CYBER MAGAZINE

Settembre 2025

CYBER Think Tank ASSINTEL

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

ESCLUSIVA

Alessio Butti | Sottosegretario di Stato alla Presidenza del Consiglio dei ministri

Cyber Think Tank Assintel

Riprogettiamo il futuro digitale, un'idea alla volta.

Unisciti al nostro think tank e costruisci con noi un mondo più sicuro e innovativo!

CYBER
Think Tank
ASSINTEL

Prossimo Incontro

17 Ottobre

10:00 - 11:30

Per Info:
segreteria@assintel.it

CYBER THINK TANK ASSINTEL

INDICE

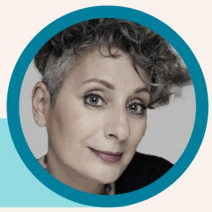
WEBINAR

CYBER Think Tank ASSINTEL

CYBER THREAT INTELLIGENCE:

anticipare le minacce per difendere la tua impresa

Relatori:



Sofia Scozzari

Jim Biniyaz

Riccardo Michetti

24 settembre 2025

12:00 - 13:00

Per info scrivi a:

segreteria@assintel.it

L’editoriale del Coordinatore del Cyber Think Tank Assintel Pierguido Iezzi

SETTEMBRE 2025

Viviamo un tempo in cui la trasformazione digitale accelera senza sosta e con essa cresce la superficie di rischio per istituzioni, imprese e cittadini. La cyber security, oggi, non è più soltanto un tema tecnico, ma un vero e proprio fattore di stabilità economica, sociale e geopolitica. In questo numero del Cyber Magazine troverete analisi e riflessioni che fotografano questa complessità. Dall’intervista con il Sottosegretario Alessio Butti, che ci guida tra le priorità del Governo su identità digitale e innovazione, agli approfondimenti sul ruolo della sicurezza nel credito e nella sanità, passando per i rischi emergenti della space economy e per le nuove forme di attacco che sfruttano linguaggio e percezioni. Uno spettro ampio di contributi che dimostra quanto la sicurezza sia intrecciata con ogni dimensione della nostra vita digitale.

Non mancano i grandi temi che animano il dibattito europeo: la sovranità tecnologica, le regole per l’intelligenza artificiale, la resilienza delle infrastrutture critiche. Questioni che non riguardano solo le istituzioni, ma ognuno di noi, perché chiamano in causa la fiducia, la consapevolezza e la capacità di scegliere con responsabilità nel mondo digitale. Vi invito, quindi, a sfogliare queste pagine con curiosità e spirito critico.

Troverete scenari, casi concreti, provocazioni intellettuali, ma soprattutto strumenti per comprendere meglio il presente e prepararvi al futuro. È questa la missione che ci accompagna da sempre: rendere la cyber security un tema di tutti, non di pochi!

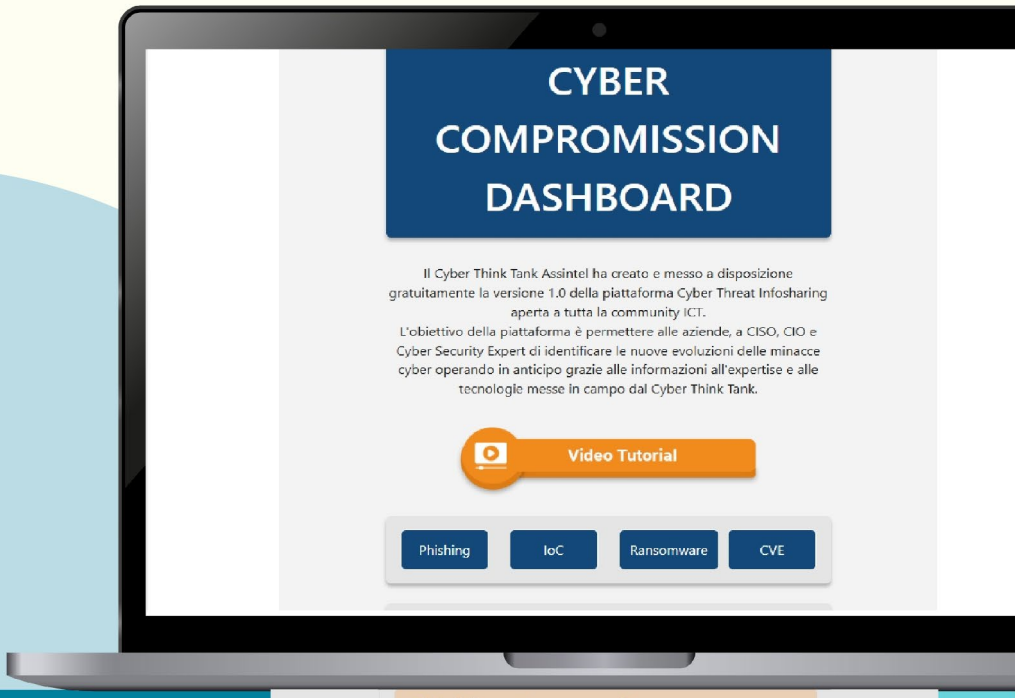
Buona lettura!

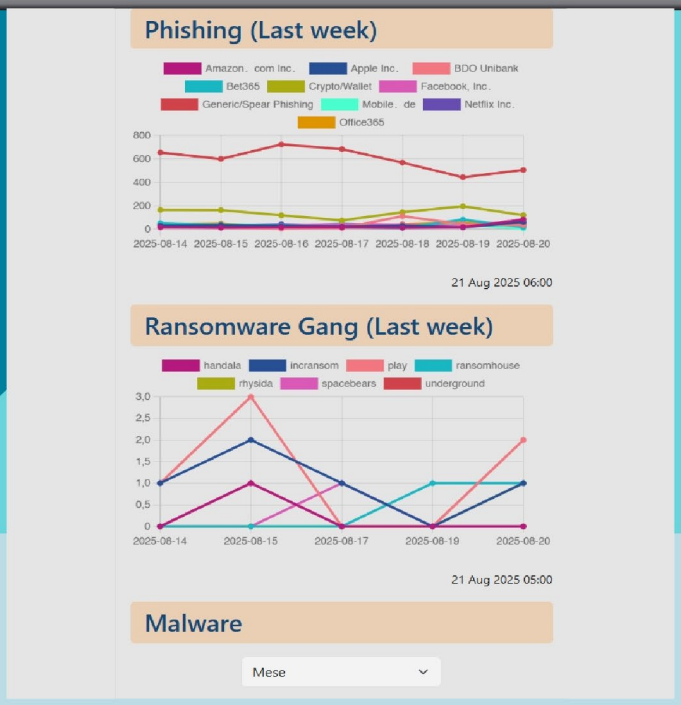
Pierguido Iezzi

CYBER Think Tank ASSINTEL

CYBER
Think Tank
ASSINTEL

Threat Infosharing





Per info scrivi a:

segreteria@assintel.it

(Cyber)Sicurezza, identità digitale e futuro

A colloquio con il Sottosegretario di Stato alla Presidenza del Consiglio con delega all'Innovazione, **Alessio Butti**

Alessio Butti, *ha lavorato come consulente nel marketing in varie aziende, in particolare nel settore editoriale e televisivo. È stato deputato nelle legislature XI, XIII, XIV, XVIII e senatore nelle legislature XV, XVI.*

Nel 1985 viene eletto consigliere comunale di Como. Nel 1992 viene eletto alla Camera dei deputati con MSI. Dal 1994 al 1996 è vicesindaco del Comune di Como, con deleghe ai lavori pubblici, all'edilizia privata, al commercio, all'industria e alle politiche giovanili. Nel 1996 viene rieletto alla Camera dei deputati, dove è membro della Commissione Parlamentare di Vigilanza. Nel 2006 viene eletto al Senato della Repubblica dove è membro, tra le altre, della Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi.

Nel 2012 aderisce a Fratelli d'Italia, di cui diventa vicecapogruppo al Senato e responsabile Media e telecomunicazioni.

Alle elezioni politiche anticipate del 25 settembre 2022 viene eletto al Senato nel collegio plurinominale Lombardia 01.

Dal 31 ottobre 2022 è Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri con delega all'Innovazione.

La sicurezza informatica è ormai considerata una priorità strategica per la sicurezza nazionale ed economica del Paese.

Allo stesso tempo, il Governo ha avviato un processo di razionalizzazione del sistema di identità digitale puntando a un unico strumento per cittadini e PA.

Ne abbiamo parlato con il Sottosegretario all'Innovazione tecnologica Alessio Butti per illustrare le linee di intervento del Governo su questi temi chiave, dalle iniziative per la cybersecurity nazionale alle recenti scelte in tema di identità digitale.

La trasformazione digitale ha reso il concetto di sicurezza informatica sempre più centrale per la resilienza del sistema Paese, aumentando la superficie di attacco esposta alle infrastrutture critiche. In questo scenario, quali sono oggi le principali sfide per garantire una protezione efficace delle infrastrutture critiche italiane?

Oggi la protezione delle infrastrutture critiche rappresenta una delle sfide più strategiche per la sicurezza nazionale ed europea. Gli attacchi informatici sono raddoppiati anno su anno e colpiscono sempre più spesso asset vitali per la nostra economia e per il funzionamento della pubblica amministrazione. Difendere i nostri dati, le nostre reti e i nostri sistemi è una priorità assoluta. Non possiamo più permetterci un approccio frammentato: servono soluzioni coordinate, condivise, fondate su alleanze internazionali, collaborazione con il settore produttivo e con le eccellenze del mondo accademico. A livello europeo, stiamo lavorando anche su progetti strutturali, come la protezione dei cavi sottomarini, che sono ormai un'infrastruttura tanto strategica quanto invisibile. Puntiamo a rafforzare la nostra sovranità digitale anche attraverso questi elementi, inserendoli in una visione più ampia, coerente con le priorità del G7 e con l'evoluzione tecnologica globale. Solo così possiamo assicurare la resilienza del sistema Paese nel lungo termine.

Le minacce cibernetiche si evolvono con rapidità impressionante, rendendo necessaria una costante innovazione nelle competenze e nelle metodologie difensive. Dunque, quali figure professionali e quali competenze ritiene fondamentali sviluppare per costruire una risposta efficace a questi nuovi scenari?

La sfida digitale non è solo infrastrutturale o tecnologica, ma soprattutto culturale. In Italia, uno dei problemi ricorrenti che abbiamo individuato riguarda la carenza di competenze qualificate in ambito cyber. Per affrontare minacce sempre più sofisticate serve una nuova generazione di professionisti formati, motivati, pronti ad agire in un contesto europeo e internazionale. Dobbiamo attrarre talenti, ma anche favorire il ritorno di tanti italiani che negli anni scorsi sono andati all'estero per mancanza di opportunità adeguate. Il Governo sta lavorando per rafforzare le nostre in house pubbliche, affinché possano diventare veri poli di competenza e sicurezza, a cominciare dalla migrazione della Pubblica Amministrazione al cloud nazionale. Accanto a questo, occorre agire sul fronte della formazione, sostenendo programmi specifici, rafforzando la collaborazione tra università, centri di ricerca e imprese. Il capitale umano è l'elemento chiave su cui si gioca la nostra capacità di difenderci e di innovare con sicurezza.

La cybersicurezza è, per definizione, un problema che nessun attore può affrontare da solo. Quali ulteriori passi intende compiere il Governo per rafforzare la collaborazione tra istituzioni e imprese? Ad esempio, è in programma lo sviluppo di nuove piattaforme per la condivisione tempestiva di informazioni sulle minacce (threat intelligence) o progetti congiunti di ricerca e sperimentazione tecnica?

La cybersicurezza è una sfida che nessun soggetto può affrontare da solo. Il Governo è pienamente consapevole di questo e sta lavorando per favorire una collaborazione sempre più strutturata tra istituzioni, imprese e mondo della ricerca. Un esempio concreto è il progetto "Cyber Harbour" di Torino, a cui ho avuto il piacere di partecipare. È una realtà innovativa che mette insieme attori pubblici e privati per sviluppare soluzioni di sicurezza avanzata, con un approccio inclusivo e aperto. Lì ho potuto constatare come le sinergie funzionino quando ci sono visione comune e obiettivi condivisi. Le nostre in house pubbliche, come PagoPA e Sogei, sono già attori fondamentali in questo processo, soprattutto nella migrazione al cloud nazionale. Il nostro impegno è quello di rafforzare questi poli, rendendoli hub tecnologici in grado di dialogare con il mondo produttivo e accademico, per generare innovazione, capacità di risposta e sicurezza su scala nazionale ed europea.

Sul fronte dell'identità digitale, il Governo ha annunciato di puntare a un sistema unico basato sulla Carta d'Identità Elettronica (CIE). Si è parlato di un passaggio a un modello «più moderno, sicuro e riconosciuto a livello europeo». In concreto, quali saranno i principali vantaggi per i cittadini e per le Pubbliche Amministrazioni di questa transizione da SPID alla CIE in termini di sicurezza, interoperabilità e facilità d'accesso ai servizi digitali?

Il Governo ha intrapreso un percorso deciso verso l'adozione di un'unica identità digitale basata sulla Carta d'Identità Elettronica. Spid è stato uno strumento utile, ma oggi comincia a mostrare delle vulnerabilità. La CIE è gratuita, più sicura, ed è una credenziale rilasciata direttamente dallo Stato, quindi più affidabile anche in termini di garanzia pubblica. Inoltre, al contrario di Spid, coniuga l'usabilità fisica con quella digitale. L'obiettivo è semplificare l'accesso ai servizi digitali per cittadini e imprese, offrendo un'unica identità forte, interoperabile, integrabile nei nuovi sistemi europei. Per accompagnare questa transizione, il Governo ha stanziato 40 milioni di euro a supporto degli identity provider di SPID e rinnoverà le convenzioni per altri due anni. Questo passaggio rappresenta anche un'opportunità per rafforzare la fiducia dei cittadini nei confronti della digitalizzazione, evitando il rischio di disorientamento dovuto alla frammentazione degli strumenti. I cittadini stanno apprezzando CIE, lo dimostrano i dati: 51 milioni di carte emesse e le attivazioni dell'app CieID passate da 5.3 a 7.3 milioni in meno di un anno.

La sfida digitale non è solo infrastrutturale o tecnologica, ma soprattutto culturale.

La digitalizzazione dell'identità è un tema di interesse strategico anche a livello europeo: l'Italia partecipa attivamente alla definizione del nuovo regolamento eIDAS e ai progetti pilota dell'UE sull'identità digitale. Quale contributo sta offrendo il nostro Paese in questi processi e in che modo il sistema basato sulla CIE si integra con gli strumenti digitali di identità promossi a livello europeo?

L'Italia è protagonista nella definizione della nuova identità digitale europea. Siamo tra i Paesi pilota del progetto EUDI Wallet, che consentirà ai cittadini di avere sul proprio dispositivo un'identità digitale completa, sicura e riconosciuta in tutta l'Unione. Il nostro contributo si concretizza attraverso l'It-Wallet, che sarà disponibile dal gennaio 2025 e che integrerà al suo interno carta d'identità, patente, tessera sanitaria e altri documenti essenziali. È uno strumento che permetterà di accedere ai servizi pubblici e privati in modo semplice e sicuro, nel pieno rispetto delle normative eIDAS. Inoltre, grazie alla piattaforma AppIO, tra le più avanzate in Europa, potremo offrire una user experience unificata, già in linea con gli standard europei. L'Italia si presenta dunque non solo come beneficiaria di queste innovazioni, ma come Paese guida nella loro implementazione. Crediamo in un'identità digitale europea interoperabile, sovrana e in grado di rafforzare la fiducia dei cittadini nella trasformazione digitale.

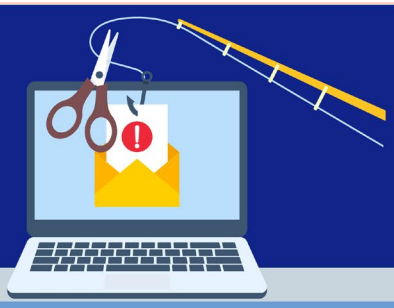
LA CYBER PER TUTTI

ISTRUZIONI SEMPLICI PER QUESTIONI COMPLESSE

CYBER Think Tank ASSINTEL

ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT

Non cadere nella trappola:
come riconoscere e evitare il phishing



Cos'è il phishing?

Una truffa online che cerca di carpire le tue informazioni personali (password, numeri di carta di credito, ecc.) fingendosi qualcuno di fidato (banca, social network, ecc.).

Come Funziona?

Email
Messaggi che sembrano provenire da enti affidabili, ma contengono link dannosi.

Siti Web falsi
Pagine che imitano perfettamente quelle originali per indurti a inserire i tuoi dati.

Messaggi
SMS o notifiche push che ti invitano a cliccare su link pericolosi.

Chiamata
furto di informazioni personali tramite telefono.

Perché lo fanno?

I cyber criminali utilizzano il phishing per:

- Rubare informazioni personali.
- Spiare le aziende.
- Crittografare i dati e chiedere un riscatto.
- Diffondere malware.

Cosa sfruttano?

Le loro armi sono:

La paura:
Ti minacciano di conseguenze negative.

L'avidità:
Ti promettono ricompense incredibili.

L'urgenza:
Ti spingono ad agire subito.

L'inganno:
Ti fanno credere di essere qualcuno di fidato.

Come difendersi?

Verifica l'indirizzo e-mail:
Controlla attentamente l'indirizzo del mittente.

Non cliccare su link sospetti:
Evita di cliccare su link presenti in e-mail o messaggi non richiesti.

Controlla l'URL:
Assicurati che l'indirizzo del sito web inizi con "https://" e abbia un certificato di sicurezza.

Non fornire mai informazioni personali:
Non comunicare mai password, codici di sicurezza o dati sensibili tramite e-mail o messaggi.

Utilizza un antivirus e un firewall:
Proteggi il tuo dispositivo con software di sicurezza aggiornati.

Tieniti aggiornato:
Informati sulle ultime truffe online.

Sovranità digitale: una sfida per il futuro del Paese

A cura di Pierguido Iezzi

L'ultimo triennio è stato, sotto molteplici punti di vista, una rivoluzione culturale, economica e politica. Un momento spartiacque che – tra i suoi innumerevoli risvolti – ha messo al centro del pubblico discorso un tema sempre più cruciale: la sovranità digitale. Parlare di sovranità digitale significa parlare della capacità di un Paese – e dell'Europa nel suo insieme – di controllare le tecnologie, i dati e le infrastrutture da cui dipendono economia, sicurezza nazionale e vita quotidiana dei cittadini. Oggi, gran parte delle informazioni che produciamo e utilizziamo si muove su piattaforme globali, spesso gestite da operatori che non hanno radici in Europa. Questa dipendenza rischia di tradursi in una vulnerabilità strutturale, che va ben oltre i confini della cybersicurezza tecnica: riguarda la nostra autonomia economica e, in ultima analisi, la nostra libertà di scelta come società. Per questo la Commissione Europea, con iniziative legislative e normative come la direttiva NIS2, ha deciso di alzare l'asticella, imponendo regole più stringenti e standard comuni a tutti gli Stati membri.

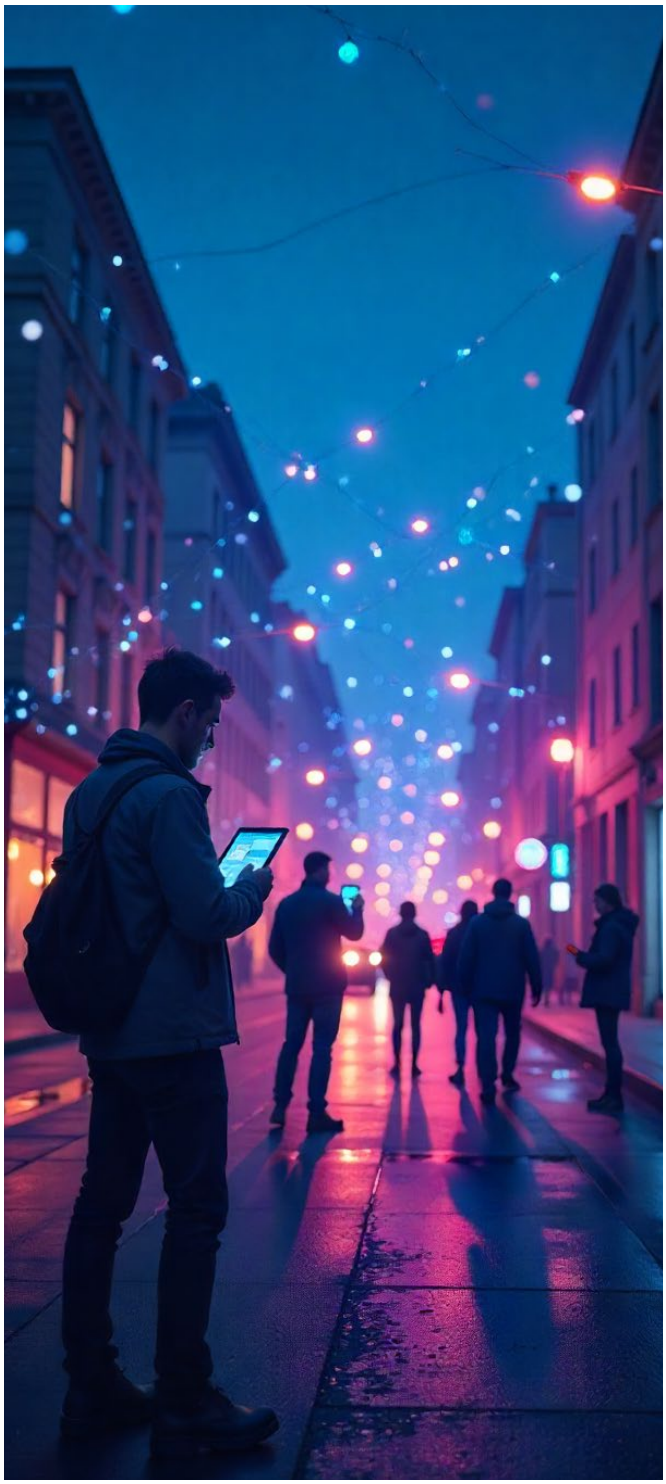
Ma le regole, da sole, non bastano. La sovranità digitale è una costruzione collettiva che nasce dall'alleanza tra pubblico e privato. Da una parte le istituzioni, che hanno il compito di stabilire cornici normative chiare, indirizzare investimenti e sviluppare infrastrutture strategiche. Dall'altra, le imprese – grandi e piccole – che devono adottare buone pratiche, rafforzare i propri sistemi di protezione e investire in formazione. Solo attraverso questa collaborazione il principio di sovranità digitale può tradursi in realtà. In Italia il tema assume un rilievo particolare. Il nostro tessuto produttivo è fatto per oltre il 90% di piccole e medie imprese, che costituiscono la spina dorsale dell'economia nazionale. Queste realtà sono innovative e dinamiche, ma spesso dispongono di risorse limitate e non sempre hanno le competenze per affrontare da sole il nuovo scenario normativo e tecnologico. Qui il ruolo delle associazioni di categoria, come Assintel, è fondamentale: fungere da ponte tra istituzioni e imprese, tradurre la complessità normativa in strumenti pratici e supportare le aziende in un percorso di crescita digitale sostenibile. La sfida della sovranità digitale non riguarda soltanto la sicurezza, ma anche la capacità di innovare. Disporre di piattaforme cloud europee, soluzioni di intelligenza artificiale sviluppate in casa e sistemi di cybersecurity governati localmente non è una scelta protezionistica: è una condizione necessaria per garantire che i dati dei cittadini e delle imprese restino sotto il controllo delle comunità che li generano. È un modo per riequilibrare rapporti di forza globali e assicurare che il valore economico e sociale dell'innovazione digitale resti in Europa.

In questo quadro, l'alleanza pubblico-privato non è sol-

tanto utile: è indispensabile. Lo Stato deve agire come garante e facilitatore, assicurando che gli investimenti europei e nazionali – a partire da quelli del PNRR – siano indirizzati verso progetti che abbiano un impatto concreto sul tessuto produttivo. Le imprese, a loro volta, devono riconoscere che la cybersecurity non è un costo aggiuntivo, ma un investimento sul proprio futuro. Ogni attacco informatico che colpisce una PMI non danneggia solo quella singola azienda: mina la fiducia dei clienti, mette a rischio le filiere produttive e indebolisce l'intero sistema economico.

Un altro tassello cruciale è la condivisione delle informazioni. La cultura del silenzio di fronte agli incidenti deve lasciare spazio a una logica di collaborazione. Solo se i dati sugli attacchi vengono raccolti, analizzati e condivisi tra istituzioni e imprese è possibile avere un quadro realistico delle minacce e predisporre contromisure efficaci. E come non citare la dimensione culturale. La sovranità digitale non si difende solo con infrastrutture e regole, ma con la consapevolezza diffusa che ogni cittadino, ogni lavoratore e ogni manager è parte di una catena di sicurezza più ampia. Promuovere la cultura della cybersicurezza come elemento di cittadinanza digitale significa rafforzare la coesione sociale e rendere più solido l'intero sistema Paese.

La partita della sovranità digitale è appena iniziata. Non sarà una sfida breve né semplice, ma rappresenta una straordinaria opportunità per l'Italia e per l'Europa. Se sapremo costruire un'alleanza solida tra istituzioni e imprese, se metteremo al centro le competenze delle nostre PMI e se diffonderemo una cultura condivisa della sicurezza, allora potremo guardare al futuro con fiducia. Perché un Paese che controlla i propri dati e le proprie tecnologie è un Paese più libero, più competitivo e più resiliente.



