente una traccia, avvisando il mittente e il destinatario.

La priorità per governi e organizzazioni di prepararsi all'era quantistica non può essere sottovalutata. Ciò include investire nella ricerca e nello sviluppo di algoritmi quantum-resistant e nell'aggiornamento delle infrastrutture di cybersecurity esistenti per far fronte alla minaccia quantistica. Molti paesi investono già molto nella tecnologia quantistica, compreso lo sviluppo di algoritmi crittografici quantum-resistant.

Lo sviluppo del quantum computing implica capacità di calcolo senza precedenti e significative sfide alla cybersecurity. I potenziali rischi per la sicurezza dei dati nell'era quantistica sono enormi ed è fondamentale comprendere queste sfide e le misure necessarie per mitigarli. La crittografia quantistica offre una soluzione promettente, ma richiederà investimenti e sviluppi significativi per essere ampiamente adottata. I governi e le organizzazioni devono agire, e molti lo hanno già fatto, per prepararsi all'era quantistica e proteggere il nostro futuro digitale

RSA (Rivest Shamir Adleman)

Approfondiamo le attuali modalità di lavoro. La crittografia RSA è una componente fondamentale per la sicurezza dell'e-commerce in quanto garantisce la riservatezza e l'integrità delle transazioni. Funziona secondo i principi della crittografia a chiave asimmetrica, che consente lo scambio sicuro di informazioni su Internet.



Per comprendere appieno la crittografia RSA, è essenziale comprenderne le basi teoriche. La Teoria dei Numeri Primi è il fondamento su cui si basa RSA. Questo principio afferma che la fattorizzazione di un grande numero nei suoi componenti primi è computazionalmente impegnativa. RSA si basa anche alla Funzione di Eulero, un concetto matematico fondamentale utilizzato per determinare la chiave privata.

Il processo di generazione delle chiavi di RSA prevede diverse fasi. Il processo inizia selezionando due grandi numeri primi casuali, p e q. Le dimensioni di questi numeri, in bit, influenzano direttamente la sicurezza dell'algoritmo RSA. Il modulo n viene calcolato moltiplicando p e q. Questo numero viene utilizzato sia nella chiave pubblica che in quella privata. Successivamente viene scelto un esponente pubblico, in genere un numero specifico, che garantisce sicurezza ed efficienza computazionale. Il calcolo della chiave privata viene effettuato utilizzando l'Algoritmo esteso di Euclide, che garantisce che d sia l'inverso moltiplicativo modulare di e. RSA utilizza un meccanismo di crittografia e decrittografia per garantire la sicurezza dei dati.

È importante sottolineare che RSA svolge un ruolo essenziale nella sicurezza delle transazioni di e-commerce. I dati della carta di credito e le informazioni personali vengono crittografati utilizzando la chiave pubblica del commerciante, rendendo i dati inaccessibili agli intercettatori.

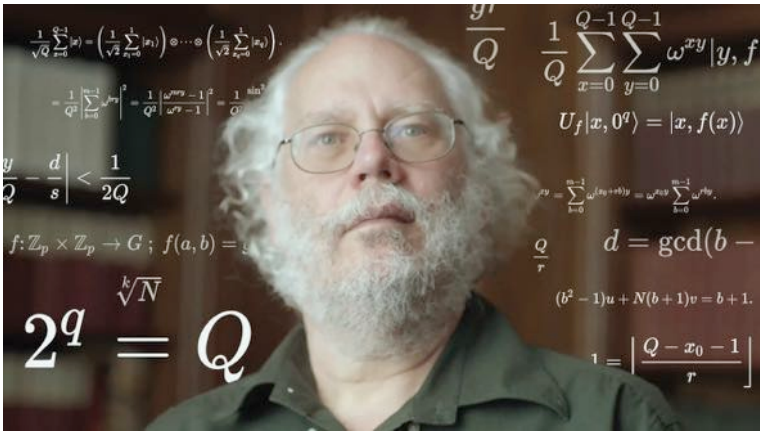
RSA garantisce inoltre che i dati inviati non vengano alterati durante il trasferimento, preservando l'integrità della transazione. Consente, inoltre, la creazione di firme digitali, che autenticano l'identità delle parti e assicurano che una parte non possa negare di aver inviato un messaggio. RSA è un elemento chiave dei protocolli come SSL/TLS utilizzati per proteggere le comunicazioni web nell'e-commerce.

La crittografia RSA deve affrontare diverse sfide contemporanee che richiedono ricerca e sviluppo continui. Una delle sfide è la scalabilità della sicurezza con le dimensioni della chiave. Le dimensioni maggiori delle chiavi sono necessarie per contrastare la crescente potenza computazionale, ma impattano sulle prestazioni. Il quantum computing è un'altra minaccia per la crittografia RSA. I computer quantistici potrebbero rompere la crittografia RSA fattorizzando efficientemente grandi numeri, portando alla creazione di algoritmi quantum-resistant. Si stanno studiando alternative alla crittografia RSA, come la Crittografia Post-Quantum.

Un po' di storia: Citazione doverosa - PhD, Peter Shor

Peter Shor, brillante matematico e scienziato computazionale americano, ha apportato contributi rivoluzionari all'entusiasmante campo del quantum computing in rapida evoluzione. Il suo risultato più noto è lo sviluppo dell'algoritmo di Shor nel 1994, che ha trasformato il modo in cui concepiamo la matematica computazionale e il quantum computing. L'algoritmo di Shor ha dimostrato che i computer quantistici potrebbero risolvere problemi in modo molto più efficiente rispetto ai computer classici, gettando le basi per una nuova era del computing.

Ha conseguito la laurea presso il prestigioso California Institute of Technology (Caltech) e il dottorato in matematica applicata presso il Massachusetts Institute of Technology (MIT), famoso in tutto il mondo, nel 1985. Dopo aver completato il dottorato, Shor ha intrapreso una straordinaria carriera nel campo della matematica e dell'informatica. Ha ricoperto incarichi presso i Bell Labs e successivamente al MIT, dove ha apportato contributi rivoluzionari nel campo emergente del quantum computing. Durante il periodo trascorso ai Bell Labs, ha sviluppato l'algoritmo che avrebbe portato il suo nome.



Algoritmo di Shor (1994):

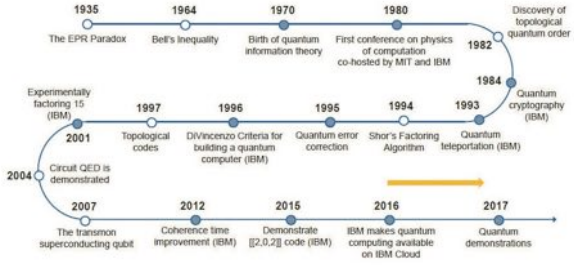
Nel 1994, Shor ha scoperto un algoritmo che poteva fattorizzare grandi numeri in modo esponenzialmente più veloce dei più noti algoritmi eseguiti sui computer classici. Si trattava di una scoperta rivoluzionaria, in quanto implicava che i computer quantistici avrebbero potuto decifrare sistemi di crittografia ampiamente utilizzati come RSA, che si basano sulla difficoltà di fattorizzazione di grandi numeri come base della loro sicurezza. L'algoritmo di Shor è ampiamente riconosciuto come uno dei principali sviluppi nel quantum computing, dimostrando un esempio chiaro e pratico del vantaggio del quantum.

Dopo il suo lavoro rivoluzionario sull'Algoritmo di Shor, Shor ha apportato significativi contributi alla computazione quantistica e alla teoria dell'informazione. Il suo lavoro gli ha valso numerosi premi e riconoscimenti.

Rimane una delle figure più influenti e rispettate nel quantum computing. Il suo lavoro pionieristico ha aperto nuove ed entusiasmanti strade per la matematica computazionale e ha suscitato un notevole interesse e investimento nella ricerca del quantum computing. Le applicazioni dell'Algoritmo di Shor hanno accelerato la ricerca nello sviluppo di sistemi crittografici quantum-resistant, un'area di studio in evoluzione di fronte al rapido progredire delle capabilities del quantum computing.

Il contributo di Shor nel campo del quantum computing è memorabile, in quanto evidenzia lo straordinario potenziale degli algoritmi quantistici per risolvere specifici problemi computazionali in modo molto più efficiente rispetto ai computer classici. Il suo lavoro ha ridefinito il panorama della sicurezza crittografica e ha indicato la strada verso un nuovo e ardito futuro per il computing.

Le tre rivoluzioni del Quantum



La meccanica quantistica, la branca della fisica che si occupa del comportamento della materia e dell'energia a livello atomico e subatomico, ha attraversato tre distinte rivoluzioni che hanno trasformato la nostra comprensione del mondo fisico e portato a rivoluzionari progressi tecnologici.

La prima rivoluzione quantistica ha messo in discussione le nozioni fondamentali della fisica classica e ha posto le basi per la teoria quantistica. Nel 1900, Max Planck propose la teoria quantistica, introducendo il concetto di quantizzazione dell'energia e la costante di Planck, che sono grandezze fondamentali nella meccanica quantistica. Cinque anni dopo, la descrizione

di Albert Einstein dell'effetto fotoelettrico diede credibilità alla teoria quantistica e introdusse il concetto del dualismo onda-particella, che prevede che la luce è composta da particelle o "fotoni".

La seconda rivoluzione quantistica, avvenuta a metà del secolo, è da considerarsi l'era delle tecnologie quantistiche. È stata contrassegnata da diverse invenzioni rivoluzionarie, tra cui il transistor, il primo laser e la tecnologia di risonanza magnetica (MRI). L'invenzione del transistor nel 1947 rivoluzionò l'elettronica, consentendo lo sviluppo di dispositivi più piccoli, più efficienti e più affidabili. Il primo laser, sviluppato da Theodore Maiman nel 1960, ha fornito uno strumento potente e preciso utilizzato in diversi campi, dalla chirurgia alle telecomunicazioni. Il lavoro pionieristico di Raymond Damadian nella tecnologia della risonanza MRI ha trasformato le diagnosi mediche, offrendo una visione dettagliata e non invasiva delle strutture interne del corpo.

La terza rivoluzione quantistica è la futura ingegneria del quantum, attualmente in corso. I ricercatori stanno lavorando per raggiungere la supremazia quantistica, dove i computer quantistici saranno in grado di risolvere problemi irrisolvibili per i computer classici. Aziende come IBM, Google e vari governi nazionali investono molto nella ricerca sul quantum computing. I computer quantistici promettono di rivoluzionare il modo in cui simuliamo le reazioni chimiche complesse, accelerando potenzialmente la scoperta di farmaci e la scienza dei materiali. I sensori quantistici offrono una precisione senza precedenti, utile in applicazioni come il monitoraggio dei terremoti, i sistemi di navigazione e le diagnosi mediche. Poiché il quantum computing minaccia i metodi crittografici attuali, si sta sviluppando una crittografia quantistica in grado di proteggere i dati da futuri attacchi quantistici. Basata su principi come l'entanglement quantistico, la comunicazione quantistica è pronta a creare canali di comunicazione sicuri e inviolabili dai mezzi convenzionali.

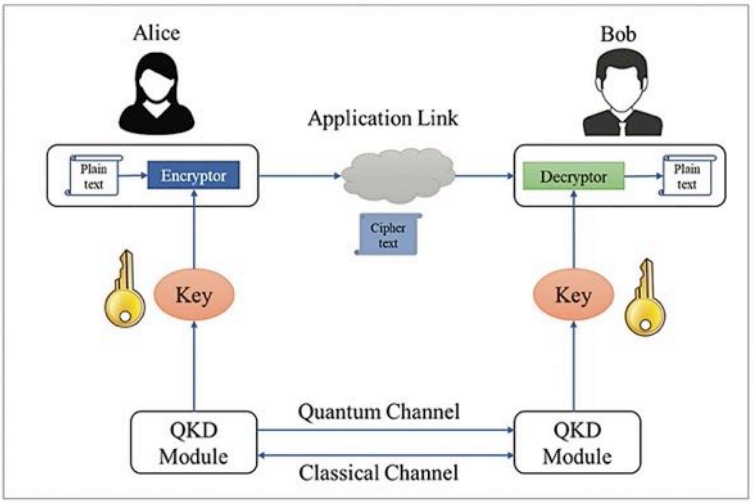
Le tre rivoluzioni quantistiche descrivono un passaggio dalla fisica teorica alle tecnologie trasformative che hanno rimodellato e continueranno a rimodellare il nostro mondo. Dall'inizio del XX secolo con pionieri come Planck e Einstein, passando per i progressi tecnologici di metà secolo nell'elettronica e nell'ottica, fino ad avventurarsi nel campo del quantum computing e delle comunicazioni sicure, la meccanica quantistica dimostra il suo impatto duraturo e il suo potenziale. Mentre ci immergiamo sempre più nel campo del quantum, ci troviamo di fronte a nuove scoperte che promettono di ridefinire i confini della tecnologia e della scienza.

Meccanica Quantistica

La sinergia tra meccanica quantistica, sicurezza e istruzione presenta sfide e opportunità uniche con implicazioni significative per la sicurezza dei dati. Lo sviluppo delle tecnologie quantistiche ha modificato il nostro approccio alla crittografia, alle tecnologie di comunicazione e all'istruzione.

Una delle sfide più significative poste dalla meccanica quantistica è il suo potenziale di rottura degli attuali algoritmi di crittografia basati sulla risoluzione di complessi problemi matematici. Gli algoritmi RSA ed ECC, ad esempio, potrebbero essere facilmente violati da computer quantistici utilizzando l'algoritmo di Shor. L'algoritmo di Shor consente di ridurre a zero le dimensioni delle chiavi RSA ed ECC con 2*N + 3 Qubit.

Tuttavia, la crittografia quantistica offre una potenziale soluzione a questo problema. La distribuzione di chiavi quantistiche (QKD) è un metodo sicuro per generare una chiave casuale segreta e condivisa tra due parti utilizzando i principi della meccanica quantistica. Si basa sull'entanglement quantistico, una proprietà per cui lo stato di una particella quantistica influenza istantaneamente un'altra, indipendentemente dalla distanza che la separa.



La meccanica quantistica sta rivoluzionando anche le tecnologie di comunicazione. Lo sviluppo di reti di comunicazione quantistica mira a creare sistemi sicuri contro gli attacchi quantistici, utilizzando i principi della meccanica quantistica per una trasmissione sicura dei dati. Tuttavia, l'attuale tecnologia di comunicazione quantistica deve affrontare delle sfide, come i limiti di distanza dovuti alla degradazione dello stato quantistico sui cavi in fibra ottica.

Con la diffusione della tecnologia quantistica, cresce l'esigenza di formazione sulla meccanica quantistica e sull'informatica che non riguardi la sola comunità scientifica. La tecnologia quantistica si interseca con vari campi come l'informatica, la matematica, la crittografia e l'ingegneria, rendendo necessario un approccio interdisciplinare alla formazione. L'aumento delle piattaforme di apprendimento online offre a professionisti e appassionati l'opportunità di apprendere il quantum computing e la crittografia. La formazione continua e l'autoapprendimento sono fondamentali per i professionisti che lavorano o si affidano alla sicurezza dei dati in questo campo in rapida evoluzione.

I ricercatori stanno sviluppando attivamente nuovi sistemi crittografici sicuri contro i computer quantistici, noti come crittografia post-quantum.

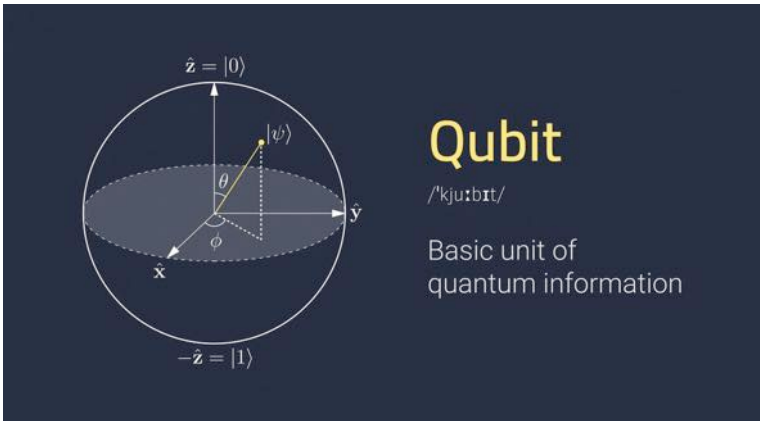
L'impiego delle tecnologie quantistiche solleva questioni etiche, in particolare per quanto riguarda la privacy e la protezione dei dati. I governi e gli organismi internazionali dovranno stabilire regolamenti e standard per l'utilizzo delle tecnologie quantistiche per garantire la sicurezza e la privacy a livello globale.

La convergenza della meccanica quantistica, della tecnologia delle comunicazioni e dell'imperativo di misure di sicurezza avanzate preannuncia una nuova era nella protezione dei dati. Il continuo adattamento delle strategie di sicurezza e dei framework formativi sarà fondamentale per affrontare le sfide e le opportunità presentate dai progressi quantistici. Solo attraverso l'apprendimento continuo e l'aggiornamento sugli ultimi sviluppi possiamo garantire la sicurezza dei nostri dati in questa nuova era.

Tecnologie di quantum computing

Come sappiamo, il quantum computing è un campo avvincente e in rapida evoluzione che utilizza i principi della meccanica quantistica per elaborare le informazioni in modi fondamentalmente diversi dall'informatica classica. Esploriamo ora le varie tecnologie di calcolo quantistico, ognuna con punti di forza e sfide uniche.

I loop superconduttori utilizzano anelli di materiale superconduttore raffreddati a temperature estremamente basse per consentire un comportamento quantistico con una resistenza minima. Questi qubit sono controllati tramite giunzioni Josephson e offrono operazioni logiche ad alta velocità, con tassi di successo che migliorano con i progressi dei metodi di correzione degli errori. Tuttavia, hanno tempi di coerenza relativamente brevi a causa della loro suscettibilità al rumore ambientale.



Gli ioni intrappolati, invece, utilizzano ioni intrappolati in un campo elettromagnetico, con informazioni quantistiche codificate nei livelli energetici di questi ioni. Questi qubit offrono tempi di coerenza più lunghi rispetto ai qubit superconduttori e forniscono porte quantistiche ad alta fedeltà. Sebbene funzionino più lentamente dei qubit superconduttori, mostrano tassi di successo e stabilità promettenti.

I punti quantici di silicio funzionano manipolando lo spin di elettroni o buchi confinati in una piccola regione all'interno di un substrato di silicio. Presentano tempi di coerenza relativamente lunghi a causa della bassa abbondanza naturale di isotopi portatori di spin nel silicio. Pur essendo ancora in fase di sviluppo, hanno dimostrato un potenziale significativo per il quantum computing scalabile con alti tassi di successo nelle operazioni logiche.

I qubit topologici si basano sui fermioni di Majorana, quasiparticelle che agiscono come antiparticelle. Il loro scopo è quello di codificare le informazioni in un modo meno soggetto a disturbi esterni, promettendo tempi di coerenza significativamente più lunghi grazie alla loro natura topologica. Sebbene siano ancora in gran parte teorici e nelle prime fasi sperimentali, i qubit topologici potrebbero rivoluzionare il quantum computing offrendo elevati tassi di successo nelle operazioni con correzione intrinseca degli errori.

Infine, le diamond vacancies prevedono l'utilizzo dei difetti dei reticoli del diamante, in particolare dei centri di vacancy dell'azoto, per creare qubit. Questi qubit offrono tempi di coerenza relativamente lunghi, anche a temperatura ambiente, il che li rende molto robusti. Sebbene i diamond vacancy qubit siano ancora nelle prime fasi di sviluppo, hanno mostrato risultati promettenti in termini di tassi di successo delle operazioni.

Con il proseguire della ricerca, l'ottimizzazione della longevità, le operazioni logiche e i tassi di successo tra queste tecnologie, saranno fondamentali per realizzare il pieno potenziale del quantum computing. Ognuna di queste tecnologie di calcolo quantistico ha i suoi punti di forza e le sue sfide, ed è emozionante vedere come avranno un impatto sul futuro del computing.

Le maggiori aziende tech

Il quantum computing è un campo in rapida evoluzione e le principali aziende tecnologiche come AWS, IBM, Google, Microsoft Azure e Alibaba Cloud sono all'avanguardia nello sviluppo di un ecosistema quantistico basato sul cloud. Questo ecosistema rappresenta un cambiamento di paradigma nell'accessibilità e nel progresso tecnologico, con computer quantistici progettati per essere cloud native. Ciò significa che possono essere accessibili a un pubblico più ampio, eliminando la necessità per i singoli utenti di disporre dell'infrastruttura fisica.

I principali attori dell'ecosistema quantistico basato sul cloud - AWS Braket, IBM Quantum, Google Cloud Quantum AI, Microsoft Azure Quantum e Alibaba Cloud

- offrono tutti un accesso unico, servizi e collaborazioni con altri provider di hardware quantistico. Ciò consente flessibilità nella sperimentazione e nella ricerca, rendendo la tecnologia più accessibile a diversi utenti.

I vantaggi di un ecosistema quantistico basato sul cloud includono:

- Riduzione dei costi.
- Democratizzazione della ricerca quantistica.
- Sviluppo di qubit ad alta fedeltà e di metodi efficaci di correzione degli errori.

Con l'evoluzione della tecnologia quantistica, l'attenzione si concentra sullo sviluppo di sistemi quantistici più affidabili e ad alta fedeltà, che aprono possibilità di calcolo senza precedenti.

L'ecosistema quantistico basato sul cloud favorisce la rapida innovazione e la collaborazione tra diversi settori e discipline, facilitando la crescita del quantum computing. Il futuro potrebbe portare a una maggiore integrazione del quantum computing con i servizi cloud tradizionali, offrendo soluzioni ibride per problemi computazionali complessi. Questa integrazione avrà un impatto significativo su diversi settore industriali, come quello farmaceutico, finanziario e della scienza dei materiali.

Tuttavia, l'avvento del quantum computing, combinato con tecnologie informatiche sempre più sofisticate, presenta rischi significativi per la sicurezza. Di conseguenza, per affrontare le minacce emergenti in un mondo digitale è necessario un approccio proattivo alla cybersecurity, che viene continuamente perfezionato e aggiornato in base all'evoluzione della tecnologia.

Le minacce

I computer quantistici rappresentano una minaccia significativa per il mondo digitale. Queste macchine avanzate hanno il potenziale per rompere molti degli algoritmi crittografici che proteggono la sicurezza digitale, rendendoli obsoleti. Anche se non esistono ancora computer quantistici su vasta scala in grado di compiere tali imprese, l'incertezza sui tempi del loro sviluppo rende indispensabile l'adozione di misure proattive di cybersecurity.

I metodi di crittografia asimmetrica, ampiamente utilizzati per le comunicazioni sicure su Internet, sono particolarmente vulnerabili agli attacchi quantistici. Sebbene anche gli algoritmi crittografici simmetrici siano a rischio, sono generalmente considerati più resistenti agli attacchi quantistici, anche se le dimensioni delle chiavi potrebbero dover aumentare per garantire un contesto di sicurezza «future-proof».

Lo stato attuale della tecnologia informatica ha assistito all'evoluzione di attacchi informatici altamente sofisticati, tra cui la guerra cibernetica state-sponsored, il ransomware e lo spionaggio. Le tecnologie informatiche vengono sempre più utilizzate come armi per ottenere vantaggi geopolitici, spionaggio aziendale e danneggiamento delle infrastrutture critiche.

La combinazione di attacchi informatici avanzati con capacità di quantum computing potrebbe aumentare la gravità e l'impatto delle minacce informatiche. Gli attaccanti potrebbero attualmente raccogliere dati criptati con l'intenzione di decriptarli in futuro utilizzando i computer quantistici. La velocità di sviluppo dei computer quantistici potrebbe accrescere le minacce informatiche esistenti, riducendo la possibilità di affrontare queste vulnerabilità.

Il quantum computing potrebbe alterare le dinamiche di potere della cybersecurity globale, con un impatto sulla sicurezza nazionale e sulle relazioni internazionali. Il settore finanziario, che si avvale della crittografia per la sicurezza delle transazioni, potrebbe essere esposto a rischi significativi da parte di attaccanti con capacità computazionale.

Per proteggersi dalle future minacce legate all'informatica quantistica, è in corso uno sforzo per sviluppare e standardizzare algoritmi crittografici quantum-resistant. La combinazione di algoritmi quantum-resistant e degli attuali metodi crittografici potrebbe offrire una soluzione di sicurezza transitoria. Le organizzazioni e i governi dovrebbero iniziare, e in alcune parti del mondo hanno già iniziato, a passare alla crittografia quantum-resistant il prima possibile e non dopo. Sarà fondamentale stabilire standard globali e politiche di cooperazione in materia di tecnologia quantistica e cybersecurity.

La sinergia tra il computing quantistico e la weaponization delle tecnologie informatiche ha portato a un cambiamento radicale nella cybersecurity. Questa convergenza non solo amplifica le minacce esistenti, ma introduce sfide nuove e anche più complesse, sottolineando la necessità di misure proattive nello sviluppo e nell'implementazione di soluzioni crittografiche quantum-resistant. Mentre navighiamo in questo territorio nuovo e inesplorato, diventa sempre più evidente che un approccio collaborativo e lungimirante è in grado di salvaguardare la sicurezza digitale nell'era quantistica.

"Memorizzare" [rubare] ora, decriptare in futuro": il problema della raccolta

Con l'avanzare dell'era digitale, il concetto di "memorizzare ora, decifrare dopo" è diventato una priorità per la cybersecurity, in particolare con l'imminente avvento del quantum computing. Sebbene i computer quantistici pienamente operativi non siano ancora una realtà (o forse sì?), diverse realtà, comprese le nazioni, stanno già raccogliendo dati criptati protetti da RSA e altri metodi di crittografia, prevedendo di decriptarli una

volta che il quantum computing sarà diventato una realtà. Questa strategia di raccolta di dati criptati per decriptarli in futuro rappresenta una minaccia significativa per la sicurezza a lungo termine, soprattutto per i dati sensibili come i segreti di Stato, la proprietà intellettuale e le informazioni personali.

Si prevede che i computer quantistici siano in grado di fattorizzare grandi numeri in modo efficiente, un aspetto fondamentale dell'RSA e di metodi crittografici simili, diventando così una minaccia significativa per gli attuali standard di crittografia. Tuttavia, la tempistica effettiva per lo sviluppo di computer quantistici in grado di decifrare gli attuali standard di crittografia è ancora in fase di definizione, il che aggiunge complessità alla gestione della cybersecurity.

Diversi Paesi sono attivamente impegnati nello spionaggio informatico, cercando di raccogliere grandi quantità di dati criptati nella speranza di decifrarli in futuro con il quantum computing. Questa attività potrebbe causare un'alterazione radicale delle dinamiche della cybersecurity globale, consentendo potenzialmente l'accesso per decenni a dati sensibili.

Per mitigare il rischio di «memorizzare ora, decriptare dopo», è urgente passare a metodi crittografici quantum-resistant. La crittografia post-quantum (PQC) prevede lo sviluppo di sistemi crittografici sicuri contro le minacce computazionali sia quantistiche che classiche. Tuttavia, la transizione alla crittografia QR è complessa e richiede un'adozione tempestiva per garantire la sicurezza a lungo termine dei dati. Stabilire e aderire a standard globali per la crittografia QR è fondamentale per una risposta coesa ed efficace alla minaccia del quantum.

Le organizzazioni e i governi dovrebbero valutare i loro attuali sistemi crittografici e pianificare la transizione al PQC in modo graduale. È essenziale comprendere il ciclo di vita dei dati sensibili e implementare soluzioni crittografiche QR fin dalle prime fasi. La cooperazione globale nello sviluppo e nella standardizzazione della crittografia QR è necessaria per affrontare la sfida collettiva posta dal quantum computing.

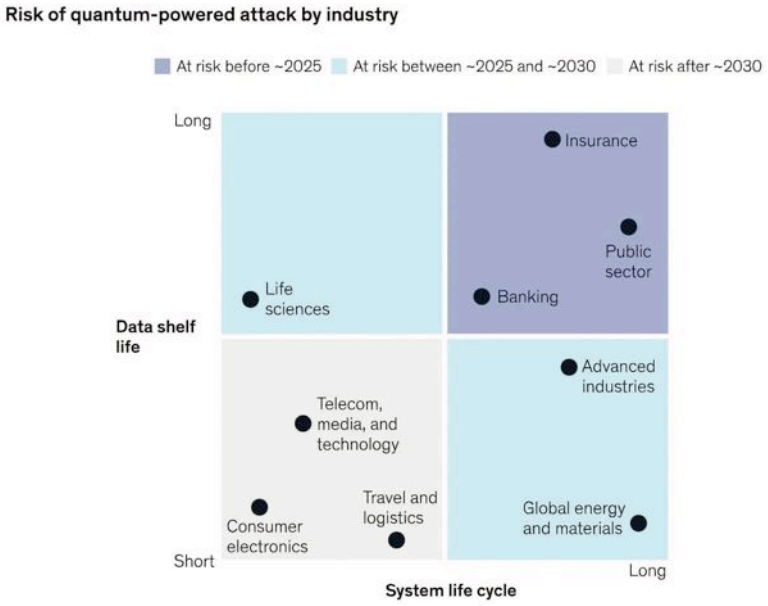
La strategia «memorizza ora, decripta dopo» rappresenta un rischio significativo e incombente nella cybersecurity, favorito dai progressi del quantum computing. La transizione verso una crittografia quantum-resistant è una prevenzione e una necessità per proteggere i dati sensibili dalla futura decrittazione abilitata dai quanti. Gli sforzi proattivi e collaborativi per aggiornare e standardizzare le pratiche crittografiche sono fondamentali per proteggere i dati dalle minacce quantistiche di domani.

Quantum e NIST

La comparsa del quantum computing rappresenta una minaccia significativa per gli attuali standard crittografici ed è una sfida che le organizzazioni di tutto il mondo stanno affrontando. Il National Institute of Standards and Technology (NIST) degli Stati Uniti è fondamentale per guidare la transizione verso metodi crittografici quantum-resistant. Le iniziative del NIST esaminano la risposta globale alle minacce quantistiche ed esplorano le potenziali implicazioni per gli standard crittografici come RSA e la crittografia a curva ellittica.

Il NIST è all'avanguardia nello sviluppo di standard resistenti alla quantistica. Ha guidato un'iniziativa per sviluppare e standardizzare gli algoritmi di crittografia post-quantum (PQC). Questo processo prevede un controllo, un test e una standardizzazione rigorosi degli algoritmi in grado di resistere agli attacchi del quantum computing. L'impegno del NIST non si limita agli Stati Uniti, ma collabora con esperti e istituzioni internazionali per garantire un approccio globale e unificato alla PQC.

Il NIST fornisce anche indicazioni e risorse alle organizzazioni per aiutarle a pianificare e a passare a sistemi crittografici quantum-resistant. Uno dei ruoli essenziali del NIST è quello di formare le parti interessate sui rischi quantistici e sulla necessità di adottare tempestivamente soluzioni PQC.



Il governo degli Stati Uniti e il NIST stanno investendo attivamente nella scienza dell'informazione quantistica e nella ricerca sulla sicurezza, ponendo l'accento sullo sviluppo di tecnologie quantum-resistant. La National Quantum Initiative, un'iniziativa che mira ad accelerare la ricerca e lo sviluppo in campo quantistico, compresi gli aspetti della cybersecurity, è una testimonianza di questo approccio proattivo.

L'Europa ha lanciato il programma Quantum Flagship, investendo molto nelle tecnologie quantistiche, tra cui la crittografia quantistica e la ricerca sulle comunicazioni. Gli enti e gli istituti di ricerca europei collaborano con il NIST e altri organismi internazionali per allineare i loro standard crittografici alle norme globali emergenti.

Come già affrontato, l'avvento del quantum computing rappresenta una minaccia significativa per i metodi di crittografia comunemente utilizzati, come l'RSA e la crittografia a curva ellittica. L'RSA si basa sulla difficoltà di fattorizzare grandi numeri, mentre la crittografia a curva ellittica si basa sulla complessità di risolvere problemi di logaritmi discreti a curva ellittica. Gli algoritmi di calcolo quantistico possono facilmente violare questi metodi di crittografia, rendendoli vulnerabili agli attacchi.

Per affrontare questa sfida, è necessario passare ad algoritmi sicuri sia contro le minacce quantistiche sia quelle dell'informatica classica. Questa transizione comporta l'adozione di nuovi metodi crittografici come la crittografia lattice-based, la crittografia hash-based e altri che il NIST sta attualmente valutando.

Si raccomanda alle organizzazioni di valutare la propria infrastruttura crittografica e di iniziare la transizione agli algoritmi di crittografia post-quantum (PQC). Con l'evoluzione delle tecnologie quantistiche, il monitoraggio e l'aggiornamento continui delle pratiche crittografiche saranno fondamentali per garantire l'integrità dei dati. Anche la ricerca e lo sviluppo continui sono necessari per essere all'avanguardia rispetto alle potenziali minacce.

In collaborazione con iniziative internazionali negli Stati Uniti e in Europa, il NIST sta guidando gli sforzi per prepararsi all'era del quantum computing. La transizione verso una crittografia quantum-resistant è un aggiornamento tecnico e un'evoluzione necessaria per salvaguardare l'integrità dei dati nell'era del quantum. La sinergia tra ricerca, standardizzazione e formazione sarà essenziale per orientarsi in questo nuovo panorama crittografico e garantire un futuro digitale sicuro.

Con la continua evoluzione della tecnologia del quantum computing, il campo della cybersecurity si trova ad affrontare nuove minacce che mettono a rischio le informazioni sensibili. Per affrontare questa sfida, cresce l'esigenza di una crittografia post-quantum (PQC) per creare sistemi crittografici che rimangano sicuri nonostante le capacità di calcolo quantistico. Inoltre, architetture di sicurezza robuste come la Zero Trust Architecture sono diventate sempre più importanti per la sicurezza dei dati.

Per guidare gli sforzi contro le minacce quantistiche, il National Security Memorandum degli Stati Uniti del gennaio 2022 e la Commercial National Security Algorithm Suite (CNSA) sono fondamentali. Il memorandum sottolinea l'urgenza di prepararsi a standard crittografici quantum-resistant per salvaguardare la sicurezza nazionale. Fornisce direttive alle agenzie federali per valutare i rischi e prepararsi alla transizione verso una crittografia quantum-resistant. La suite CNSA delinea gli standard crittografici per proteggere le informazioni dei sistemi di sicurezza nazionale degli Stati Uniti fino al livello top-secret.

Zero Trust è un paradigma di cybersecurity che opera secondo il principio del minimo privilegio, verificando ogni richiesta di accesso indipendentemente dalla provenienza per garantire l'assenza di fiducia implicita. In un panorama in cui il quantum computing potrebbe mettere in crisi la crittografia tradizionale, Zero Trust potrebbe offrire un ulteriore livello di sicurezza grazie all'autenticazione e a controlli di accesso rigorosi continui.

Sebbene l'Advanced Encryption Standard (AES) con chiavi a 256 bit sia attualmente uno dei metodi di crittografia più sicuri, in quanto offre una forte resistenza agli attacchi computazionali classici, è vulnerabile agli attacchi quantistici. Allo stesso modo, l'Elliptic Curve Diffie-Hellman (ECDH) e l'Elliptic Curve Digital Signature Algorithm (ECDSA) con curva P-384 sono ampiamente utilizzati rispettivamente per lo scambio sicuro di chiavi e per le firme digitali, ma sono anch'essi vulnerabili agli attacchi quantistici. Per questo motivo, il passaggio a PQC è necessario per garantire la sicurezza dei dati.

L'algoritmo SHA-2 (Secure Hash Algorithm-2) con 384 bit viene utilizzato per l'hashing sicuro, fornendo integrità e autenticazione dei dati. Lo scambio di chiavi Diffie-Hellman con un modulo minimo di 3072 bit offre un alto livello di sicurezza contro gli attacchi classici, ma deve evolversi per resistere alle tecniche di decrittazione quantistica, proprio come RSA.

Per rispondere efficacemente alle sfide poste dal quantum computing, sarà necessario stabilire standard globali e sforzi di collaborazione nel campo della cybersecurity. È importante notare che la convergenza dell'architettura PQC e Zero Trust rappresenta un approccio proattivo alla cybersecurity.

La crittografia post-quantum (PQC) è attualmente all'avanguardia nella sicurezza delle comunicazioni digitali contro la minaccia emergente del quantum computing. Questo campo esplora vari approcci crittografici che si ritiene resistano agli attacchi quantistici. Inoltre, è importante comprendere il concetto di funzioni trapdoor nelle infrastrutture a chiave pubblica, in particolare nel contesto della PQC.

Mentre il mondo si prepara all'era del quantum, la necessità di standard crittografici quantum-resistant robusti diventa sempre più urgente. Il National Security Memorandum degli Stati Uniti e la suite del CNSA sottolineano l'importanza di questa transizione. L'integrazione di metodi crittografici avanzati con architetture di sicurezza robuste sarà fondamentale

per salvaguardare le informazioni sensibili dalle minacce quantistiche emergenti.

Nel complesso, l'evoluzione del quantum computing rappresenta una minaccia crescente per la cybersecurity. Per affrontare questa minaccia, le organizzazioni e i governi devono iniziare presto a passare alla Crittografia Post-Quantum (PQC), seguendo le linee guida del NIST e gli standard internazionali. Inoltre, la ricerca e lo sviluppo costanti di algoritmi quantum-resistant saranno fondamentali per essere all'avanguardia rispetto alle potenziali minacce quantistiche che potremmo trovarci ad affrontare.

Approcci PQC

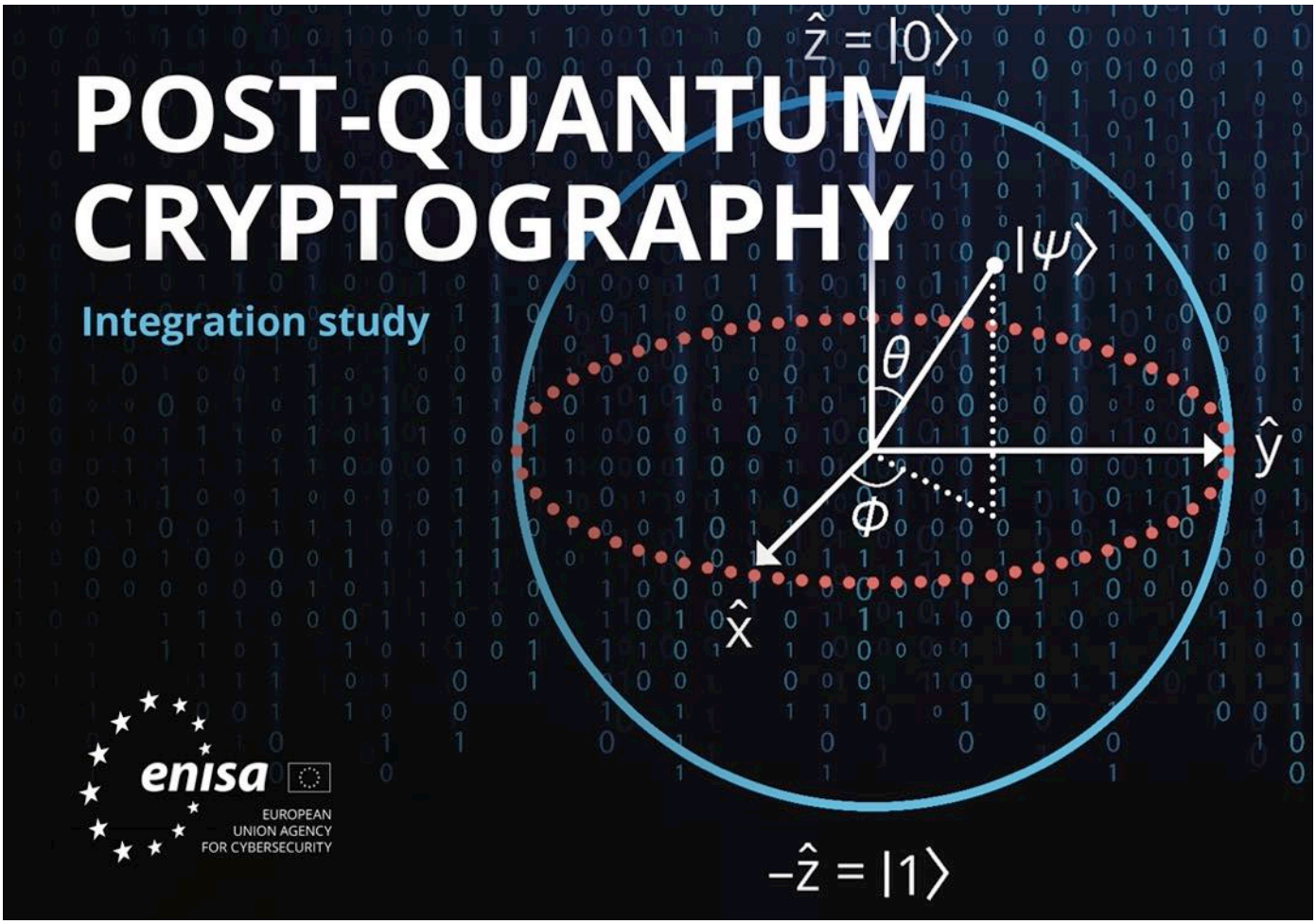
I sistemi crittografici tradizionali su cui si basa la sicurezza delle comunicazioni digitali stanno diventando sempre più vulnerabili. Per affrontare questa sfida, sono stati sviluppati approcci Crittografia Post-Quantum (PQC) per garantire la sicurezza contro gli attacchi classici e quantistici.

Uno degli approcci più promettenti alla PQC è la crittografia basata sui reticoli, che si basa sulla robustezza dei problemi reticolari. Questo approccio viene utilizzato per lo scambio di chiavi, le firme digitali e la crittografia completamente omomorfa. Gli Error Correction Codes sono un altro approccio che utilizza i principi dei codici correttori di errore per creare sistemi crittografici. Questi codici possono essere progettati per proteggere dalle minacce quantistiche, soprattutto nella trasmissione di dati su canali inaffidabili o compromessi.

Le Isogenies Between Elliptic Curves sono un altro approccio che offre una soluzione promettente ai meccanismi di scambio di chiavi quantum-resistant. Si basa sulla difficoltà computazionale di trovare isogenie (mappature che preservano la struttura) tra curve ellittiche. La crittografia basata su hash è un altro approccio PQC che utilizza funzioni hash sicure per creare firme digitali. In base alle conoscenze attuali, il quantum computing non indebolisce in modo significativo le funzioni hash, rendendole un candidato forte per la PQC.