"Se sapremo costruire un'alleanza solida tra istituzioni e imprese, se metteremo al centro le competenze delle nostre PMI e se diffonderemo una cultura condivisa della sicurezza, allora potremo guardare al futuro con fiducia, perché un Paese che controlla i propri dati e le proprie tecnologie è un Paese più libero, più competitivo e più resiliente."

Cybertrappole verbali in grado di hackerare la mente

Nella cybersecurity le parole valgono quanto il codice

A cura di Gennaro Fusco

Le Parole come Strumento di controllo e di protezione

Nel mondo della cybersecurity, spesso, pensiamo a firewall, crittografia, malware, ransomware, vulnerabilità zero-day, ecc. ecc. Dimentichiamo, invece, ciò che è nato prima di tutto: la parola. Essa è sì un mero veicolo di informazione, ma è anche una vera e propria arma, è uno scudo e, addirittura, un campo di battaglia. La parola è una lama a doppio taglio. Può, infatti, costruire ponti o innalzare muri, guidare verso scelte consapevoli o indurre a commettere errori catastrofici. Lo stesso Papa Leone XIV, agli operatori della comunicazione, ha chiesto di disarmare le parole per disarmare la Terra. E, in un mondo sempre più digitale, che progredisce a una velocità impressionante, la parola ha un potere innegabile.

Siamo bombardati da minacce sempre più sofisticate: phishing, spear phishing, social engineering e persino manipolazione delle masse attraverso fake news e disinformazione. Comprendere, allora, la differenza tra persuasione e manipolazione diventa cruciale, al fine di riconoscere le potenziali trappole, spesso invisibili.

Persuasione e Manipolazione: due facce (quasi) della stessa medaglia

La persuasione e la manipolazione sono due termini utilizzati, spesso, in modo intercambiabile. Entrambe sono forme di influenza, due facce, o quasi, della stessa medaglia. C'è un filo sottilissimo che le separa. Si distinguono per etica, intento e trasparenza.

La persuasione si fonda sul principio del rispetto e dell'autonomia dell'individuo. Implica una comunicazione aperta e onesta, mirata a influenzare le decisioni altrui attraverso argomenti veri o verosimili, facendo appello alla razionalità, all'emotività o alla credibilità, per indurre una decisione libera, consapevole e informata. È il terreno della retorica classica, come ci ha insegnato Aristotele con i tre principi base: ethos, pathos, logos.

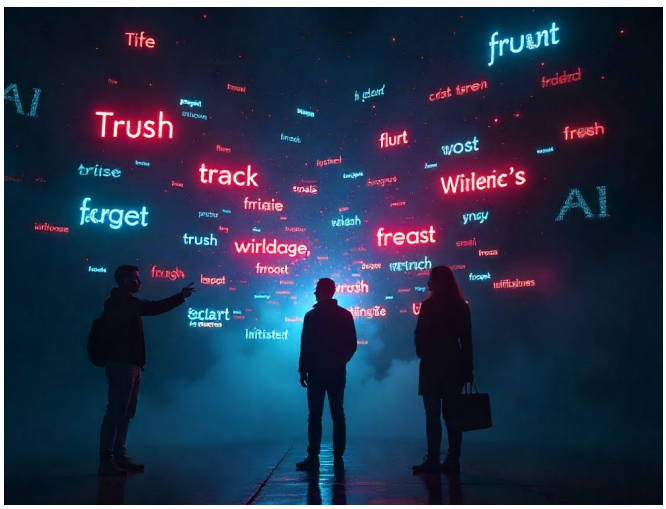
La manipolazione, invece, si nutre di asimmetrie informative e psicologiche. È caratterizzata da un uso ingannevole delle informazioni e da un intento di controllo. Vengono celate le vere intenzioni, distorti i fatti e sfruttate le vulnerabilità cognitive, per estorcere il consenso a scapito della libertà dell'altro.

Robert Cialdini, nel suo libro "Influence", scrive che le tecniche di persuasive diventano manipolative quando vengono applicate in modo subdolo, automatico e privo di trasparenza, sfruttando la mente delle persone più che informandola.

La parola crea. Nella Bibbia (Gn 1,1-3) Dio disse: "Sia la luce!". E la luce fu. La parola, infatti, è l'inizio del tutto. Con le parole si può fare qualsiasi cosa, si può creare la realtà che si desidera o, addirittura, ciò che si teme di più. Dipende dall'uso che ne facciamo.

Esse, quindi, sono in grado di provocare un impatto notevole sulle decisioni e hanno la capacità di evocare emozioni e reazioni istintive. Parole specifiche possono generare paura, fiducia o urgenza. Ad esempio, la frase come "La tua sicurezza è a rischio!" può indurre panico, mentre la frase più rassicurante "Siamo qui per aiutarti a proteggerti" può costruire fiducia.

Nell'ambito della cybersecurity, i professionisti possono sfruttare questo "potere" per educare gli utenti sull'importanza delle pratiche di sicurezza. L'importanza di una comunicazione chiara, infatti, è supportata dalla ricerca di Hogg (2001). Essa sottolinea che la chiarezza nella comunicazione può migliorare notevolmente la compliance degli utenti alle politiche di sicurezza.



La parola come vettore d'attacco

Le parole, nel contesto digitale, diventano un vero e proprio codice sociale. I messaggi di phishing, ad esempio, sono costruiti su schemi linguistici persuasivi, che diventano, poi, manipolativi: urgenza, autorità, scarsità, reciprocità, ecc…, che sono esattamente le "armi della persuasione", enunciate da Cialdini.

Una e-mail, ad esempio, che recita "Il tuo account verrà disattivato entro 24 ore. Clicca qui per verificarlo", sfrutta: l'urgenza (scarso tempo per riflettere), l'autorità (firma apparentemente ufficiale), il linguaggio tecnico (per mascherare l'inganno sotto l'aspetto dell'autenticità).

Questa forma di attacco è molto più efficace della violazione di un firewall. Essa entra, infatti, dalla porta principale, sfruttando un bug nel nostro sistema operativo più vulnerabile: la mente umana.

Essa è sì un mero veicolo di informazione, ma è anche una vera e propria arma, è uno scudo e, addirittura, un campo di battaglia.

Comunicazione efficace: strumento di difesa

Una buona formazione in comunicazione efficace può aumentare la nostra resilienza digitale. Paul Watzlawick, nel suo libro "Pragmatica della comunicazione umana", scrive che ogni atto comunicativo ha una componente contenutistica e una relazionale. Un messaggio manipolativo è in grado di alterare la componente relazionale, posizionandosi, spesso, come "più competente" o "più autorevole".

Sapere riconoscere questi segnali, costituisce un'abilità cruciale nella cybersecurity. Dall'analisi del linguaggio utilizzato, infatti, si evince come una singola parola possa cambiare l'esito di una decisione.

Confrontiamo, ad esempio, due frasi: "Gentile cliente, abbiamo notato un accesso sospetto"; "URGENTE: accesso non autorizzato rilevato. AGISCI ORA!"

In entrambi i casi, c'è la presenza di un inganno informativo. Il secondo messaggio, però, di carattere più manipolativo, attiva il circuito della paura e riduce la capacità critica. Il vero attacco, praticamente, è meramente di tipo linguistico.

Le parole come armi inverse

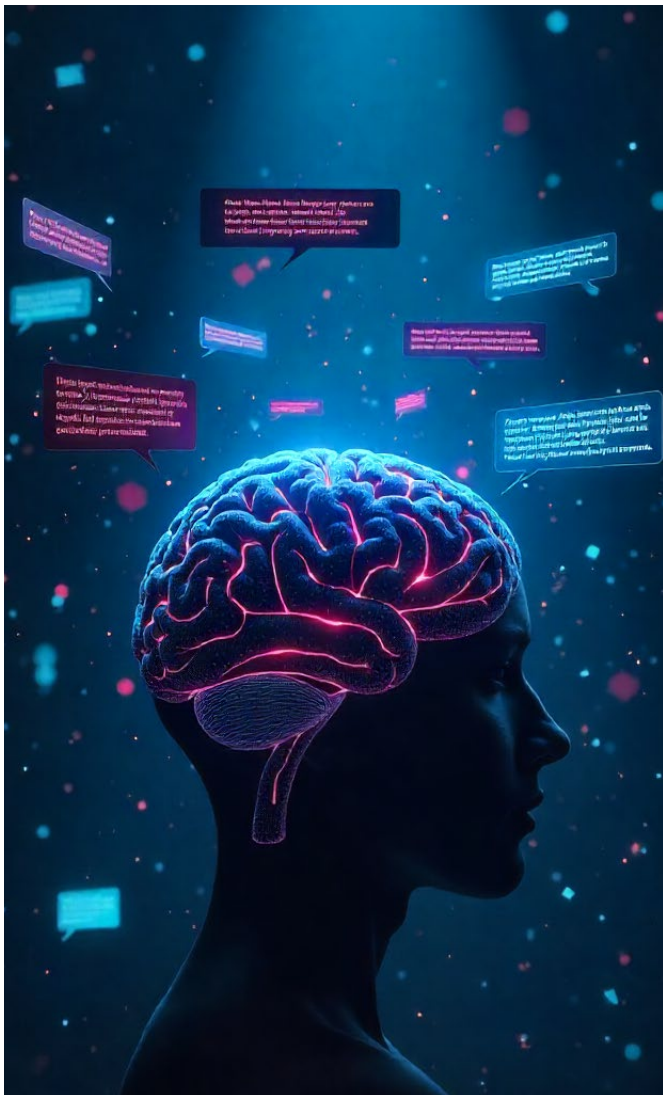
Il linguaggio, nel campo della difesa, può essere un'arma inversa. Specializzarsi nel linguaggio serve a smascherare le trame dell'inganno. Dobbiamo prendere consapevolezza che la cybersecurity non è solo una questione tecnica, ma anche una questione di retorica. Chi lavora nel settore deve conoscere gli schemi argomentativi distorti usati nei messaggi manipolativi.

Una comunicazione chiara, empatica e coerente da parte delle istituzioni digitali (banche, aziende, enti pubblici) può ridurre drasticamente la vulnerabilità dell'utente finale. Un linguaggio semplice e trasparente, come dimostrano ricerche sulla risk communication, aumenta la fiducia e riduce la probabilità di cadere in trappole linguistiche (Cfr. Sandman; Covello).

Conclusione

In un mondo sempre più esposto alla guerra informativa, la vera frontiera della cybersecurity è linguistica. Non basta proteggere i dati: bisogna proteggere la percezione, l'attenzione e la consapevolezza.

Chi domina le parole è in grado di dominare anche le scelte.



Aumento degli attacchi alle telecomunicazioni negli ultimi due anni: una breve storia

A cura di Corradino Corradi

Negli ultimi due anni, il numero di attacchi contro le infrastrutture e i servizi di telecomunicazione è aumentato notevolmente in termini di numero e complessità.

Molte aziende di telecomunicazioni hanno subito significative violazioni dei dati dei clienti, con la necessità di segnalarli all'Autorità Garante per la Privacy; molti degli attacchi erano legati a gruppi di criminalità informatica con finalità prevalentemente economica. In questo articolo, invece, mi concentrerò sugli attacchi denominati Advanced Persistent Threat (APT), legati prevalentemente a cyberspionaggio o competizione geo-tecnica-politica ed in casi estremi a cyber-war.

Senza un ordine particolare, riporto i 5 principali attacchi alle infrastrutture di telecomunicazione nel 2024 e nel 2025, con un breve riassunto e un'analisi più approfondita, realizzata con il supporto di AI (in particolare Microsoft Co-pilot per la sicurezza e Perplexity) e mappata in base alle tattiche, tecniche e procedure (TTP) MITRE. The TTPs sono lasciate in inglese in modo da favorire una veloce mappatura con MITRE ATTACK®. [1]

Attacco cyber di Weaver Ant

Chi: fornitore di servizi di telecomunicazioni asiatico.

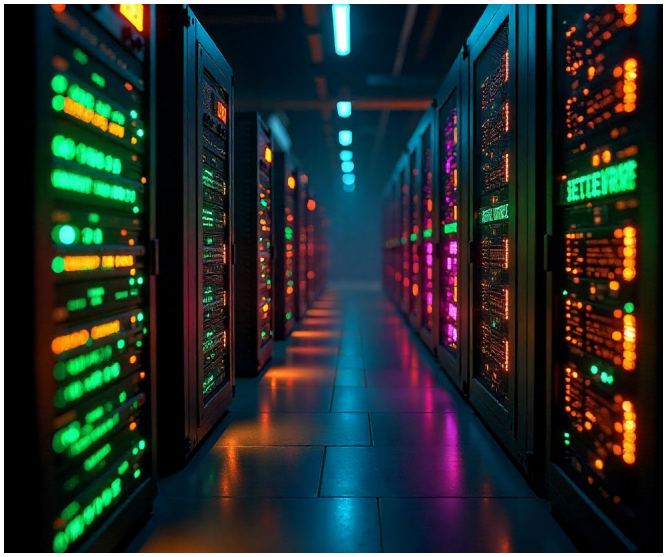
Quando: l'attacco è durato quattro anni, concludendosi nel 2024.

Da chi: l'attacco è stato condotto dagli hacker della Chinese Weaver Ant.

Tecnica: gli hacker hanno spiato la rete utilizzando tecniche ATP.

Gli hacker della Chinese Weaver Ant (1) si sono infiltrati presso un importante fornitore di servizi di telecomunicazioni asiatico per oltre quattro anni, mantenendo un accesso persistente a fini di spionaggio informatico sfruttando i router Zyxel vulnerabili e implementando web shell avanzate come China Chopper e INMemory crittografati, che hanno consentito il controllo remoto stealth, l'accesso alle credenziali dell'Active Directory dell'operatore ed infine l'esfiltrazione dei dati

MITRE ATT&CK-TTPs: include initial access via exploitation of public-facing applications, persistence through web shells, defence evasion using encryption and web shell tunneling, credential access and discovery targeting Active Directory, lateral movement with recursive HTTP tunnels, and data exfiltration through covert network traffic capturing.



Attacco cyber di APT29

Chi: diverse compagnie telefoniche europee.

Quando: gennaio-febbraio 2024.

Tecnica utilizzata: gli aggressori hanno utilizzato spear-phishing e malware per infiltrarsi nelle reti e rubare informazioni sensibili.

APT29 detto anche Cozy Bear (2), è un gruppo sponsorizzato dallo stato russo e collegato all'SVR, conduce attività di cyberspionaggio contro governi, aziende di telecomunicazioni e think tank, in particolare attraverso attacchi alla catena di approvvigionamento (vedi SolarWinds) e campagne di cloud targeting che utilizzano la forza bruta e l'uso di password spraying su account di servizio e credenziali dei dipendenti inattivi.

MITRE ATT&CK-TTPs: include Initial Access via Exploit Public-Facing Application and Supply Chain Compromise, Persistence through Valid Accounts and Web Shells, Credential Access via Unsecured Credentials, Lateral Movement with HTTP tunneling, and Defence Evasion using encrypted proxies (PyRDP) and Magic Web malware to masquerade as legitimate users.

Attacco cyber di Salt Typhoon

Chi: diverse compagnie telefoniche asiatiche

Quando: giugno-luglio 2024.

Tecnica: gli aggressori hanno sfruttato vulnerabilità zero-day per accedere alle reti e condurre attività di sorveglianza.

Salt Typhoon (3), un gruppo di hacker legato allo stato cinese, ha condotto prolungate campagne di cyberspionaggio contro fornitori di telecomunicazioni globali ed enti governativi, sfruttando le vulnerabilità delle applicazioni per infiltrarsi nelle reti, rubare dati di comunicazione sensibili e monitorare obiettivi di alto profilo come funzionari statunitensi.

MITRE ATT&CK TTP: include initial access via Exploit Public-Facing Application, credential harvesting through Windows Command Shell, registry modification for persistence, lateral movement using HTTP tunneling, and stealthy data exfiltration via encrypted DNS or ICMP channels.

Attacco cyber di Earth Lusca

Chi: diverse compagnie telefoniche dell'Europa occidentale.

Quando: novembre 2024.

Tecnica utilizzata: gli aggressori hanno utilizzato malware avanzato per compromettere le reti ed esfiltrare dati.

MITRE ATT&CK TTP: include Initial Access via Exploit Public-Facing Application, Execution through Command and Scripting Interpreter, Persistence using Web Shells and Backdoors, Lateral Movement via Remote Services and Cobalt Strike, Credential Access through Credential Dumping, and Command and Control over TCP with custom protocols.

Attacco cyber di Velvet Ant

Chi: compagnie telefoniche nordamericane.

Quando: nel corso del 2024.

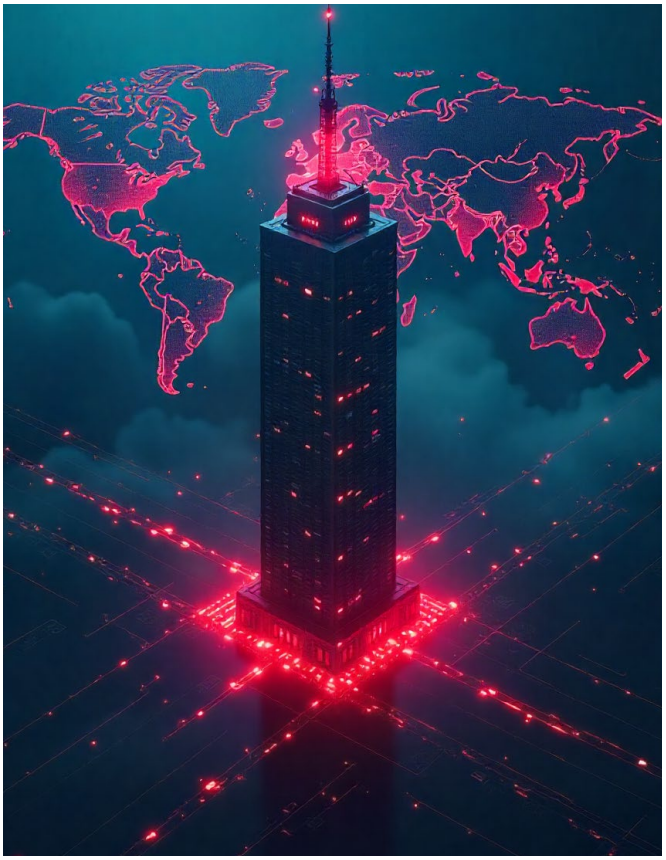
Tecnica utilizzata: gli aggressori hanno utilizzato una combinazione di ingegneria sociale e malware avanzato per infiltrarsi nelle reti e rubare informazioni sensibili.

Il gruppo di hacker Velvet Ant (5), legato alla Cina, ha condotto una prolungata campagna di cyberspionaggio sfruttando i dispositivi F5 BIG-IP legacy come server interni di comando e controllo per mantenere la persistenza, eludere il rilevamento ed esfiltrare dati sensibili per circa tre anni.

MITRE ATT&CK TTP: include Initial Access via Exploit Public-Facing Application targeting vulnerable F5 BIG-IP systems, Persistence through use of PlugX backdoor with DLL side-loading, Defence Evasion by blending C2 traffic with legitimate network traffic, Lateral Movement using open-source tools like Impacket, and Command and Control via internal C2 infrastructure leveraging compromised load balancers.

In conclusione, gli esempi elencati mostrano quanto numerosi gruppi di spionaggio informatico sponsorizzati da stati (state sponsored cyber crime groups) siano attivi in attacchi APT contro le aziende di telecomunicazioni e quanto sofisticate siano diventate le loro tattiche, tecniche e procedure (TTPs). La loro capacità di sfruttare le vulnerabilità dei server pubblici per l'accesso iniziale, impiegare malware e backdoor avanzati per la persistenza, manovrare lateralmente all'interno di reti compromesse e utilizzare protocolli personalizzati per il comando e il controllo sottolinea l'evoluzione del panorama delle minacce cyber.

L'integrazione del social engineering e dello sfruttamento di dispositivi legacy evidenzia ulteriormente l'ingegnosità di questi aggressori nell'aggirare le misure di sicurezza informatica tradizionali. Le aziende di telecomunicazioni devono rimanere vigili e proattive nel rafforzare le proprie difese contro queste minacce informatiche per salvaguardare i dati sensibili e mantenere l'integrità operativa delle infrastrutture di rete (in larga parte elemento portante delle Critical Infrastructure); devono inoltre interagire attivamente per la gestione degli incidenti con i C-SIRT nazionali e l'unità di contrasto del cyber-crime della polizia e contribuire attivamente alla partnership pubblica e privata (PPP), in particolare con le agenzie nazionali per la sicurezza informatica.



Citazioni per China Wever Ant (1):

- *https://www.infosecurity-magazine.com/news/china-weaver-ant-hackers-telco/*
- *https://www.pcmag.com/news/chinese-hackers-remained-inside-an-asian-telecom-firm-for-4-plus-years*
- *https://www.msspalert.com/brief/multi-year-telco-hack-conducted-by-chinese-apt*
- *https://www.bleepingcomputer.com/news/security/chinese-weaver-ant-hackers-spied-on-telco-network-for-4-years/*
- *https://www.linkedin.com/pulse/china-nexus-apt-weaver-ant-caught-multiyear-web-shell-attack-cv-9ze*
- *https://www.sygnia.co/threat-reports-and-advisories/weaver-ant-tracking-a-china-nexus-cyber-espionage-operation/*
- *https://hivepro.com/threat-advisory/web-shell-warfare-weaver-ants-covert-cyber-espionage-campaign/*
- *https://www.scworld.com/brief/multi-year-telco-hack-conducted-by-chinese-apt*
- *https://therecord.media/chinese-hackers-spent-years-telco*
- *https://industrialcyber.co/ransomware/sygnia-details-weaver-ant-tactics-in-battle-against-china-linked-cyber-threats-on-telecoms/*
- *https://socprime.com/blog/detect-weaver-ant-apt-attacks/*
- *https://www.linkedin.com/pulse/router-based-cyberattacks-mitre-attck-ttp-analysis-cary-d7zkc*
- *https://securityonline.info/china-chopper-inmemory-weaver-ants-arsenal-of-advanced-web-shells/*
- *https://en.wikipedia.org/wiki/ATT&CK*
- *https://www.picussecurity.com/resource/blog/cyber-threat-intelligence-report-may-2023*

Citazioni for APT 29 (2):

- *https://fieldeffect.com/blog/russia-linked-apt29-increasingly-targeting-cloud-services*
- *https://www.cybereason.com/blog/understanding-the-mitre-attck-apt29-round-2-evaluation*
- *https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques*
- *https://fieldeffect.com/blog/apt-29-hustles-high-profile-organizations-with-malicious-rdp-files*
- *https://www.linkedin.com/pulse/analyzing-apts-ttps-using-mitre-attck-framework-martin-norris-5xf3e*
- *https://thehackernews.com/search/label/APT29*
- *https://www.kaspersky.com/enterprise-security/mitre/apt29*
- *https://attack.mitre.org/groups/G0016/*
- *https://socradar.io/apt-profile-cozy-bear-apt29/*

- *https://securityboulevard.com/2020/08/21-cybersecurity-products-to-combat-apt29-mitre-weighs-in/*

Citazioni per Salt Typhoon (3):

- *https://techcrunch.com/2025/02/13/chinas-salt-typhoon-hackers-continue-to-breach-telecom-firms-despite-us-sanctions/*
- *https://www.picussecurity.com/resource/how-breach-and-attack-simulation-helps-you-to-operationalize-mitre-attck*
- *https://osintteam.blog/deception-playbook-for-volt-typhoon-and-salt-typhoon-bf9478fd5d-1d?gi=53d586701cd7*
- *https://www.vectra.ai/threat-actors/salt-typhoon*
- *https://www.pcmag.com/news/chinas-salt-typhoon-hackers-breached-us-networks-using-existing-flaws*
- *https://osintteam.blog/deception-playbook-for-volt-typhoon-and-salt-typhoon-bf9478fd5d-1d?gi=a7a84286aa23*
- *https://www.nextgov.com/cybersecurity/2025/02/salt-typhoon-hackers-exploited-stolen-credentials-and-7-year-old-software-flaw-cisco-systems/403146/*
- *https://www.cybersecuritydive.com/news/fbi-china-salt-typhoon-hack-telecom-tips/746490/*
- *https://cyberscoop.com/salt-typhoon-us-government-response/*
- *https://en.wikipedia.org/wiki/Salt_Typhoon*

Citazioni per Earth Lusca (4):

- *https://www.trendmicro.com/en_za/research/22/a/earth-lusca-sophisticated-infrastructure-varied-tools-and-techni.html*
- *https://www.broadcom.com/support/security-center/protection-bulletin/malicious-activities-by-the-earth-lusca-threat-actor*
- *https://thehackernews.com/2023/09/earth-luscas-new-sprysocks-linux.html*
- *https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Earth+Lusca*
- *https://thecyberpost.com/news/security/earth-lusca-cyber-espionage-with-crypto-theft-on-the-side/amp/*
- *https://www.infosecurity-magazine.com/news/chinese-group-linux-backdoor/*
- *https://vulnera.com/newswire/earth-luscas-advanced-sprysocks-linux-backdoor-targets-global-government-entities/*
- *https://attack.mitre.org/groups/G1006/*
- *https://www.linuxjournal.com/content/linux-threat-report-earth-lusca-deploys-novel-sprysocks-backdoor-attacks-government*

Citazioni per Velvet Hunt (5):

- *https://www.darkreading.com/cyberattacks-data-breaches/china-velvet-ant-apt-multiyear-espionage*
- *https://socprime.com/blog/velvet-ant-activity-detection-china-backed-cyber-espionage-group-launches-a-prolonged-attack-using-malware-deployed-on-the-f5-big-ip-devices/*
- *https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/*
- *https://socradar.io/velvet-ants-strategic-targeting-a-long-term-cyber-espionage-campaign-against-f5-big-ip-systems/*
- *https://www.bankinfosecurity.com/researchers-uncover-chinese-hacking-cyberespionage-campaign-a-25558*
- *https://hackread.com/chinese-velvet-ant-hackers-target-f5-devices/*
- *https://www.anvilogic.com/threat-reports/chinese-cyber-espionage*
- *https://www.netizen.net/news/post/4594/china-linked-velvet-ant-uses-f5-big-ip-malware-in-cyber-espionage-campaign*
- *https://malware.news/t/velvet-ant-s-strategic-targeting-a-long-term-cyber-espionage-campaign-against-f5-big-ip-systems/83664*

"Negli ultimi due anni, il numero di attacchi contro le infrastrutture e i servizi di telecomunicazione è aumentato notevolmente in termini di numero e complessità."

La Cybersecurity dal punto di vista del DPO di un'Azienda Sanitaria

A cura di Elisabetta Fortunato

La cybersecurity non è materia a sé stante, ma costituisce parte delle politiche di resilienza complessiva di una PA. Il rischio informatico, infatti, è insito nell'operatività dei sistemi informativi delle Aziende Sanitarie. Al fine mitigare questo rischio, viene mappato periodicamente e correlato con altri rischi aziendali, in modo da garantire una visione unitaria e strategica. Attraverso analisi di vulnerabilità, rilevazioni tecniche sugli asset critici e analisi degli scenari di minaccia, i rischi informatici vengono classificati in base a impatto, probabilità e capacità di rilevazione. Tale approccio consente di concentrare le risorse sulle aree a maggiore esposizione, anche in relazione al perimetro NIS2 e ai dati trattati.

Tuttavia, per le Aziende Sanitarie sussistono fattori di rischio ulteriori costituiti dalla frammentazione dei dati tra sistemi eterogenei, dall'assenza di strumenti di raccolta centralizzata del rischio e dalla mancanza di standard operativi condivisi tra funzioni (es. IT, legale, acquisti) che richiederebbero la costruzione di un modello di Integrated Risk Management per il quale è necessario un investimento culturale prima che tecnologico.

Nel settore sanitario, le principali criticità riscontrate sono sicuramente rappresentate da ambienti cloud gestiti con scarsa segmentazione logica, credenziali deboli nei sistemi di accesso remoto e fornitori che non aggiornano tempestivamente le patch di sicurezza. Una efficace misura di contrasto consiste nell'avvio di azioni volte ad introdurre requisiti minimi di sicurezza nei contratti e a migliorare la visibilità sulla catena di fornitura.

Le recenti normative europee hanno avuto un impatto significativo sulla governance della sicurezza nella supply chain. In particolare, la Direttiva NIS2 ha imposto l'adozione di misure minime comuni anche ai fornitori critici, mentre il Cyber Resilience Act ha posto l'accento sulla sicurezza dei prodotti digitali. In quest'ottica, un supporto può essere offerto da piattaforme software per la gestione digitale del ciclo di vita dei fornitori, comprensive di funzionalità per la raccolta di documentazione, generazione automatica di alert, punteggi di rischio aggiornati dinamicamente e tracciabilità delle verifiche eseguite. In ogni caso è opportuno che i contratti con i fornitori critici contengano clausole specifiche in materia di misure minime di sicurezza, gestione degli incidenti, notifiche tempestive, audit di verifica, requisiti per i subfornitori.

Inoltre, gli incidenti verificatisi nell'ambito della supply chain hanno evidenziato l'importanza di un piano di continuità operativa condiviso con i fornitori e, al contempo, alcuni disservizi hanno mostrato l'inadeguatezza dei piani di risposta agli incidenti da parte di terzi, con conseguenti aggiornamenti contrattuali e revisioni delle policy di onboarding. In questo scenario è facile prevedere una crescita dei rischi derivanti dall'integrazione di

software di terze parti dovuta, in particolare, ad aggiornamenti compromessi (attacchi alla catena di fornitura software).

La minaccia è in continua crescita, con specifico riferimento all'ambito sanitario, dall'uso di dispositivi medicali connessi, che necessitano di controlli più stringenti e tempestivi.

Occorre, pertanto, predisporre specifiche misure di contrasto quali, ad esempio, l'adozione di un percorso di rafforzamento della sicurezza della catena di fornitura nonché il ricorso a tecnologie innovative che possono rappresentare un fattore abilitante fondamentale per garantire una gestione efficace, trasparente e resiliente dei rischi.

La cybersecurity non è materia a sé stante, ma costituisce parte delle politiche di resilienza complessiva di una PA.

In particolare, anche nel mondo sanitario si stanno consolidando tre approcci tecnologici ritenuti particolarmente promettenti:

- **Zero Trust Architecture (ZTA):**

Si tratta di un modello di sicurezza basato sul principio "never trust, always verify", che supera la logica perimetrale tradizionale. Ogni accesso – sia interno che esterno – viene valutato dinamicamente in base a identità, contesto, dispositivo e livello di rischio. L'adozione progressiva di questo paradigma nella rete informatica delle aziende sanitarie consentirebbe di minimizzare la superficie d'attacco, proteggere i dati sanitari critici e limitare le possibilità di movimento laterale da parte di attori malevoli in caso di compromissione. ZTA risulta particolarmente efficace per la protezione delle interfacce tra sistemi interconnessi (es. repository VNA, telemedicina, portali fornitori).

- **Blockchain e tecnologie DLT (Distributed Ledger Technology):**

Sebbene ancora in fase di valutazione sperimentale, l'applicazione della blockchain alla gestione della supply chain sanitaria potrebbe offrire notevoli vantaggi in termini di tracciabilità, trasparenza e integrità dei dati. In particolare, la registrazione immutabile delle operazioni legate alla fornitura di dispositivi medicali, dei log di accesso a piattaforme critiche o degli eventi di manutenzione può aumentare la fiducia nei rapporti con i fornitori e facilitare la gestione ex post di audit e verifiche. Un utilizzo mirato, su domini specifici ad alto rischio (es. tracciabilità di farmaci o kit diagnostici), potrebbe offrire un valore aggiunto concreto.

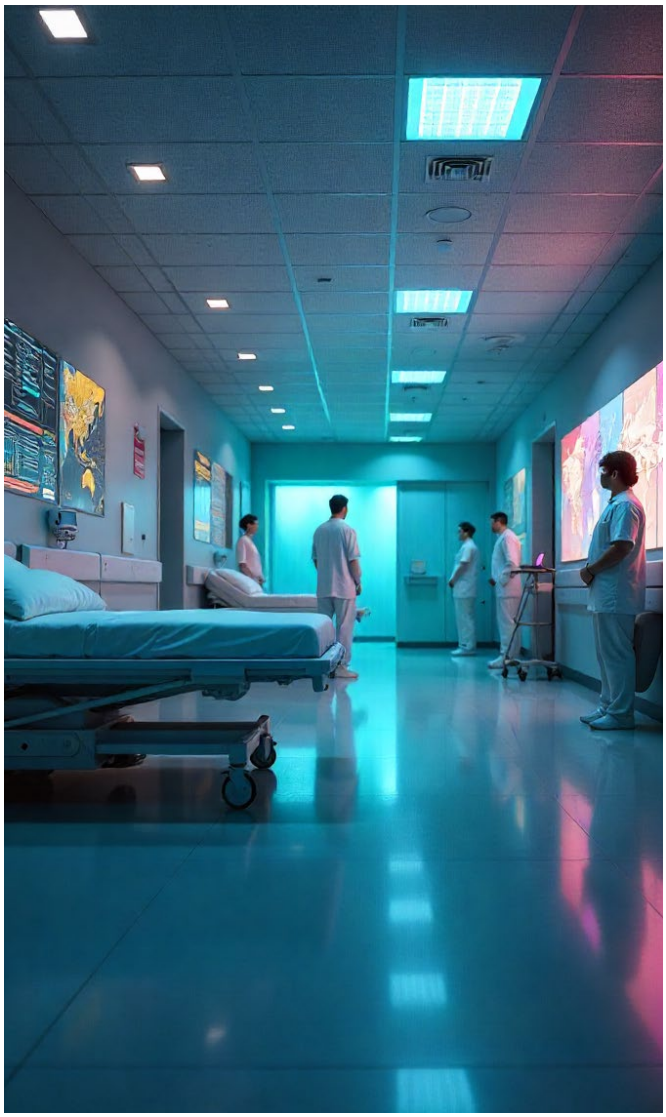
- **Intelligenza Artificiale (AI) applicata alla sicurezza:**

L'integrazione dell'AI nei sistemi di monitoraggio consente di analizzare grandi volumi di dati eterogenei, identificare pattern di rischio e supportare il team di sicurezza nella gestione degli eventi. Nell'ambito della supply chain, l'AI può essere utilizzata per:

» identificare anomalie nei comportamenti dei fornitori (es. accessi anomali, ritardi non giustificati);

» stimare proattivamente l'esposizione a vulnerabilità note (es. prodotti non aggiornati o non conformi);

» supportare il processo decisionale nei sistemi di risk scoring dei terzi.



Tuttavia, l'uso dell'AI richiede un presidio costante e competenze specifiche, soprattutto per garantire l'affidabilità e l'intelligibilità degli output, in conformità ai principi del Regolamento AI e del GDPR. Nel contesto sanitario le maggiori difficoltà si concentrano sulla trasparenza e sulla comprensibilità delle decisioni automatizzate, specie quando queste hanno impatti diretti sulla presa in carico del paziente. Dal punto di vista della sicurezza, è forte la preoccupazione per i potenziali usi impropri dell'AI generativa da parte di soggetti interni o esterni, come veicolo di esfiltrazione dei dati, creazione di contenuti fuorvianti o simulazioni fraudolente. D'altro canto la gestione dei dati sanitari rappresenta una delle sfide più complesse in ambito pubblico, dovendo contemperare, da un lato, l'esigenza di un accesso tempestivo e agevole da parte degli operatori sanitari, dall'altro, la necessità di assicurare un elevato livello di protezione dei dati personali degli assistiti, In tale contesto, è fondamentale adottare un approccio che integri misure organizzative, tecniche e comunicative, finalizzate a semplificare i processi senza compromettere la compliance normativa. Risulta fondamentale la collaborazione tra il Data Protection Officer (DPO) e il Chief Information Security Officer (CISO) per garantire una protezione effettiva dei dati personali e una gestione sicura delle infrastrutture informatiche nel settore sanitario. La crescente digitalizzazione dei processi sanitari, l'interconnessione dei sistemi e l'aumento esponenziale delle minacce informatiche rendono imprescindibile un approccio sinergico, strutturato e continuo tra queste figure anche attraverso la creazione di specifiche strutture aziendali trasversali in cui DPO e CISO possano collaborare sin dalla fase di progettazione "privacy by design" dei nuovi sistemi o iniziative sanitarie. Tanto al fine di evitare la frammentazione tra sicurezza informatica e protezione dei dati, promuovendo un approccio olistico basato sulla valutazione congiunta dei rischi e sulla definizione dei ruoli e delle responsabilità.

In conclusione, solo attraverso un equilibrio tra innovazione digitale, sicurezza informatica e presidio organizzativo è possibile conseguire una efficace e rispettosa gestione del dato sanitario. Le auspicate sinergie possono rafforzare la cultura della protezione del dato e orientare le scelte aziendali verso una gestione responsabile e sicura del patrimonio informativo, inteso come bene comune.

CYBER
Think Tank
ASSINTEL

LA CYBER PER TUTTI

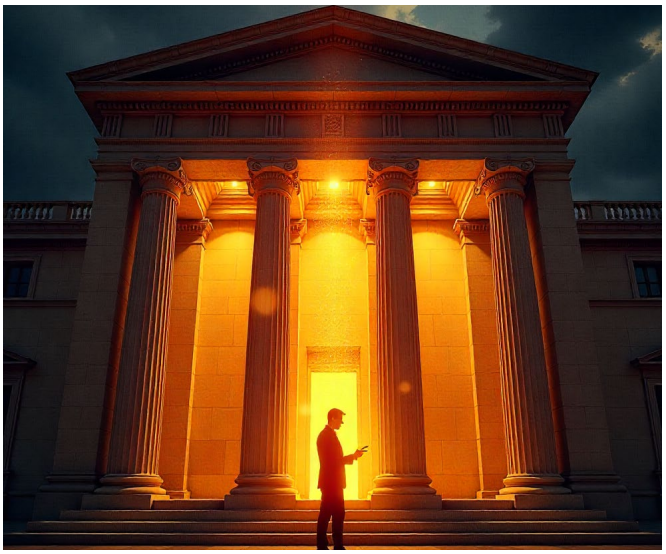
Cybersecurity e credito: il tempo del fare è adesso

A cura di Sandro Sana

Viviamo in un tempo in cui la solidità economica di un'impresa non si misura più solo con bilanci ben redatti, flussi di cassa in ordine o margini operativi competitivi. Nell'era digitale, dove ogni azienda è potenzialmente esposta a minacce informatiche che possono paralizzare intere filiere produttive o compromettere dati sensibili, anche la "solidità digitale" diventa un criterio imprescindibile per valutare l'affidabilità di un'impresa. E oggi, a sancire questo cambio di paradigma, sono proprio le banche.

Già nel febbraio 2023, la Vice Direttrice Generale della Banca d'Italia, Alessandra Perrazzelli, in un intervento ufficiale ha parlato apertamente dell'importanza della resilienza operativa digitale delle imprese. Un concetto che fino a pochi anni fa era materia per addetti ai lavori e tecnici IT, ma che ora diventa una leva fondamentale nella valutazione del merito creditizio da parte degli istituti finanziari.

Dimenticate quindi l'idea che il rischio di credito sia legato soltanto a fattori economici e patrimoniali. Le banche stanno evolvendo il proprio approccio e oggi prendono in considerazione elementi che fino a poco tempo fa sarebbero sembrati roba da geek con il badge al collo. Parliamo di backup e piani di disaster recovery, della presenza (vera, non scritta su carta) di un piano di business continuity, di tecnologie come EDR, MFA, PAM, o ancora di quanto spesso si conducono penetration test e vulnerability assessment.



In parole povere: se la tua azienda non avesse un assetto di cybersecurity serio, potresti vederti chiudere le porte in faccia da chi dovrebbe finanziarti. O, nella migliore delle ipotesi, vederti applicare condizioni economiche peggiorative rispetto a un concorrente che ha fatto i compiti a casa. E le banche – che non sono note per il romanticismo – iniziano a pensare che prestare soldi a chi ha buchi di sicurezza sia un po' come prestare l'auto a un diciottenne senza patente. Il botto, prima o poi, arriva.

Secondo quanto riportato recentemente anche da ItaliaOggi, gli istituti di credito si stanno attrezzando concretamente. Non è solo teoria da convegno: ci sono già strumenti di valutazione attivi, come il cosiddetto "cyber credit scoring". E chi pensa che si tratti di una moda passeggera, rischia di fare la fine di chi nel 2008 diceva che il cloud era solo un hype.

Il vento del cambiamento, peraltro, non soffia solo da Roma o da Milano. È Bruxelles che ha tracciato la rotta con normative sempre più stringenti. Tra Digital Operational Resilience Act (DORA), Cyber Resilience Act e la famigerata NIS2, le imprese europee si trovano davanti a un bivio: adeguarsi, o restare fuori dal mercato. Anche se non sei una banca, se sei parte di una filiera strategica devi dimostrare di non essere l'anello debole. Perché oggi, il danno reputazionale viaggia a una velocità ben maggiore dei tuoi fornitori: basta un breach, e sei sulle prime pagine.

E non è un caso se nella Relazione annuale 2025 della nostra intelligence nazionale, il tema della sicurezza cibernetica è stato esplicitamente indicato come una delle principali sfide trasversali alla tenuta del sistema Paese. Il documento parla chiaro: la digitalizzazione è sì una leva di sviluppo, ma è anche una superficie d'attacco sempre più estesa, dove ogni vulnerabilità può essere sfruttata da attori ostili per destabilizzare economia, finanza e fiducia. Questo scenario, in continua evoluzione, impone una presa di coscienza anche da parte dei board e dei decisori finanziari: oggi, non puoi permetterti di prestare denaro a chi è un bersaglio ambulante.

La ragione è semplice quanto spietata: un attacco ransomware a una PMI può avere un effetto domino su clienti, fornitori e perfino su interi comparti industriali.

La storia recente ce lo ha insegnato a suon di blackout, supply chain ferme e disastri mediatici. E allora, se una banca deve decidere a chi prestare soldi, è ovvio che guardi anche quanto sei esposto e quanto sei pronto a reggere l'urto.

Ed ecco che entra in gioco la famosa "lista della spesa" della cybersicurezza. L'Agenzia per la Cybersicurezza Nazionale (ACN) l'ha messa nero su bianco: non basta dire di essere sicuri, bisogna dimostrarlo con misure concrete. Parliamo di sistemi aggiornati, gestione attenta degli accessi, backup cifrati e testati regolarmente, antivirus e firewall attivi, ma anche di formazione del personale (quello vero, non il corso fatto solo per firmare il registro) e di piani ben scritti per la gestione degli incidenti e la continuità operativa.

La cybersicurezza oggi è un sistema, un insieme di pratiche e tecnologie integrate, verificabili e... possibilmente funzionanti.

Non è più tempo per affidarsi a un antivirus gratuito e a una password scritta su un post-it. La cybersicurezza oggi è un sistema, un insieme di pratiche e tecnologie integrate, verificabili e... possibilmente funzionanti. E soprattutto non improvvisabili: non si può "acquistare" sicurezza con una fattura a fine anno, come si fa con le cartucce della stampante. Serve metodo, serve governance, servono teste pensanti.

Proprio per questo, alcune banche stanno strutturando vere e proprie checklist digitali. Le aziende che vogliono accedere al credito dovranno rispondere punto per punto, e fornire prove tangibili. In prospettiva, non è assurdo immaginare un vero e proprio "cyber rating" ufficiale, da affiancare al classico rating finanziario.

E questa non è solo una seccatura in più. È un messaggio chiaro ai consigli di amministrazione, ai CEO e ai CFO: la sicurezza IT non è più roba da lasciare in mano solo al CIO, al CISO o al IT Manager. Diventa una responsabilità di vertice. Un asset da gestire, misurare, comunicare e integrare nella strategia d'impresa.

Anzi, chi sa leggere tra le righe capisce che qui si gioca anche una partita di vantaggio competitivo. Le aziende che investono davvero nella sicurezza potranno ottenere condizioni migliori, mostrarsi più affidabili sul mercato e attrarre partner e clienti di livello superiore. Senza contare le gare pubbliche o le selezioni fornitore dove, ormai, certificazioni come ISO/IEC 27001 o l'adesione ai framework NIST CSF sono diventate un lasciapassare. In sostanza, la sicurezza sta diventando un moltiplicatore di business.

Tutto questo accade mentre, come evidenziato anche nell'Inserto Intelligence 2025 dedicato all'intelligenza artificiale, si moltiplicano le minacce ibride, le disinformazioni e le vulnerabilità tecnologiche. Il documento ci ricorda che lo sviluppo di tecnologie come l'IA deve andare di pari passo con un'etica della responsabilità e una governance affidabile. Perché non è solo questione di sicurezza informatica: è questione di sicurezza nazionale, democratica, industriale. È questione di fiducia.

In definitiva, il mondo del credito sta cambiando pelle. La sicurezza informatica è diventata un elemento chiave, al pari del patrimonio netto o del margine operativo lordo. Le imprese devono adeguarsi. Serve investire in tecnologie, certo, ma anche in cultura e governance. E soprattutto, serve capire che il tempo del "poi ci pensiamo" è finito. Ogni ritardo, in un mondo dove i cybercriminali agiscono in tempo reale, si paga. A volte, con interessi a sei zeri.

E qui entra in gioco il ruolo di chi si occupa di cybersecurity. Non solo tecnici, ma traduttori culturali. Figure in grado di fare da ponte tra il linguaggio tecnico e quello finanziario, di spiegare a una azienda cosa significa avere un SOC attivo h24, un processo di incident response o un'attività di Risk Analysis. Il futuro è di chi sa essere solido, competente, e soprattutto preparato.

E oggi, essere preparati significa anche questo: sapere difendere non solo i propri dati, ma anche la propria credibilità economica. Perché ormai, se non sei cyber, potresti anche non essere bancabile. E nel business, come nella vita, essere affidabili non basta: bisogna dimostrarlo. Altrimenti, il prossimo bonifico lo vedrai… col binocolo. O peggio: te lo sognerai in deepfake.

Space Economy in crescita - Cybersecurity in affanno

A cura di Federica Maria Rita Livelli

Space Economy in crescita, cybersecurity in affanno

Negli ultimi anni, la Space Economy è cresciuta rapidamente grazie agli investimenti pubblici e privati, ma questa espansione comporta nuove sfide cyber, rendendo la cybersecurity essenziale per la protezione dei dati e delle infrastrutture spaziali.

Un ecosistema in rapida evoluzione

La Space Economy è oggi un settore in rapida espansione, con applicazioni che vanno dalle telecomunicazioni satellitari all'osservazione della Terra, fino al turismo spaziale e all'estrazione di risorse extraterrestri. Inoltre, le tecnologie spaziali sono ormai parte delle infrastrutture critiche globali, essenziali per comunicazioni, navigazione e gestione dei dati.

Tuttavia, questa crescita espone il settore a minacce informatiche sempre più complesse, in un contesto in cui l'economia globale dipende da reti spaziali e sistemi digitali sempre più interconnessi. Di fatto, l'innovazione tecnologica - guidata dalla AI - e la trasformazione delle filiere stanno ampliando la superficie d'attacco, aumentando le opportunità per i cybercriminali.

Space Economy: AAA una nuova cybersecurity cercasi

Le tradizionali strategie di sicurezza – basate su perimetri, accessi e ruoli – non sono più sufficienti. È necessario orientarsi verso un'architettura di sicurezza Zero Trust, fondata su una verifica continua di identità, accessi e integrità del sistema, in grado di mettere costantemente in discussione affidabilità e vulnerabilità, rafforzando così la resilienza complessiva delle infrastrutture spaziali.

In quest'ottica si inserisce anche la recente approvazione della legge quadro italiana sullo Spazio, che riconosce la cybersecurity e la resilienza come requisiti essenziali per operare.

Le principali minacce alla sicurezza spaziale

Di seguito le principali sfide in termini di cybersecurity che l'ecosistema della Space Economy si trova a gestire:

- Attacchi informatici avanzati, spesso condotti da attori statali o gruppi APT, possono compromettere dati e interrompere sistemi critici.
- Tecnologie legacy, ancora in uso, rendono molti asset vulnerabili, in quanto progettati senza criteri moderni di cybersecurity.
- Convergenza sistemi IT/OT, ovvero, l'adozione di soluzioni con DNA IT in ambiti OT può facilitare il lavoro degli attaccanti.
- Attacchi elettronici, quali jamming, spoofing e meaconing, mirano a disturbare o manipolare i segnali radio e GPS.
- Minacce procedurali, legate al fattore umano e a tecniche di social engineering, possono aggirare anche i sistemi più sicuri.
- Compromissione delle reti digitali, tramite inserimento di dati corrotti o infiltrazioni nei sistemi di controllo.
- Rischi nella supply chain, spesso globale e frammentata, che può diventare un punto d'accesso per gli aggressori.
- Errore umano, dovuto alla complessità operativa,

che può causare danni per disattenzione o configurazioni errate.

- Scarsa visibilità, data dalla natura remota e distribuita delle infrastrutture spaziali, che rende difficile il rilevamento in tempo reale di incidenti o vulnerabilità.

Le contromisure strategiche

Si tratta di implementare misure tecniche e di adottare una governance collaborativa a livello europeo e internazionale. Alcuni strumenti fondamentali includono:

- Crittografia avanzata per proteggere la comunicazione tra Terra e orbita.
- Controlli di accesso basati su autenticazione forte e logica zero trust.
- Sistemi di rilevamento e prevenzione attiva delle intrusioni, supportati da tecnologie di threat intelligence.
- Simulazioni di attacco e audit continui, per testare la resilienza dei sistemi e rafforzare la difesa.

Il contesto normativo

La digitalizzazione dello spazio impone un ripensamento delle regole: occorre un sistema normativo adatto all'ambiente orbitale, che tenga conto dei rischi legati a software-defined networks e applicazioni cloud. In Europa si sono sviluppati quadri regolatori, quali: il Cyber Resilience Act, la direttiva NIS2, il Nuovo Regolamento Macchine e l'AI Act, che si caratterizzano per un approccio risk-based e resilience-based. Tuttavia, a livello globale manca ancora un framework condiviso per garantire la sicurezza delle attività spaziali, il che rende urgente un coordinamento internazionale.

Focus su NIS2

L'Unione Europea ha incluso il settore spaziale tra le infrastrutture critiche soggette alla direttiva NIS2, sottolineando l'urgenza di proteggere asset e servizi contro minacce cyber sempre più sofisticate. La direttiva introduce obblighi stringenti per garantire continuità operativa, resilienza e gestione efficace degli incidenti informatici, fondamentali anche nel contesto spaziale. Vediamo in particolare di che si tratta.