La Crittografia Multivariata è un approccio che prevede la risoluzione di sistemi di equazioni polinomiali multivariate, un problema difficile sia per i computer classici che per quelli quantistici. Viene utilizzata principalmente per costruire firme digitali e schemi di crittografia.

Le funzioni trapdoor sono state identificate come il fondamento della crittografia a chiave pubblica, consentendo la creazione di un'infrastruttura sicura a chiave pubblica. Una funzione trapdoor è una funzione facile da calcolare in una direzione, ma difficile da invertire a meno che non si conoscano informazioni segrete specifiche (la "trapdoor"). Nella crittografia a chiave pubblica, un utente genera una coppia di chiavi - una



chiave pubblica e una chiave privata. La chiave pubblica è derivata dalla chiave privata utilizzando una funzione trapdoor. Chiunque può crittografare un messaggio utilizzando la chiave pubblica, ma solo il possessore della chiave privata può decifrarlo in modo efficiente, poiché possiede la conoscenza della trapdoor.

Nel contesto della PQC, le funzioni trapdoor devono essere scelte in modo da rimanere difficilmente invertibili anche con le capacità di calcolo quantistico. Garantire la sicurezza delle infrastrutture a chiave pubblica nell'era del quantum implica l'identificazione e l'utilizzo di funzioni trapdoor quantum-resistant, un'area di interesse chiave nella ricerca PQC.

Lo sviluppo di approcci PQC e di funzioni trapdoor è fondamentale per prepararsi alle sfide poste dal quantum computing. La ricerca e lo sviluppo continui in queste aree sono fondamentali per il futuro delle comunicazioni digitali sicure.

Inoltre, l'avvento del quantum computing ha reso necessario lo sviluppo di soluzioni crittografiche quantum-resistant per proteggere queste comunicazioni da potenziali attacchi. Tra le soluzioni più promettenti ci sono il Learning with Errors (LWE) e il Ring Learning with Errors (Ring-LWE), che consentono di resistere agli attacchi del quantum computing e di essere versatili nell'ambito delle applicazioni crittografiche.

Il Learning with Errors (LWE) si basa sulla complessità computazionale della risoluzione di equazioni lineari perturbate dal rumore. Si tratta di creare un sistema di equazioni lineari in cui la soluzione è oscurata da errori casuali, rendendo la soluzione computazionalmente impegnativa. LWE può essere utilizzato per costruire una serie di primitive crittografiche, tra cui la crittografia, lo scambio di chiavi e la crittografia completamente omomorfa. Tuttavia, gli schemi crittografici che utilizzano l'LWE spesso richiedono chiavi di grandi dimensioni e overhead computazionale, limitando le implementazioni pratiche. Per superare questa limitazione, la ricerca in corso si concentra sull'ottimizzazione delle implementazioni LWE per renderle più pratiche per le applicazioni reali.

Il Ring Learning with Errors (Ring-LWE) è una variante più avanzata di LWE che utilizza anelli polinomiali per semplificare la struttura del problema LWE. Questo approccio offre implementazioni più efficienti riducendo la complessità e la dimensione delle chiavi e dei calcoli coinvolti. Ring-LWE è considerato resistente agli attacchi quantistici e ha prestazioni migliori di LWE, il che lo rende più adatto alle applicazioni crittografiche pratiche. Tuttavia, la sicurezza di Ring-LWE si basa su alcune ipotesi sulla durezza dei problemi negli anelli polinomiali, che sono ancora oggetto di ricerca e validazione. Ulteriori ottimizzazioni e standardizzazioni di Ring-LWE sono necessarie per garantirne l'ampia adozione e l'efficacia in varie applicazioni.

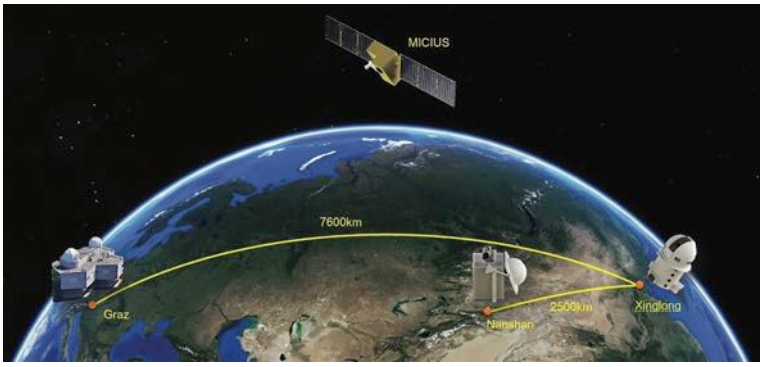
Mentre LWE offre un approccio più generale, Ring-LWE è spesso preferito per le applicazioni pratiche grazie alla sua maggiore efficienza. Tuttavia, la scelta tra i due dipende dai casi d'uso specifici e dai requisiti di sicurezza. Sia LWE che Ring-LWE hanno un potenziale significativo nel panorama della crittografia post-quantum. Per questo motivo, la loro adozione e il loro sviluppo svolgeranno probabilmente un ruolo cruciale nella transizione verso sistemi crittografici quantum-resistant.

Il Learning with Errors (LWE) e il Ring Learning with Errors (Ring-LWE) rappresentano approcci all'avanguardia per lo sviluppo di soluzioni di crittografia post-quantum. Le loro proprietà quantum-resistant e la loro flessibilità di applicazione li rendono candidati principali per la sicurezza delle comunicazioni digitali contro le minacce quantistiche. Nonostante le sfide in termini di prestazioni e ottimizzazione, le attività di ricerca e sviluppo in corso ne migliorano continuamente la fattibilità per l'implementazione nel mondo reale, rendendole tecnologie fondamentali nell'era post-quantum.

Mondo e QKD

La Distribuzione di Chiavi Quantistiche (QKD) è una tecnologia che stabilisce canali di comunicazione sicuri utilizzando i principi della meccanica quantistica. Questa tecnologia è diventata un punto essenziale nella corsa globale verso comunicazioni sicure dal punto di vista quantistico, in quanto nazioni importanti come la Cina, gli Stati Uniti, l'Europa e altre stanno investendo molto su di essa. Ciascuno di questi Paesi, insieme a Singapore, Russia, Canada e Giappone, sta sviluppando iniziative uniche per sfruttare il potenziale della QKD e garantire canali di rete sicuri contro la minaccia incombente del quantum computing.

Con il lancio del satellite Micius, la Cina ha fatto passi da gigante nel campo della QKD. Questo satellite facilita la comunicazione quantistica sicura su lunghe distanze. Oltre alle iniziative spaziali, la Cina sta sviluppando anche ampie reti QKD a terra per creare un'infrastruttura sicura dal punto di vista quantistico.



Gli Stati Uniti hanno intensificato la ricerca quantistica attraverso varie agenzie governative e collaborazioni con il settore privato. Questa ricerca si concentra sia sul QKD che sulla crittografia post-quantum. La National Quantum Initiative sottolinea l'impegno del Paese a far progredire le tecnologie nazionali, compresi i sistemi di comunicazione quantistica sicuri. In Europa, il programma Quantum Flagship investe in modo significativo nelle tecnologie quantistiche, con diversi progetti dedicati allo sviluppo di sistemi QKD. I Paesi europei sono anche impegnati in sforzi di ricerca

collaborativi per creare e distribuire reti di comunicazione sicure dal punto di vista quantistico.

Singapore ha avviato un programma spaziale quantistico basato sul QKD. Il CQT della NUS sta sviluppando l'esperimento SPEQS, basato sulla tecnologia QKD e conforme allo standard CubeSat. SpooQy-1, un CubeSat 3U, dimostrerà una sorgente di luce quantistica compatibile con lo spazio per aumentare il TRL delle future reti QKD globali. Il QKD genera chiavi di crittografia private che vengono condivise solo tra due parti. I principi della meccanica quantistica sono utilizzati per garantire la privacy e per eliminare le chiavi che potrebbero essere state intercettate. Gli schemi QKD basati sull'entanglement quantistico forniscono forti garanzie di privacy e casualità.

L'agenzia spaziale russa Roscosmos ha annunciato l'intenzione di sviluppare sistemi di comunicazione quantistica per stabilire canali di comunicazione sicuri nello spazio.

Il Canada sta facendo progressi nelle comunicazioni quantistiche con il progetto QUEYSSAT, che si concentra sulla creazione di collegamenti di comunicazione abilitati alla QKD.

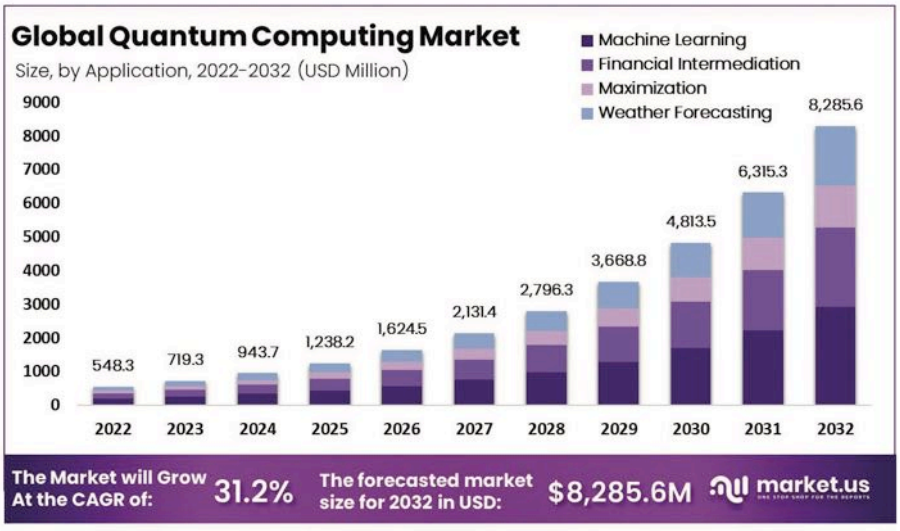
La European Quantum Communication Infrastructure (EuroQCI) rappresenta uno sforzo collaborativo per costruire un'infrastruttura di comunicazione quantistica all'avanguardia e altamente sicura che collegherà tutti gli Stati membri dell'Unione europea e i loro territori oltreoceano. L'iniziativa mira a creare una rete altamente resistente alle intercettazioni e agli hackeraggi, garantendo la privacy e la sicurezza di tutte le comunicazioni che vi transitano. L'EuroQCI è pronta a rivoluzionare le comunicazioni all'interno dell'UE, fornendo una base per la futura innovazione e crescita territoriale.

Socrates è un'entusiasmante missione microsatellitare lanciata dal National Institute of Information and Communications Technology (NICT) di Koganei, Tokyo, Giappone. Questa missione innovativa mira a dimostrare e convalidare il funzionamento dello Small Optical TrAnsponder (SOTA), un sistema di comunicazione laser progettato per lo spazio. Con le tecniche di Distribuzione di Chiavi Quantistiche (QKD), la missione cerca di sperimentare nuovi e avanzati metodi di comunicazione sicura. La missione si concentra anche sulla diffusione di comunicazioni ottiche nello spazio libero in microsatelliti e, eventualmente, in nanosatelliti. Queste comunicazioni ottiche offrono una velocità di trasmissione dati più elevata rispetto alle comunicazioni RF convenzionali, rendendole una tecnologia di comunicazione più efficiente e avanzata per lo spazio. Con questa missione, il NICT spera di aprire la strada a sistemi di comunicazione spaziale più avanzati e sicuri.

L'investimento globale nella distribuzione di chiavi quantistiche riflette il bisogno comune di sistemi di comunicazione sicuri dal punto di vista quantistico. Nazioni come la Cina, gli Stati Uniti, l'Europa, Singapore, la Russia, il Canada e il Giappone stanno contribuendo a questo campo, sfruttando le loro capacità e risorse uniche. Questi sforzi, che vanno dalle reti terrestri alle sofisticate missioni spaziali, sottolineano l'importanza strategica della QKD nel mantenere canali di comunicazione sicuri nell'imminente era del quantum. Con lo sviluppo di queste tecnologie, esse promettono di ridefinire il panorama della sicurezza delle comunicazioni globali, consentendo canali di comunicazione sicuri e resistenti ai tentativi di hacking, compresi quelli provenienti da sistemi informatici basati sulla quantistica.

Conclusioni

Le tecnologie quantistiche avranno un impatto profondo su diversi campi, in particolare sulla cybersecurity, sulla crittografia e sul panorama digitale emergente. L'articolo ha affrontato vari argomenti, come il ruolo della crittografia RSA, le sfide poste dal quantum computing e lo sviluppo moderno della meccanica quantistica. La nascita di piattaforme di quantum computing basate su cloud da parte delle principali aziende tecnologiche è in corso, sottolineando la democratizzazione e il potenziale. Il rischio cyber rappresentato dall'archiviazione dei dati crittografati che in futuro potrebbero essere decifrati con il quantum computing non può essere ignorato, sottolineando l'urgenza di una crittografia quantum-resistant. Abbiamo approfondito vari approcci alla crittografia post-quantum e gli sforzi globali nello sviluppo delle tecnologie QKD. Nel complesso, ho cercato di evidenziare la necessità di misure proattive, di ricerca e di collaborazione per affrontare le sfide e le opportunità poste dalle tecnologie quantistiche.



Il quantum è presente e il settore è in crescita. I computer quantistici saranno in grado di violare la crittografia e i nostri dati sono già vulnerabili. La preparazione è fondamentale, quindi è necessario creare consapevolezza, effettuare l'audit dei sistemi attuali per individuare eventuali punti deboli e pianificare la transizione post-quantum. ■

Il mercato assicurativo italiano sempre più dedicato alla copertura del rischio cyber.

Autore: Annamaria Damiani

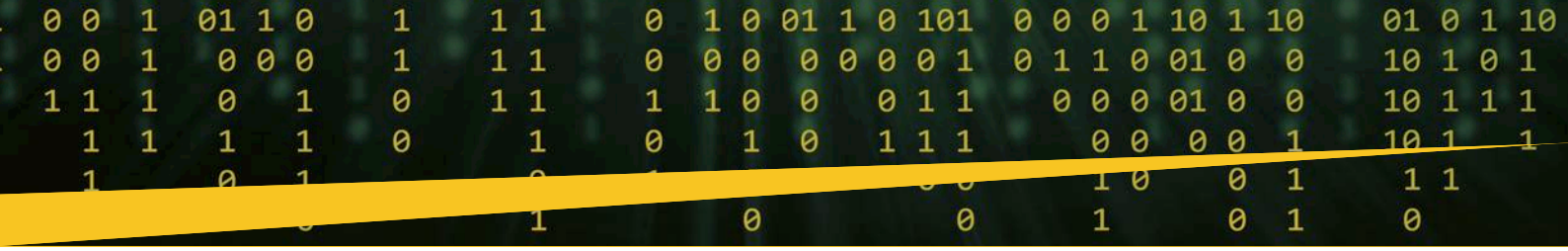
L'utilizzo del *web* scandisce il nostro quotidiano. Un acquisto, una ricerca, una ricarica telefonica, una prenotazione alberghiera, un bonifico sono alcune delle numerose operazioni che grazie allo sviluppo tecnologico oggi riusciamo a fare dalla poltrona di casa. Inutile dire che i benefici sono numerosi: basta pensare al risparmio di tempo. Le imprese utilizzano il *web* per le più svariate attività. Pensiamo alle transazioni commerciali e al loro regolamento. Sono tutte operazioni attraverso le quali riversiamo sul *web* una miriade di informazioni personali e sensibili, attraverso le quali comunichiamo abitudini, stili di vita, desideri e tanto altro. L'informazione che veicoliamo in questo contenitore è un valore in sé e proprio per questo attira l'attenzione e l'interesse di possibili malfattori.

Se da una parte, come si diceva, i benefici sono enormi, anche in termini di accorciamento delle distanze, dall'altra sempre più aumenta il rischio di possibili attacchi informatici, cadute di linea, perdite e sottrazioni di dati, raggiri, operazioni fraudolente, truffe *online*. Insomma, il rischio *cyber*. Da qui l'aumentata attenzione alla sicurezza informatica da parte di imprese, cittadini, pubblica amministrazione e l'accresciuta consapevolezza di dover accedere a qualche forma di protezione dal rischio *cyber*. Proprio per conoscere qual è la risposta del mercato a questo tipo di esigenza dei consumatori, quali polizze assicurative vengono proposte alla clientela e con quali caratteristiche, IVASS ha realizzato l'indagine sulle c.d. *"polizze cyber"* presenti sul mercato italiano al 30 luglio 2023, per clienti *retail* e Piccole e Medie Imprese (PMI) [1].

L'indagine

L'indagine ha riguardato **50 polizze**, di cui 26 rivolte alle **PMI e le altre al *retail***, sia come **prodotti *stand alone (disegnate per la copertura di un rischio specifico)*** che **di tipo modulare** (offrono un'ampia gamma di garanzie, a copertura della persona o dei beni, variamente combinabili fra loro e in cui la copertura *cyber* è opzionabile, da acquistare in abbinamento ad altre garanzie. Si tratta di polizze in cui la copertura cyber è di portata contenuta).

Le polizze per le PMI, in prevalenza *stand alone* e standardizzate, offrono coperture per i danni pecuniari subiti dall'azienda a seguito dell'attacco informatico, per quelli causati a terzi per effetto dell'attacco medesimo (coperture per **responsabilità civile**) e per le spese legali collegate a cause giudiziarie derivanti dall'evento assicurato. Solitamente le polizze prevedono **garanzie di base** alle quali spesso vengono affiancate coperture, cosiddette **accessorie, che proteggono** l'assicurato per vulnerabilità esistenti anche prima di un attacco informatico e nella gestione *post*-evento (in quest'ultimo



caso, ad esempio, per il ripristino dell'operatività informatica o la gestione del danno reputazionale).

Nelle coperture offerte alla **clientela *retail* prevale**, invece, la polizza di tipo modulare.

Le coperture spesso possono essere estese all'intero nucleo familiare e riguardano, come per quelle offerte alle imprese, le **perdite pecuniarie** (danni diretti all'assicurato), la **responsabilità civile** (danni a terzi), la **tutela legale** per vertenze derivanti dall'evento assicurato, in diversi casi accompagnate dall'**assistenza alla persona**.

Le polizze offerte a singoli e famiglie, **molto frequentemente**, assicurano i danni conseguenti a furto o clonazione di carte di credito/debito e prepagate, truffe subite *online*, furto di identità digitale. Spesso all'assicurato viene fornita **assistenza telefonica e digitale**, ad esempio attraverso l'intervento di tecnici per il ripristino della piena operatività dei *device* o nei casi di **frodi nella prenotazione *online* di un viaggio all'estero**.

Sono anche previste coperture per la **consulenza psicologica laddove l'attacco informatico possa determinare un evento traumatico alla persona, pensiamo al *cyberbullismo, cyberstalking***, ai casi di ***revenge porn***.

In un numero ridotto di polizze, all'assicurato sono offerte anche coperture quali: un supporto informatico per eliminare/ridurre gli effetti dell'attacco subito; il rimborso delle spese legali sostenute per l'istanza di oscuramento di siti *web*/pagine di social media o per rivolgersi al Garante per la Protezione dei Dati Personali.

Alcune compagnie richiedono prerequisiti o condizioni per rendere il rischio *cyber* assicurabile, come ad esempio che siano stati adottati adeguati presidi informatici per far fronte agli attacchi, installati e aggiornati idonei sistemi *antivirus* e *firewall*, svolti periodici e frequenti *backup* dei sistemi informatici, ecc... Per alcune compagnie il rispetto di queste condizioni è motivo di esclusione o limitazione della garanzia, per altre invece non consente di assicurarsi contro il rischio *cyber*.

Proprio per queste ragioni e per l'ulteriore circostanza che, secondo quanto emerso dall'indagine, i glossari che accompagnano i contratti non sono esaustivi né del tutto chiari, è necessario prestare particolare attenzione alla **presenza di esclusioni, limitazioni e franchigie** che possono ridurre ampiezza e applicabilità delle coperture. Ed è importante soffermarsi sulla piena comprensibilità delle polizze perché il linguaggio più o meno complesso in cui sono espresse può generare ambiguità nell'identificare il perimetro di protezione che si sta sottoscrivendo.

Conclusioni e uno sguardo al futuro

L'indagine porta a concludere che il mercato assicurativo italiano sta sempre più dedicando attenzione alle polizze a copertura del rischio *"cyber"* e che in parallelo è anche cresciuta la sensibilità verso questo rischio da parte di famiglie e imprese.

È probabile che questo porti ad una più ampia riflessione sull'opportunità di passare da polizze assicurative standardizzate a polizze di tipo granulare, ritagliate sulle specifiche esigenze e sugli effettivi bisogni del consumatore. Possibile che si arrivi a una **revisione delle esclusioni per meglio tararle** sulle esigenze effettive dei *Target Market,* o all'**adozione di un glossario unico così da attribuire maggiore** omogeneità e certezza al linguaggio. È chiaro che questo comporterà investimenti nella formazione **della rete distributiva** e nel suo aggiornamento.