Continuità operativa e gestione del rischio - NIS2 impone alle organizzazioni del settore spaziale di dotarsi di piani strutturati per garantire il funzionamento ininterrotto dei servizi, anche in caso di attacchi gravi. Ciò richiede:

- Politiche di sicurezza delle informazioni basate su analisi sistematiche dei rischi e delle vulnerabilità.
- Piani di continuità operativa e gestione delle crisi per reagire prontamente e limitare i danni.
- Procedure di ripristino dei sistemi, per minimizzare interruzioni e tempi di inattività.

Preparazione e risposta agli incidenti - Le organizzazioni devono sviluppare capacità operative concrete, tra cui:

- Procedure di emergenza documentate, testate e aggiornate regolarmente.
- Team di risposta alle crisi, formati da esperti capaci di coordinare l'intervento.
- Piani di prevenzione, rilevamento e risposta agli attacchi, inclusi backup, esercitazioni e catene di comando chiare.
- Gestione trasparente delle vulnerabilità, con obbligo

di divulgarle per evitare che vengano sfruttate altrove.

Sicurezza della supply chain - NIS2 impone di valutare la cybersecurity dei fornitori lungo tutta la catena del valore. Le organizzazioni spaziali dovranno attivare controlli, audit e misure di sicurezza che coprano l'intero ciclo di vita dei sistemi, assicurando conformità alle normative in continua evoluzione.

Dunque, la cybersecurity non è più un'opzione, ma una condizione essenziale per garantire uno sviluppo sicuro, resiliente e sostenibile dell'ecosistema spaziale.

Obblighi di segnalazione e cooperazione europea - La direttiva stabilisce tempistiche precise per la notifica degli incidenti significativi: segnalazione iniziale entro 24 ore, notifica dettagliata entro 72 ore, relazione finale entro un mese. Inoltre, promuove:

- Condivisione delle informazioni tra le autorità europee.
- Risposta coordinata agli incidenti su scala UE, attraverso reti come EU-CyCLONe.
- Cooperazione strutturata tra enti nazionali per affrontare crisi di cybersecurity anche nel contesto della Space Economy.

Conclusione

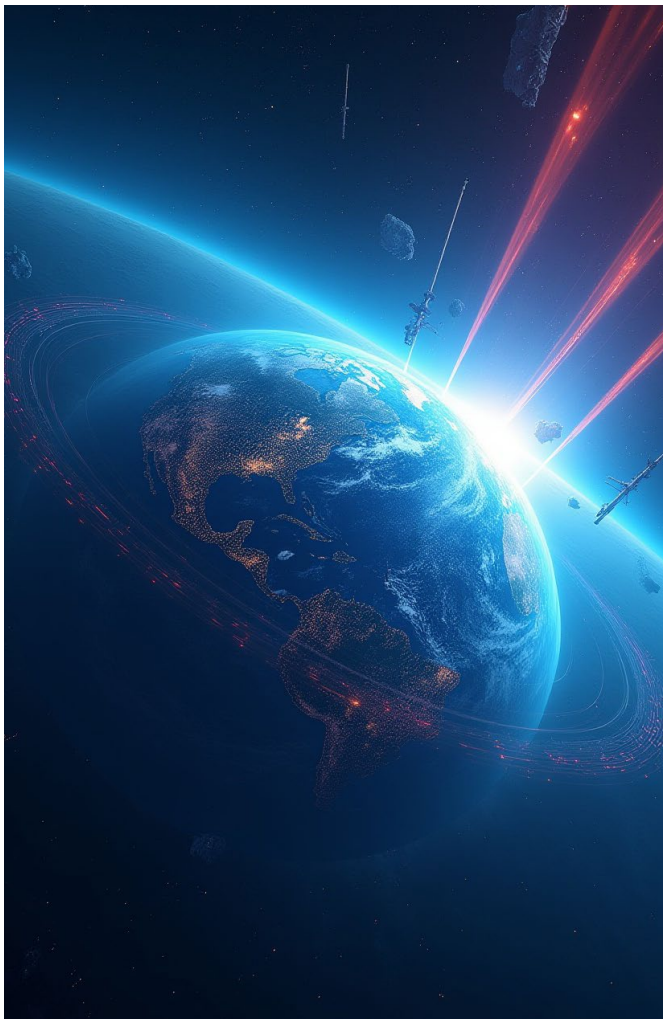
L'innovazione tecnologica e la crescente interconnessione tra infrastrutture spaziali, sistemi terrestri, cloud e reti wireless stanno ampliando la superficie d'attacco, offrendo nuove opportunità agli hacker per individuare vulnerabilità.

In questo scenario, diventa urgente un cambio di paradigma nella gestione della sicurezza informatica nello spazio, considerando che le strategie tradizionali - basate su difese perimetrali e controllo degli accessi - non sono più sufficienti a contrastare minacce complesse, incluse quelle interne. Serve un modello di cybersecurity dinamico, fondato su architetture Zero Trust, capaci di mettere continuamente alla prova sicurezza, resilienza e affidabilità dei sistemi.

Inoltre, garantire la protezione delle risorse spaziali richiede la collaborazione di tutti gli attori coinvolti, l'adozione di tecnologie avanzate e un approccio proattivo. Investire nella cybersecurity significa non solo tutelare gli asset spaziali, ma anche costruire le fondamenta per uno sviluppo sostenibile dell'attività spaziale. Ancora, è essenziale monitorare costantemente l'evoluzione della sicurezza spaziale e integrarla con la governance, le normative e le buone pratiche.

È doveroso ricordare che la cybersecurity coinvolge anche competenze umane e processi organizzativi: occorre quindi promuovere una solida cultura della sicurezza, basata su formazione e sensibilizzazione a livello nazionale e internazionale. Inoltre, la cooperazione tra Stati e organismi sovranazionali sarà decisiva per affrontare le sfide comuni della Space Economy, attraverso lo scambio di informazioni, la condivisione di best practice e l'adozione di standard comuni per una cybersicurezza globale, efficace e armonizzata.

Dunque, la cybersecurity non è più un'opzione, ma una condizione essenziale per garantire uno sviluppo sicuro, resiliente e sostenibile dell'ecosistema spaziale, su cui si fonda la nostra società moderna.



Assintel Cyber Hub

CYBER Think Tank ASSINTEL

Connettiti alla rete della sicurezza!

Obiettivo:

Mappare ed elencare le aziende associate ad Assintel con competenze in ambito Cyber.

Per info scrivi a:

segreteria@assintel.it

Intelligenza artificiale e cyberlaundering

A cura di Ranieri Razzante

L'intelligenza artificiale (AI) ha rivoluzionato molti settori e, per quel che qui interessa, il comparto dei servizi finanziari. Ciò in via positiva, migliorando l'offerta e la fruizione di servizi da parte della clientela (si pensi, ad esempio, alle nuove possibilità di accesso a servizi on line, sia di trading che di informazione economica e fiscale). Ma la tecnologia tanto celebrata in questo momento viene anche sempre più sfruttata dalla criminalità organizzata, che ne riconosce il potenziale per massimizzare i profitti illeciti e minimizzare i rischi di discovery.

Ad esempio, l'AI viene utilizzata per potenziare i malware cosiddetti "adattivi", in grado di eludere i sistemi di sicurezza aggiornandosi continuamente. Questi programmi possono - in sintesi - analizzare i meccanismi di difesa di un sistema e modificarne il codice in tempo reale, aumentando le difficoltà per gli esperti di cybersecurity nel prevenirne la diffusione. A ben vedere, l'utilizzo dell'apprendimento automatico permette al malware di individuare rapidamente sistemi vulnerabili e replicarsi in modo estremamente efficiente. Si pensi a ciò che queste evenienze possono produrre sui sistemi finanziari e gli apparati di trading bancario e borsistico.

Nel 2022, una nota vicenda ha visto un'organizzazione criminale utilizzare un deepfake vocale per sottrarre oltre 35 milioni di dollari da una banca degli Emirati Arabi Uniti. Inoltre, una frode multimilionaria compiuta da criminali mediante utilizzo di un deepfake vocale per impersonare un amministratore delegato, convincendo un dirigente a trasferire fondi su un conto controllato da truffatori. Prima che il riciclaggio, le frodi finanziarie sono in aumento esponenziale; ne sono vittime persino gli exchangers di criptovalute.

Il riciclaggio di denaro rappresenta un settore dove l'intelligenza artificiale ha permesso alla criminalità organizzata di raggiungere livelli di sofisticazione senza precedenti. L'AI viene utilizzata per elaborare schemi complessi, che frammentano e distribuiscono i flussi di denaro attraverso reti globali, rendendo estremamente difficile il loro tracciamento.

Si diceva prima che le piattaforme di criptovalute sono spesso al centro di queste operazioni. L'intelligenza artificiale consente di analizzare in tempo reale le transazioni su blockchain pubbliche e private, identificando percorsi e canali meno sorvegliati. Questi algoritmi mescolano abilmente fondi legali e illegali tramite servizi come i mixer di criptovalute, oscurando la provenienza del denaro e rendendo quasi impossibile risalire alla sua origine.

Queste transazioni, frazionate in importi minimi, passano pressoché inosservate ai sistemi di monitoraggio tradizionali.

Un altro esempio malevolo è l'impiego dell'AI per creare false aziende o reti di fatturazione fittizia. Questi sistemi simulano operazioni commerciali legittime, sfruttando modelli di apprendimento automatico per generare documentazione contabile credibile. Attraverso questo processo, il denaro sporco viene integrato nei circuiti finanziari legali con una precisione quasi perfetta.

La portata del problema è ulteriormente amplificata dal dark web, dove l'AI viene utilizzata per facilitare la compravendita di strumenti finanziari illeciti, come conti bancari compromessi e carte di credito rubate. Attraverso queste piattaforme, i gruppi criminali accedono a reti globali che consentono loro di espandere le operazioni su scala internazionale.

Le autorità si trovano quindi ad affrontare un nemico tec-

nologicamente avanzato, capace di sfruttare ogni lacuna nei sistemi di controllo finanziario e regolamentazione. Per contrastare queste attività, è necessario un uso altrettanto avanzato dell'AI da parte di enti di vigilanza e forze dell'ordine, accompagnato da una stretta collaborazione internazionale.

In Italia, le nostre Autorità di vigilanza di settore, e le Forze dell'ordine dedicate, stanno utilizzando sistemi di machine learning per l'analisi massiva di dati, come quelli rivenienti ad esempio dalle cosiddette "segnalazioni di operazioni sospette" previste dalla normativa di prevenzione del riciclaggio (il d.lgs. 231 del 2007).

Questi metodi rappresentano una sfida enorme per le autorità, che devono fronteggiare un nemico sempre più tecnologicamente avanzato, capace di sfruttare le lacune nei sistemi di regolamentazione e controllo finanziario.

La criminalità organizzata sfrutta l'AI per massimizzare i profitti illeciti.

La criminalità organizzata sfrutta le potenzialità dell'AI anche in riferimento al traffico di droga e al contrabbando. I cartelli della droga, in particolare, hanno investito in queste tecnologie per ridurre i costi logistici e minimizzare i rischi.

In un caso documentato, una rete criminale ha utilizzato il machine learning per coordinare un'operazione su larga scala che ha coinvolto più punti di sbarco in diversi paesi, riducendo al minimo il rischio di intercettazione.

L'applicazione dell'intelligenza artificiale non si limita alla logistica o al marketing illecito, e può osservarsi come l'AI stia trasformando il traffico di droga e contrabbando, rendendo le operazioni criminali più efficienti e difficili da contrastare.

I gruppi criminali e terroristici utilizzano l'AI anche per ottimizzare la logistica. Alcuni esempi includono:

- L'uso di droni autonomi per il trasporto di droga e altre merci illegali.
- L'impiego di algoritmi per scegliere percorsi di traffico meno monitorati.
- Previsioni sulla domanda di mercato grazie all'analisi dei dati provenienti dai social media e dal dark web.

Con particolare riferimento alla sorveglianza e al monitoraggio delle operazioni, l'impiego del riconoscimento facciale da parte della criminalità organizzata ha introdotto - giova ripeterlo - nuove possibilità di controllo e gestione delle attività illecite. Grazie a software avanzati, le organizzazioni possono seguire i loro movimenti in tempo reale attraverso sistemi di sorveglianza urbana o telecamere private.

In alcuni casi, i sistemi analizzano non solo i volti ma anche i comportamenti, segnalando automaticamente eventuali anomalie che potrebbero indicare un'infiltrazione o un rischio di esposizione.

Infine, questi gruppi stanno iniziando a sperimentare l'uso del riconoscimento facciale per condurre analisi preliminari nei luoghi pubblici. Ad esempio, prima di organizzare incontri o scambi di merci, i criminali utilizzano droni o telecamere nascoste per scansionare l'area e verificare l'assenza di minacce, come agenti sotto copertura o dispositivi di sorveglianza.

Questi sviluppi evidenziano come la criminalità organizzata sfrutti l'AI non solo per migliorare la sicurezza delle proprie operazioni, ma anche per anticipare e neutralizzare eventuali interventi delle autorità. Per contrastare questi abusi, è fondamentale che le istituzioni sviluppino tecnologie di rilevamento altrettanto avanzate, accompagnate da regolamentazioni rigorose che limitino l'uso illecito del riconoscimento facciale. E magari lo consentano di più a fini di difesa, contrariamente alle previsioni dell'AI Act e del Gdpr in questa materia.

Il cyberlaundering era già noto almeno due decenni fa, ma si perpetrava con la penetrazione di conti bancari, ove far transitare somme, o attraverso carte di credito e piattaforme di pagamento.

Oggi, come sopra è stato accennato, il web offre ancora di più, ma le Autorità antiriciclaggio, non ultima la nuova AMLA europea, si stanno muovendo alacremente per colmare un evidente gap generazionale.

Controllo interno, cybersecurity e umanesimo digitale

A cura di Carlo Guastone

Il framework COSO

Il framework COSO (acronimo che identifica il gruppo di lavoro che lo ha realizzato nel 1992) è universalmente riconosciuto come la bibbia del Controllo interno delle aziende, concepito come strumento di verifica dell'operato del management nei confronti degli stakeholders (portatori di interesse), azionisti in primis ma anche dipendenti, clienti, fornitori, parti sociali, e così via.

Il framework consiste in un insieme di principi e linee guida per la gestione del controllo interno e della corporate governance nelle organizzazioni, con particolare riferimento ai processi aziendali che assicurano la conformità normativa, la sicurezza, l'efficacia e l'efficienza delle operazioni, la assegnazione di ruoli e responsabilità.

Nel 2013 è stata pubblicata la versione COSO ERM centrata sull' enterprise risk management, che ha l'obiettivo di garantire che le organizzazioni siano in grado di raggiungere i loro obiettivi strategici, operativi, di reporting e di compliance, riducendo al minimo il rischio di non riuscire a raggiungere tali obiettivi.

COSO ERM si basa su cinque componenti chiave (ambiente di controllo, valutazione dei rischi, attività di controllo, informazioni e comunicazioni, monitoraggio delle attività) ed estende la gestione dei rischi a tutta l'organizzazione, non solo ai rischi finanziari, considerando gli obiettivi strategici dell'impresa. Il framework è stato adottato in particolare dalle grandi imprese quotate (ad esempio negli USA in ottemperanza alla legge SOX, in Italia in ottemperanza alla Legge 262/2005 dedicata al Risparmio e al Codice di autoregolamentazione società quotate), ed è utilizzato in molti settori e può essere adattato alle specifiche esigenze di ciascuna organizzazione.

Nel 2023 il COSO ha pubblicato delle linee guida supplementari per le organizzazioni relative alla rendicontazione della sostenibilità (ICSR), mentre nel 2024 ha pubblicato un documento specifico relativo ai controlli della robotica. Per approfondimenti https://www.coso.org/guidance-on-ic.

Fin dalla prima pubblicazione del framework COSO nel 1992, e in particolare dalla versione 2013, la sicurezza informatica era considerata una componente rilevante del Controllo Interno, centrata prevalentemente sulla continuità operativa e sull'integrità delle informazioni, senza una specifica focalizzazione sulla cybersecurity

COSO ERM e rischi Cyber

L'integrazione di COSO ERM e cybersecurity è fondamentale per garantire la sicurezza e la resilienza di un'organizzazione, permettendo di gestire i rischi informatici in modo efficace e strategico. L'integrazione tra COSO ERM e la cybersecurity è cruciale per garantire la sicurezza aziendale e la continuità operativa. Per identificare l'ambito da considerare ci viene in aiuto un recen-

te contributo di ACN di cui riportiamo l'abstract:

"Il dominio Cyber Risk Management consiste nell'insieme di pratiche volte alla gestione del rischio cyber entro un determinato livello conformemente a valutazioni svolte e obiettivi dell'organizzazione. Sviluppare capability di sicurezza all'interno di questo dominio coinvolge diverse attività, tra cui: (i) identificazione e analisi del rischio cyber, (ii) trattamento del rischio cyber, (iii) comunicazione del rischio cyber, (iv) gestione del rischio cyber di terze parti. Il "Cyber Risk Management" si integra all'interno dell'"Enterprise Risk Management" (ERM) per l'intera organizzazione ed ha lo scopo di definire e implementare un programma di gestione del rischio cyber che minimizzi la possibilità che l'organizzazione possa essere danneggiata dal verificarsi di attacchi cibernetici."

L'integrazione tra COSO ERM e la cybersecurity è cruciale per garantire la sicurezza aziendale e la continuità operativa.

Tutti i rischi cyber devono essere considerati, dai rischi relativi alle infrastrutture IT e al software applicativo, ai dati sensibili e alla catena di approvvigionamento, alla implementazione di misure di sicurezza per proteggere i sistemi e le informazioni da attacchi e minacce, al controllo accessi, alla formazione del personale, alla protezione dei sistemi IT e al monitoraggio della rete, alla gestione degli incidenti per rispondere in modo tempestivo e efficace agli attacchi informatici, al monitoraggio e controllo delle misure di sicurezza, etc.

Come sottolineato da ACN, per lo svolgimento del rischio Cyber "possono essere utilizzati i diversi framework di controlli disponibili come, ad esempio, ISO/IEC 27001, il CSF 2.0, l'"Italian Cybersecurity Report – Controlli Essenziali di Cybersecurity", il "CIS Critical Security Controls" o il NIST SP 800-53."

La valutazione del rischio cyber deve coinvolgere (come richiesto per tutti i rischi rilevanti considerati dal framework COSO ERM) le posizioni apicali dell'Impresa, adempimento di compliance richiamato con chiarezza dalla direttiva NIS2, con particolare focalizzazione sui rischi delle subforniture, sulla formazione cyber dei dipendenti e sui controlli di vulnerabilità dei sistemi digitali.

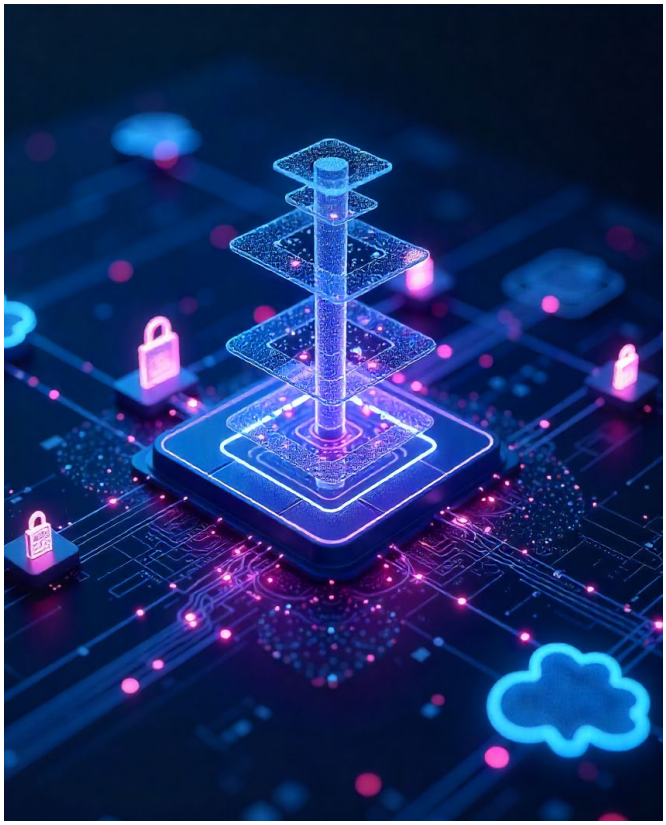
Umanesimo digitale, Intelligenza artificiale e cybersecurity

Consultando i motori di ricerca con la chiave "Umanismo digitale" si ha un' evidenza concreta della attualità del temine in numerose pubblicazioni e in articoli riportati su riviste che trattano tematiche di gestione aziendale e di formazione manageriale.

L'umanesimo digitale promuove un approccio più equilibrato e responsabile alla tecnologia, cercando di sfruttare i suoi vantaggi senza rinunciare ai valori umanistici che caratterizzano la società. Si tratta di un movimento che si rivolge a diverse aree, dall'istruzione alla salute, dal lavoro alla politica, con l'obiettivo di creare un'era digitale più inclusiva e umana.

Per le aziende l' Umanesimo digitale consiste, in particolare, nella progettazione e gestione di soluzioni digitali nel rispetto dell'etica e della sostenibilità, favorendo l'innovazione e uno sviluppo tecnologico inclusivo, utilizzando le tecnologie digitali in modo responsabile per ridurre l'impatto ambientale e promuovere uno sviluppo sostenibile, nel rispetto dei diritti delle persone. Soluzioni che, inevitabilmente, richiedono adeguati approcci metodologici di Controllo interno in grado di favorire anche la governance della tematica "Umanesimo digitale".

Abbiamo lasciato al termine dell'articolo un accenno alle implicazioni del Controllo Interno con l'Intelligenza artificiale, implicazioni che richiedono di considerare il rispetto dell'etica in generale e in particolare i contenuti dell' AI ACT, con l'inevitabile approfondimento dei controlli relativi alla cybersecurity e all' Umanesimo digitale, che rappresenta un nuovo paradigma che potrebbe aiutare le organizzazioni a navigare nel mondo digitale in modo più etico, responsabile e sostenibile.



Ransomware nel Retail: siamo pronti al prossimo attacco?

A cura di Andrea Ceiner

L'incubo inizia con una chiamata (i nomi di persone e organizzazioni sono inventati).

Francesca, dal negozio in aeroporto, chiama concitata Marco del supporto tecnico:

"Ciao Marco, lo schermo in vetrina è diventato nero con una scritta bianca "LockBit Black, all your important files are stolen and encrypted! You must find zwWXthZ2C. README.txt file and follow the instruction!".

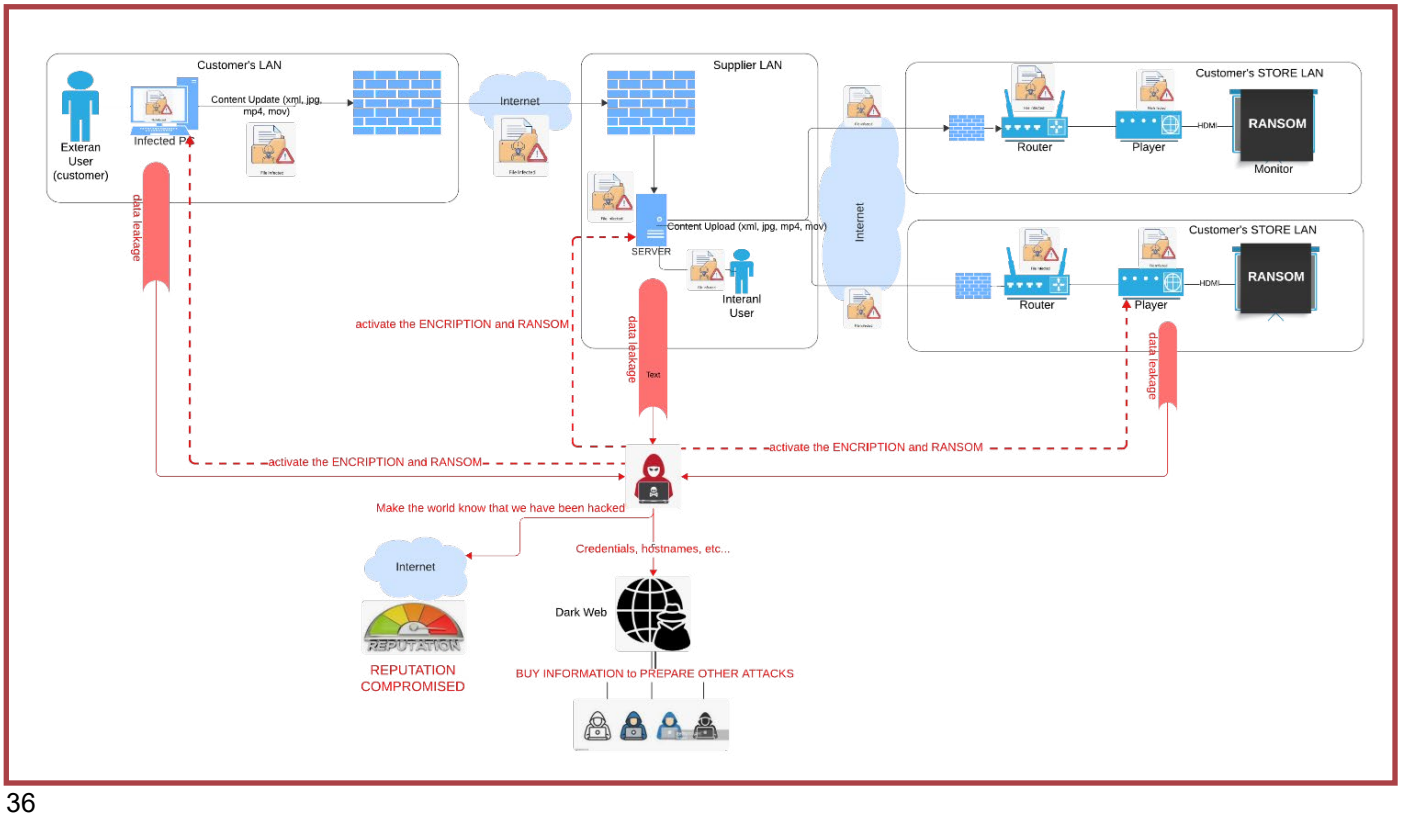
Marco, si fa mandare una foto sul cellulare e chiama subito Pietro, il responsabile della sicurezza. "Ciao Pietro, sono Marco, abbiamo un problema con un ransomware, guarda la foto. Che facciamo?". Pietro: "Di a Francesca di staccare immediatamente il cavo di rete dal pc dietro allo schermo e di staccare anche il cavo video. Dille di lasciare il pc acceso. Mandiamo un tecnico immediatamente a portare un nuovo PC e a prelevare quello infetto. Marco, a che server è collegato quel pc?".