BIO

Annamaria Damiani è Capo della Divisione Vigilanza prodotti nell'ambito del Servizio Vigilanza Condotta di mercato (IVASS) Nata a Roma il 18 novembre 1969, si laurea in Giurisprudenza presso l'Università degli Studi "La Sapienza" di Roma nel 1993. Nel 1996 consegue l'abilitazione all'esercizio della professione di avvocato. Assunta all'ISVAP nel 1996 presso il Servizio di Vigilanza, nel2003 è assegnata al Servizio Tutela degli Utenti.Dal 2012 al settembre 2019 è Responsabile del Contact Center Consumatori, di cui ha curato direttamente lo start up. Dal mese di luglio 2013 coordina le attività della Divisione Imprese Estere di cui assume la titolarità a febbraio 2015, si occupa della vigilanza delle imprese di assicurazione estere a tutela degli assicurati italiani e opera in stretto contatto con le Autorità dei Paesi di origine partecipando anche ai Supervisory Colleges sui gruppi assicurativi transfrontalieri. Dal 2019 al 2022 è Capo della Divisione Vigilanza Distribuzione II e Operatori Esteri nell'ambito del Servizio Vigilanza Condotta di Mercato. A livello internazionale è membro di gruppi di lavoro in sede EIOPA, tra gli altri in materia di Payment Protection Insurance, travel insurance, segue la tematica Brexit e si è occupata dei "Consumers Trends".

Per famiglie e imprese, è importante una valutazione dei propri rischi specifici e del livello appropriato di copertura informatica di cui si ha bisogno.

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

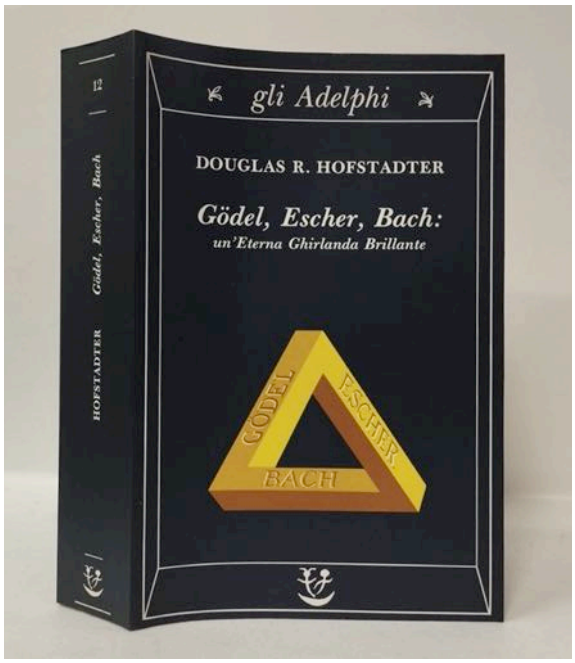
L'IVASS dal canto suo continuerà per un verso a sensibilizzare gli utenti verso il rischio cyber e per altro a seguire gli sviluppi del mercato assicurativo e vigilare sui prodotti offerti. IVASS partecipa alle campagne informative sulla sicurezza informatica, lanciate con il CertFin e l'Agenzia per la cybersicurezza nazionale (ACN), destinate alla clientela retail e alle PMI e ha aperto una sezione **sul proprio sito *web*** (https://www.ivass.it/cyber/index.html) che raccoglie documenti, informazioni, comunicati stampa e quant'altro necessario ai consumatori, individui e imprese, per proteggersi dalle minacce alla sicurezza informatica e dalle truffe *online*, in particolare quelle realizzate attraverso i siti abusivi. ■

1 https://www.ivass.it/pubblicazioni-e-statistiche/pubblicazioni/altre-pubblicazioni/2023/indagine-cyber-risk/index.html

AI, Blockchain e Quantum Computing: una Nuova Ghirlanda Brillante.

Autore: Giovanni Assolini

Nel 1979 fu pubblicato "Gödel, Escher, Bach: un'Eterna Ghirlanda Brillante" che, collegando le opere del matematico Kurt Gödel, dell'artista grafico M.C. Escher e del compositore Johann Sebastian Bach, esplorava idee legate all'autoriferimento, alla logica, alla consapevolezza e all'identità tramite collegamenti nati dall'analisi di concetti chiave nella matematica, nell'arte e nella musica



in un intreccio complesso in cui i fili della trama si chiamano teorema di Gödel, intelligenza artificiale e macchina di Turing.

Alcune di queste tecnologie si sono evolute molto velocemente per affrontare sfide sempre più complesse e nel corso del 2024, grazie alla loro sinergia si avvierà un salto evolutivo in grado di aprire nuove aree di studio e sviluppo.

Ambiti specifici del perimetro sicurezza trarranno enormi vantaggi da queste nuove tecnologie che includono ad esempio: l'uso diffuso di artificial intelligence per rilevare minacce in tempo reale, l'implementazione di blockchain per migliorare la sicurezza delle transazioni e il quantum computing per risolvere problemi computazionali legati alla crittografia.

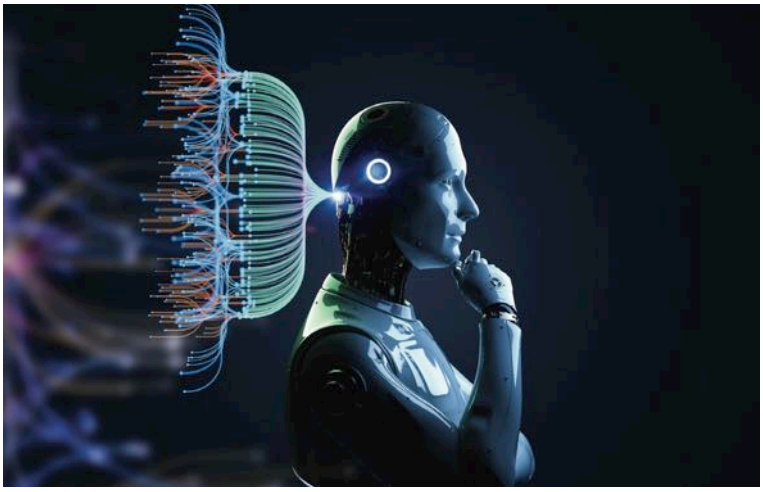
I fili della nuova Ghirlanda Brillante

A più di quarant'anni dall'uscita del libro, l'Artificial Intelligence (AI), la Blockchain e il Quantum Computing (QC) diventano i fili che compongono la trama di una nuova ghirlanda brillante e rappresentano le tre linee di sviluppo che, attraverso il loro intreccio, tesseranno l'evoluzione del mondo della sicurezza informatica, così come lo conosciamo.

Artificial Intelligence

L'integrazione dell'AI nella sicurezza informatica consente di affrontare le sfide in modo molto più dinamico, in un mondo in cui anche le minacce evolvono rapidamente e richiedono risposte altrettanto veloci e intelligenti.

La sua integrazione risulta fondamentale nell'affrontare le sempre crescenti minacce digitali e può essere impiegata in vari ambiti della sicurezza informatica. Alcuni di questi sono ad esempio: l'analisi comportamentale e il rilevamento delle minacce attraverso l'utilizzo di modelli di comportamento nei dati di rete e nei sistemi per rilevare attività sospette o minacce in tempo reale superando gli approcci basati su firme; l'autenticazione evoluta attraverso l'implementazione di metodi biometrici avanzati come il riconoscimento facciale, dell'iride o delle impronte digitali; la conseguente prevenzione delle frodi in settori come le transazioni finanziarie online



grazie all'identificazione di schemi di comportamento fraudolento; il miglioramento nella capacità di prevenzione delle stesse; l'introduzione di sistemi di prevenzione grazie analisi avanzate delle vulnerabilità; l'utilizzo di algoritmi basati su regole e apprendimento automatico per adattarsi alle nuove minacce e migliorare continuamente le capacità di difesa.

Blockchain

L'applicazione della blockchain in sicurezza informatica si basa sulla sua capacità di fornire un ambiente sicuro, trasparente e resistente alla manipolazione dei dati digitali.

Concepita originariamente per supportare le criptovalute come il Bitcoin, ha dimostrato di avere molteplici applicazioni in ambito della sicurezza

informatica. Alcune delle sue applicazioni principali sono: l'utilizzo di registri immutabili delle transazioni che rendono difficile la manipolazione dei dati e garantisce l'integrità delle informazioni, utile per rilevare eventuali modifiche non autorizzate ai file di sistema; la creazione di sistemi di identità digitali sicuri e decentralizzati in cui gli utenti controllano le proprie informazioni e possono concedere autorizzazioni senza dover affidare a terze parti centralizzate la custodia dei dati sensibili, garantendo al contempo una gestione degli accessi più sicura; l'utilizzo di contratti intelligenti che consentono l'esecuzione automatica di condizioni predefinite utili, ad esempio, per l'automazione di processi di sicurezza come l'applicazione di patch o la risposta a minacce specifiche.

BIO

Giovanni Assolini inizia il proprio percorso occupandosi per oltre un decennio della progettazione di datacenter e reti geografiche complesse nelle telecomunicazioni per poi passare al mondo finance dove, da 15 anni, sviluppa e approfondisce le proprie conoscenze in ambito continuità operativa, cybersecurity e antifrode.

Inoltre, la blockchain può essere utilizzata per garantire una visibilità completa sulla catena di approvvigionamento digitale, consentendo di tracciare l'origine e l'intera storia dei componenti hardware o software e minimizzando il rischio legato alla compromissione della catena di fornitura. Permette, ancora, di garantire un più elevato livello di sicurezza dei dati condivisi in ambienti in cui più entità devono condividere dati, come nel settore sanitario, dove può essere utilizzata per garantire la sicurezza e la privacy dei dati, consentendo solo a chi è autorizzato di accedere a informazioni specifiche.

Quantum Computing

L'applicazione del quantum computing (QC) in ambito sicurezza informatica offre nuovi approcci per affrontare sfide legate alla crittografia e alla risoluzione di problemi computazionali complessi.

Tra gli aspetti chiave specifici del QC ci sono la crittografia quantistica che sfrutta le proprietà della meccanica quantistica, come l'entanglement e la sovrapposizione, per creare sistemi crittografici teoricamente inviolabili che, abbinato alla generazione di chiavi crittografiche quantistiche, offrono un metodo di scambio di informazioni sicuro e immune a potenziali attacchi basati sulla computazione quantistica.

Altri ambiti di applicazione potrebbero portare a un miglioramento generale della sicurezza risolvendo rapidamente problemi di ottimizzazione complessi, migliorando così l'efficacia nella gestione delle risorse e delle strategie di sicurezza.

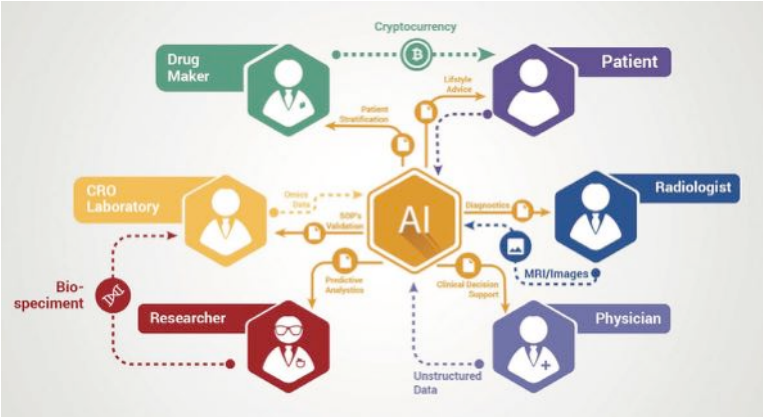
Tuttavia, è importante notare che il quantum computing è ancora in fase di sviluppo e non è ampiamente disponibile. Le sfide attuali includono la coerenza quantistica e la riduzione degli errori quantistici. La sua integrazione pratica in applicazioni di sicurezza informatica richiederà ulteriori progressi tecnologici e standardizzazione.

La creazione della nuova Ghirlanda Brillante

Le singole tecnologie sopra descritte sono un importante passo evolutivo di per sé, ma è la loro interazione che rappresenta la vera chiave di volta.

AI e Blockchain

L'integrazione sinergica di intelligenza artificiale e blockchain già oggi offre un approccio completo alla sicurezza informatica, migliorando la trasparenza, l'affidabilità e l'efficacia delle soluzioni di difesa ed è possibile utilizzarla in modo complementare per affrontare diverse sfide in alcuni ambiti chiave tra cui:



- Autenticazione sicura: la blockchain può essere utilizzata per garantire un'identità digitale sicura e immutabile; mentre l'AI, a sua volta, può migliorare l'autenticazione attraverso l'analisi comportamentale e l'identificazione biometrica, rafforzando ulteriormente la sicurezza dell'accesso.
- Contratti intelligenti sicuri: la blockchain facilita l'esecuzione di contratti intelligenti, protocolli autoeseguibili con condizioni definite; l'AI a sua volta può essere incorporata per analizzare dinamicamente le condizioni contrattuali e rilevare potenziali problemi o attività sospette.
- Rilevamento delle minacce: l'AI analizza i dati provenienti da reti e sistemi per identificare comportamenti anomali o minacce; mentre la blockchain può essere utilizzata per garantire l'integrità dei dati, rendendo più difficile per gli attaccanti alterare le informazioni rilevanti per eludere i sistemi di sicurezza.
- Gestione degli accessi e delle autorizzazioni: la combinazione di blockchain e AI può migliorare la gestione degli accessi, consentendo la definizione di regole e autorizzazioni in modo più dinamico e adattivo, sulla base dell'analisi continua dei modelli di utilizzo.
- Tracciabilità delle transazioni: la blockchain fornisce un registro immutabile delle transazioni. Integrando l'IA, è possibile analizzare questi dati per individuare attività sospette o irregolarità, migliorando la capacità di rilevare frodi o intrusioni.
- Protezione della privacy: la blockchain può essere utilizzata per consentire la gestione e il controllo granulare delle informazioni personali, l'IA può contribuire a monitorare l'accesso e l'uso di queste informazioni, rafforzando la protezione della privacy degli utenti.

AI e QC

L'integrazione di intelligenza artificiale (IA) e quantum computing (QC) nella sicurezza informatica offre un potenziale rivoluzionario. Tra i maggiori ambiti di iterazione tra queste tecnologie ci sono:

- Analisi predittiva avanzata: l'AI può essere utilizzata per analizzare enormi quantità di dati e identificare pattern o comportamenti anomali, aiutando a prevedere e prevenire minacce. Quando combinata con QC, questa analisi può essere eseguita in tempi record.
- Ottimizzazione di algoritmi di apprendimento automatico: il QC può migliorare l'efficienza e l'addestramento degli algoritmi di apprendimento automatico, consentendo alle soluzioni di AI di analizzare rapidamente e apprendere dai dati per rilevare minacce in modo più avanzato.
- Risposta rapida agli incidenti: l'AI può automatizzare la risposta agli incidenti di sicurezza, mentre il QC può accelerare le simulazioni e le analisi necessarie per comprendere a fondo la portata di un attacco.
- Analisi delle vulnerabilità avanzate: l'IA può identificare e analizzare potenziali vulnerabilità nei sistemi, e il QC può affrontare problemi di complessità elevata legati alla verifica e alla correzione di vulnerabilità.
- Simulazioni molecolari e sicurezza biologica avanzata: l'unione di QC e AI può migliorare notevolmente la simulazione di scenari molecolari complessi e minacce biologiche, contribuendo a prevenire attacchi in settori come la sicurezza sanitaria.

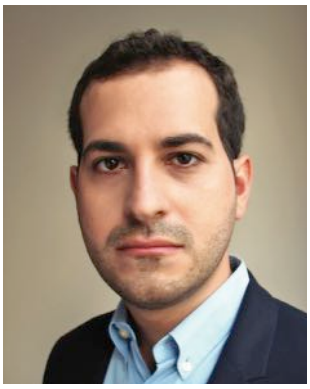
L'implementazione pratica di queste tecnologie richiederà un progresso significativo nella stabilità e nell'accessibilità del quantum computing, oltre a un continuo sviluppo di algoritmi di artificial intelligence specifici per la sicurezza informatica.

L'integrazione dell'intelligenza artificiale con il quantum computing apre nuove prospettive e sfide. Il quantum computing potrebbe accelerare significativamente la risoluzione di problemi computazionalmente intensivi, migliorando le prestazioni di algoritmi di apprendimento automatico e ottimizzazione utilizzati nell'IA.

Con l'aumento della potenza di calcolo fornita dai computer quantistici, si potrebbero ottenere risultati più veloci nell'addestramento di modelli complessi e nella risoluzione di problemi di ottimizzazione. Tuttavia, ci sono sfide da affrontare, come la coerenza quantistica e la suscettibilità agli errori quantistici, che richiedono nuovi approcci per la programmazione e l'implementazione degli algoritmi.

In sintesi, l'integrazione di intelligenza artificiale, blockchain e quantum computing offre un enorme potenziale per avanzare nelle capacità computazionali e mostrano la futura trama della ghirlanda brillante, sarà però necessario superare sfide tecniche e teoriche per sfruttare appieno questi benefici. ■

Svelare il Shadow Market: esplorare l'allarmante aumento delle acquisizioni di account vendute sulla Darknet.



Autore: **Liran Cohen**

Il furto delle credenziali degli utenti è un settore in crescita e l'Italia ne sente l'impatto. Infatti, solo nell'ultimo trimestre oltre 31mila singole macchine in Italia sono state infettate da malware information stealer. Ciò ha portato a oltre 12.400 credenziali uniche leaked dall'Italia che sono state messe in vendita da autori di minacce sui mercati del deep web e del dark web. Il mercato delle credenziali leaked è vasto e ha un enorme potenziale grazie a:

- la disponibilità online di kit malware economici;
- l'aumento delle operazioni di furto attive in tutto il mondo;
- la crescente sofisticazione delle tecniche implementate dagli autori delle minacce.

Questi fattori hanno creato un mercato redditizio per i criminali informatici che sono in grado di rubare credenziali e venderle sul mercato nero. Le credenziali rubate possono quindi essere utilizzate per accedere a informazioni personali e finanziarie, commettere furti di identità o lanciare altri attacchi informatici.

Quasi tutti i siti Web e le applicazioni utilizzano password per autenticare gli utenti, che devono gestire un numero crescente di account online. Con l'aumentare

della necessità, gli utenti tendono a riutilizzare le stesse combinazioni account-password per molti dei servizi online che utilizzano.

Sfortunatamente, l'uso diffuso e il riutilizzo delle password le rendono bersagli attraenti per i criminali informatici, in quanto sanno che le password rubate forniscono un punto di accesso ad altri account e servizi. Queste credenziali vengono utilizzate per attacchi di furto di account, frodi e furto di dati.

Mentre le aziende cercano di proteggere le proprie informazioni sensibili dagli attacchi, le informazioni dei clienti vengono archiviate in database vulnerabili sparsi sul Web. L'identificazione di account cliente compromessi, domini presi di mira e password vulnerabili consente alle organizzazioni di costruire in modo proattivo una migliore difesa contro il furto di account e

le attività fraudolente. Inoltre, la costante identificazione degli account dei clienti che sono stati compromessi, fornisce un monitoraggio costante delle frodi senza influire sull'esperienza dell'utente.

I dati raccolti possono essere utilizzati per ottenere informazioni su quali domini vengono presi di mira e quali sono le password più vulnerabili. Ciò aiuta a dare priorità alle strategie di mitigazione del rischio e a proteggere i clienti dell'organizzazione e la loro stessa reputazione.

Usi delle credenziali leaked

Le credenziali dei clienti di un'organizzazione sono un bene prezioso nel mercato dei criminali informatici per 2 ragioni principali:

1 Sono relativamente facili ed economici da ottenere e richiedono poco sforzo da parte degli autori di minacce

2 Le credenziali possono essere abusate e sviluppate in una varietà di altre attività fraudolente, quali:

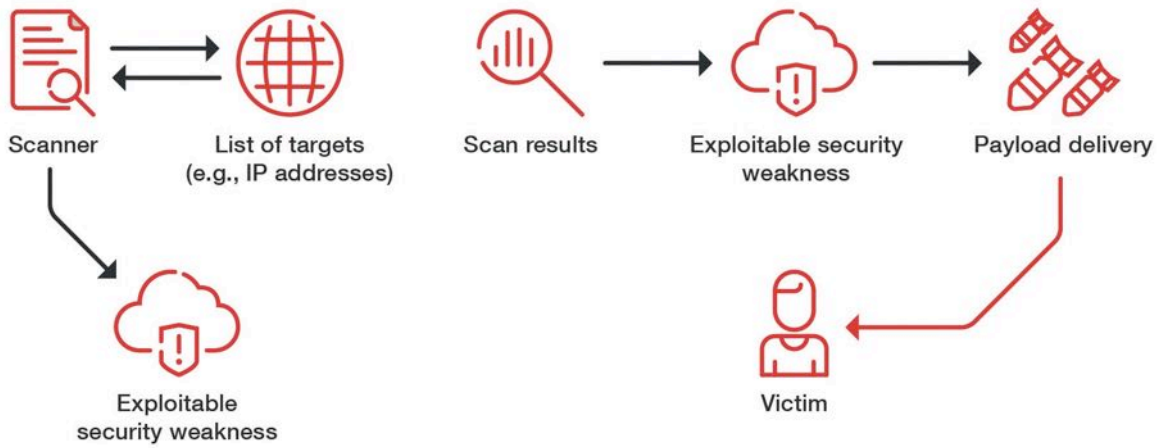
- **Acquisizione di PII e dati aggiuntivi:** dopo aver inserito un account, gli autori delle minacce possono raccogliere più informazioni, ad esempio carte di credito, numeri di telefono, indirizzi, ID, ecc.
- **Spam:** un account legittimo è un ottimo strumento per truffe e altre attività ingannevoli.
- **Phishing:** sotto mentite spoglie di account legittimi, gli autori delle minacce prendono di mira i contatti del proprietario dell'account.
- **Attacchi ransomware:** i proprietari di account di valore potrebbero essere costretti a pagare un riscatto per accedere nuovamente ai propri account.
- **Frode finanziaria:** gli account con accesso ai dati finanziari e la capacità di eseguire transazioni, come carte di credito, prelievo di fondi e trasferimento di denaro, sono particolarmente preziosi per gli autori delle minacce.
- **Abuso promozionale:** gli autori delle minacce si affidano a tecniche multi-accounting per ottenere il maggior numero di iscrizioni o bonus di riferimento possibili.
- **Test delle carte:** alcuni account vengono utilizzati solo per effettuare piccoli acquisti o per testare le carte di credito. Ciò aiuta gli autori delle minacce a verificare la validità delle carte di credito rubate.
- **Acquisizione dell'accesso ad account Premium:** particolarmente apprezzati per i servizi a pagamento e abbonati, come Netflix, Spotify oppure Money Laundering o transazioni Money Mule.
- **Coinvolgimento sui social media:** gli account compromessi vengono utilizzati per gestire "bot farm" per la manipolazione del coinvolgimento sui social media, come follower e likes.

Tattiche e tecniche relative alle credenziali leaked

La base per l'esposizione delle credenziali dei clienti è l'accesso fraudolento alle credenziali dell'account di un utente.

Di seguito sono riportate alcune tattiche con cui gli aggressori solitamente compromettono gli account legittimi:

- **Brute-force attacks, incluso 'dictionary attacks':** l'aggressore collega una combinazione nome utente/password su più account finché non si ottengono risultati.
- **Credential Stuffing:** l'aggressore utilizza la cattiva abitudine di utilizzare la stessa password per più account. Se una di queste password viene divulgata a causa di una violazione dei dati, qualsiasi altro account con lo stesso nome utente e password è a rischio.
- **Dark Markets:** gli aggressori possono scaricare password crackate dai mercati della darknet per tentare l'ATO sugli stessi account utente sul sito di destinazione.
- **Phishing:** rimane un modo efficace per ottenere la password della vittima in assenza di controlli come l'autenticazione a più fattori (MFA).
- **Attacchi malware:** keylogger, stealers e altri tipi di malware possono esporre le credenziali degli utenti, offrendo agli aggressori il controllo sugli account delle vittime.
- **Sfruttamento delle vulnerabilità della sicurezza:** le falle di sicurezza senza patch vengono utilizzate per ottenere l'accesso non autorizzato a un sistema. Ad esempio, Cross-Site Scripting (XSS) e Server Side Request Forgery (SSRF).
- **Attacchi di ingegneria sociale:** gli autori delle minacce contattano le persone e tentano di estorcere i dati di accesso agli account.



Con le credenziali leaked, il tempo è denaro

Quanto più sono recenti le credenziali leaked, tanto maggiore è la possibilità che gli autori delle minacce possano raggiungere il loro obiettivo finanziario. Tuttavia, le credenziali vengono raramente utilizzate dagli autori

delle minacce in "tempo reale". A meno che le credenziali non vengano compromesse in attacchi altamente mirati, gli autori delle minacce hanno bisogno di tempo per analizzare i dati che hanno catturato. Questo processo di analisi consente loro di estrarre credenziali "raw" per venderle su mercati illegali o utilizzarle per ulteriore sfruttamento. Tuttavia, quanto prima vengono rilevate le credenziali leaked, tanto più velocemente i team di sicurezza potranno intervenire.

L'impatto delle credenziali dei clienti leaked

Le credenziali leaked dei clienti potrebbero non rientrare tra le responsabilità della sicurezza in azienda. Tuttavia, possono essere molto dannosi per la reputazione dell'azienda ed avere anche implicazioni finanziarie e persino legali. Inoltre, va tenuto presente che molto probabilmente gli utenti incolperanno l'azienda per eventuali danni che si verificano attraverso l'esposizione di credenziali e l'acquisizione di account, attribuendo la colpa alla mancanza di misure di sicurezza e di prevenzione delle frodi da parte dell'azienda stessa.

Quali sono le implicazioni finanziarie delle credenziali dei clienti leaked?

- Aumento delle controversie sulle transazioni
- Aumento dei riaddebiti
- Elevato tasso di abbandono dei clienti
- Perdita di entrate
- Eventuali sanzioni/multe
- I chargeback sono costosi per i siti web di e-commerce, soprattutto quelli che utilizzano gateway di pagamento di terze parti. Tassi elevati di chargeback possono comportare un aumento delle commissioni di transazione

Quali sono le implicazioni sulla reputazione delle credenziali dei clienti leaked?

- Fidelizzazione dei clienti
- Sanzioni/multe finanziarie
- Perdita di reputazione presso le istituzioni finanziarie
- Il marchio e la reputazione potrebbero risentirne, poiché l'azienda potrebbe trovarsi ingiustamente accusata di violazione dei dati, il che potrebbe portare a pubblicità negativa, multe e perdita di affari. Inoltre, la perdita di clienti e cattiva pubblicità per l'azienda.

Come identificare un account di un cliente compromesso

Gli attacchi che comportano "leaking customer credentials" vengono spesso identificati dalle aziende dopo che un cliente ha presentato un reclamo. Un'adeguata protezione da bot e frodi online dovrebbe essere implementata in azienda al fine di rilevare questo tipo di attacco e prevenire l'esposizione delle credenziali dei clienti e il furto degli account. Di seguito sono riportati alcuni segnali importanti per rilevare tentativi di attacco sui siti Web dell'azienda:

- Indirizzi IP da posizioni geografiche insolite
- Più account condividono gli stessi dettagli
- Modelli di dispositivi sconosciuti/offuscati
- Più account a cui si accede dallo stesso dispositivo o IP
- Rilevamento di proxy VPN o utilizzo TOR sospetti
- Numero insolito di richieste di chargeback
- Tentativi di accesso di massa su un account
- Richieste di reimpostazione di massa della password

Raccomandazioni per prevenire la fuga di credenziali dei clienti

Le credenziali dei clienti leaked sono così diffuse che la maggior parte delle aziende non possono evitarle. Pertanto, qualsiasi azienda che mantenga account online per i propri clienti dovrebbe disporre di un piano di sicurezza dei dati che includa forti garanzie per proteggere i clienti.

Inoltre, i furti di account che coinvolgono credenziali dei clienti compromesse sono difficili da individuare perché si basano su tecniche di ingegneria sociale: gli autori delle minacce possono impersonare la vittima o utilizzare altri metodi per indurre il titolare dell'account a fornire i propri dati di accesso. I proprietari degli account spesso non si rendono conto che il loro account è stato compromesso finché non avviene la truffa.

Le organizzazioni dovrebbero adottare un approccio olistico quando si tratta della loro difesa informatica,

BIO

Liran Cohen ha una vasta esperienza nel campo delle vendite e della tecnologia. Attualmente, Liran lavora come Sales Director EMEA presso Cyberint dall'aprile 2021. In precedenza, Liran ha lavorato presso Hewlett Packard Enterprise dal 2009 al 2021, dove ha ricoperto vari ruoli tra cui Regional Sales Manager - Security Solutions per Israele, Spagna e Italia, Business Unit Manager per Cyber, Security e Microsoft Solutions e Business Unit Manager per Client Infrastructure Consulting. Inoltre, Liran ha lavorato come consulente Microsoft e Unified Communications presso Hewlett Packard Enterprise dal 2009 al 2012. Prima di entrare in Hewlett Packard Enterprise, Liran ha prestato servizio nell'aeronautica militare israeliana come ingegnere di sistemi infrastrutturali dal 2006 al 2009. Liran Cohen ha conseguito un Master of Business Administration (MBA) presso la Reichman University dal 2020 al 2022. In precedenza, Liran ha conseguito un Bachelor of Arts (BA) in Economia presso la The Open University of Israel, dove ha studiato dal 2009 al 2015. Oltre alle lauree, Liran possiede una certificazione come Certified Information Systems Security Professional (CISSP) ottenuta da (ISC)² nell'agosto 2017.

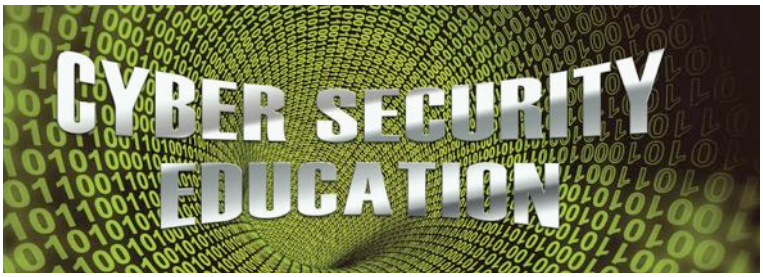
poiché non esiste una singola misura o tecnologia in grado di raggiungere una copertura totale.

L'uso intelligente delle password è essenziale: il riutilizzo delle password dovrebbe essere evitato e dovrebbe essere adottata una solida politica sulle password per ridurre il rischio di password facili da indovinare. Dovrebbe essere impostata anche l'autenticazione a più fattori (MFA).

Viene suggerito di mettere in atto diverse soluzioni complementari per ridurre al minimo sia il rischio che l'impatto.

Inoltre, è importante notare che l'efficacia delle raccomandazioni sopra menzionate probabilmente cambierà nel tempo man mano che gli autori delle minacce adotteranno nuove tattiche e tecniche. Le imprese dovrebbero valutare regolarmente l'efficacia dei propri controlli e implementare nuove strategie adeguate.

L'education è fondamentale per mitigare gli attacchi. È nell'interesse di entrambe le parti, aziende e clienti, sapere come identificare attività potenzialmente dannose.



Azioni immediate da intraprendere quando vengono trovate credenziali del cliente compromesse

Congelare l'account compromesso per impedire all'autore della minaccia di eseguire attività fraudolente

- Bloccare/Annullare tutte le transazioni in corso: chiedere la verifica al legittimo proprietario dell'account
- Forzare la reimpostazione della password
- Informare il legittimo proprietario dell'account

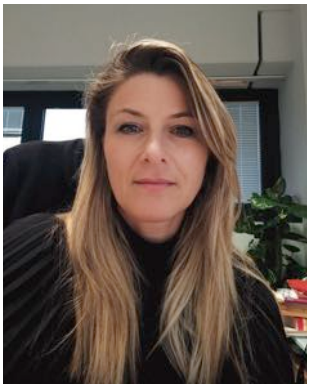
Una continua igiene informatica può aiutare a prevenire gli attacchi, nonché a mitigarne l'impatti quando si verificano.

Come prevenire gli account takeover attacks

- Educare i clienti sui pericoli del phishing
- Implementazione del Multifactor Authentication (MFA)
- Impostare un limite ai tentativi di accesso
- Configurazione dei sistemi di rilevamento delle frodi per visualizzare un CAPTCHA dopo un numero specifico di tentativi di autenticazione
- Inviare notifiche di eventuali modifiche all'account ai clienti

Le vulnerabilità continuano a manifestarsi in forme diverse ed è impossibile risolverle tutte, comprese le credenziali trapelate, da un giorno all'altro. Per proteggere l'organizzazione, è necessario innanzitutto concentrarsi sulle vulnerabilità che contano di più. Cyberint evidenzia le vulnerabilità note e sconosciute e vengono automaticamente correlate alle risorse digitali dell'azienda e alla superficie di attacco, evidenziando quelle minacce imminenti che devono essere gestite con la massima urgenza. ■

Cyber Security, a Jesolo un evento di nuova generazione.



CITTÀ DI JESOLO

Autore: Alessandra Pernechele, Comune di Jesolo

L'amministrazione ha organizzato un incontro interattivo per Enti pubblici, Aziende e privati cittadini, sull'argomento: "come difendersi nell'era dei pirati digitali".

Phishing, password scricchiolanti e chiavette USB senza protezioni. Sono alcuni dei temi sui quali si è focalizzato l'evento di *edutainment* dal titolo **"CYBERLAND – Alla ricerca del tesoro di Atlantide"** organizzato dall'amministrazione comunale di Jesolo giovedì 19 ottobre, la sala consiliare si è trasformata in un contenitore di informazioni ma anche di emozioni: l'incontro, infatti, si è svolto secondo una formula del tutto innovativa mediante l'accompagnamento guidato in un viaggio virtuale e il coinvolgimento del pubblico attraverso i dispositivi digitali degli invitati mediante l'utilizzo di un'applicazione che permette di interagire con la presentazione.

BIO

Dal 2004 l'arch. ing. Alessandra Pernechele è Funzionario della Pubblica Amministrazione nei settori Edilizia, Urbanistica, Commercio e SUAP a partire dal 2022 assume nuove competenze dell'ambito ICT come Dirigente dell'Ufficio Sistemi Informativi del Comune di Jesolo e Responsabile per la Transizione Digitale dell'ente (RTD).

Sempre di più, come evidenziato anche dal Ministero degli Interni, gli Enti pubblici e le Istituzioni si trovano coinvolti in vere e proprie guerre cibernetiche. Recentissimi gli attacchi ai portali di alcuni Ministeri, del Consiglio Superiore della Magistratura e dell'Arma dei Carabinieri. Ma i cyber criminali non risparmiano nessuno, compresi colossi del commercio internazionale, piccole aziende e privati cittadini. I pirati della rete, infatti, non sfruttano più soltanto i nostri computer come ponti per compiere i loro attacchi, ma con la diffusione di nuovi strumenti tecnologici possono farsi largo attraverso smartphone, telecamere di sicurezza e persino televisori o frigoriferi. Il loro obiettivo? A volte tenere sotto scacco un'istituzione per chiedere un vero e proprio riscatto in denaro, altre volte razziare tutti i dati possibili compresi quelli sensibili e delicati. **"CYBERLAND – Alla ricerca del tesoro di Atlantide"** ha proprio l'obiettivo di portare sotto i riflettori un campo della sicurezza personale a volte ancora sottovalutato.

Per queste ragioni, l'amministrazione comunale di Jesolo ha avviato un ampio progetto dedicato alla sicurezza informatica che vede affiancarsi l'organizzazione di incontri pubblici come quello effettuato il 19 ottobre, interventi sull'infrastruttura informatica dell'Ente e un percorso di formazione per i dipendenti del Comune. A conferma di ciò, proprio in queste settimane si sta perfezionando un investimento per implementare e potenziare la dotazione dell'ente in fase di prevenzione dei rischi di attacchi digitali. Gli interventi si inseriscono in un percorso già avviato e focalizzato alla tutela, nonché al corretto uso entro i termini di legge, dei dati personali dei cittadini jesolani così come di quelli degli ospiti che visitano la città durante l'anno. **"CYBERLAND – Alla ricerca del tesoro di Atlantide"** è riconosciuto dall'Ordine degli Architetti di Venezia, dal Collegio Geometri e Geometri laureati di Venezia e dall'Ordine degli Ingegneri di Venezia come evento che dà diritto all'acquisizione di crediti formativi.

L'incontro è stato aperto da un intervento del giornalista Massimo Scattolin, caposervizio de La Nuova Venezia, che da oltre vent'anni contribuisce al coordinamento dei giornalisti della propria testata giornalistica in ambito provinciale. A guidare poi rappresentanti degli Enti pubblici, imprenditori e cittadini nei meandri della Cyber Security il 19 ottobre sono stati Veronica Patron e Roberto Patricolo.

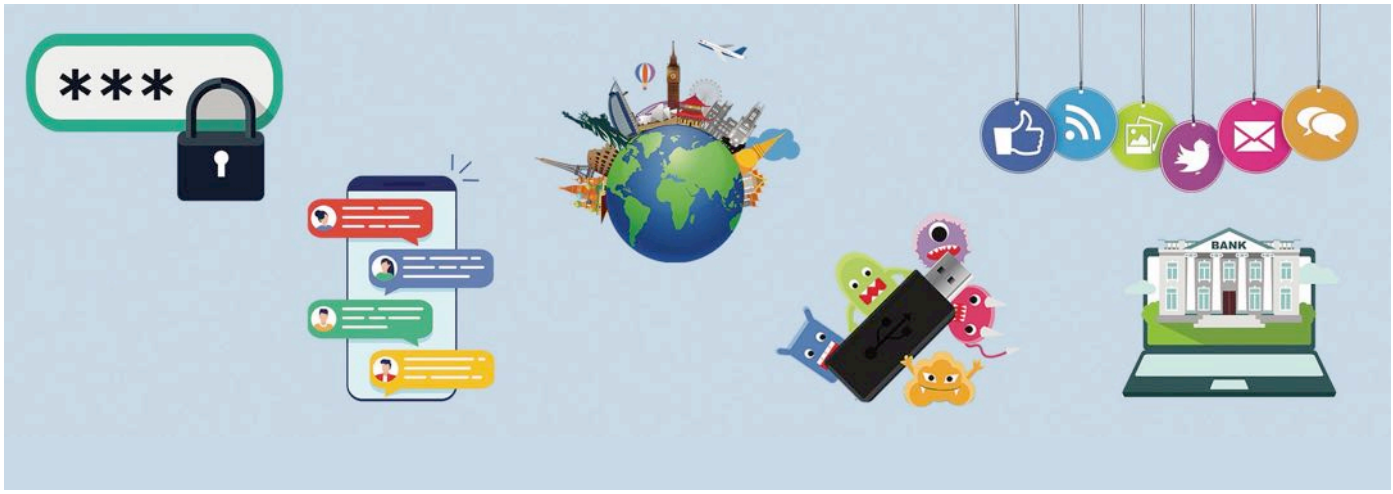
Veronica Patron, laureata in psicologia con specializzazione in comunicazione e programmazione neuro-linguistica, è formatrice in ambito cybersecurity e psicologia dei comportamenti, redattrice per la rivista CybersecurityTrends edizione italiana della rivista internazionale dedicata ai temi della cybersecurity. Patron è inoltre co-fondatrice della Società Security Mind nonché ideatrice della piattaforma Security Mind Awareness con l'intento di agire sui comportamenti di ogni membro dell'organizzazione, promuovendo comportamenti idonei a rafforzare il livello di sicurezza aziendale.

Roberto Patricolo è business coach e practitioner neuroagility, associato ICF (International Coach Federation) e AICP (Associazione Italiana Coach Professionisti). Ideatore del modello di neurocoaching PerFormare, Patricolo è esperto di neuroscienze, consulente in Cybersecurity e Data Privacy, docente di coaching presso la scuola Karakter Coaching sul territorio nazionale e collaboratore di associazioni di imprenditori per lo sviluppo della leadership e del management.

I loro interventi sono stati dei veri e propri viaggi capaci di coinvolgere il pubblico attraverso temi come il phishing, la sicurezza delle password, quella delle Pen Drive, il travelling, i social media, i dispositivi mobili e più in generale, la navigazione in internet.

Alla realizzazione dell'evento ha collaborato per lo sviluppo della parte sensoriale Andrea Patron, direttore di scena per dieci anni in diverse produzioni che hanno visto come protagonista Marco Paolini tra le quali dirette Rai de "Il Vajont" e "Il Milione – Quaderno veneziano".

L'organizzazione dell'evento nasce dall'idea che prima ancora della formazione è utile far maturare un'adeguata sensibilità sulla delicatezza del problema e sulla diffusione dei rischi insiti nella pratica quotidiana di ciascuno, sia lavorativa che privata. Inoltre, l'incontro permette al Comune di agire come volano sul territorio sensibilizzando sulle buone pratiche, generando curiosità e interesse. A volte sottovalutiamo il valore dei dati che, spesso con troppa facilità, condividiamo in rete oppure non difendiamo adeguatamente. Conoscere e sapere è fondamentale per circondarsi di tecnologie innovative. ■



Allargare la visuale: la cyber security ha trovato il giusto metodo.

Intervista VIP ad Agnese Scappini.

Autore: Massimiliano Cannata

"Il metodo e la disciplina credo siano fondamentali in ambito cybersecurity, poiché trovare un metodo applicativo ed efficace, significa trovare la strada di applicazione di quei nuovi meccanismi di difesa di cui oggi necessitiamo, e credo che un metodo funziona solo se la sua applicazione sia accompagnata da disciplina che è anche costanza del lavoro". Abbiamo sollecitato Agnese Scappini a darci un parere sul focus attorno a cui ruota questo numero di ***Cybersecurity Trends*** che vuole offrire una *overview* sull'anno che verrà.

Professoressa, la sua formazione filosofica e psicologica consente di offrire interessanti spunti al management che opera in questo delicato settore. In* Grandangolo temporale. *Il metodo (Fausto Lupetti editore) il suo ultimo saggio, emerge un messaggio di fondo molto netto: occorre allargare la visuale per affrontare le grandi questioni del nostro tempo. La sicurezza è una di queste.

Aveva ragione Freud che sosteneva che l'uomo di ogni tempo ha sempre rinunciato a un po' di libertà per avere maggiore sicurezza?

Questa società ha bisogno di sicurezza e protezione esattamente come le precedenti; tuttavia, oggi ciò che è cambiata è la minaccia e la natura stessa della minaccia. Questo stravolgimento fa sì che sia necessario ricreare nuove difese e metodi difensivi. Ci sentiamo costantemente più vulnerabili. Il pericolo oggi non è infatti individuabile in qualcosa o qualcuno di esterno, può entrare con sembianze difficili da definire nelle nostre case, nelle nostre mani attraverso uno *smartphone,* compromettere i nostri dati, la nostra

BIO

Sono Psicologa ad indirizzo lavoro e contesti; esperta in comunicazione. Sono Specializzanda in Psicoterapia interpersonale umanistica. Attualmente sto svolgendo la libera professione di Psicologa clinica; Psicologa del Lavoro e dello Sport, mi occupo di terapia individuale e di coppia, di adolescenza e infanzia. La mia formazione è strettamente legata alla psicologia clinica, alla psicologia sociale e del lavoro, alla psicologia giuridica, alle metodologie inclusive, al team building, al miglioramento della propria performance e di quella collettiva, alla prevenzione e gestione delle problematiche inerenti a stress lavoro/ correlato e traumi. Ho eseguito docenze presso Luiss.
Nel settembre 2017 presento il mio primo romanzo "Una Rosa per un Santo", a maggio 2020 pubblico la mia seconda opera "Diario di un pesce... in Quarantena"; Ho scritto diversi articoli di ordine psicologico. Nel 2022 esce il mio libro di Metodo "Grandangolo Temporale. Il metodo" edito Lupetti editore; lo stesso anno esce "100 sessanta secondi di psicologia" testo motivazionale.