Marco: "Al server del cliente MODA TOPOLINO PAPERINO, a cui solo collegati altri 250 negozi!"

Pietro: "Cavoli! Avviso l'IT che isoli subito quel server dalla rete! Qui c'è il rischio che contagiamo tutti i punti vendita! Se quel server fosse nella stessa rete di altri server di altri clienti il perimetro di rischio si amplierebbe ancora".

Come prosegue la storia dipende dalle tante possibili varianti.

Ad esempio, uno scenario potrebbe essere quello descritto dalla fig.1, dove un grafico del reparto creativo del cliente, vittima di un attacco phishing, è stato contagiato da un malware che può attivare il ransomware. Questo malware ha contagiato altri file nel suo pc, tra cui quelli che lui ha preparato per la prossima campagna di broadcasting sui suoi negozi. Il malware si potrebbe quindi propagare a tutti i negozi collegati. Per qualche settimana il malware potrebbe trasmettere dati rubati dalla rete del cliente e permettere all'attaccante di elaborare varie forme di attacco, tra cui il riscatto, attivando la crittografia di tutti i nodi compromessi e la richiesta di riscatto e il tentativo di estorsione.



Quello che impressiona nello scenario sopra descritto sono la quantità di punti di attacco possibili (almeno 8) e le opportunità di guadagno dell'attaccante sia dalla vendita delle informazioni rubate sia dal riscatto.

Secondo Hackaman Global Cyber Attacks Report, Il settore retail rientra nei top10 targets, registrando circa 8% degli attacchi.

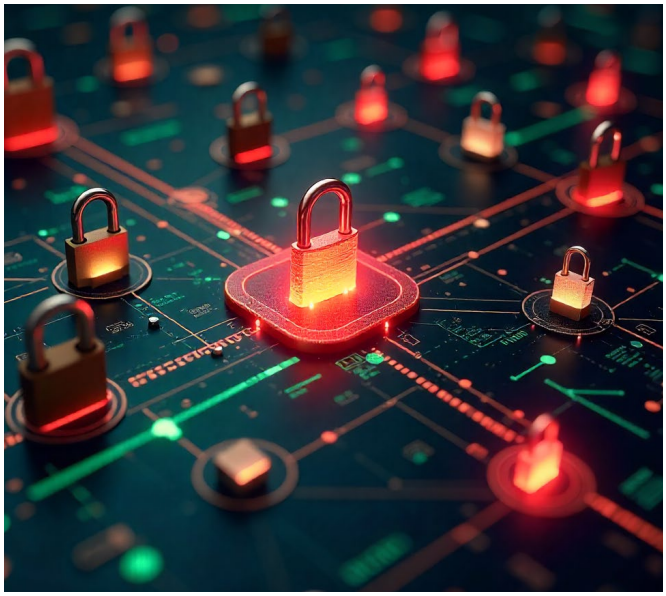
La filiera dei retailers nel settore delle tecnologie audio/video nel negozio fisico riguarda diversi attori, con posture di sicurezza e vulnerabilità diverse: ci sono i vendor di tecnologie hardware (schermi, led, computer, apparati di rete, sistemi di pagamento elettronico…) e software specializzati (piattaforme di digital signage, di omnichannel customer experience, di digital retail, di media content design, ecc..) e ovviamente i cloud provider. Poi, più "vicini" al cliente, troviamo le media agencies con i creativi che producono i contenuti grafici, molti piccoli system integrator e service providers locali e pochi grandi che mettono tutto assieme, inclusa la logistica e i servizi post vendita di gestione dei dispositivi per anni. In ultimo, non possiamo dimenticare i consumatori, che usano lo smartphone e il pc per fare i loro acquisti, dentro e fuori il negozio.

Concludendo, la sfida per i retailer è come arrivare a un livello di rischio sostenibile e accettabile, considerando tutta la filiera.

Dunque, il punto di partenza sta proprio nel:

a) calcolare questo livello di rischio accettabile e nel condividerlo con tutti gli attori della filiera;

b) introdurre, nel disegno iniziale di ogni soluzione, i requisiti di sicurezza che retailer e fornitori dovranno implementare per arrivare al risultato.



Sicurezza negli ambienti ibridi: guida strategica per Manager e Decision Maker

A cura di Mohammed Bellala

Negli ultimi anni, il concetto stesso di “ambiente IT” è cambiato radicalmente. Quello che una volta era un perimetro ben definito – uffici, data center, firewall fisici – oggi è diventato un ecosistema fluido, interconnesso e, soprattutto, ibrido.

Un ambiente ibrido integra infrastrutture on-premises, servizi cloud (pubblici e privati), applicazioni SaaS, dispositivi remoti e persino ambienti OT o edge. Una trasformazione spinta da esigenze di agilità, costi, flessibilità operativa. Ma ogni elemento di libertà introduce un grado di complessità e, spesso, una nuova superficie di attacco.

Per i manager e i decisori, non si tratta solo di scegliere “dove mettere i server” o “quale piattaforma adottare”. Si tratta di ripensare l’intera strategia di sicurezza con una mentalità nuova. E senza l’accompagnamento di esperti, l’ambiente ibrido rischia di diventare un boomerang.

Il falso senso di sicurezza del Cloud

Molte aziende che migrano verso ambienti ibridi, spinte dalla promessa di semplificazione e risparmio, presumono che “il cloud sia sicuro per definizione”. È un errore comune.

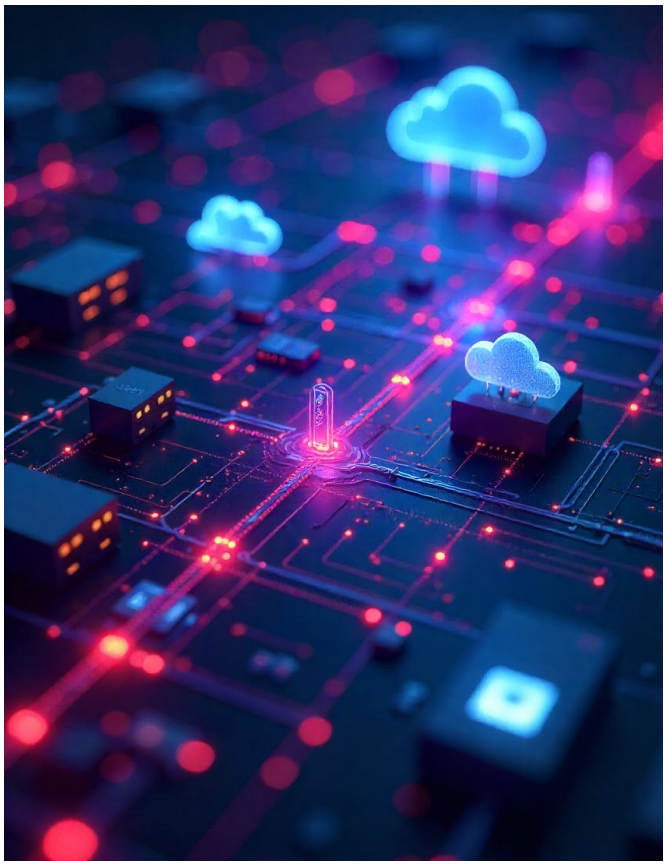
In realtà, i principali provider cloud adottano modelli di responsabilità condivisa: loro garantiscono la sicurezza dell’infrastruttura, ma la configurazione, la gestione degli accessi, la protezione dei dati ricadono quasi interamente sull’organizzazione cliente.

Nessun firewall perimetrale può proteggere un’applicazione SaaS mal configurata o un account amministratore cloud esposto senza MFA.

L’adozione di ambienti ibridi porta con sé vantaggi innegabili: scalabilità dinamica, maggiore continuità operativa, accesso globale alle risorse.

Ma ogni apertura – ogni tunnel VPN, ogni sincronizzazione ibrida tra AD locale e Entra ID (ex Azure AD), ogni workload containerizzato in cloud – rappresenta una nuova potenziale vulnerabilità.

Il manager moderno si trova davanti a una sfida: come governare un’infrastruttura fluida senza sacrificare la sicurezza o rallentare il business?



L’errore più grande: non farsi accompagnare da esperti

Una delle trappole più diffuse è quella della “sufficienza digitale”. Ovvero pensare che l’IT interno possa “capire tutto” o “fare da solo”. Ma la sicurezza ibrida non è una somma di tecnologie: è un equilibrio delicato tra governance, architettura e minacce in continua evoluzione.

Farsi affiancare da professionisti specializzati in cybersecurity ibrida – non solo consulenti, ma architetti con esperienza concreta in ambienti complessi – è un investimento, non un costo.

Un esperto può:

- Validare le scelte architetturali.
- Identificare configurazioni rischiose prima che diventino exploit.

- Formare il personale tecnico su minacce e strumenti avanzati.
- Supportare in incidenti reali, dove il tempo fa la differenza.

Una configurazione cloud errata, un privilegio eccessivo o un tunnel dimenticato possono aprire la porta a un attacco catastrofico. Serve qualcuno che sappia dove guardare.

Ma la sicurezza ibrida non è una somma di tecnologie: è un equilibrio delicato tra governance, architettura e minacce in continua evoluzione.

I 5 pilastri della sicurezza in ambienti ibridi

1. Identità come Nuovo Perimetro

Nel mondo ibrido, il concetto di perimetro fisico è obsoleto. L'identità digitale è oggi il vero gatekeeper. Questo rende cruciale adottare:

- MFA obbligatorio per tutti gli accessi, interni e remoti
- Conditional Access basato su rischio, geolocalizzazione, device posture
- Gestione delle identità privilegiate (PIM) per limitare e tracciare gli accessi elevati
- Audit continuo su gruppi, ruoli e deleghe cloud (IAM drift)

Le identità compromesse sono oggi il vettore d'attacco più frequente nei breach ibridi.

2. Segmentazione e contenimento del rischio

In molte realtà aziendali, la rete rimane "piatta", con ambienti cloud e on-premise interconnessi senza barriere adeguate. Questo facilita il movimento laterale di un attaccante una volta ottenuto l'accesso iniziale.

Per ridurre il rischio, è fondamentale:

- Separare logicamente gli ambienti, come rete utenti, server gestionali e risorse cloud.
- Limitare gli accessi in base ai ruoli, applicando il principio del minimo privilegio.
- Proteggere le connessioni ibride (es. VPN, sincronizzazioni directory) con controlli rigorosi.
- Monitorare i flussi di rete tra ambienti diversi, per rilevare comportamenti anomali.

Ogni connessione tra ambienti deve essere considerata un potenziale vettore di attacco e trattata come tale.

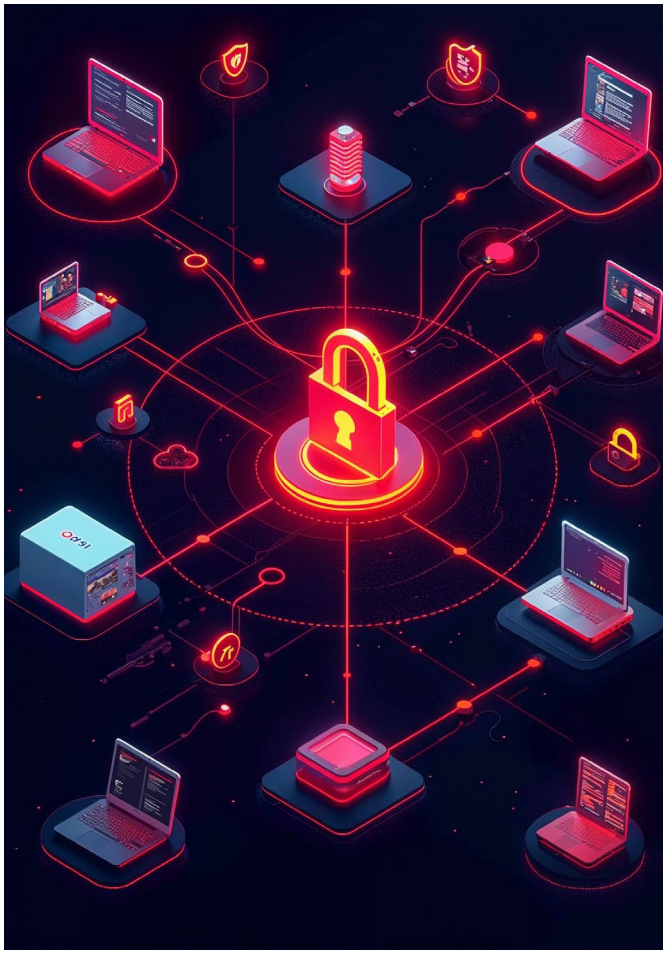
3. Visibilità, telemetria e correlazione tra ambienti

Non si può proteggere ciò che non si vede. In ambienti ibridi, è fondamentale garantire una visione unificata e continua di ciò che accade, sia on-premise che nel cloud.

Ogni organizzazione dovrebbe implementare:

- SIEM centralizzato, con log provenienti da tutti i sistemi e applicazioni.
- Soluzioni di rilevamento e risposta estese (XDR), per endpoint, server e ambienti virtualizzati.
- Monitoraggio continuo di eventi e configurazioni, sia nei sistemi fisici che in quelli cloud.
- Correlazione automatica delle minacce, per evitare che alert isolati passino inosservati.

L'assenza di integrazione tra i vari sistemi di sicurezza spesso porta a una risposta tardiva agli incidenti. Un approccio unificato riduce drasticamente i tempi di rilevamento e contenimento.



4. Rafforzare sistemi, dispositivi e piattaforme

Uno dei punti più trascurati – ma tra i più efficaci – è il rafforzamento (hardening) dell'intera infrastruttura. Non richiede grandi investimenti, ma attenzione e costanza.

Per i dispositivi aziendali:

» Disattivare funzionalità obsolete e non necessarie.

» Limitare i privilegi amministrativi degli utenti.

» Isolare i dispositivi personali in ambienti separati.

» Utilizzare strumenti che impediscano l'uso di software non autorizzato.

Per i sistemi e i servizi aziendali:

» Usare configurazioni sicure già validate per server e applicazioni.

» Rimuovere l'esposizione diretta dei sistemi di gestione su internet.

» Monitorare costantemente lo stato di configurazione dell'infrastruttura cloud.

Per gli account con privilegi elevati:

» Evitare ruoli con accessi troppo ampi, se non strettamente necessari.

» Monitorare costantemente l'uso di chiavi, token e permessi critici.

» Applicare il principio del minimo privilegio e accessi temporanei solo quando servono.

L'hardening riduce la superficie d'attacco e aiuta a prevenire compromissioni. Deve essere visto come un processo continuo, non un'attività isolata.

5. Preparazione, Incident Response e Test periodici

Anche con le migliori difese, gli incidenti accadono. La differenza la fa la reazione.

- Un piano di incident response ibrido deve includere cloud, on-prem e dispositivi remoti.
- I test periodici (pentration test, red team, breach simulation) aiutano a scoprire punti ciechi.
- Devono esserci contatti e procedure già pronti per escalation su fornitori cloud, MSSP, legali e assicurazioni cyber.

Conclusione

Governare l'Ibrido richiede maturità e consapevolezza

Non esiste sicurezza perfetta, ma esiste una sicurezza matura, misurabile, adattiva.

Un ambiente ibrido ben governato è un fattore abilitante, non un rischio. Richiede visione strategica, supporto da esperti, e la consapevolezza che la sicurezza non è mai "finita", ma è parte integrante del ciclo di vita aziendale.

Chi guida oggi la trasformazione digitale – CEO, CIO, CISO, CTO – ha una responsabilità chiave: non solo costruire infrastrutture performanti, ma soprattutto costruirle in modo sicuro, resiliente e sostenibile nel tempo.

"Ibridare" senza proteggere significa solo moltiplicare i punti deboli. Ma farlo con metodo può diventare il punto di forza più potente dell'intera strategia aziendale.

Gemelli digitali e cybersecurity: la protezione degli asset nel mondo fisico-digitale

A cura di Elena Vaciago

Nel contesto della trasformazione digitale, i gemelli digitali (digital twin) si affermano come una delle tecnologie più promettenti per il settore manifatturiero e industriale. Un digital twin è la replica virtuale di un oggetto, sistema o processo fisico, alimentata da dati raccolti in tempo reale tramite sensori, piattaforme IoT e sistemi di controllo. Questo consente non solo il monitoraggio continuo delle prestazioni, ma anche la simulazione, la diagnostica predittiva e l'ottimizzazione dei processi.

Sebbene i gemelli digitali siano nati per finalità industriali – come la previsione dei guasti o la riduzione dei tempi di fermo macchina – oggi il loro impiego si estende a settori sempre più critici: dalla sanità all'energia, dalla logistica alle infrastrutture. Tuttavia, con il crescere della loro complessità e rilevanza, aumentano anche le sfide legate alla loro protezione: i digital twin devono innanzitutto essere sicuri per garantire l'integrità delle informazioni e la continuità operativa, inoltre vanno protetti perchè possono essi stessi diventare bersagli o vettori di attacco.

Casi d'uso dei digital twin in ambito sicurezza

I digital twin possono diventare strumenti di cybersecurity avanzata. Tra i casi d'uso emergenti si segnalano:

- **simulazione di attacchi informatici:** ambienti virtuali che aiutano a testare la resilienza delle infrastrutture digitali, senza mettere a rischio i sistemi reali.
- **threat intelligence and detection:** replicano il comportamento di un impianto o di un'intera rete per analizzare pattern sospetti e identificare anomalie prima che si traducano in incidenti.
- **analisi forense e risposta agli incidenti:** il digital twin aiuta a ricostruire la sequenza degli eventi e a valutare l'impatto di una violazione.

In questo senso, i gemelli digitali rappresentano una nuova frontiera anche per il cyber range e i centri di simulazione destinati alla formazione dei professionisti della sicurezza. I cyber range sono ambienti controllati per la simulazione di attacchi informatici e l'addestramento alla difesa, e i digital twin possono potenziarne radicalmente il realismo e l'efficacia, ad esempio, simulando un attacco informatico che possa portare a conseguenze anche a livello del comportamento fisico (es. un guasto simulato a una turbina o a un impianto di refrigerazione), nella direzione di una sempre maggiore integrazione tra IT e OT; identificando vulnerabilità e dipendenze critiche; addestrando il personale a reagire a minacce zero-day senza rischiare danni reali.

Dopo un attacco reale, un digital twin può anche essere integrato nel cyber range per ricostruire l'accaduto in ambiente controllato; simulare alternative ("cosa sarebbe successo se...") per migliorare la risposta futura; testare nuove contromisure o patch in modo sicuro. Con l'arrivo dell'AI, in cyber range avanzati, i digital twin possono anche essere usati per addestrare algoritmi di machine learning per l' anomaly detection, testare AI difensive in ambienti dinamici e complessi o costruire "digital red team" che simulano attacchi intelligenti su target realistici.

Sfide e considerazioni etiche nell'utilizzo del gemello in cybersecurity

Vanno considerate le sfide implementative di un digital twin, che valgono in generale per qualsiasi utilizzo di questa tecnologia. Al primo posto abbiamo il costo e la difficoltà di realizzazione del gemello virtuale. Sviluppare e mantenere un sistema di questo tipo richiede un notevole impegno, sia finanziario sia di competenze ed effort: sicuramente non si tratta di una soluzione per chiunque.

Importantissimo poi considerare il rischio cyber di un sistema di questo tipo: così come i digital twin aiutano a incrementare la cybersecurity, essi stessi possono introdurre nuove vulnerabilità di sicurezza se non si tengono in conto tutti gli accorgimenti per proteggerli. Un attaccante potrebbe infatti – accedendo al gemello virtuale di un sistema – apprendere moltissimo sul funzionamento reale degli apparati o dei processi virtualizzati. Per prevenire questi rischi è importante che il gemello sia dotato esso stesso di meccanismi di autenticazione, crittografia e monitoraggio continuo.

Abbiamo quindi problematiche di privacy e integrità dei dati: queste tecnologie, duplicando la realtà, raccolgono grandissime quantità di dati, che in caso di compromissione potrebbero finire nelle mani sbagliate. È fondamentale aver predisposto tutte le misure tecniche per una corretta data protection e comunicazioni che rispettino la riservatezza delle informazioni.

Infine, ma non da ultimo, assicurare un utilizzo etico dei dati: il gemello virtuale potrebbe ricevere in tempo reale dati molto sensibili dal mondo reale. Le norme ci dicono che qualsiasi processo di raccolta, elaborazione, condivisione di informazioni deve avvenire rispettando principi etici, come la trasparenza e la responsabilità sugli utilizzi relativi a questi dati, per prevenire qualsiasi attività potenzialmente pericolosa per le persone.

I digital twin non sono solo oggetti da proteggere, ma alleati nella costruzione di sistemi resilienti e sicuri.

Nuove superfici di attacco introdotte dai digital twin

Con riferimento ai rischi legati a questa tecnologia, va considerato che i gemelli digitali, essendo fortemente interconnessi con sistemi fisici e virtuali, ampliano la superficie d'attacco dell'organizzazione. Le vulnerabilità possono emergere a vari livelli:

- sensori e dispositivi IoT, che raccolgono i dati dal mondo fisico, spesso non dispongono di protezioni adeguate.
- reti di comunicazione, attraverso cui i dati transitano in tempo reale, possono essere intercettate o compromesse.
- piattaforme di analisi e modellazione, che elaborano i dati per generare simulazioni, possono essere manipolate per influenzare i risultati o deviare il comportamento dei sistemi fisici.

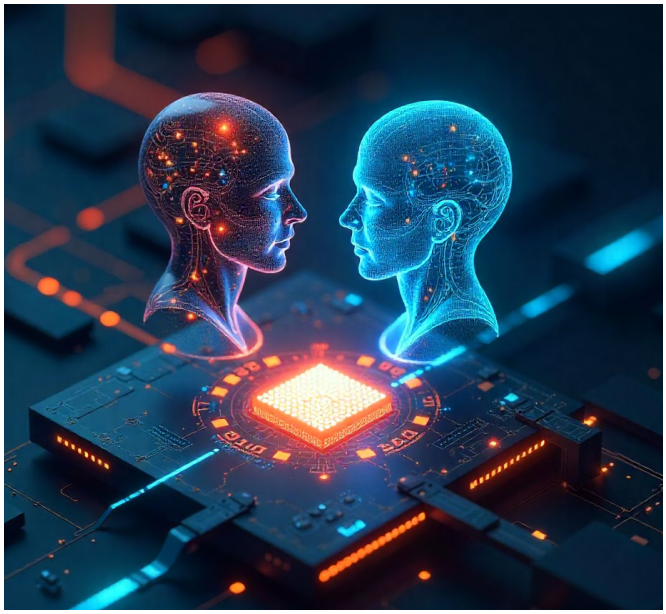
L'esposizione ai rischi non riguarda solo la confidenzialità delle informazioni, ma anche l'integrità e la disponibilità dei dati e delle simulazioni. Un attacco mirato a un digital twin può avere ripercussioni dirette sulla controparte fisica, alterandone il funzionamento o generando decisioni errate da parte degli operatori.

Come proteggere un digital twin

Proteggere un digital twin significa intervenire lungo tutta la sua filiera, adottando – come avviene in ogni ambito della cybersecurity - un approccio olistico e a più livelli che comprenda almeno i seguenti aspetti: sicurezza dei dispositivi edge e IoT (con cifratura dei dati, autenticazione forte, gestione delle vulnerabilità); protezione delle reti di comunicazione (segmentazione, crittografia end-to-end, monitoraggio del traffico); sicurezza delle piattaforme digitali (controllo degli accessi, logging, protezione delle API e delle interfacce uomo-macchina, o HMI); monitoraggio e rilevamento delle minacce.