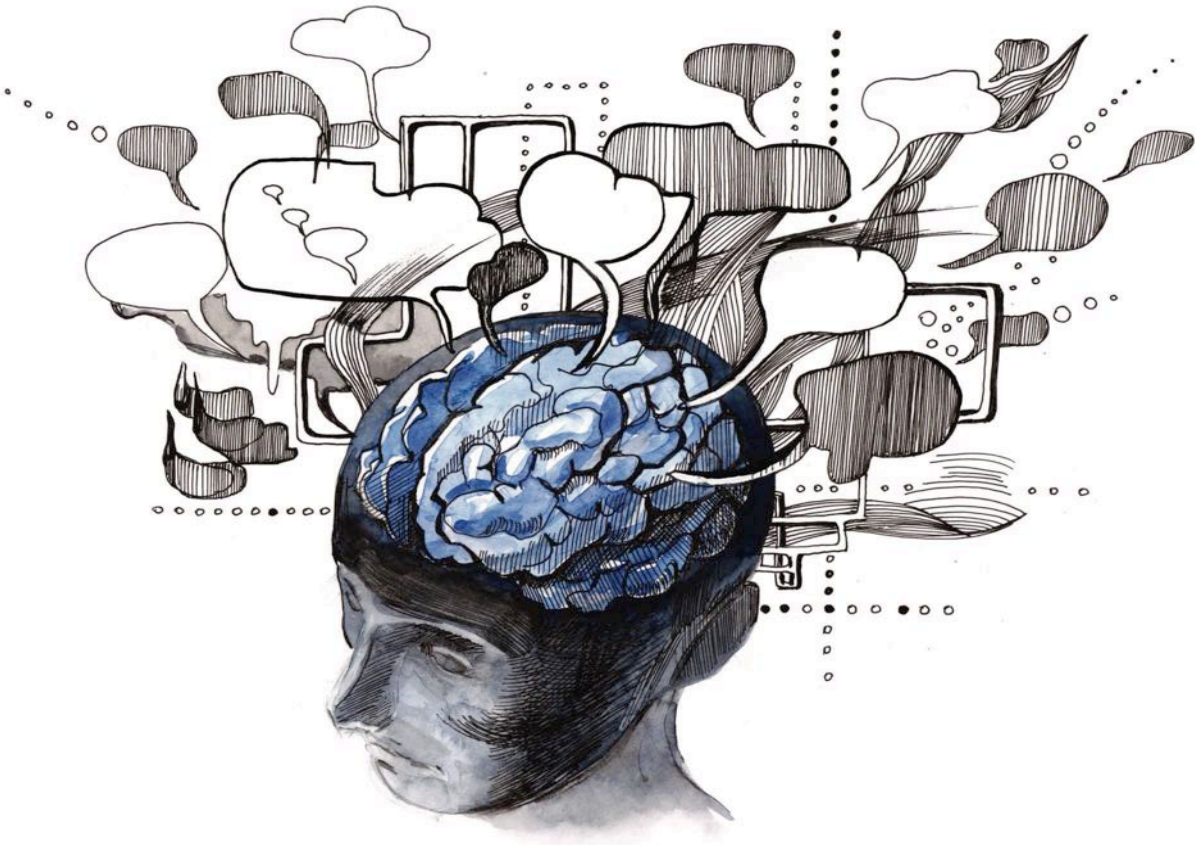
identità… Oggi la minaccia non è vitale ma identitaria e questo provoca grandi stravolgimenti sociali. La stessa identità di gruppo nasce come bisogno di protezione verso cui rinunciamo alla componente istintuale. Tuttavia, oggi questa rinuncia non sembra più sufficiente a garantire appunto protezione. Per questo nel mio libro propongo di allargare la visuale, solo così è possibile trovare nuove risorse e spunti creativi.

Viviamo in un'epoca della dimenticanza, così comincia il primo capitolo del suo libro. Nella* governance *del rischio, come in ogni attività umana, relazionale e produttiva conoscere è ricordare come ci insegna Platone. Siamo troppo schiacciati sul presente. Quali sono le conseguenze di questo atteggiamento?

Credo piuttosto che siamo nell'epoca trasfigurata dal futuro. Siamo passati dalla nostalgia del passato, un'epoca caratterizzata dalla melanconia, la patologia prevalente: la depressione; all'epoca, con l'invenzione dell'auto, della velocità, manifestata dalla patologia della schizofrenia. Non riusciamo ad arrestare quel *divenire* impetuoso di eraclitiana memoria, siamo essere in divenire sì, ma oggi quel divenire è accelerato, mentre noi non riusciamo più a memorizzare nulla, e senza memoria non vi è pensiero, senza memoria non vi è identità. Ecco che di nuovo emerge la minaccia identitaria, il pericolo è la perdita d'identità. Chi sono? È la nuova vera domanda esistenziale.

Il divenire legge eraclitea, cui lei faceva riferimento, segna profondamente la contemporaneità. La rivoluzione tecnologica è un divenire, non abbiamo fatto in tempo a "capire" internet che è sopraggiunta l'esplosione dei social e oggi dell'intelligenza artificiale. La nostra psiche nel dualismo con la tecnè, dicotomia analizzata da Galimberti, sta cambiando anch'essa configurazione?

Oggi quel dualismo di cui ci parla Galimberti è estremizzato in quella che in psicoanalisi definiamo dissociazione, un vero e proprio meccanismo di difesa che mantiene la realtà separata, non permette un'integrazione della dimensione del reale. È infatti divenuta talmente multidimensionale la realtà, pensiamo non solo ai social, ma anche al metaverso, agli avatar, nuovi fenomeni proiettivi, da non poter più essere definibile e quindi contenibile. Questo provoca frammentazione nella psichè, o preferirei dire nel logos,



inteso come ragionamento. Da qui il fenomeno della dimenticanza, il metodo, che propongo nel mio libro per contrastare la dimenticanza è semplice: riattiviamo la capacità di ricordare.

Siamo esseri in relazione, la sicurezza è relazione e si costruisce su un ecosistema che deve cementarsi attraverso la consapevolezza di ciascuna parte. Eppure, questa visione sistemica, che dovrebbe guidare anche le attività di formazione, stenta a farsi strada. Quali sono a suo giudizio le ragioni di tale ritardo?

La frammentazione del reale, che si traduce nella frammentazione della collettività, ci sta facendo perdere la nostra più grande risorsa e forza, la relazione. Oggi la maggior parte degli ambiti formativi sono volti a restaurare, a formare, a incentivare, la connessione reale tra le persone, la relazione è infatti la prima grande forma protettiva da qualsiasi patologia, come da qualsiasi crisi. Dobbiamo lavorare su questo antidoto per riannodare i legami sociali e produttivi.

Il metodo è il cuore della sua riflessione. Almeno da Cartesio in poi è stato anche il fondamento del pensiero occidentale di impianto logico-razionale e del progresso della scienza. Applicato al management e alla cyber security il metodo che valenza assume?

Il metodo e la disciplina si identificano con la strada e il rigore con cui la percorriamo. Metodo deriva infatti dal greco meta (attraverso) odós (la via). Credo ancor più che il metodo e la disciplina siano fondamentali in ambito *cybersecurity,* poiché trovare un metodo applicativo ed efficace, significa trovare la strada di applicazione di quei nuovi meccanismi di difesa di cui oggi necessitiamo, e credo che un metodo funziona solo se la sua applicazione sia accompagnata da disciplina che è anche costanza del lavoro. Sono virtù che la velocità ci sta facendo dimenticare a favore, dell'instabilità e dell'incostanza che diventa inconsistenza; dobbiamo invece recuperarle. Nella mia ricerca suggerisco l'applicazione di un metodo basato sulla conoscenza, fondato sulla memoria.

La società autistica di cui parla nel saggio trova una sua corrispondenza nell'era di Internet. I social sono lo specchio riflettente della nostra identità, le intrusioni degli hacker ma anche di chi viola la nostra privacy feriscono la nostra coscienza quando non generano violenza. Come ci si può difendere da tutto questo?

La strategia credo sia sempre appunto il sapere, la capacità critica che mi permette di discernere (dal verbo greco *Krino* separare, cernere quindi giudicare n.d.r.) ciò che è valido da ciò che non lo è. Insieme a un metodo educativo che deve partire dalle famiglie, la società autistica, è appunto una società che isola i suoi elementi, ho già precisato quanto questo sia pericoloso. Aristotele ci dice che nessun uomo può vivere da solo, come ricorda Umberto Galimberti: *"O è bestia o è Dio"*. Allora la strategia praticabile è il dialogo, la connessione reale tra le persone, l'educazione al sentire, l'educazione al vivere pienamente.

Nel prossimo futuro da quali pericoli reali e virtuali dovremo difenderci a suo giudizio?

Il pericolo futuro? È reale e immaginario allo stesso momento. Direi che lo slogan dell'imminente generazione sarà "Non è quello che sembra" e questo è un pericolo reale per la nostra mente, che ha bisogno di *affordances,* sicurezze logiche, per muoversi nel mondo. Ma sono realmente convinta che le nuove generazioni, cosiddette "native digitali", saranno in grado di affrontare tutto questo. ■

L'era digitale? Una rivoluzione epocale paragonabile alla scoperta del fuoco e della ruota.

Intervista VIP ad Agostino Ghiglia.

Autore: Massimiliano Cannata

L'era digitale non è una semplice evoluzione della rete, non è una evoluzione di Internet, è una rivoluzione epocale e culturale. La definirei come una nuova scoperta del fuoco con una differenza molto netta: viviamo dentro questa scoperta alimentando il nostro gemello virtuale per oltre metà della nostra vita vigile. Un fenomeno senza precedenti che richiede conoscenza, educazione, allenamento della testa.

BIO

Laureato in Giurisprudenza con Master in Diritto Sanitario, Agostino Ghiglia attualmente è Componente del Collegio del Garante per la Protezione dei Dati. Già giornalista e imprenditore nel campo della formazione e dell'ICT, è stato Parlamentare dal 2001 al 2005 e dal 2008 al 2013 col ruolo di Capogruppo della VIII Commissione Ambiente e LLPP nonché membro della Commissione d'inchiesta sul ciclo dei rifiuti. Ha inoltre ricoperto il ruolo di Assessore regionale per la Regione Piemonte con deleghe a innovazione, sviluppo, ricerca, internazionalizzazione, commercio, energia, artigianato e società partecipate.

Agostino Ghiglia, che fa parte del Collegio dell'Autorità Garante per la Protezione dei Dati Personali, svolge un costante e prezioso lavoro di sensibilizzazione e di studio dell'ambiente digitale, che è ormai il nostro mondo, quello in cui viviamo immersi come in una dimensione omeopatica. Con la collaborazione di Alessandra Genisio e Silvia Sequi, ha dato alle stampe "Educazione civica digitale" (ed. Apogeo), un brillante scritto sui percorsi di sviluppo dell'information society.

Comincerei la nostra conversazione traendo spunto dal "manuale delle banalità sconosciute", come Lei stesso lo ha definito. Come nasce questo interessante progetto editoriale?

Partiamo da un assunto che può fare da premessa ad ogni riflessione successiva: in una società digitale non conoscere a sufficienza i "nuovi alfabeti" connessi alla strumentazione tecnologica, è come non conoscere la lingua del Paese nel quale si vuole lavorare e affermarsi. Sta accadendo questo, ad una porzione molto ampia della popolazione. Ce ne accorgiamo quando lasciamo i nostri figli davanti al cellulare, per poter ottemperare alle nostre faccende e attività, abitudine molto diffusa per altro. L'errore che commettiamo è semplice: pensiamo che essere nativi digitali vuol dire avere piena consapevolezza e conoscenza dei rischi. Vediamo i piccoli già bravissimi a manipolare cellulare e tastiere, perché preoccuparci? In realtà il vero pericolo di oggi è dato da un eccesso di informazione e da una grave assenza di educazione. Torniamo dunque all'ABC, all'abbecedario essenziale, quello che ci ha guidato fin da bambini alla conoscenza e alla "lettura" del mondo. Il manuale nasce così.

La scuola è centrale in questo ragionamento che sta facendo, ed è anche nell'occhio del ciclone per quello che ogni giorno avviene e che la cronaca ci racconta. Che riflessione dobbiamo fare in proposito?

Fin dal primo ciclo scolastico bisogna imparare a comprendere i significati di tante parole che usiamo con superficialità. La Competenza digitale passa attraverso un uso appropriato del linguaggio che, come diceva Heidegger, è *"la casa dell'essere"*. Il deficit dell'Italia in questo ambito risulta molto evidente rispetto ad altri Paesi Europei. Bisognerà aumentare sforzi e investimenti a tutti i livelli, non mi riferisco solo alla scuola ovviamente, penso alle istituzioni e alle imprese che devono essere coinvolte in un piano educativo che ci consenta di esercitare una cittadinanza piena, bilanciando diritti e doveri nuovi, nell'orizzonte mutante dell'information society.

Alleniamo testa e muscoli per capire il digitale

Lei è uno dei Componenti del Collegio del Garante per la Protezione dei Dati Personali. Che funzione può e deve avere l'Authority in questo impegnativo cammino di sensibilizzazione ai temi della sicurezza digitale?

Molto stiamo già facendo per equilibrare una corsa frenetica che non sappiamo ancora bene dove ci porterà. Ad un anno dal lancio di chat GPT l'intelligenza generativa è esplosa, siamo di fronte a una rivoluzione nella rivoluzione. Se la corsa va verso l'ammodernamento della nazione, fa bene a tutti, ma in questa corsa come fa ogni buon *runner* dovremmo allenare i muscoli e sottolineerei la testa, in questo caso. Torna il tema dell'*education* e della cyber sicurezza, fattore centrale nel discorso che stiamo facendo. Non penso solo ai più giovani, ma anche agli adulti che spesso subiscono la tecnologia senza approfondire il fenomeno che si trovano di fronte. Siamo portati a dare il nostro consenso ai *cookie* senza sapere di cosa è fatto il tessuto profondo delle parole. Non dico che bisogna imporre pagine e pagine di norme prima di aprire un sito, ma almeno imparare a "navigare" in sicurezza con poche semplici indicazioni sarebbe già un bel passo avanti. Ricordiamoci che la tecnologia non è più neutra come si pensava in passato, può diventare molto pericolosa se usata in modo sbagliato.

Cosa si può concretamente fare per innalzare il livello di sicurezza nella fruizione di questi straordinari, ma anche "insidiosi" strumenti?

Faccio qualche rapido concreto esempio. L'Authority solo quest'anno ha limitato l'utilizzazione di tre *chatbot,* due anni fa fummo costretti a bloccare TikTok perché aveva dei meccanismi insufficienti di verifica anagrafica. La maggior parte delle piattaforme sono sprovviste di misure di protezione, sono di fatto dei gate aperti, fuori controllo. Per questa ragione stiamo lavorando di

concerto all'AGCOM per mettere a punto dei processi rigorosi di verifica anagrafica. Abbiamo bloccato l'uso di "replika", un chatbot sentimentale, che dopo un primo approccio amicale fa spingere oltre gli utenti, chiedendo somme di denaro, senza alcuna garanzia in termini di sicurezza del trattamento dei dati sensibili.

A proposito di misure di contenimento della violazione della Privacy. Recentemente il Garante ha lanciato un alert molto importante sul* webscraping*, Possiamo spiegare la natura dell'intervento?

Si tratta di un'indagine conoscitiva sui siti internet pubblici e privati che abbiamo messo in atto per verificare l'adozione di idonee misure di sicurezza adeguate a impedire la raccolta massiva, che si definisce appunto *webscraping* di dati personali a fini dell'addestramento degli algoritmi di intelligenza artificiale da parte di soggetti terzi. Questo "rastrellamento" indiscriminato di dati, che tutti noi forniamo con finalità precise e limitate, viene operato a nostra insaputa per conoscere abitudini, gusti, interessi, attività che attengono alla nostra sfera più intima. Il divieto intimato da Mediaset a Open AI di utilizzare dati reperibili sui propri sistemi aziendali per "allenare" gli algoritmi" avvenuto nei giorni scorsi, è destinato a fare "scuola" e a inaugurare una tendenza che prenderà certamente piede nel prossimo futuro.

Il destino della nostra identità in Rete e il Metaverso

Fenomeni nuovi quelli di cui Lei parla, con cui dovremo imparare a rapportarci e che hanno a che fare con il destino della nostra identità in rete. Il primo lemma del suo vocabolario non a caso è: "Account". La nostra identità in rete, che va a comporre quello che Stefano Rodotà definiva "il nostro corpo elettronico". Questione non da poco, non crede?

Stefano Rodotà ha posto per primo la grande questione della protezione dei dati personali nella società telematica. L'account è la visualizzazione della nostra identità virtuale. Non possiamo comprendere quello di cui parliamo se non ci rendiamo conto che l'era digitale non è una semplice evoluzione della rete, non è una evoluzione di Internet, è una rivoluzione epocale e culturale. La definirei una nuova scoperta del fuoco. Non è un'iperbole.

In che senso, può spiegarcelo?

Quando l'uomo scoprì il fuoco, non passava tutta la vita usando o "giocando" col fuoco, e neanche con la ruota. Oggi, i nostri ragazzi tra gli otto e i diciannove anni passano oltre la metà della vita vigile in rete. Un fenomeno antropologico che ha una portata senza precedenti. Da quando ci svegliamo e guardiamo l'ora sul telefonino, creiamo il nostro gemello digitale, che cresce con noi nel corso della giornata. Entriamo in rete impariamo molte cose, è vero, ma diamo anche cose preziose, dati e informazioni su di noi. Nell'era digitale la persona è un "dato" ed è fatto oggetto di aggressione, manipolazione, patrimonializzazione, scambio, violenza.

A proposito di violenza. Bambini e Internet, cyberbullismo e non solo. Le chiederei di toccare rapidamente questo ulteriore fronte molto delicato. A che punto siamo?

L'educazione civica serve oggi come ieri. Le norme di buona educazione aiutano anche nella information society con un'aggiunta: uno dei pericoli della rete è la defisicizzazione del male. Pensiamo a quanto avvenuto a Caivano. Ho compiuto un atto violento, me ne rendo conto ex post a mente fredda, certo, ma c'è qualcosa che va oltre. Dopo aver brutalizzato una persona, filmando il suo dolore la stupro per l'eternità, questo spesso sfugge alla coscienza. Forse non ci rendiamo conto, che la defisicizzazione e la diseducazione digitale estende il male medesimo, lo rende "metafisico" incontrollabile. È un fatto molto grave, la perdita dell'uso del corpo, della fisicità, ci fa perdere ogni autocontrollo ogni rispetto dell'educazione e della continenza.

Intanto si affaccia il metaverso. Le chiedo in conclusione: è un'agorà ancora tutta da esplorare?

Siamo diventati testimoni inconsapevoli della più grande campagna pubblicitaria mediatica della storia. Un bel giorno Mark Zuckerberg fa proprio il termine molto evocativo coniato da Neal Stephenson, ma cosa c'è dietro? Ad oggi è una suggestione vuota. Una realtà aumentata, non una novità. Non esiste una interoperabilità tra i 235 metaversi fino a ora censiti che aumentano ogni giorno. Provocatoriamente li chiamerei ultraversi per evitare pubblicità occulta a un solo brand. Mi riservo comunque il giudizio. Se la potenza di calcolo dei PC consentirà una reale interoperabilità tra le piattaforme, potremo sperimentare una vita virtuale in questi "altri mondi", posto che iniziativa utile, piacevole, vantaggiosa, chi lo sa…. Ne riparleremo molto presto, credo… ■

La sicurezza, un bene comune da tutelare.

Intervista VIP a Bruno Frattasi.

Autore: Massimiliano Cannata

"La strategia che serve è basata anzitutto sulla protezione cibernetica degli asset nazionali, ma anche sull'attenzione e sulla consapevolezza. Solo da una presa di coscienza forte del problema possono nascere gli investimenti e la riorganizzazione aziendale necessari a far fronte, insieme, alla minaccia". Il Prefetto Bruno Frattasi, Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, offre uno sguardo ampio sulle dinamiche connesse al rischio cyber, che presenta implicazioni in tutti gli ambiti della vita sociale, economica, chiamando in causa la responsabilità delle Istituzioni e delle classi dirigenti di ogni angolo del pianeta.

BIO

Il 9 marzo 2023, il Prefetto Bruno Frattasi è stato nominato Direttore Generale dell'Agenzia per la cybersicurezza nazionale su proposta del Presidente del Consiglio dei ministri. Entrato in Amministrazione nel 1981, nel 2005 è stato nominato Prefetto della Repubblica. Nel corso di oltre quaranta anni di esperienza, ha ricoperto numerosi incarichi, tra cui quelli di Prefetto di Latina e di Roma, Capo Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile, Capo dell'Ufficio Legislativo e Capo di Gabinetto del Ministro dell'Interno. È stato anche direttore dell'Agenzia Nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata (ANBSC).

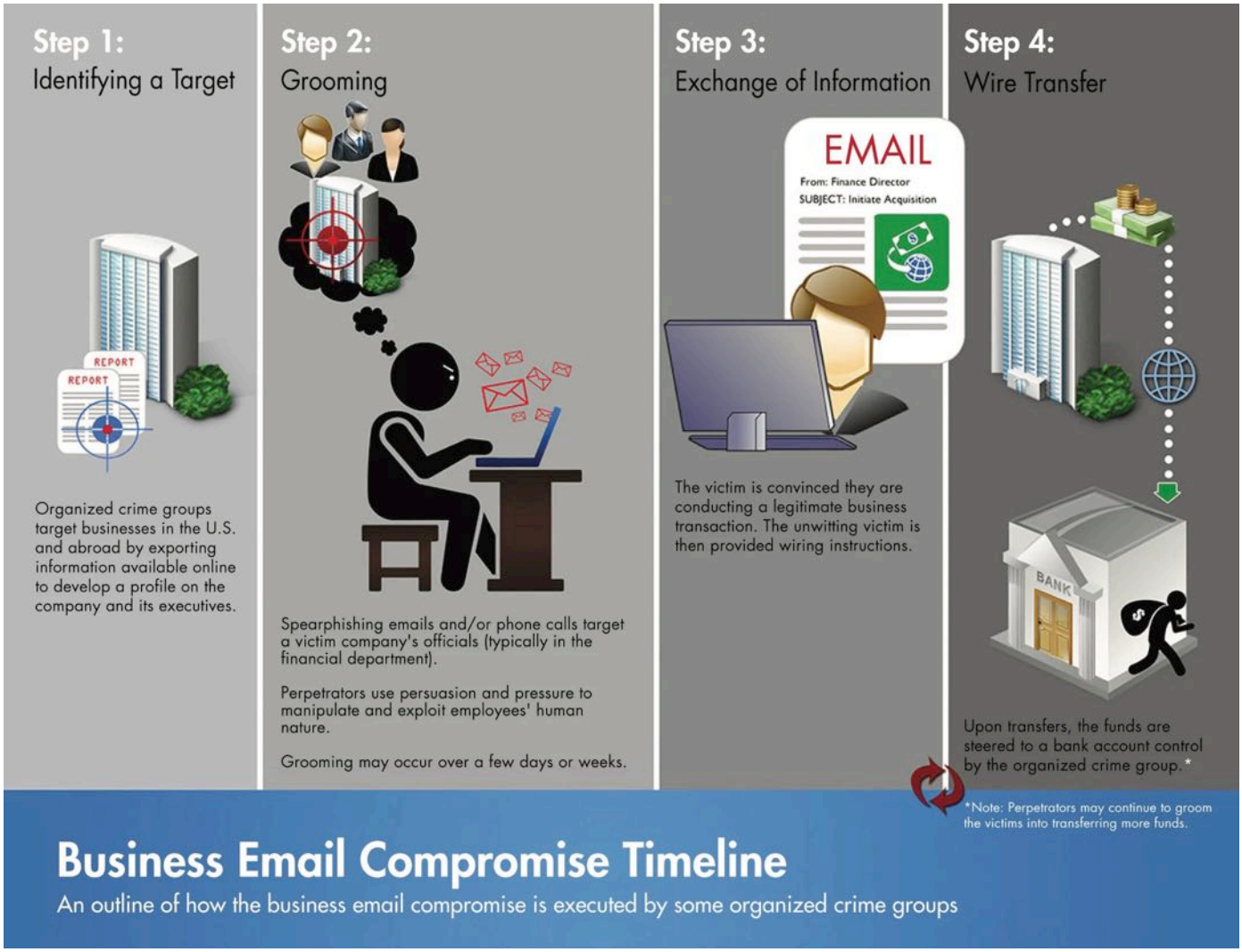
AGENZIA PER LA CYBERSICUREZZA NAZIONALE

Direttore, partirei dalla stretta attualità. Il recente vertice a Palazzo Chigi è la dimostrazione netta del peso strategico che riveste la protezione dello spazio cibernetico nella società digitale. I conflitti in Ucraina e in Medio Oriente rendono il quadro più complesso. Qual è il livello di rischio delle nostre infrastrutture critiche?

Gli attacchi ci sono stati e sono aumentati anche a causa dei conflitti geopolitici, ma ricordiamoci che l'Italia viene attaccata ogni giorno da criminali in cerca di profitto: lanciano campagne di phishing, in particolare di tipo Bec (business e-mail compromise), oppure diffondono ransomware per estorcere denaro. Lo abbiamo visto soprattutto nel settore manifatturiero, energetico e delle vendite al dettaglio. L'Italia è terza in Europa e sesta nel mondo per attacchi ransomware. Il motivo per cui questo accade è molto chiaro, l'Italia è un paese del G7, tra le prime manifatture in Europa e con un capillare sistema bancario.

Un tema sempre più sentito è quello relativo all'awareness. Il capitale umano rimane il fattore di forza ma anche di fragilità delle organizzazioni produttive. ACN è molto impegnata su questo fronte, cosa si può fare rafforzare le competenze digitali e far crescere una consapevolezza diffusa sui rischi che l'uso della rete e degli strumenti digitali oggi comporta?

Noi abbiamo proposto di avviare gli studenti allo studio dell'informatica e della cybersecurity già dalle scuole elementari. È importante partire dai più piccoli perché, come mi piace dire, i bambini a quell'età sono creta da plasmare a livello formativo ed hanno grande apertura mentale. Non tutti da grandi dovranno lavorare nel settore, ma a scuola si insegna anche la



musica e certo non tutti da grandi faranno i musicisti. È importante dotare tutti di solide competenze di base affinché abbiano conoscenza e consapevolezza delle opportunità e dei rischi che l'uso del mezzo digitale, e in particolare dell'Intelligenza Artificiale, comporta.

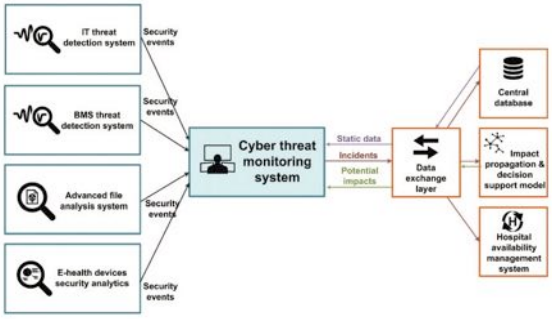
L'impegno di ACN sul fronte della formazione avanzata

L'accordo di collaborazione che* l'Agenzia per la Cybersicurezza Nazionale *(ACN) ha definito con la Conferenza dei Rettori delle Università Italiane, finalizzato a promuovere lo sviluppo di attività formative di cultura del digitale, aprirà capitolo nuovo nel modo di approcciare il digitale. Quali iniziative intendete attuare?

Partiamo da una premessa. Prima di entrare nel merito della sua domanda mi consenta di dire che l'Italia ha bisogno di crescere, come tutti gli altri paesi europei, nelle competenze di carattere digitale. Il divario è ancora troppo elevato rispetto al fabbisogno, anche se i numeri in questo ultimo anno tendono lievemente a crescere. Cosa bisogna fare dunque? Bisogna investire nella formazione, non solo quella universitaria e post-universitaria, ma anche in quella che riguarda il ciclo scolastico secondario, licei e ITS. Sotto il profilo universitario e post-universitario certamente l'accordo di collaborazione con la CRUI rappresenta il presupposto necessario perché l'Accademia possa introdurre percorsi formativi di laurea e post laurea che abbraccino il tema digitale e in particolar modo quello della cybersicurezza. Infine, vorrei ricordare anche il ruolo che può svolgere la formazione da parte delle Digital Academy, ossia i centri di formazione e di competenza che enti pubblici e grandi società stanno costruendo.

ACN sta investendo 20 milioni di euro per un sistema di supercalcolo avanzato per il monitoraggio della minaccia cyber. Quali sono gli obiettivi di questa importante iniziativa?

L'obiettivo è quello di avere informazioni in tempo reale sullo stato della minaccia cibernetica nel nostro paese. Nelle nostre intenzioni questo sistema di calcolo consentirà all'Agenzia di diventare un protagonista anche nel campo dell'Intelligenza Artificiale. Il sistema, infatti, darà maggiori capacità e consentirà all'Agenzia di contribuire allo sviluppo di strumenti in grado di rilevare le minacce e i rischi informatici con maggiore precisione e prontezza, contribuendo così alla resilienza del sistema Paese. Complessivamente, gli investimenti per la realizzazione del centro di calcolo, l'acquisizione dei sistemi HPC (High Performance Computing) e i costi operativi e di gestione saranno dell'ordine di circa 50 milioni di euro, di cui oltre 20 messi a disposizione dall'ACN. Un grande investimento che sostiene e consolida il ruolo del Mezzogiorno nell'ambito dell'innovazione tecnologica. Con questo progetto l'infrastruttura di calcolo nazionale si arricchisce di un importante nodo HPC, integrato nel sistema europeo di supercalcolo. Il sistema, collocato presso la sede del Cineca di Napoli, infatti, farà parte di una rete di sistemi complementari del super computer Leonardo, e consentirà di supportare non solo le applicazioni consolidate della fisica, della chimica, delle scienze ambientali e dell'ingegneria, ma soprattutto le applicazioni di apprendimento automatico e di intelligenza artificiale sia classica che generativa.



La ricerca di un modello di governance condivisa della rete

Si sta cercando di attuare una governance della rete, nel tentativo di garantire la Privacy, i diritti della persona e la trasparenza oltre che la sicurezza delle transazioni e delle relazioni sul web. Rodotà vagheggiava la definizione di una "Costituzione per Internet". Con il Metaverso e l'avvento delle "minacce ibride" (lo si sta vedendo molto bene con il conflitto in Ucraina) la sfida etico - giuridica oltre che tecnologica diventa ancora più alta, rendendo attuale quella intuizione. Come va affrontato questo "secondo tempo" di Internet e del digitale?

La sua domanda pone il tema delle cosiddette *disruptive technologies*, tra le quali non solo va incluso lo sviluppo di IA e algoritmi, ma anche la crittografia post quantum, che ci servirà a difendere meglio i nostri dati, proprio rispetto a un uso malevolo dell'IA da parte degli attaccanti. Non dimentichiamo che l'Intelligenza Artificiale è una tecnologia *dual use*, che cioè si presta ad essere utilizzata sia da chi ha intenzione di rivolgere un attacco verso una superficie digitale, sia da chi da quell'attacco deve difendersi. A causa dell'IA sarà possibile, ad esempio, mettere a punto campagne di *spear phishing* più insidiose.

L'utilizzazione dell'Intelligenza Artificiale passa attraverso l'uso di una regolazione il più possibile condivisa sulle regole e sui criteri che dovranno presiedere allo sviluppo di questo formidabile strumento. Si è più volte ripetuto che il problema non sta tanto nella potenzialità distopica dello strumento ma nella nostra capacità di stabilirne i confini, quel famoso guard rail di cui parla padre Paolo Benanti. Il problema, tuttavia, è questo: l'Europa si sta dotando di un Regolamento, non mancano le differenze e le divisioni sulla sua visione complessiva, ma, nonostante l'Europa sia una Federazione di paesi con storie politiche diverse, a forza di compromessi sta faticosamente raggiungendo un punto di arrivo, e nel 2024 si spera che il Regolamento europeo diventi una realtà.

Fin qui il vecchio Continente, nel resto del mondo cosa accade?

L'Europa rappresenta però una parte del mondo Occidentale, e non sappiamo se negli USA questa posizione sarà completamente condivisa e se altri paesi che si affacciano come potenze mondiali, abbiano o non abbiano in mente la stessa idea di sviluppo dell'IA. Sappiamo, ad esempio, che in Cina esistono delle forme di IA per fare il rating sociale che non sono accettabili dal sistema valoriale occidentale ed europeo, in cui si dà centralità ai diritti fondamentali della persona.

Qualche giorno fa il fisico italiano, premio Nobel, Giorgio Parisi, ha detto – e trovo del tutto ragionevole questa posizione, peraltro così autorevole - che in tema di intelligenza artificiale bisogna arrivare allo stesso tipo di accordo attraverso il quale le potenze globali sono giunte ai trattati di non proliferazione nucleare. Si tratta di concordare su principi basilari orientati alla protezione della persona e della dignità umane e al ripudio di un uso dell'IA contrario a questi principi, cioè a un uso rispettoso degli individui che non devono essere considerati soggetti da sfruttare, si pensi alla profilazione commerciale e all'orientamento di gusti e comportamenti. Poi, certo abbiamo il grande tema dell'IA al G7 del prossimo anno. Un tema, direi in conclusione, rilevantissimo anche per l'Italia che avrà il ruolo e la responsabilità di guidare questo nuovo e importante esercizio. ■

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

Qual è l'impatto Psicologico dell'AI nella Cyber Security?

In un mondo sempre più connesso, l'intelligenza artificiale è diventata un pilastro fondamentale nella Cyber Security.

Parallelamente, la Psicologia svolge un ruolo cruciale nel comprendere come gli esseri umani interagiscono con queste tecnologie avanzate.

Intelligenza Artificiale, Cyber Security e la Mente Umana: Un Futuro Interconnesso

Essendo la relazione tra AI, Cyber Security e Psicologia in continua evoluzione, è necessaria una comprensione approfondita di queste dinamiche. Nel panorama futuro, possiamo aspettarci che l'AI continui ad evolversi, diventando sempre più sofisticata e integrata nelle nostre vite quotidiane.

Questo progresso tecnologico solleverà nuove domande e sfide, sia dal punto di vista della sicurezza informatica che dal punto di vista psicologico, poichè comprendere come le persone percepiscono, interagiscono e rispondono all'AI è fondamentale per il successo della sua implementazione nella sicurezza informatica.

Mentre avanziamo in questo futuro interconnesso, la nostra sfida sarà quella di armonizzare i progressi tecnologici con una profonda comprensione della psicologia umana, creando così un ambiente digitale che sia oltre che sicuro, anche etico, inclusivo e rispettoso delle identità umane.

Ottimizzare la Sinergia tra AI e Psicologia nella Cyber Security

GESTIONE EMOTIVA
Affina una gestione delle emozioni quando interagisci con l'AI per mantenere una presa di decisioni calma e razionale anche in situazioni di cyber security.

APERTURA AL CAMBIAMENTO
Sii aperto alle evoluzioni nel campo dell'AI, accogliendo le innovazioni come opportunità di miglioramento. della sicurezza.

ADATTABILITÀ EMOTIVA:
Sviluppa l'adattabilità emotiva per gestire i cambiamenti rapidi nel campo dell'AI e della sicurezza informatica.

La nostra Missone è passare dall' Informazione alla Trasformazione

www.securitymind.cloud

Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.

Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

Scaricatele su: www.distrettocybersecurity.it/linee-guida-itu

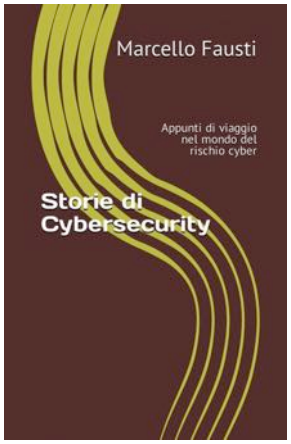
www.itu.int/cop

Bibliografia - Cybersecurity Trends

Marcello Fausti
Storie di cybersecurity.
Appunti di viaggio nel mondo del rischio cyber

Autore: Massimiliano Cannata

La governance del rischio nella società complessa



Gli appunti di Marcello Fausti, Cybersecurity Advisor e CISO di molte grandi aziende italiane, costituiscono un forte condensato di esperienza e di visione. Identità professionale e percorso emergono in una sintesi alta in questo lavoro, finalizzato a sensibilizzare il mondo delle istituzioni e delle imprese a investire in un settore strategico. Le storie, raccontate con eleganza stilistica e con l'occhio attento del tessitore di trame, sono lo strumento di una modalità avanzata di formazione, che adotta nuovi linguaggi per arrivare ai pubblici di riferimento. *"Qualsiasi ambito dell'attività umana - commenta l'autore – il lavoro, le arti, i servizi, la moneta, tutto è ormai basato sulle tecnologie digitali che negli ultimi venticinque anni hanno compiuto progressi che visti con gli occhi di ieri ci appaiono realmente miracolosi. Purtroppo, però, in questi ultimi anni ci siamo comportati come i costruttori che spinti dalla fretta di erigere magnifiche cattedrali si sono dimenticati di dedicare la giusta attenzione alla solidità delle fondamenta. La nostra società è poggiata su una piattaforma digitale debole per sua natura, esposta agli attacchi di chi abbia intenzione e interesse a minarla alle fondamenta, cosa che stiamo drammaticamente vedendo ai giorni nostri in cui i conflitti convenzionali si trasformano dinamicamente in conflitti cibernetici".*

Consapevolezza, formazione, attitudine all'innovazione sono ingredienti necessari, ma niente si improvvisa, lo sforzo deve essere preparato e continuo per dare risultati. Dal paradigma del controllo al paradigma della governance come insegna l'epistemologia della complessità, è cambiato il modo di approcciare e di concepire la sicurezza. *"Il rischio che può minarne in modo drammatico la capacità di sviluppo: è il rischio cyber, ovvero, il rischio che i mattoni digitali con cui stiamo costruendo il nostro futuro siano troppo deboli per resistere ai colpi di chiunque voglia arrecarci danno allo scopo di cambiare le traiettorie di crescita di nazioni e, addirittura, di interi blocchi geopolitici".* Siamo oltre quel corpus di fatti ed eventi che definivamo convenzionali. La difesa dello spazio cibernetica è divenuta un "affare di stato", come dimostra l'istituzione dell'ACN (Agenzia Nazionale della Cyber security) e il recente vertice convocato dalla Premier per valutare il livello di vulnerabilità delle infrastrutture critiche del Paese, particolarmente esposte ai venti di crisi sospinti dai venti di guerra che provengono dal Medio Oriente e dall'Ucraina. Gli effetti dell'instabilità geopolitica, possono riverberarsi in tutti gli ambiti della quotidianità, con conseguenze molto gravi.

Cosa dobbiamo fare? Si chiede e ci chiede Fausti. Come possiamo impegnarci per invertire questa tendenza ormai così evidente? "Formare e allenare", i termini usati, hanno a che fare con la mente e con la fisicità, d'altra parte ce lo ricorda in un celebre scritto Umberto Galimberti *psiche e technè* devono andare all'unisono. Se si dà una scorsa ai capitoli, si ritrovano tutte le grandi questioni che sono al centro delle attenzioni non solo del mondo manageriale, ma anche delle istituzioni. L'excursus storico iniziale è importante per avere una lettura diacronica delle fenomenologie attinenti al divenire di una materia come la cyber security dove non possono esistere punti fermi. Dalle tecniche di attacco, alla ridefinizione del profilo degli hacker che stanno mutando volto e strategie come si vede molto bene con i recenti attacchi sferrati ai gangli vitali delle amministrazioni pubbliche e alle strutture sanitarie di molti paesi, il ventaglio del rischio si allarga, coinvolgendo, come si vede dall'attenzione per la difesa della supply chain, un terreno ampio di relazioni. In tutto questo il CISO è un manager o stregone, è il titolo di uno dei capitoli. Difficile dare una risposta, se si considera il peso delle responsabilità che riveste, il sofisticato ambiente tecnologico che deve governare, e le implicazioni sulla catena del valore di ogni sua decisione, forse deve essere entrambe le cose: manager, stregone e ci permettiamo di aggiungere, "miracolato". ■

Mauro Ceruti
Francesco Bellusci
Umanizzare la modernità
Ed. Raffaello Cortina

Autore: Massimiliano Cannata

Sicurezza vuol dire consapevolezza e senso del limite

Mauro Ceruti, filosofo e pensatore tra i più influenti del secolo, Premio Nonino 2022 in qualità di "maestro del nostro tempo" con questo saggio concepito e scritto con Francesco Bellusci suggerisce un modo nuovo di pensare il futuro nella società digitale. Il saggio si inserisce in un'ampia riflessione che prende le mosse dal "Il tempo della complessità", attraversa titoli più recenti, quali: "Sulla stessa barca", "Abitare la complessità", opere di fortissimo impatto sull'attualità in cui viene tematizzata la crisi del "paradigma tecnocratico". La civiltà umana deve ricucire il suo rapporto con la natura e con gli altri esseri viventi, per recuperare un equilibrio sostenibile e alimentare una positiva sete di innovazione. "Più nessuno è incolpevole" si potrebbero utilizzare i celebri versi di Montale, per sintetizzare la tesi di fondo di una ricerca che mette l'uomo al centro in una dimensione di corresponsabilità, che coinvolge tutti, classi dirigenti, istituzioni, imprese, sistemi della rappresentanza cittadini. In questo XXI secolo l'imperativo non sarà "modernizzare", ma "umanizzare

la modernità". È stata la modernità ad inventare i valori della libertà e dell'uguaglianza, ma ha anche preteso di creare corpi sociali e culturali omogenei e di sacralizzare i confini, spesso entrando in contraddizione con la proclamata universalità dei suoi valori. Oggi quel paradigma è obsoleto e tragicamente inadeguato rispetto all'orizzonte planetario in cui già viviamo. Anche se progresso è un termine ambivalente, avere un rapporto con il futuro è necessario, sia per gli individui sia per le società, per sviluppare speranze, aspettative e desideri. Va, però, detto che qualche decennio fa questo rapporto è entrato in crisi. L'angoscia che pervade le nostre vite è legata a questa perdita di futuro. Fino agli anni '70 il progresso era sentito, prima ancora che pensato, come certo. Ma le crisi globali degli ultimi anni mettono in discussione il futuro dell'umanità: pandemie, catastrofi climatiche, guerra, crisi energetica ci rivelano che ci vuole un radicale cambiamento di paradigma. La fiducia nel futuro vacilla, perché c'è poca fiducia. La crisi della modernità ha, infatti, prodotto due tipi di risposte: da un lato il postmodernismo, cioè la convinzione che non ci sia più storia o divenire, solo un "eterno ritorno" del già detto, del già pensato; dall'altro lato risposte regressive come i fondamentalismi religiosi, i nazional-populismi, i neoimperialismi. Il futuro è avvolto dalla nebbia. Viviamo in una tirannia del presente, che fa prevalere il pensiero e l'azione a breve termine, la sensazione sulla memoria, l'impulso sulla visione. Il progresso si è rovesciato in un regresso. Quello scientifico e tecnico non si è tradotto automaticamente in progresso umanitario, come pensava l'Illuminismo.