Con l'espansione dell'Industria 5.0 e la crescente convergenza tra OT, IT e AI, i digital twin diventeranno sempre più pervasivi e critici. La loro protezione non può essere un'aggiunta a posteriori, ma va integrata fin dalla fase progettuale (security by design) con una piena consapevolezza del rischio. Per le organizzazioni, ciò significa dotarsi di competenze multidisciplinari – ingegneristiche, informatiche, cyber – e definire policy chiare su ruoli, responsabilità e flussi di dati. Per i professionisti della sicurezza, significa estendere la propria capacità di analisi e difesa a un perimetro ibrido, in continua evoluzione.

In definitiva, i digital twin non sono solo oggetti da proteggere, ma alleati nella costruzione di sistemi più resilienti, intelligenti e sicuri. Investire nella loro sicurezza oggi significa garantire la fiducia nei sistemi complessi del futuro.



WEBINAR

CYBER Think Tank ASSINTEL

Dalla Cybersecurity alla Privacy:

come affrontare le sfide normative per le PMI

21 Ottobre 2025

12:00 - 13:00

Relatori:

Enzo Veiluva

Fabio Zanoli

Fabio Murri

Cosa potrà mai andare storto?

La Business Continuity nella gestione di un evento elettorale

A cura di Massimo Poletti

Ogni servizio erogato, digitale o meno, prevede modalità operative che generano una ragionevole aspettativa nell'utenza. In gergo tecnico, tali modalità vengono definite SLA (Service Level Agreement). Un esempio basico di SLA è il cartello con gli orari di apertura del fruttivendolo di quartiere: trovare il negozio chiuso quando dovrebbe essere aperto rappresenta un mancato rispetto del livello di servizio atteso. Il ripetersi dell'evento può allontanare il cliente che potrebbe preferire un altro esercizio.

Nel mondo ICT le variabili in gioco sono moltissime e ci sono servizi che, perlomeno in teoria, dovrebbero essere garantiti anche in caso di imprevisti. Negli anni trascorsi gestendo infrastrutture in ambito sanitario ho sempre cercato di adottare tutte le ridondanze ragionevolmente possibili (le risorse non sono infinite) data la criticità dell'ambiente o di sue parti.

Naturalmente le ridondanze per garantire la continuità di un servizio digitale possono essere anche analogiche. Ad esempio, in caso di indisponibilità della procedura informatica per le richieste di prestazioni di laboratorio in Pronto Soccorso veniva allertato un messo incaricato di fare fisicamente la spola con il laboratorio portando le richieste e ritirando le risposte.

L'organizzazione dell'evento elettorale di giugno 2025 comporta, per le Amministrazioni Comunali, un'intensa attività da parte delle OO.PP. (allestimento seggi, cartellonistica, ecc.), della Polizia Locale, dell'Ufficio Elettorale (aggiornamento elenchi, spedizione tessere, rilascio duplicati, ecc.) e, naturalmente, dell'ICT.

I seggi da gestire sono 160, distribuiti in 51 plessi diversi, per un totale di circa 101mila elettori. In ogni plesso c'è un incaricato che raccoglie le informazioni dai presidenti di seggio. Per i plessi principali i dati raccolti vengono inseriti nel programma elettorale direttamente in loco, utilizzando un notebook, mentre per gli altri la trasmissione avviene tramite "fonogramma", termine tecnico che indica una telefonata che segue un preciso protocollo per la dettatura dei dati.

La corretta metodologia prevede un'analisi del rischio. Nel nostro caso come è avvenuta in pratica? Ci siamo riuniti, abbiamo definito lo scenario nella maniera più completa possibile e abbiamo fatto un brainstorming ipotizzando tutti gli imprevisti immaginabili. Lo scopo è garantire che le operazioni di spoglio e l'invio dei dati al Ministero dell'Interno avvengano nei tempi standard previsti.

Scenario operativo (weekend elettorale: sabato-lunedì)

- **L'Ufficio Elettorale** deve poter rilasciare a vista le tessere elettorali (utilizzando la procedura anagrafica) dalla mattina di sabato fino alle 15 del lunedì.
- **La procedura elettorale** deve funzionare da domenica per raccogliere le affluenze e da lunedì ore 15 per l'inserimento dei voti, la generazione in tempo reale delle pagine web relative allo spoglio e l'invio automatico dei dati al Ministero dell'Interno (portale Eligendo).
- **Le postazioni di data entry,** collocate in 10 plessi scolastici (36 seggi, con notebook a noleggio), devono potersi connettere all'applicativo elettorale dalle 15 del lunedì fino al termine dello spoglio.

Sono dotate di “saponette” per la connessione Internet. È la prima volta che viene sperimentata questa modalità. Se l’esito sarà soddisfacente la estenderemo in futuro a tutti i plessi con almeno tre seggi.

- **La sala data entry** presso l’Ufficio Elettorale deve poter ricevere telefonate dai seggi residuali (dotati di cellulare) per inserire manualmente i dati nella procedura.

Continuità operativa da garantire

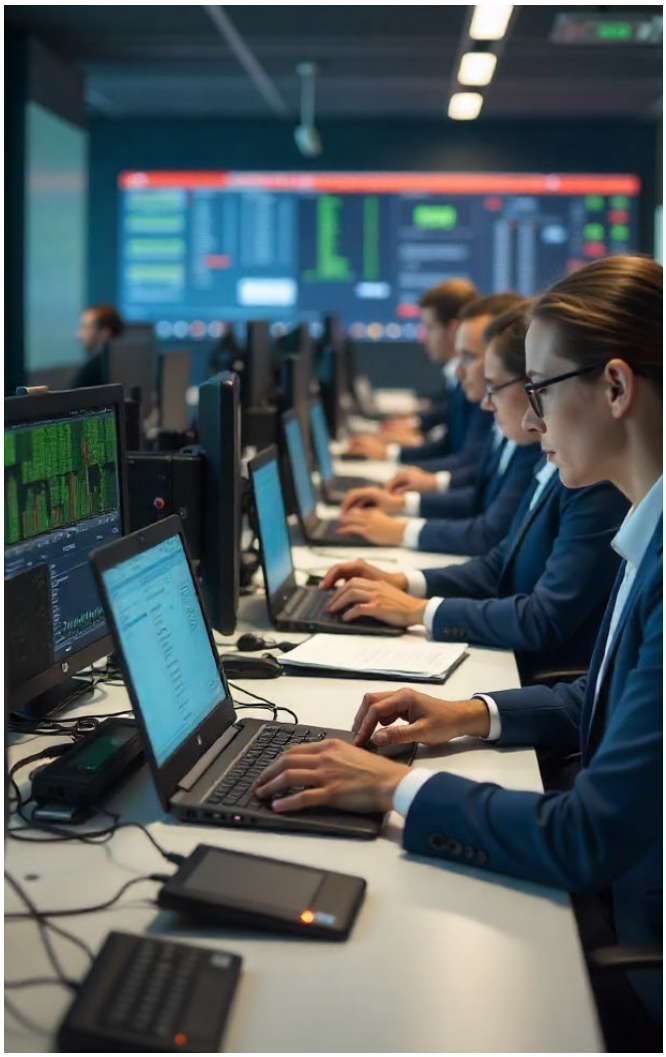
- delle **procedure** (anagrafica e elettorale)
- delle **postazioni tessere**
- della **sala data entry**
- della **comunicazione dai seggi** (via data entry diretto o via telefonica)

Lo scopo è garantire che le operazioni di spoglio e l’invio dei dati al Ministero dell’Interno avvengano nei tempi standard previsti.

Cosa potrebbe andare storto?

Ecco un elenco non esaustivo (non dimentichiamo il chiodo che ha fermato le ferrovie) degli imprevisti considerati, con le relative azioni di mitigazione:

- **Blocco delle procedure anagrafica e/o elettorale:** trattandosi di servizi in cloud SaaS certificati ACN, la continuità nel funzionamento delle procedure è considerata garantita. Tuttavia, è stato attivato un servizio di assistenza telefonica per supportare eventuali difficoltà operative tenendo conto che si tratta di ambienti attivati solo saltuariamente e che molti operatori sono alla prima esperienza. Con il medesimo canale si possono ovviamente segnalare eventuali problemi di procedura.
- **Malfunzionamenti nelle postazioni tessere o data entry:** presenza fissa di un tecnico per l’assistenza postazioni e disponibilità di PC “muletto” in loco.
- **Guasti nelle infrastrutture aziendali:** reperibilità dell’assistenza sistemistica e presenza di tecnici interni per interventi negli armadi di rete, con switch di riserva pronti all’uso. In caso di problemi elettrici, è attiva la reperibilità della manutenzione OO.PP.
- **Indisponibilità della connettività:** in caso di problemi del provider (Lepida Scpa), sono disponibili saponette da utilizzare come hotspot per le postazioni. Per i PC fissi sono previste chiavette USB per il collegamento WiFi.
- **Malfunzionamento del sistema telefonico comunale:** assistenza telefonica in reperibilità e disponibilità di cellulari di riserva per gli operatori del data entry. Abbiamo un “arsenale” di cellulari base, destinati esclusivamente alle elezioni o ad altre emergenze.
- **Problemi nei PC dei plessi scolastici:** abbiamo inserito nelle borse cavi di alimentazione sia Schuko che a pettine. In caso di guasti agli apparati, gli operatori procederanno con l’inserimento manuale, comunicando via telefono con la sala data entry.
- **E se ci fossimo dimenticati qualcosa?** Si mitiga con il buon senso, risorsa fondamentale in ogni reparto ICT.



Considerazioni finali

È stato necessario attivare varie reperibilità straordinarie e noleggiare notebook, con la conseguente gestione degli atti amministrativi, del ciclo degli acquisti, della logistica e del presidio tecnico.

Pur trattandosi di attività ormai consolidate (ci sono elezioni quasi ogni anno), è comunque necessario riconsiderare ogni volta il contesto: può essere cambiato qualcosa (infatti questa volta abbiamo il data entry dai seggi) e potrebbero emergere nuovi rischi.

Questo è un caso emblematico di gestione del rischio e della continuità operativa ICT in un Comune. Vorrei concludere con una riflessione più ampia sugli enti pubblici e la loro capacità di erogare servizi.

Le normative – in primis il **GDPR e la NIS2** – impongono analisi del rischio per valutare minacce ai dati e alla continuità operativa. Ma le variabili sono tante, e cambiano rapidamente.

Esistono contesti sicuramente molto controllati: ad esempio, nel Comando della Polizia Locale gli ingressi sono presidiati e i locali tecnici chiusi a chiave. Ma in enti con decine di sedi, grandi e piccole, non sempre è così semplice: può capitare che in una piccola delegazione l'accesso al locale tecnico non sia vigilato, o che in certi giorni la sede sia chiusa ma vulnerabile alle intrusioni, esponendo a rischio di accesso non autorizzato gli switch di rete. Anche in sedi principali ci sono armadi periferici accessibili.

In questi casi servirebbe un sistema di **Network Access Control (NAC)**, tecnologia complessa e dai costi non trascurabili.

Serve quindi, a mio avviso, una logica di miglioramento continuo. Piccoli passi, ma costanti. Questo però richiede un impegno che non può ricadere solo sull'ICT: deve essere l'intera organizzazione a integrare nel proprio processo "sicurezza e continuità operativa" la volontà di investire risorse per costruire progressivamente una postura ottimale.

Che ci sia o meno una norma come la NIS2 a responsabilizzare i vertici.

Le backdoor di stato stanno arrivando. Ma questa volta, con il timbro UE!

A cura di Massimiliano Brolli

Un tempo la sorveglianza era silenziosa, nascosta tra le pieghe del codice e delle reti. Oggi, invece, si presenta a volto scoperto, con l'appoggio della politica e la benedizione di normative che la vogliono rendere legale, strutturata, persino necessaria. Dopo Echelon, il Datagate con Edward Snowden nel 2013 accese i riflettori sulle pratiche di sorveglianza di massa svolta dalla NSA e dell'FBI. Tale scandalo ha mostrato come le democrazie più avanzate non siano immuni dal desiderio di ascoltare tutto, sempre.

Poi è arrivato Vault 7, la più grande fuga di documenti della CIA mai registrata. In questa fuga di dati veniva mostrato come gli Stati Uniti riuscissero ad infiltrarsi in smartphone, smart TV e computer di mezzo mondo. Fino ad allora, le backdoor erano qualcosa di sussurrato nei corridoi dell'intelligence, strumenti d'uso esclusivo delle agenzie, senza discussione pubblica.

Ma oggi il dibattito si è fatto politico, pubblico, globale.

La dichiarazione di Trump di Novembre

A novembre 2024, Donald Trump ha dichiarato che servono "normative flessibili in termini di intelligence". Sostenne apertamente l'utilizzo di tecnologie di tipo spyware per proteggere la sicurezza nazionale. Un'affermazione forte, che ha avuto conseguenze quasi immediate. Nel giro di qualche mese, diversi vertici dell'NSA sono stati rimossi dopo incontri a porte chiuse con Elon Musk. L'impressione è che stia prendendo forma una nuova dottrina americana: la sorveglianza legalizzata, esplicita, che non ha più bisogno di nascondersi.

Pertanto la tecnologia spyware riceverà un "secondo vento". È probabile che le aziende che producono programmi come NSO Group e Paragon trovino sostegno nella nuova mministrazione. Questo nonostante le critiche ai loro strumenti per violare i diritti umani.

Nel frattempo, Cina e Russia osservano. Loro il modello lo hanno già consolidato da tempo: sorveglianza pervasiva, controllo dei dati, nessuna illusione sulla privacy. Ma la differenza – sottolineano spesso i governi occidentali – è che quei due paesi sono sotto regime.

L'Occidente, invece, è un mondo di diritti e trasparenza. Almeno, lo era.

La discussione sulle Backdoor in Europa e nel Regno Unito

Anche l'Europa, infatti, si muove. Recentemente è stato presentato il piano ProtectEU – un documento che, tra le righe – scritte in burocratese – segna un altro punto di svolta. Sebbene l'UE abbia sempre espresso riserve sull'uso di backdoor nella crittografia, il piano parla chiaro: entro il 2025 verrà sviluppata una tabella di marcia per consentire un accesso legale ed efficace ai dati da parte delle forze dell'ordine, con una roadmap tecnologica prevista per l'anno successivo.

"Stiamo lavorando a una tabella di marcia ora e vedremo cosa è tecnicamente possibile", ha affermato Henna Virkkunen, vicepresidente esecutivo della CE per la sovranità tecnologica, la sicurezza e la democrazia. "Il problema è che ora le nostre forze dell'ordine stanno perdendo terreno sui criminali perché i nostri investigatori di polizia non hanno accesso ai dati", ha aggiunto e ha detto che "nell'85 percento" le forze dell'ordine non riescono ad accedere ai dati di cui avrebbero bisogno. La proposta è di modificare l'attuale Cybersecurity Act per consentire queste modifiche.

Stesso tema si sta dibattendo nel Regno Unito, dopo che le autorità hanno chiesto ad Apple di creare una

backdoor che consentisse l'accesso ai dati cloud crittografati degli utenti. Apple ha deciso di disattivare del tutto la funzionalità Advanced Data Protection (ADP) nel Regno Unito.

Le autorità britanniche avrebbero emesso un ordine chiedendo ad Apple di fornire l'accesso ai dati criptati degli utenti in tutto il mondo. Secondo la pubblicazione, l'ordine imponeva ad Apple di creare una backdoor che avrebbe consentito l'accesso a qualsiasi contenuto caricato sul cloud da qualsiasi utente.

In altre parole: si comincia a costruire l'infrastruttura legale e tecnica per aprire varchi nei sistemi di protezione dati. Varchi "legalizzati", ma sempre varchi.

Tutto questo solleva una domanda scomoda: dove finisce la sicurezza e dove comincia il controllo?

Il rischio della backdoor e le sue derive

Nel tempo, la guerra informatica ha subito una profonda evoluzione, trasformandosi da strumento sperimentale a vero e proprio teatro operativo. Inizialmente, fu la NSA (National Security Agency) a detenere la leadership mondiale nelle capacità offensive cibernetiche, sviluppando strumenti avanzatissimi per penetrare e manipolare sistemi informatici ostili. Una delle conferme più clamorose di questa superiorità tecnica emerse nel 2017, con la pubblicazione di Vault-7 da parte di WikiLeaks: una serie di documenti top secret della CIA che rivelarono l'esistenza di un vasto arsenale di malware, exploit zero-day e tecniche di hacking sviluppate internamente dagli Stati Uniti per operazioni clandestine in tutto il mondo.

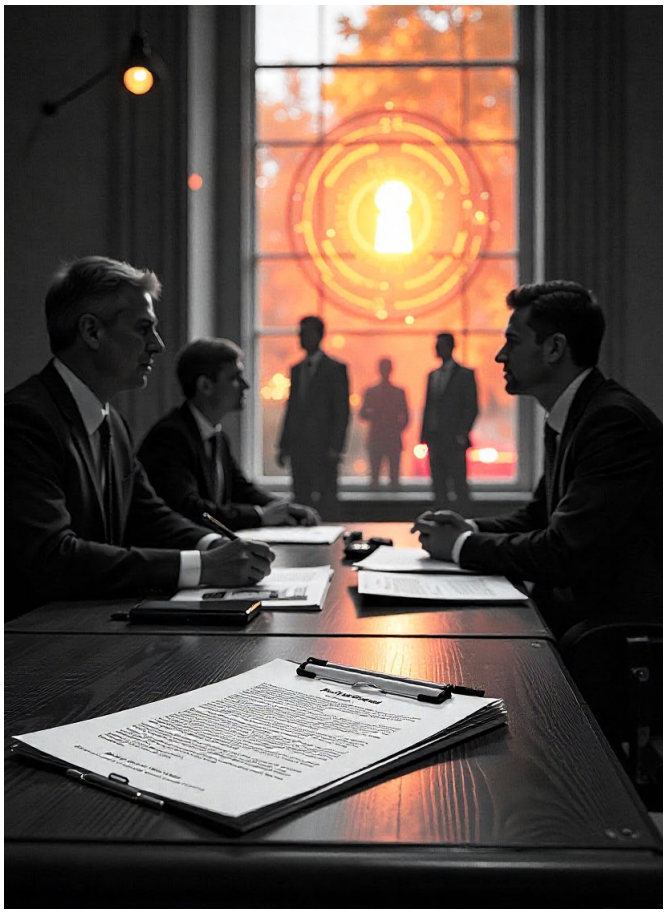
Non esiste una backdoor 'solo per i buoni': una volta creata, può essere sfruttata da chiunque riesca a trovarla.

Ma anche prima di Vault-7, la potenza di fuoco della cyber intelligence americana era emersa in modo devastante. Il primo ransomware della storia a diffusione globale, WannaCry, si basava su un exploit chiamato EternalBlue, sottratto dai server della National Security Agency (NSA) degli Stati Uniti D'America dal gruppo hacker Shadow Brokers. EternalBlue sfruttava una vulnerabilità di Windows che l'NSA aveva individuato anni prima e mantenuta segreta, utilizzandola per accedere silenziosamente a qualsiasi sistema operativo Windows connesso in rete. Questo exploit rappresentava una vera e propria backdoor universale, e il fatto che sia stato rubato e poi usato (dagli hacker del gruppo Lazarus associati alla Corea Del Nord) contro il mondo intero ha dimostrato quanto sia sottile il confine tra arma strategica e boomerang incontrollabile.

Tra le più note operazioni militari cibernetiche nella storia, spicca Operation Olympic Games, una missione congiunta tra Stati Uniti e Israele. Il malware protagonista fu Stuxnet, uno strumento di guerra informatica mai visto prima, capace di sabotare fisicamente l'infrastruttura industriale della centrale nucleare iraniana di Natanz. Armato con quattro vulnerabilità zero-day (due su Microsoft Windows e due sui PLC Siemens), Stuxnet rappresentò l'alba di una nuova era: quella in cui un malware può danneggiare impianti reali, senza sparare un colpo, ma alterando algoritmicamente la realtà.

Oggi, però, il dominio statunitense è stato ridimensionato

La Cina, in particolare, ha dimostrato negli ultimi sei mesi di aver superato il livello tecnologico statunitense, con operazioni come Volt Typhoon, Salt Typhoon e Liminal Panda, condotte con precisione chirurgica e capacità stealth avanzate. In questo scenario di "guerra grigia", dove le regole sono fluide e le frontiere invisibili, sfruttare un accesso backdoor può offrire un vantaggio significativo nella raccolta di intelligence.



Pertanto dobbiamo ricordare che una backdoor, una volta scoperta, può essere usata anche dal nemico.

La realtà del cyberspazio è fluida e imprevedibile: uno zero-day, in media, viene scoperto da altri ricercatori circa un anno dopo la sua prima individuazione. Questo significa che un exploit può essere utilizzato simultaneamente da più agenzie di intelligence, senza che l'una sappia nulla dell'altra. In tale contesto, la backdoor non è sempre un vantaggio: può trasformarsi rapidamente da un vantaggio in un'arma rivoltata contro chi l'ha forgiata.

Conclusioni

Come abbiamo visto, le backdoor, per loro natura, sono strumenti a doppio taglio. Non esiste una backdoor "solo per i buoni": una volta creata, può essere sfruttata da chiunque riesca a trovarla. E soprattutto, apre un varco non solo nei dispositivi, ma in uno dei principi fondamentali degli esseri umani: il diritto alla riservatezza.

La verità è che ci stiamo pericolosamente avvicinando a quei modelli autoritari che per anni abbiamo criticato. Il confine tra sicurezza nazionale e sorveglianza di massa si fa sempre più sottile. E, paradossalmente, la difesa della libertà rischia di passare proprio per la sua negazione.

La politica vuole la backdoor. Ma il mondo – quello fatto di cittadini, esperti di sicurezza, attivisti per i diritti digitali e banalmente a persone estranee all'argomento – non la vuole. Perché una volta che apri una porta sul tuo mondo privato e sulla tua sicurezza nazionale, è difficile dopo richiuderla, pertanto occorre rifletterci molto bene.

Sicurezza concreta, oltre lo storytelling

A cura di Rita Takacs

Sì, il tema della sicurezza mi appassiona – e non ne ho mai fatto mistero. Ne parlavo con entusiasmo, in monologhi (letterari) passati, quando il focus era più sul valore culturale del concetto. Oggi, invece, sento l'urgenza di tornare a parlarne, ma con uno sguardo diverso: più operativo, più lucido. E, forse, più necessario.

Una riflessione che nasce da osservazioni raccolte online – tra forum tematici OSINT e CLOSINT – e da conversazioni con amici e peer, dalle quali si profila con chiarezza un trend. Viviamo in un'epoca in cui, di sovente, il racconto prende il posto della realtà, anche (e soprattutto) laddove servirebbe concretezza: nella sicurezza informatica. A vincere non è chi protegge, ma chi sa presentare bene ciò che "sembra" protezione.

Nei canali di comunicazione prossimi ai centri decisionali si moltiplicano ruoli assegnati più per affinità percepite che per reale competenza, incaricati di "tradurre" – semplificando fino alla banalizzazione – una lingua tribale che non comprendono. Come insegna la psicologia cognitiva, ogni trasmissione orale deforma il contenuto originario, la memoria seleziona (malauguratamente dalla RAM, se non presente una sedimentata knowledge base), l'intenzione modella, il tempo smussa, la narrazione si adatta a chi la ascolta. E così, da verità tecnica si scivola facilmente in mito condiviso.

E allora, via libera a policy di alto livello, a gusci vuoti (di quelli che ne scarichi cento per trecento euro) da riempire con informazioni di massima, in… zero day – giusto per restare in tema. Tanto poi, momentum sine fine, si potrà sempre aggiornare. (Certo, con l'entusiasmo selvaggio di chi lavora a riflettori ormai spenti, su un tema di proporzioni gigantesche che si dà per risolto da tempo. Eureka!)

File dopo file, tab dopo tab, si costruisce un castello di carta che nessuno leggerà davvero, e che non verrà mai aggiornato. Una produzione seriale, automatizzata, che trasforma un tema vivo e tecnico in una pratica notarile.

Non che la carta non serva – intendiamoci – ma la carta senza censimento realistico, senza manutenzione, senza un'architettura viva, diventa solo zavorra.

Lo scopo diventa dimostrare di aver fatto, non fare veramente. Eppure la differenza è abissale. **Nessun attaccante è mai stato fermato da un template.**

La sicurezza non è compliance (e viceversa)

La sicurezza vera è fatta di sistemi che si parlano, di aggiornamenti continui, di log che vengono letti, di vulnerabilità che vengono cercate attivamente. È fatta di persone che comprendono la tecnologia, non solo il diritto. La compliance è importante, certo, ma non è sempre il punto di partenza. Se ben gestita, è il naturale punto di arrivo della buona sicurezza.

La sicurezza vera ha mille sfaccettature, sa essere **preventiva**, come anche **predittiva (o proattiva)**, avvalendosi di tool avanzati di threat intelligence e collaborando con l'AI-buono che sulla scena odierna combatte una battaglia serrata e senza tregua con l'AI-cattivo, sempre più onnipresente e "istruito" e "social engineerizzato", grazie al nostro crescente bisogno di sentirci un po' influencer, pubblicando i fatti nostri online.

E la sicurezza vera sa essere **rilevativa (o detective)**, intercettando IOC (Indicators of Compromise) tramite sistemi di rilevamento intrusioni (IDS) e sistemi di monitoraggio dei log, SIEM (Security Information and Event Management). E sa essere **reattiva**, rispondendo prontamente agli attacchi o incidenti con azioni concrete di contenimento o mitigazione del rischio. Conscia che la reattività implica saper essere **correttiva,** correggendo (appunto!) le vulnerabilità o i danni dopo un attacco, ripristinando i sistemi e i dati. Migliorando costantemente le difese e le policy di sicurezza in base alle nuove minacce e contesti, perché sa che oggi dev'essere soprattutto **adattiva (o dinamica)** per mantenere il passo con la frenesia del zeitgeist (sintetizzato splendidamente da una persona che stimo, e che molti conoscete, in un noto articolo: "siamo passati […] dalla deterrenza atomica all'incertezza digitale").