L'uomo tecnologico o sarà uomo di pace o non sarà

È evidente che il futuro è consegnato nelle mani di una nuova e rinnovata responsabilità, di una nuova visione umanistica. La prossima guerra condotta fino alle estreme conseguenze - ci stiamo purtroppo avvicinando - non avrà più vinti da una parte e vincitori dall'altra, grandi distruzioni per alcuni e grandi opportunità per altri: lascerà sul campo solo dei vinti, non soltanto per le conseguenze dirette, distruzioni e morti, ma perché le nuove tecnologie introducono mutamenti nella biosfera che renderanno non sostenibile, o comunque ridotta ai minimi termini la sopravvivenza della specie umana, e anche di moltissime altre specie viventi.

Si parla ormai, tra scienziati, di una possibile sesta estinzione di massa: la pellicola di vita che circonda la Terra è fragile. Una grande sfida per chi si occupa di sicurezza a diversi livelli. Il rischio è endogeno, si sviluppa all'interno della specie umana, a causa del progresso della sua potenza, e può diventare motivo della nostra estinzione. L'uomo del futuro – come diceva già padre Balducci – "sarà uomo di pace o non sarà". L'uomo di guerra si estinguerà. Abbiamo pochissimo tempo a disposizione. Il futuro dell'umanità è legato alla costruzione di una comunità di destino tenuta insieme dagli stessi pericoli. Questa fragilità può far emergere un pensiero nuovo spiega l'autore. Una sfida di fiducia, che va oltre la semplice tutela tecnologica di reti e sistemi. È un'opportunità che ci è data per costruire una cultura della relazione e non del dominio. Bisogna andare avanti, non si può entrare nel nuovo millennio indietreggiando». "Scommettere sull'improbabile" concludono gli autori, è il compito più arduo, ma necessario, l'unico realistico". ■

La sicurezza nel Cyberspazio Federico Ursi (a cura di) Ed. Franco Angeli

Autore: Massimiliano Cannata

I profili giuridici del Cyber spazio

"Il cyberspazio è un ambiente in cui gli esseri umani e le loro organizzazioni utilizzano le tecnologie per agire e produrre effetti rilevanti sia al suo interno sia nell'ambito di altri domini. In questo contesto, per poter affrontare il tema della dimensione giuspubblicistica della sicurezza, occorre domandarsi che cosa si intenda oggi per rete sicura, in che modo il "Leviatano" riesca ancora a svolgere il suo ruolo in un mondo senza confini, in che senso il diritto possa regolare l'azione dei privati e i compiti delle istituzioni pubbliche". Questa nota dell'editore restituisce molto bene la profondità e il senso della raccolta di saggi curata da Riccardo Ursi, Professore ordinario di diritto amministrativo dell'Università di Palermo. Riportiamo alcuni passaggi del saggio introduttivo di Ursi, che meritano attenzione per il crocevia di tematiche che affronta.

La sicurezza informatica come funzione pubblica è il perno della trattazione, che grazie all'apporto di esperti di caratura internazionale, si inoltra a definire i profili giuridici della materia, il ruolo strategico dell'ACN, i compiti del Ministero dell'interno, il perimetro della sicurezza cibernetica, la collaborazione tra pubblico e privato, le modalità di trattamento dei dati personali. L'ultimo intervento, di Andrea Mattarella, nipote di Piersanti Presidente della Regione tragicamente assassinato dalla criminalità organizzata, è dedicato all'approfondimento degli aspetti penali del cybercrime in rapporto a quanto previsto dalla Convenzione ONU sulla criminalità informatica.

"Il mondo interconnesso in cui viviamo – scrive Ursi - dipende integralmente dalle informazioni, dall'informatica e dalle comunicazioni. Si tratta di una condizione che se, da un lato, agevola lo sviluppo delle relazioni e rende i sistemi economici, sociali ed istituzionali maggiormente efficienti e performanti, li espone, dall'altro, a numerosi pericoli, dato che la vita quotidiana di ogni cittadino, l'economia nazionale e la sicurezza stessa degli Stati sono ormai indissolubilmente legati alla stabilità e alla sicurezza del cyberspazio. Quest'ultimo viene definito come un ambiente globale, caratterizzato dall'uso dell'elettronica e delle ICT per creare, immagazzinare, modificare, scambiare e sfruttare informazioni attraverso reti e sistemi interdipendenti. In sostanza, come espressamente indicato dalle linee guide ISO/IEC del 2018, si è in presenza di un «complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form». Queste reti e sistemi informativi risiedono, simultaneamente, nello spazio fisico e nello

spazio virtuale, così come all'interno e all'esterno dei confini geografici. In questo senso, il cyberspazio è un ambiente in cui gli esseri umani e le loro organizzazioni utilizzano le tecnologie per agire e produrre effetti rilevanti sia al suo interno sia nell'ambito di altri domini fisici: un nuovo dominio operativo di natura artificiale, trasversale agli altri quattro domini tradizionali (dominio terrestre, dominio aereo, dominio marittimo, dominio spaziale) (…)

Negli ultimi trent'anni la crescita di Internet e dell'innovazione che ne è derivata è stata facilitata da un ambiente relativamente privo di controlli. Tuttavia, la profonda integrazione nel quadro sociale del World Wide Web ha messo in discussione l'idea tradizionale di sicurezza, intesa come predisposizione di un perimetro normativo funzionale al libero esplicarsi della sfera individuale. Ad essa sembra progressivamente sostituirsi un modello legato al concetto di protezione, caratterizzato dalla disponibilità (anche implicita) a scambiare/ sacrificare spazi di libertà personale a fronte della possibilità di operare in un ambiente sociale e tecnologico politicamente e giuridicamente protetto (secondo il paradigma dello Stato preventivo (…)

Questi due flash possono bastare per comprendere la molteplicità delle implicazioni che comporta l'analisi della sfera giuspubblicistica ai temi della sicurezza cibernetica. Non ci si può rifare a una ricostruzione di quanto è già noto, né a un semplice adattamento delle categorie tradizionali, perché ne occorrono di nuove per affrontare la rivoluzione in corso. Se Hobbes scriveva: "senza sicurezza non c'è posto per l'applicazione del lavoro perché il frutto di esso è incerto, e perciò non si coltiva la terra, non ci si dedica alla navigazione, (…) non si coltiva la storia, le arti, le lettere, i rapporti sociali, e ciò che è peggio si vive in uno stato di continuo timore e pericolo di morte violenta, e la vita dell'uomo è solitaria, misera, ripugnante brutale e breve", la colta citazione richiamata dallo studioso può essere utile a farci comprendere come senza un'adeguata protezione del cyber spazio, che è una quarta dimensione ibrida fatta di reale e virtuale, tutto è precario, non solo sarebbe impossibile intraprendere qualsiasi attività lavorativa e relazionale, ma la nostra stessa sopravvivenza sarebbe seriamente messa sotto scacco. ■

57° Rapporto del Censis Ed. Franco Angeli

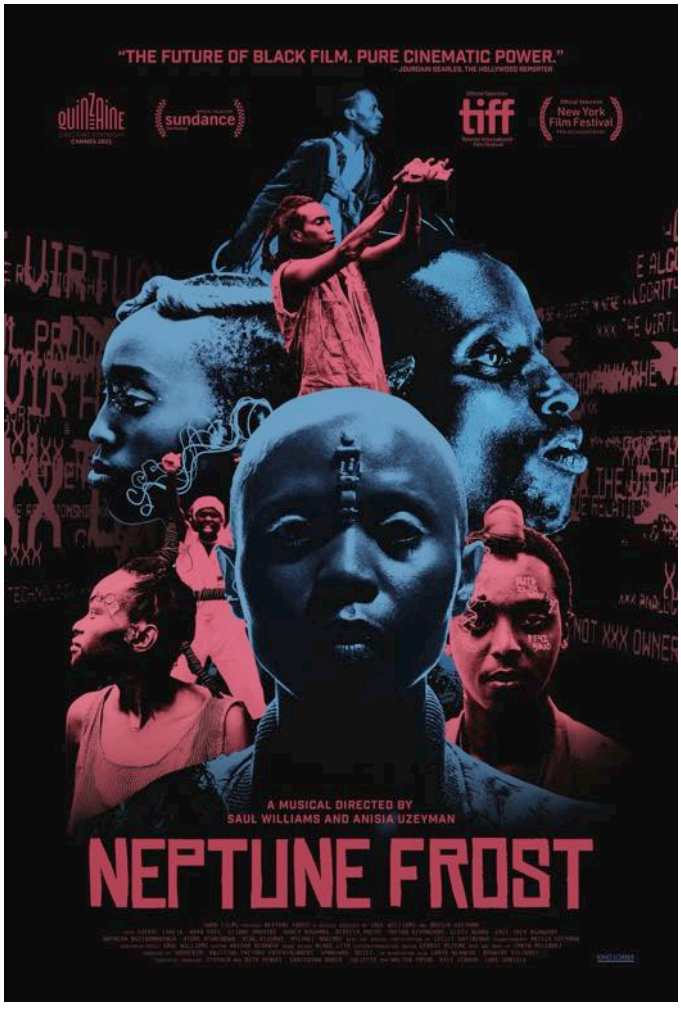
Autore: Massimiliano Cannata

L'Italia dei "sonnambuli"

Il nostro è un paese *"sonnambulo"* apparentemente vigile, ma di fatto cieco rispetto agli oscuri presagi. L'immagine dell'Italia che arriva dal 57° Rapporto del Censis non lascia adito a dubbi. "Il calcolo raziocinante – ha spiegato il direttore generale Massimiliano Valerii nel corso della presentazione effettuata a Roma come da tradizione presso la sede del CNEL - non viene esercitato dalle nostre élites, che tendono a sottovalutare i molteplici rischi cui è esposto il sistema paese". La transizione demografica è la prima "bomba" pronta a scoppiare. Nel 2050 avremo quasi 8 milioni di persone in età lavorativa

in meno, con una diminuzione della popolazione residente di 4,5 milioni di persone, pari a Roma e Milano messe insieme. Sono dati che avranno un peso fortissimo sulla struttura produttiva e sulla creazione di valore delle nostre imprese, ma nessuno sembra occuparsene. Siamo presi da desideri minori, lo stile di vita non è più quello degli anni ruggenti, che ci proiettava verso grandi prospettive. I piccoli desideri non trainano la società, che ristagna. In passato il Censis ci aveva offerto la visione di un paese in preda al rancore, che aveva accumulato ritardi evidenti ma con una grande voglia di risalire la china, aveva parlato di "sovranismo psichico" tratteggiando un fenomeno prepolitico, che serpeggiava e ancora serpeggia nella società. La diagnosi di quest'anno è più difficile da interpretare. Per l'80% degli italiani il nostro è un paese in declino, per il 69% sono maggiori i danni che i vantaggi dalla globalizzazione, mentre più della metà della popolazione ha paura che scoppierà una guerra mondiale, rispetto a cui non saremmo in grado di difenderci. "Eppure – osserva il sociologo Giorgio De Rita – alcune note positive a livello macroeconomico si possono cogliere. L'inflazione sta diminuendo, gli occupati crescono, lo spread si mantiene basso. Ma qualcosa ci preoccupa, il Paese trascina i piedi, vecchio mentalmente non solo anagraficamente". È evidente che il modello di sviluppo adattativo, la proverbiale capacità di arrangiarsi analizzata da Giuseppe De Rita in tutti i risvolti che hanno segnato il tratto antropologico prevalente della società italica dal dopoguerra ad oggi, non funziona più. È sempre più diffusa la consapevolezza che bisogna crescere a tutti i livelli. Salari, investimenti, aziende non possono rimanere su standard così lontani dall'Europa. "Sembra – prosegue de Rita – che gli obiettivi siano chiari a tutti, ma eludiamo i percorsi, le tappe, gli strumenti per dare effetto concreto alla svolta che la radice profonda del nostro essere vorrebbe realizzare". Così accade che si moltiplicano i "piani collettivi", il PNRR, la riforma della giustizia, del fisco, persino la modifica sostanziale della forma costituzionale che dovrebbe condurci al premierato, invocano l'adesione di un corpo sociale che non è compatto, pronto a partecipare e a decidere, ma frammentato, diviso, slabbrato da una crisi che ha tolto capacità di intervento e di progetto. I "mille sciami" che avevano spinto fuori le migliori energie del made in Italy, consentendoci di superare la drammatica crisi pandemica, si sono assopiti anch'essi. L'ampio ventaglio di fenomeni individuati dal Censis comprende anche il rovesciamento del senso del lavoro, che non apre più percorsi di mobilità e di ascesa sociale. Si avverte una "siderale incomunicabilità generazionale", va in scena un dissenso senza conflitto come dimostra il plotone degli esuli in fuga che sono stati più di 36.000, nella fascia di età tra 18 e 34 anni nel 2023. Tradite le legittime aspettative esistenziali dei nostri figli, alla ricerca di un'identità professionale, scomparso il "Cipputi" di Altan emblema di una borghesia in divenire, verso quale prospettiva ci incamminiamo? L'interrogativo rimane pesando come un macigno sul futuro di una collettività sempre più passiva e scettica. ■

Saul Williams e Anisia Uzeyman
Neptune Frost
USA, Rwanda 2021



In Africa, nel cuore del Burundi, si apre un panorama ricco di significato, una miniera di coltan, il minerale essenziale presente in tutti i telefoni cellulari che le nazioni sviluppate e le grandi multinazionali estraggono nel continente nero sfruttandone le risorse. Qui, i minatori vivono una vita di sfruttamento e privazione, senza prospettive se non quella tragica di perderla, prima o poi, nelle profondità della miniera.

Ma c'è un destino diverso per Neptune (Cheryl Isheja e Elvis Ngabo), un intersessuale, e Matalusa (Bertrand Ninteretse), i due protagonisti, uniti da una connessione che è per metà spiritismo africano e per metà tecnologia avanzata. Una connessione che li unisce e li spinge a varare una rivoluzione. La loro missione, un audace progetto di hackeraggio filosofico e ideologico, diventa un inno di libertà per gli abitanti del villaggio, gli schiavi delle miniere e, simbolicamente, per l'intero continente africano.

Neptune Frost, diretto dal rapper americano Saul Williams e da sua moglie, la regista ruandese Anisia Uzeyman, è un musical fantascientifico, improntato all'afrofuturismo, che, attraverso la magia della musica e la potenza di immagini evocative, narra un'epopea di emancipazione in salsa sci-fi attraverso cavi, connessioni che raggiungono livelli neurali e azioni di hacker in una guerriglia tecnologica che aspira a una liberazione globale.

Le selvagge colline del Burundi, il colonialismo, gli sfruttatori, il coltan, e poi ancora i computer e la Rete: *Neptune Frost* mette in scena una favola in musica epica e futuristica con il sogno di spezzare le catene dell'oppressione.

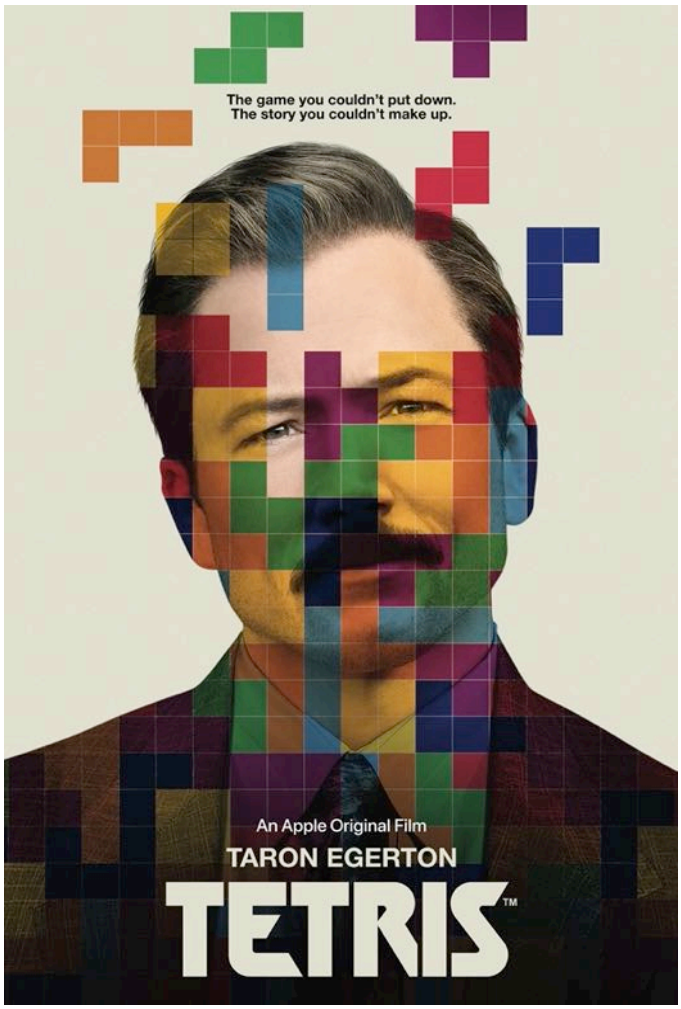
Presentato in anteprima mondiale al Festival di Cannes nel 2021, *Neptune Frost* è un'opera cinematografica visionaria e rivoluzionaria unica nel suo genere che esplora tematiche profonde come la lotta per la libertà, l'identità di genere e la resistenza contro le forze oppressive, trasportando lo spettatore in uno straordinario viaggio surreale tra realtà e virtualità. La brillante regia di Anisia Uzeyman e la sensibilità artistica di Saul Williams trasformano la visione del film in un'esperienza coinvolgente, in cui la colonna sonora avvincente e la fusione di elementi afrofuturistici creano un caleidoscopio emotivo. Il film si erge come una gemma nell'universo cinematografico contemporaneo, offrendo un invito a osare sognare e immaginare un mondo dove l'amore e la ribellione sono gli artefici di un nuovo destino. ■

Jon S. Baird
Tetris
USA, Gran Bretagna 2023

Una serie di piccole figure composte da quadretti (dette polimini) e riprodotte a forma di quadrato, rettangolo, lettere T, S, Z e L; una caduta dall'alto casuale, per incastrare le une alle altre fino a formare una riga piena, senza spazi vuoti, e cancellarla dallo schermo; velocità sempre crescente, punteggi altissimi, record, campionati e fuoriclasse. È il celeberrimo Tetris, uno dei videogiochi più diffusi, famosi e amati di tutti i tempi, opera del genio di un programmatore russo, Leonidovic Pazitnov, che negli anni '80 ha trasformato in videogame la passione tutta russa per i polimini.

In *Tetris* di Jon S. Baird, il racconto di come il software del videogioco che stava già spopolando nella patria Russia è arrivato in Occidente, diventa quasi una spy story che coinvolge persino il KGB. Trattative commerciali estenuanti, giochi d'azzardo sulle future vendite e persino sul vero possesso dei diritti di diffusione, incontri tra le antitetiche culture russa e americana per cercare di trovare un accordo, centinaia di milioni di dollari in ballo, giganti dell'industria videoludica a contendersi i polimini: nella pellicola di Baird c'è davvero tutto quello che può lasciare lo spettatore col fiato sospeso.

Filmografia - Cybersecurity Trends



L'opera, una produzione anglo americana, sicuramente ci mette fantasia nel romanzare una realtà che però non è stata poi troppo dissimile da quanto si vede nel film: negli anni '80, come si sa, la Guerra Fredda era la costante storica con cui doveva confrontarsi il mondo intero, e permea di per sé il contesto in cui si muovono i personaggi della pellicola. Sarebbe finita di lì a poco, davanti al crollo dell'intero sistema sociale sovietico, ma i programmatori di software, i funzionari moscoviti e gli spregiudicati uomini d'affari che volteggiavano attorno a Tetris non potevano saperlo. E così il film inchioda lo spettatore, scena dopo scena, a seguire le vicende di Henk Rogers, il produttore olandese che si innamora del gioco, e proprio di Pazitnov, il papà del Tetris: si conoscono, si studiano, diffidano l'uno dell'altro, infine superano ogni differenza tra loro, mentre la storia procede verso il finale di gloria che tutti conosciamo per il videogame.

Una storia di spigoli, ostacoli, difficoltà, incastri. Proprio come una caduta di polimini da mettere in fila. ■

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

www.swissacademy.eu

www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

DONA ORA

Il tuo contributo è prezioso 💎
www.cybertrends.it/donate/


Cybersecurity
Trends