E la sicurezza **operativa?** Ah, che noia! Sono le pratiche di ogni giorno, la gestione degli account, la lettura degli avvisi dell'early warning giornaliero, il patching dei sistemi, la formazione degli utenti…

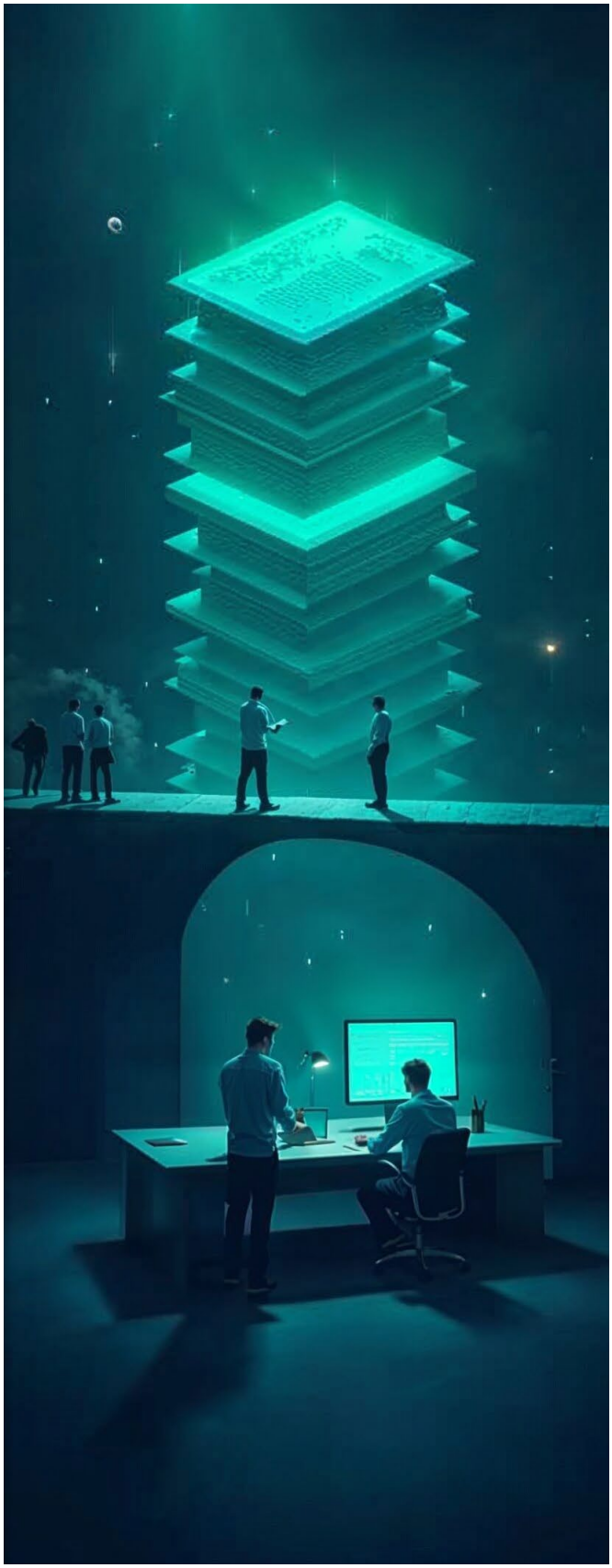
La sicurezza vera è fatta di sistemi che si parlano, di aggiornamenti continui, di log che vengono letti, di vulnerabilità che vengono cercate attivamente.

Il ruolo che manca

Serve un ponte. O meglio: servono figure in grado di abitare entrambi i lati del ponte...

Servono competenze certificate. E norme che impongano la scelta di competenze certificate, sopratutto con riferimento a ruoli che rappresentano i delicati anelli di congiunzione – verticali, interni, ma anche orizzontali, fino a oltre il perimetro aziendale, verso un ecosistema più ampio (Responsabile IT, Responsabile sicurezza informatica, Punto di contatto NIS2, DPO). Non è forse vero che "una catena è forte soltanto quanto il suo anello più debole"?

Il rischio – altrimenti – è di rimanere intrappolati in una fiction di sicurezza. Una narrazione rassicurante, ma fragile. E ogni giorno, un dado viene lanciato...



La Formazione sulla Cybersicurezza per gli Organi Direttivi e Amministrativi

A cura di Enzo Veiluva

La Direttiva NIS2 (Network and Information Security), adottata dall'Unione Europea, e recepita dall'Italia a partire 16 ottobre 2024 con decreto legislativo del 4 settembre 2024, n. 138 sta creando molto fermento all'interno dei consigli di amministrazione degli oltre 25.000 soggetti essenziali ed importanti che sono stati identificati in base ai requisiti di dimensioni, fatturato ed attività in perimetro.

Tra le novità più importanti introdotte dalla direttiva vi è difatti una serie di responsabilità , sancite dall'Articolo 23, ove viene ribadito che gli organi direttivi e amministrativi possono essere ritenuti legalmente responsabili per la mancata conformità alle disposizioni della direttiva NIS2.

In particolare ai vertici sono assegnate le responsabilità di supervisione e monitoraggio dell'applicazione della normativa al proprio interno, di valutazione e comprensione dei rischi, di garanzia di un flusso efficace di informazioni riguardanti la sicurezza verso le autorità competenti e di promuovere una cultura della sicurezza adeguata all'interno della propria organizzazione.

Per svolgere questi compiti gli stessi membri dei consigli di amministrazione e organi direttivi devono in primis formarsi ed acquisire le competenze necessarie . Sorge quindi immediatamente la domanda: come organizzare un programma di formazione efficace ed efficiente per i vertici amministrativi? I temi da trattare non sono banali , specialmente quando i "discenti" non sempre posseggono un backgroud di competenze tecniche o normative.

A mio parere personale è fondamentale impostare il giusto mix di competenze cibernetiche, di gestione del rischio e di conoscenza della normativa puntando a far comprendere in modo chiaro e semplice come questi elementi possono influire in modo significativo, tramite le decisioni strategiche prese dai vertici, sulla resilienza complessiva dell'organizzazione.

Gli organi direttivi devono apprendere e comprendere in primis gli asset critici e le vulnerabilità della propria organizzazione, devono garantire che le risorse necessarie per la protezione delle infrastrutture siano adeguatamente allocate, devono adottare strategie che bilancino la sicurezza con le esigenze operative e di business.

Comprendere questi aspetti significa comprendere cosa significa "fare cybersicurezza" all'interno del proprio Ente / Azienda, come costituire un Modello Organizzativo di gestione della Sicurezza ICT, come deve essere organizzato (dai propri collaboratori tecnici) un piano di gestione dei rischi.

Comprendere come monitorare le attività attraverso azioni e richieste di informazioni che il CISO, il DPO, il responsabile Formazione, Ufficio Legale/contratti, il fornitore IT devono mettere a disposizione dei Vertici.

Quanti sono i consigli di amministrazione che richiedono evidenza degli esiti di applicazione di simulazioni di incidenti o esiti dei risultati di campagne di phishing pilotate per valutare, anche a seguito della formazione effetuata, quanto il personale dell'azienda è pronto a gestire un evento di incidente reale? Quanta evidenza hanno che l'azienda si è dotata (o si sta dotando) di un insieme di processi, di regole, di un impianto documentale che costituisce la base per attuare e rendere evidente il raggiungimento di una "compliance" alla normativa?

E' fondamentale che la formazione effettuata spinga gli

organi direttivi e amministrativi ad assumere un ruolo attivo e proattivo nella gestione della sicurezza delle reti e dei sistemi informativi. La responsabilità non si limita alla supervisione, ma include anche la garanzia di conformità, la gestione dei rischi e la promozione di una cultura della sicurezza.

Le misure di sicurezza di base (i 116 controlli per i soggetti essenziali e 84 per i soggetti importanti) chiedono che gli Organi direttivi e amministrativi sottoscrivano direttamente una serie di piani che vanno dal piano di adeguamento, al piano dei rischi, al piano di gestione degli incidenti al piano di formazione dei dipendenti, etc e sono questi elementi che devono guidare gli aspetti formativi dei vertici, altrimenti se la sottoscrizione costituirà solo la risoluzione di un dì mero adempimento burocratico sarà stato tutto inutile. La conformità a queste disposizioni non solo proteggerà l'Azienda da potenziali incidenti, ma rafforzerà anche la fiducia dei clienti e delle autorità verso l'organizzazione.

"Gli organi direttivi devono apprendere e comprendere in primis gli asset critici e le vulnerabilità della propria organizzazione, devono garantire che le risorse necessarie per la protezione delle infrastrutture siano adeguatamente allocate , devono adottare strategie che bilancino la sicurezza con le esigenze operative e di business."

Gang sotto Assedio: siamo di fronte al Tramonto del Ransomware?

A cura di Luca Mella

Introduzione

Negli ultimi tempi, le forze dell'ordine stanno colpendo i principali ecosistemi ransomware con operazioni congiunte senza precedenti: dalle prime collaborazioni internazionali, fino alla recentissima operazione "Endgame", questi successi hanno giovato alla sicurezza delle imprese del territorio. Tuttavia, queste importanti iniziative di contrasto sono purtroppo soggette a dei limiti incomprimibili. In questo articolo, analizzeremo come la cooperazione internazionale stia colpendo il crimine informatico organizzato, e cercheremo di orientarci nel comprendere come l'underground criminale informatico ne sia effettivamente impattato.

Le Operazioni contro il Ransomware

Negli ultimi anni, le autorità di diversi paesi occidentali hanno unito le forze per smantellare le infrastrutture e arrestare membri di alcune tra le più pericolose gang di ransomware. Ma quello che oggi vediamo - in termini di successi contro il crimine - fonda le sua radici in tempi informaticamente remoti. Già nel 2016 l'operazione "Avalanche", azione congiunta in 30 paesi, portò all'arresto di 5 criminali e alla rimozione di oltre 200 server usati per diffondere malware (inclusi alcuni ransomware). Questo fu solo l'inizio. Nello stesso anno nasceva anche "No More Ransom", iniziativa pubblico-privata che da allora ha aiutato oltre 1,5 milioni di vittime a decriptare i propri file senza pagare riscatti, sottraendo circa un miliardo e mezzo di dollari ai cybercriminali.

Questo primo approccio cooperativo si è piano piano espanso nelle agenzie di Polizia di un maggior numero di Paesi, intensificandosi negli anni recenti tanto che ad oggi possiamo contare successi contro molte delle gang criminale che, in passato, hanno fatto tremare le nostre Aziende.

REvil: gang operante tra il 2018 e il 2021, prima sotto l'egida di GandCrab e poi REvil (Sodinokibi) che ha colpito migliaia di vittime nel mondo. In un'operazione globale denominata GoldDust (fine 2021), Europol e FBI hanno coordinato 17 paesi riuscendo ad arrestare 7 affiliati di REvil/GandCrab in Europa, Asia e Nordamerica. In seguito, a sorpresa, anche l'FSB russo annunciò nel gennaio 2022 di aver smantellato REvil su richiesta degli USA, con perquisizioni in 25 località e 14 arresti. Fu un raro caso di collaborazione USA-Russia in piena tensione geopolitica, che portò al sequestro di contanti, crypto e auto di lusso del gruppo. Tuttavia, dopo l'invasione russa dell'Ucraina, questo tipo di cooperazione si è interrotto, lasciando molti leader di ransomware impuniti.

Conti: attiva tra il 2020 e il 2022, la famigerata gang ha estorto decine di milioni di dollari colpendo, tra gli altri, la sanità irlandese e il governo del Costa Rica. Nel febbraio 2022 il gruppo dichiarò pubblicamente il suo supporto alla Russia per l'attacco all'Ucraina, minacciando ritorsioni contro gli Stati Uniti. Questa mossa si ritorse invece contro Conti stessa: una gola profonda pubblicò infatti oltre 60.000 chat interne, il famoso ContiLeaks, rivelando dettagli sull'organizzazione interna e gli illeciti della gang. Contestualmente, gli Stati Uniti misero una taglia da 15 milioni di dollari sui leader di Conti. Sotto questa pressione – e probabilmente per dissidi interni – Conti annunciò lo scioglimento nel maggio 2022. Tuttavia, in realtà i membri non scomparvero: molti confluirono in altri gruppi RaaS o ne fondarono di nuovi, come BlackCat, BlackBasta, Karakurt e Royal. Proprio Royal (apparsa nel 2022) sarebbe capeggiata da un veterano di Conti: il ricercato Vitaly Kovalev, alias "Stern", identificato da un recente leak di ulteriore informatore: "GangExposed". Questo misterioso whistleblower ha infatti pubblicato a giugno 2025 foto, alias, dati personali e chat che smascherano Kovalev come mente di Conti, Trickbot e Royal. La polizia tedesca (BKA) ha confermato queste informazioni, indicando Kovalev come fondatore del gruppo Trickbot/Conti. Nonostante l'enorme mole di prove (si parla di oltre 500 milioni di dollari in crypto accumulati da Kovalev), il fatto che egli e altri leader risiedano in certi paesi rende la loro cattura impraticabile.

Hive: una delle operazioni di maggior impatto è stata condotta contro la gang Hive all'inizio del 2023. Hive era un servizio RaaS (Ransomware as a Service) che in meno di due anni aveva colpito oltre 1300 vittime in tutto il mondo, tra cui molte strutture sanitarie. In un'azione sotto copertura, gli agenti FBI sono riusciti a infiltrarsi nei sistemi di Hive per circa sette mesi, da luglio 2022 a gennaio 2023. In questo periodo hanno sottratto alla gang le chiavi di decrittazione dei ransomware, distri-

buendo di nascosto oltre 300 decryptor gratuiti alle vittime colpite attivamente e altre 1000 chiavi a vittime passate. Questa mossa ha impedito che circa 130 milioni di dollari in riscatti finissero nelle casse dei criminali. A fine operazione, il 26 gennaio 2023, il Dipartimento di Giustizia USA ha annunciato il takedown di Hive: i server e il sito di leak del gruppo sono stati sequestrati, sferrando un colpo decisivo alla gang. L'importanza di questo caso risiede anche nel cambio di strategia: invece di limitarsi ad arrestare alcuni membri, le forze dell'ordine hanno colpito al cuore l'infrastruttura e, soprattutto, aiutato le vittime a mitigare i danni. Questa operazione congiunta (FBI, Europol, Germania e altri) ha segnato un precedente importante mettendo "le vittime" al centro della strategia, accendendo luce sulle potenzialità del supporto che le operazioni di polizia possono dare alle vittime del ransomware, oltre che all'efficacia nel contrasto e nella deterrenza.

LockBit: attiva dal 2019, LockBit è diventata nel 2022 la più prolifica organizzazione ransomware a livello globale, responsabile di oltre il 40% degli attacchi noti. A differenza di Conti e REvil, il gruppo LockBit è rimasto operativo nonostante alcuni arresti di affiliati. Nel 2022 un suo membro fu arrestato in Canada ed estradato negli USA, e altri due sospetti furono fermati in Ucraina e a Singapore. La vera offensiva contro LockBit però è arrivata nel tra il 2023 e il 2024 con l'operazione Cronos, coordinata da Europol, FBI e le polizie di 10 paesi. In una prima fase, febbraio 2024, i portavoce di Cronos hanno annunciato di aver compromesso i server chiave di LockBit, arrestato 2 membri chiave del gruppo e congelato oltre 200 wallet di criptovalute legati ai profitti illeciti. Clamorosamente, gli investigatori sono persino riusciti a prendere temporaneo controllo del sito di pubblicazione dei dati rubati di LockBit: sul dark web campeggiava un messaggio delle forze di polizia a mo' di sfida, prova tangibile dell'accesso ottenuto (la NCA britannica ha pubblicato screenshot denominati ironicamente "oh_no.png"). In una seconda fase, settembre 2024, l'operazione Cronos ha portato ad altri quattro arresti: un sospetto sviluppatore di LockBit catturato in Francia, due affiliati arrestati nel Regno Unito e un amministratore dei servizi di hosting arrestato in Spagna (con contestuale sequestro di 9 server). Contestualmente, sono state emanate sanzioni finanziarie contro diversi individui collegati a LockBit ed EvilCorp (noto gruppo cybercriminale russo), suggerendo legami tra le due organizzazioni. Durante le operazioni di polizia, le autorità inoltre hanno recuperato oltre 1000 chiavi di decrittazione di vittime di LockBit, distribuite poi tramite il progetto "No More Ransom". Secondo Europol, questa serie di azioni coordinate ha "colpito l'operatività di LockBit a tutti i livelli, danneggiando gravemente le sue capacità e la credibilità". In altre parole, la gang si è trovata con infrastruttura e fondi in parte bloccati, costretta a ripiegare temporaneamente su sistemi di riserva.

BlackCat: emersa a fine 2021, la gang ALPHV (nota anche come BlackCat) è stata considerata una sorta di erede di DarkSide/BlackMatter (il gruppo dietro l'attacco al Colonial Pipeline nel 2021). Nel 2023 BlackCat è diventata il secondo RaaS più attivo dopo LockBit, con oltre 300 milioni di dollari estorti in un migliaio di attacchi riusciti. Come per LockBit, i suoi leader operano in libertà presumibilmente in Russia, ma le forze di polizia sono riuscite comunque a infliggere dei duri colpi all'organizzazione. Nel dicembre 2023 il Dipartimento di Giustizia USA ha rivelato un'operazione sotto copertura contro ALPHV simile a quella condotta su Hive: l'FBI aveva ottenuto accesso alle chiavi di decrittazione di BlackCat, sviluppando un tool gratuito fornito a 500 vittime in tutto il mondo, prevenendo pagamenti per 68 milioni di dollari. Inoltre, sono stati sequestrati diversi siti web usati dalla gang per le comunicazioni e la pubblicazione dei dati rubati. Anche in questo caso, "gli hacker sono stati hackerati": ancora una volta le autorità hanno penetrato le difese di un gruppo ransomware e lo hanno colpito dall'interno. Questo ha causato forte diffidenza all'interno della community cybercriminale: dopo il breach, alcuni affiliati BlackCat hanno abbandonato la gang migrando verso LockBit, mentre altri hanno iniziato a trattare direttamente con le vittime temendo che l'infrastruttura non fosse più sicura. Addirittura, i boss di LockBit e BlackCat hanno discusso online l'idea di formare un "cartello" del ransomware per unire le forze contro la pressione delle forze dell'ordine. Esperimenti simili in passato (e.g. l'alleanza Maze-Egregor nel 2020) non hanno impedito arresti e scioglimenti, anzi Egregor stesso fu smantellato dalla polizia ucraina meno di un anno dalla sua creazione.

Operation Endgame: oltre alle azioni mirate alle singole gang, va evidenziata negli ultimi periodi l'adozione di una strategia più ampia volta a colpire l'ecosistema del ransomware. Nell'ultimo anno le forze di polizia hanno infatti concentrato gli sforzi sui "broker di accesso iniziale": gruppi e malware che forniscono ai ransomware un punto d'ingresso nei sistemi delle vittime. Nel maggio 2024 un'azione internazionale coordinata dall'FBI con Europol e ben 11 paesi (USA, Regno Unito, EU e altri) ha smantellato le infrastrutture di sette diverse famiglie di malware usate per distribuire ransomware. Questa operazione, denominata "Endgame", ha abbattuto circa 300 server e neutralizzato 650 domini usati per controllare malware come QakBot, Emotet, IcedID, Trickbot, e Bumblebee. Sono stati emessi mandati di cattura per 20 indagati in vari paesi e sequestrati oltre 21 milioni di euro in criptovalute. Colpendo i cosiddetti "dropper" e "loader", i malware usati come precursori dell'attacco ransomware, gli investigatori puntano a "spezzare la kill chain all'origine", impedendo ai ransomware di arrivare alle reti bersaglio. Europol ha sottolineato come questa operazione di polizia rappresenti un approccio nuovo, sostenuto e tutt'altro che sporadico: dopo la prima ondata di maggio 2024, ne sono seguite altre (una seconda ondata a maggio 2025 ha portato a nuovi indagati e sequestri). Si tratta della più ampia offensiva mai condotta contro l'infrastruttura del cybercrime, resa possibile soltanto dalla stretta cooperazione internazionale e dallo scambio in tempo reale di informazioni tra continenti.

La minaccia non è diminuita, ma si è evoluta.

I limiti del contrasto e i Santuari del crimine

Nonostante i successi, ci sono limiti strutturali nella lotta al ransomware, specie quando ci si scontra con barriere geopolitiche. Molte gang di ransomware hanno base in paesi che di fatto offrono un porto sicuro ai loro membri, sia per mancanza di volontà politica sia per implicita convenienza. La Russia in primis, e alcuni stati dell'ex CSI, sono i casi più evidenti: finché gli hacker operano dal territorio filo-russo, e non colpiscono obiettivi domestici, sanno di essere relativamente al sicuro. I vertici di vari gruppi ransomware sono noti agli investigatori occidentali, tant'è che Washington ha emesso taglie milionarie e sanzioni contro di loro, eppure rimangono intoccabili. L'episodio di REvil, con 14 arresti lampo in Russia nel 2022, è stata l'eccezione che conferma la regola: l'operazione avvenne in un breve spiraglio di dialogo USA-Russia, oggi praticamente inesistente.

Peggio ancora, emergono indizi di connivenza tra cybercriminali e apparati statali in quei paesi. Il recente leak di chat interne di BlackBasta è illuminante: i log, oltre 200.000 messaggi trapelati nel marzo 2025, indicano che il leader del gruppo, Oleg Nefedov (alias "GG"), avrebbe ottenuto aiuto da funzionari russi per sfuggire all'arresto. In una conversazione, Nefedov racconta di essere stato fermato in Armenia e di aver chiamato "contatti ad alto livello" a Mosca, i quali gli avrebbero garantito un "corridoio verde" per tornare indenne in Russia . Il leak rivela anche che Black Basta operava tranquillamente con due uffici fisici a Mosca e confidava di essere al riparo da interventi stranieri grazie alla protezione delle autorità locali. In un altro passaggio, GG afferma che se fosse mai arrivata una richiesta ufficiale di estradizione tramite Interpol, le forze dell'ordine russe l'avrebbero "strangolata sul nascere" per evitare grane ai suoi "amici" in alto loco. Queste pericolose relazioni rendono quasi impossibile colpire i vertici delle gang: arrestarli richiederebbe che le autorità del loro paese agissero contro di loro, cosa improbabile se vengono tacitamente tollerati o addirittura considerati una risorsa ufficiosa (ad esempio, per attività di spionaggio o sabotaggio informatico all'estero compatibili con gli interessi nazionali).

Oltre alla Russia, altri rifugi per cybercriminali sono paesi che non estradano i sospetti verso l'Occidente. Spesso gli operatori ransomware pianificano di risiedere (o fuggire) in nazioni come l'Iran o la Cina, sapendo che da lì difficilmente potranno essere raggiunti legalmente. Il leak di GangExposed ha persino evidenziato attività del gruppo Conti/Trickbot effettuate in Emirati Arabi Uniti e Cina, ipotizzando che fossero modi per ottenere protezione in quei paesi o per complicare l'azione giudiziaria internazionale . In pratica, i cybercriminali più navigati sfruttano arbitraggi legali e lacune diplomatiche: si spostano in giurisdizioni sicure e magari investono lì i proventi (in immobili, imprese di copertura, ecc.), ben consci che le forze dell'ordine estere non potranno facilmente metterci mano.

Questa situazione crea un doppio binario di giustizia: gli affiliati "minori" o sprovveduti vengono arrestati quando commettono errori, ad esempio viaggiando in paesi collaborativi, usando provider occidentali, riciclando denaro tramite circuiti controllati, mentre i grandi boss restano nell'ombra, protetti da confini e, in alcuni casi, da ombrelli politici.

Dopo il takedown

Un'altra realtà emersa chiaramente è che lo smantellamento di una gang non coincide necessariamente con la fine della minaccia. Al contrario, il cybercrimine ha dimostrato una notevole capacità di adattamento e riorganizzazione di fronte ai takedown. Gli affiliati e i leader sfuggiti agli arresti tendono a disperdersi per poi riaggregarsi in nuove formazioni o inserirsi in altre esistenti. È un po' il principio dell'idra: tagliata una testa, ne spuntano due

altrove. Abbiamo visto come Conti si sia "frammentata" dando linfa a nuove sigle come BlackCat, Black Basta, Royal e altri; analogamente, dopo la chiusura forzata di REvil alcuni membri sono confluiti in LockBit (che all'epoca era un gruppo emergente) o in altre operazioni RaaS.

Spesso il know-how tecnico e le infrastrutture non vanno persi con il takedown ma vengono riutilizzati. Nel caso di Conti, ad esempio, i leak hanno mostrato che il gruppo manteneva contatti con Trickbot e altre reti: quando Conti è "imploso", molti sviluppatori e operatori sono semplicemente passati a usare quelle stesse reti per nuovi scopi, come le campagne BazarLoader o i finti call-center di BazarCall. Alcuni gruppi hanno effettuato dei rebranding per confondere le acque: è successo con DarkSide → BlackMatter → BlackCat, o con DoppelPaymer → Grief, o anche con HuntersInternational → WordLeaks. Questo rende difficile per le forze dell'ordine attribuire nuovi attacchi a gruppi formalmente "sciolti". Inoltre i criminali imparano dagli errori: dopo ogni arresto eccellente, i forum del dark web brulicano di discussioni su come migliorare l'OPSEC (sicurezza operativa): ad esempio riducendo la propria esposizione, usando solo criptovalute più anonime, comunicando via sistemi più cifrati o decentralizzati, o evitando certi comportamenti a rischio (come viaggiare all'estero).

Gang meno pericolose?

Alla luce di questi sviluppi, il fenomeno ransomware è oggi a un punto di svolta. La buona notizia è che non è più incontrastato: la cooperazione internazionale ha iniziato a conseguire risultati tangibili, dimostrando che "si può fare". Gang un tempo ritenute intoccabili sono ora state smantellate, o quantomeno seriamente danneggiate, infrastrutture criminali sono state disarticolate e ingenti somme sottratte ai pirati informatici. Inoltre, il messaggio lanciato è forte: chi commette attacchi ransomware può essere individuato e punito, anche a distanza di anni, e i riscatti non sono più garantiti come un tempo. Molte aziende vittime hanno riavuto i loro dati gratis grazie alle operazioni di polizia, aumentando la fiducia nel denunciare gli incidenti invece di pagare.

Tuttavia, sarebbe ingenuo affermare che le gang ransomware siano sconfitte o siano "meno pericolose" in senso assoluto. Piuttosto, stanno diventando più elusive. Le campagne ransomware odierne tendono a essere più mirate, condotte da gruppi che adottano misure di sicurezza operativa maniacali e verso bersagli meno propensi alla cooperazione con le autorità.

Si osserva una sorta di darwinismo criminale: gli elementi improvvisati o sprovveduti vengono eliminati, mentre sopravvivono i gruppi più organizzati, spesso con possibili protezioni ad alti livelli. Questi ultimi agiscono nell'ombra, magari cambiando nome spesso, frammentando in sottogruppi per confondere gli investigatori e affidandosi a reti di collaboratori sempre più distribuite e difficili da tracciare. La minaccia quindi non è diminuita, ma si è evoluta. Alcune gang storiche sono sparite, ma nuove ne sono emerse; molte infrastrutture di supporto (forum, broker di accesso, riciclatori di criptovalute) restano operative nel dark web, pronte a servire la prossima generazione di criminali.

In definitiva, le recenti operazioni di polizia internazionale hanno alzato il costo e il rischio per chi fa ransomware, obbligando i cybercriminali a continui traslochi digitali e a guardarsi le spalle, ma non hanno eliminato il problema alla radice. Finché vi saranno enormi profitti da estorcere e scappatoie giuridiche da sfruttare, i ransomware rimarranno una minaccia.

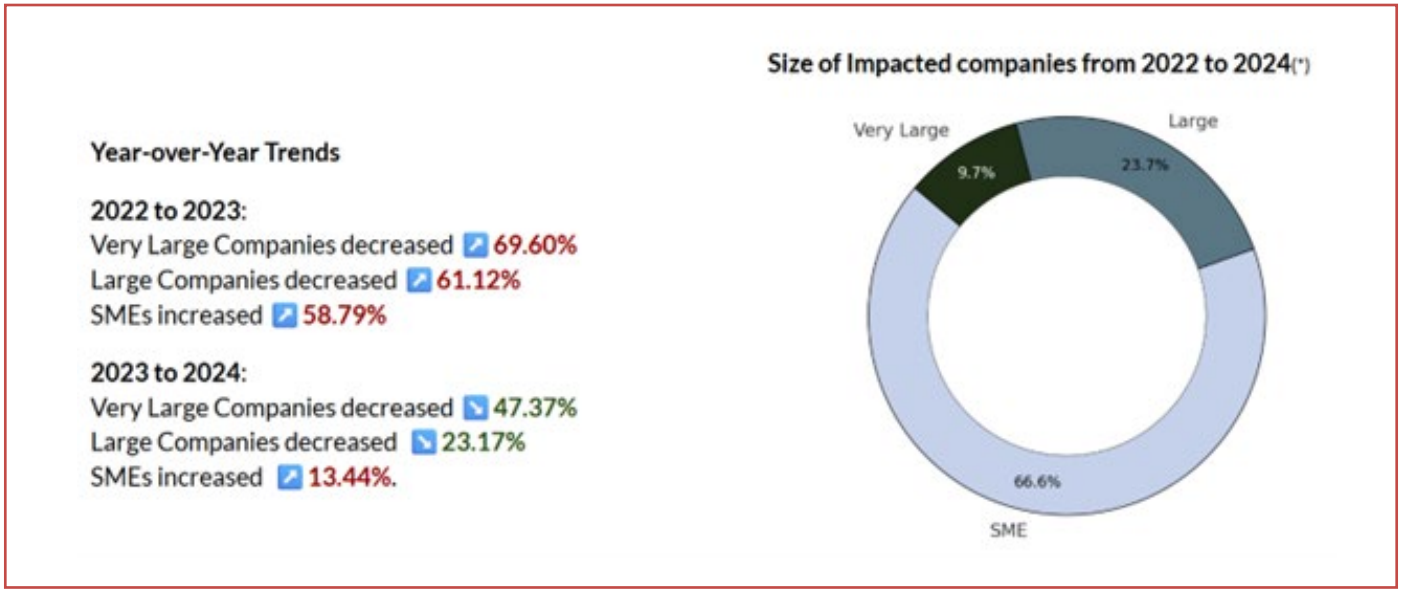


Figura. Variazione dei trend di attacco ransomware a fronte delle operazioni di Polizia (fonte:doubleextortion.com)

Dall’epica alla cybersecurity: l’hybris di chi si crede al sicuro

La superbia della sicurezza: perché l’awareness senza strumenti è un’illusione

A cura di Simonetta Sabatino

Nel panorama attuale della cybersecurity, si sta assistendo a un pericoloso oscillare tra due estremi: prima, un’eccessiva fiducia nella tecnologia, oggi una crescente sopravvalutazione del solo fattore umano come unico antidoto alla vulnerabilità. Entrambe, se elevate a dogma esclusivo, rischiano di alimentare un senso di falsa sicurezza.

Come spesso accade, l’errore non risiede nella scelta di una via rispetto all’altra, ma nell’illusione che una sola dimensione sia sufficiente. L’unica risposta efficace è l’equilibrio: un’integrazione armonica tra consapevolezza umana e strumenti tecnologici evoluti.

Hybris: l’errore supremo

Nella tragedia greca, hybris era la colpa di chi osava sfidare i confini imposti dalla natura o dagli dèi. Un atto di superbia che conduceva inevitabilmente alla catastrofe, alla nemesis. Un concetto antico che oggi torna prepotentemente attuale nella gestione del rischio digitale.

Oggi, affidarsi a un’unica dimensione – tecnica, razionalità o forza – espone a errori altrettanto pericolosi.

Affidarsi esclusivamente alla tecnologia – logica, automatismi, efficienza – equivale a costruire ali perfette come quelle di Dedalo, ma senza insegnare come usarle. Come Icaro, voliamo troppo in alto e, accecati dalla potenza degli strumenti, dimentichiamo il nostro limite. Così precipitiamo, vittime di un attacco semplice, ma inaspettato.

Allo stesso modo, confidare solo nell’ingegno umano, senza il supporto delle tecnologie, può rivelarsi fallimentare. Ulisse non avrebbe mai superato mostri e tempeste senza il sostegno della sua nave e dell’equipaggio. L’intelligenza strategica è preziosa, ma inefficace se non accompagnata da una dotazione adeguata.

La vera sicurezza digitale nasce dalla consapevolezza che nessuno strato da solo è sufficiente. Un tempo si è mitizzata la tecnologia, oggi si rischia di idolatrare l’elemento umano. Entrambe le visioni, isolate, rappresentano una forma moderna di hybris.

A contrastarla, nella saggezza greca, c’è la sophrosyne: il senso del limite, la misura, l’equilibrio. Ed è proprio lì, nell’incontro tra intuito e automazione, che si trova la chiave della resilienza.

Dal mito della tecnologia alla centralità dell’utente

Negli anni iniziali della sicurezza informatica, la difesa era vista come dominio esclusivo della tecnologia: firewall, antivirus, protezioni perimetrali. La percezione diffusa era che bastasse installare software per essere al sicuro. Ma la fiducia cieca in queste barriere è crollata sotto il peso di nuove minacce, invisibili ai sistemi: l’in-

gegneria sociale, le manipolazioni emotive, la psicologia dell'errore.

Le tecnologie, da sole, non sono più sufficienti a intercettare attacchi sempre più sofisticati che colpiscono non tanto le macchine, quanto i comportamenti. Attacchi che non violano direttamente un sistema informatico, ma manipolano chi lo utilizza. Ed è proprio su questa vulnerabilità – la psicologia umana – che i cybercriminali hanno spostato il loro mirino.

È emersa allora una nuova consapevolezza: il fattore umano è spesso il vero punto di ingresso per gli attacchi. I moderni attacchi si insinuano nelle abitudini, nei riflessi, nelle emozioni di chi lavora in azienda. Phishing, smishing, social engineering: : tecniche che fanno leva su paure istintive, urgenze costruite ad arte, senso di colpa o ingenuità. Tutto ciò per indurre la vittima al clic sbagliato.

Così si è compreso che l'utente è il primo bersaglio: le organizzazioni hanno reagito avviando campagne di awareness: formazione, phishing simulati, promozione della "cultura del dubbio". È una direzione virtuosa. Si è passati da una sicurezza perimetrale a una sicurezza distribuita, in cui ogni utente diventa un attore attivo.

Ma questa evoluzione, per quanto promettente, non è sufficiente da sola.

La superbia della sicurezza: perché l'awareness senza strumenti è un'illusione.

Perché l'awareness non basta: tre verità da considerare

Tuttavia, così come un tempo si sopravvalutava la tecnologia, oggi si rischia di sopravvalutare la sola formazione, con un'illusione che si scontra con la realtà.

Tre verità lo dimostrano:

1. **Le minacce evolvono rapidamente**

   Oggi il phishing sfrutta l'intelligenza artificiale per generare messaggi iper-realistici, personalizzati, basati su dati esfiltrati da precedenti breach o dalla supply chain aziendale. È irrealistico pensare che l'utente, da solo, possa sostenere una corsa alla sofisticazione.

2. **La scala degli attacchi è fuori scala umana**

   Anche un utente molto preparato, in un contesto di centinaia di messaggi automatizzati, può sbagliare. L'errore umano è fisiologico, ma nel contesto cyber può bastarne uno per aprire la porta a danni enormi. Basta un clic.

3. **L'utente non è un firewall umano**

   Nessun training può annullare i limiti cognitivi, il sovraccarico di lavoro o le distrazioni. Il fattore umano deve essere supportato da difese automatiche, in grado di poter funzionare come rete di protezione automatica.

L'AI nella minaccia: il phishing potenziato

Il phishing è in continua espansione, sia in Italia che a livello globale. Ma non si tratta solo di un aumento quantitativo: il fenomeno sta evolvendo in profondità. La vera discontinuità è rappresentata dall'integrazione di componenti automatiche e generative, rese sempre più potenti dall'utilizzo malevolo dell'intelligenza artificiale.

Campagne di phishing oggi sono:

- Automatizzate con LLM (Large Language Models) per creare email indistinguibili da quelle legittime.
- Basate su dati rubati da breach precedenti (data poisoning).
- Ottimizzate con tecniche di clustering comportamentale per colpire specifici profili aziendali.

In questo scenario, l'essere umano, da solo, non può reggere l'urto.

Serve un nuovo equilibrio: awareness + tecnologia

Educare l'utente è come insegnargli a guidare: fondamentale. Ma neanche il pilota esperto farebbe a meno di cinture di sicurezza, ABS, assistenti alla frenata. La sicurezza stradale funziona perché unisce capacità umane e supporti tecnologici. Lo stesso vale nella cybersecurity: la guida umana ha bisogno di supporti intelligenti.

Serve una difesa multilivello:

- Email filtering avanzato (anti-phishing, anti-malware)
- Autenticazione multifattoriale (MFA)
- Sandboxing, URL rewriting, quarantene automatiche
- EDR/XDR con detection AI-based
- UEBA per analisi comportamentale su utenti e asset
- SIEM intelligenti per correlazioni in tempo reale
- AI contro AI: strumenti che riconoscono pattern generativi, sintassi algoritmica, anomalia semantica

Solo così si crea un ecosistema resiliente, dove l'utente è preparato e responsabilizzato, ma protetto e non lasciato solo.

Conclusione: il sophrosyne digitale

La sicurezza non è una scelta binaria: non è un software né una cultura da installare. È un sistema vivo e un equilibrio mobile tra tre pilastri: persone, processi, tecnologie.

Pensare che basti una sola leva – awareness o tecnologia – è il primo passo verso l'insicurezza.

L'AI genera messaggi, gli utenti cliccano. Serve una doppia risposta:

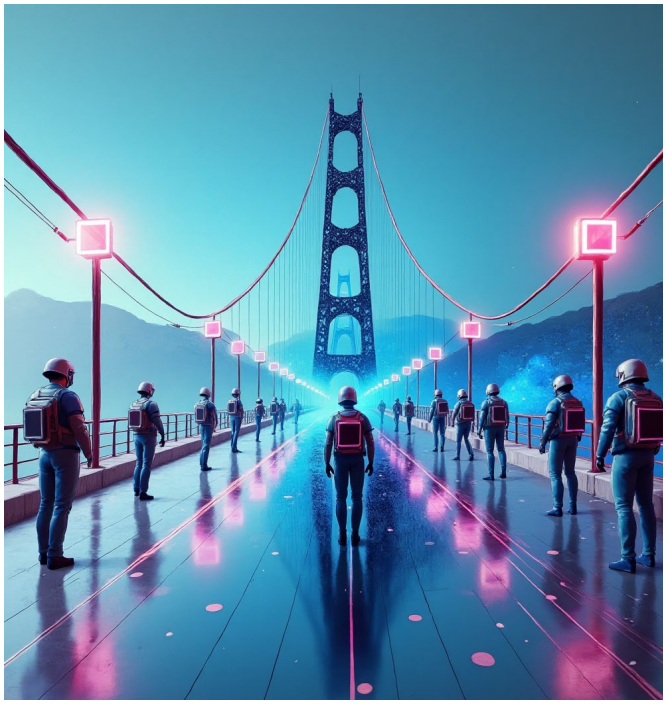
- L'awareness riconosce, segnala, sviluppa, reagisce.
- La tecnologia blocca, filtra, protegge.

La formazione è la prima linea.

La tecnologia, la retroguardia.

Il vero punto di forza è l'equilibrio: il sophrosyne digitale che ci rende davvero capaci di resistere.

Pensare che basti una sola leva – awareness o tecnologia – è il primo passo verso l'insicurezza.



Cambiamo il modo di scrivere le regole e educhiamo le persone all'AI per renderla nostra alleata e non nemica

A cura di Guido Scorza

Una delle sfide più importanti, ambiziose, direi epocale davanti alle quali l'impatto dell'intelligenza artificiale sulla società ci pone è quella di riuscire a cogliere le straordinarie opportunità che l'intelligenza artificiale ha da offrirci limitandone quanto più possibile i rischi.

In questa prospettiva ci sono due questioni che a me appaiono più importanti delle altre.

La prima riguarda il tempo.

Ci sono voluti sessantadue anni perché cinquanta milioni di persone utilizzassero un'automobile per spostarsi, sessanta perché avessero un telefono a casa, quarantotto perché disponessero dell'elettricità e ventidue perché possedessero un televisore.

Il computer, per conquistare lo stesso pubblico di cinquanta milioni di persone ci ha messo quattordici anni, il telefonino dodici e Internet sette.

ChatGPT, il servizio online basato sugli algoritmi di intelligenza artificiale generativa di OpenAI, in meno di due mesi ha raggiunto cento milioni di utenti attivi mensili, il doppio di quelli raggiunti da YouTube in quattro anni.

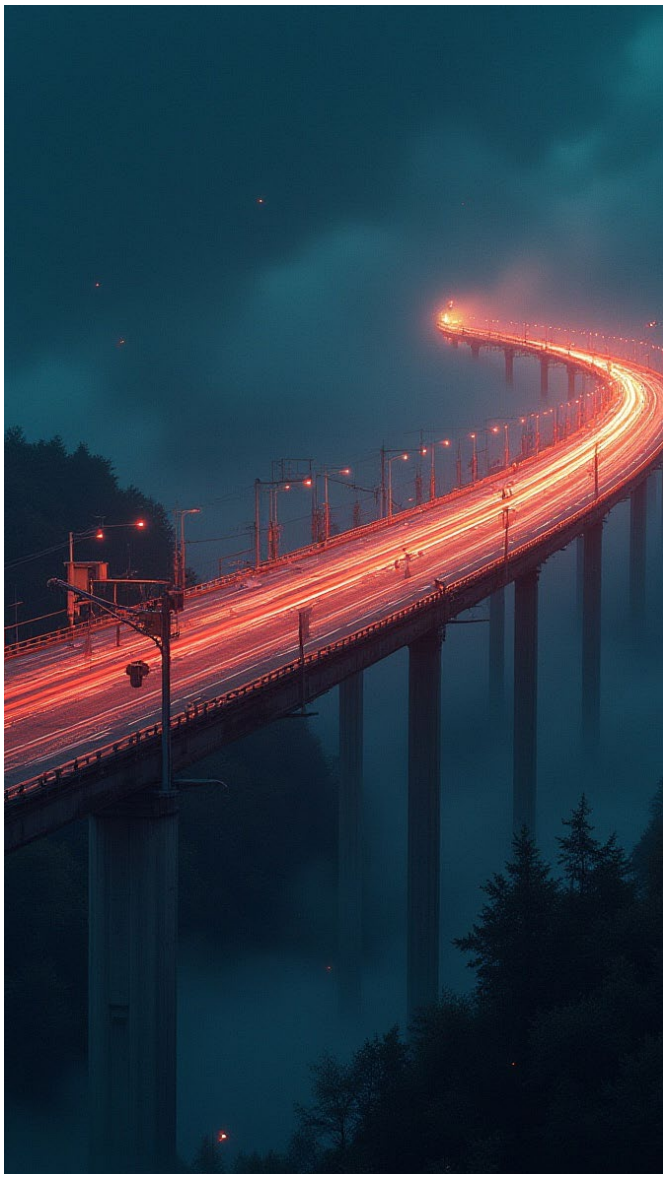
Sono numeri che mi sembrano sufficienti a raccontare la costante e inarrestabile accelerazione del ritmo di diffusione di prodotti e servizi che hanno indiscutibilmente cambiato significativamente le nostre vite e avuto un impatto rivoluzionario sulla società.

Senza dire che le innovazioni di oggi sono straordinariamente più complesse di quelle di ieri e hanno un impatto enormemente più trasversale sulla società.

Non c'è paragone, tanto per fare un esempio, tra l'unica funzione di un telefono fisso di ieri che serviva solo per parlare con un interlocutore a distanza e le migliaia di possibili funzioni di uno smartphone, anche di non più nuovissima generazione, nel quale la funzione di comunicazione vocale è, ormai, diventata quasi residuale rispetto a tutte le altre possibili forme di impiego.

Questa accelerazione del ritmo dell'innovazione tecnologica, dunque, rappresenta, a mio avviso, uno dei fattori più rilevanti da tenere presente nell'interrogarci sulle forme e i modi con i quali provare a governare questa era del cambiamento perché sappiamo tutti che la migliore delle regole se non è tempestiva è irrilevante nel migliore dei casi, e controproducente nel peggiore.

Quando nella seconda metà dell'800 le prime auto hanno iniziato a circolare sulle strade inglesi, il Parlamento varò il c.d. Red Flag Act, datato 1865, una legge che imponeva un limite di velocità di 3,2 chilometri orari e, soprattutto, stabiliva che un uomo, con una bandiera rossa in mano, dovesse precedere ogni automobile di circa 55 metri per segnalare il pericolo.



Il Red Flag Act rimase in vigore per oltre trent'anni, fino al 1896.

Mi sembra abbastanza evidente che la migliore delle regole con la quale oggi volessimo provare a governare una tra le infinite applicazioni dell'intelligenza artificiale non potrebbe mai avere una vita tanto lunga perché diventerebbe immediatamente obsoleta e rischierebbe di ritrovarsi abrogata per desuetudine come sarebbe accaduto al Red Flag Act se a qualche mese dalla sua entrata in vigore le macchine avessero cominciato a volare, non potendo, più, evidentemente, lo sbandieratore precederle in volo.

Questo è il contesto che abbiamo oggi davanti.

Non ho risposte definitive al problema ma, personalmente, credo che dovremmo avere il coraggio di modificare radicalmente approccio rispetto al passato, smettere di pretendere di disciplinare a livello di dettaglio taluni fenomeni e delegarne la governance, sulla base di una manciata di criteri di delega stringenti nel metodo più che nel merito, alle Agenzie e alle Autorità indipendenti.

Solo così, forse, possiamo sperare di scongiurare il rischio di continuare a prevedere per legge che uno sbandieratore cammini davanti alle automobili per avvisare del pericolo quando le automobili frattanto volano.

Cambiamo il modo di scrivere le regole ma non rinunciamo, come qualcuno inizia a suggerire, a scriverle, non rinunciamo a regolare l'innovazione cadendo nel tranello di chi vorrebbe farci credere che le regole frenano l'innovazione.

Non è vero.

Al contrario le regole – ovviamente a condizione che siano quelle giuste e soprattutto che arrivino in tempo – orientano e promuovono l'innovazione spingendola nell'unica direzione nella quale è giusto che vada la massimizzazione del benessere collettivo e la maggiore possibile distribuzione delle opportunità che offre.

Rinunciare a regolamentare l'innovazione, significa lasciare che la tecnologia diventi regolamentazione e che la società sia governata da software, algoritmi e interfacce progettati e disegnati in nome di interessi privati di pochi, normalmente orientati prevalentemente al profitto.

Significa insomma lasciare che la tecnocrazia abbia la meglio sulla democrazia.

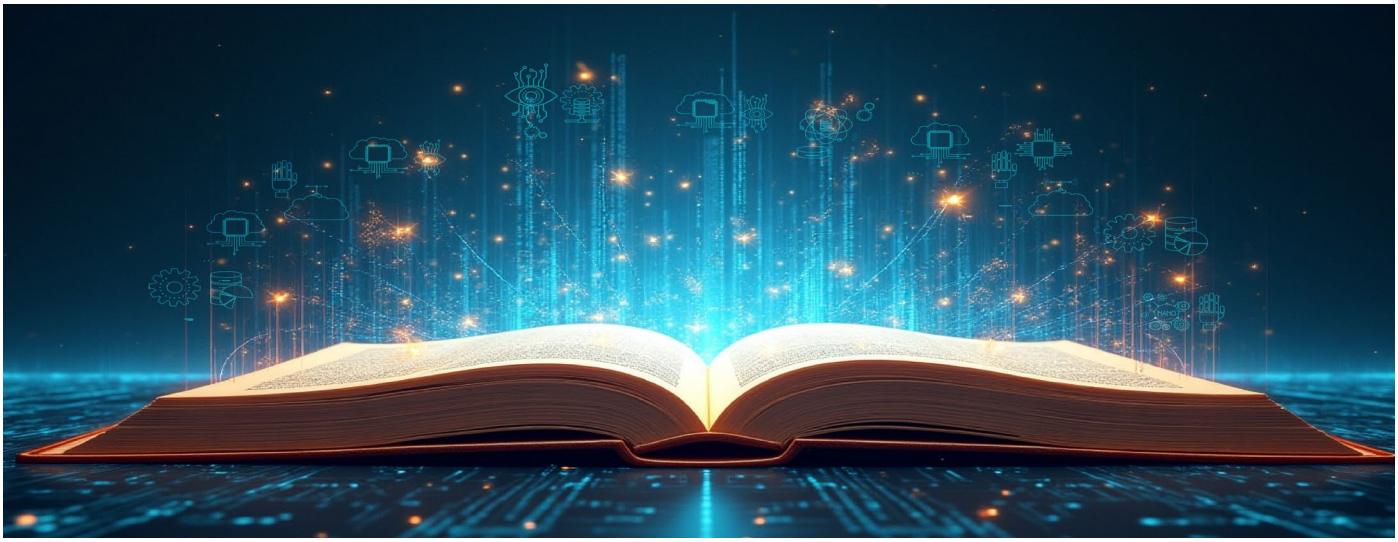
Significa insomma lasciare che la tecnocrazia abbia la meglio sulla democrazia.

La seconda questione, non meno importante della prima e ad essa strettamente correlata riguarda l'educazione digitale.

La società è sempre più digitale e conoscere il digitale, almeno nei suoi rudimenti, è sempre di più un pre-requisito di cittadinanza irrinunciabile.

Chi non ha un livello di adeguate competenze digitali è un cittadino di serie B, anzi, peggio, è una persona di serie B, perché l'impatto di questo deficit di competenze si abbatte senza pietà in ogni ambito della nostra vita.

Eppure, l'Italia non ce la fa, non ce la facciamo a capire per davvero questo principio elementare e a correre ai ripari con la determinazione e l'urgenza che servirebbero.



L'ultimo rapporto ISTAT lo certifica in maniera impietosa.

"Le competenze digitali giocano un ruolo fondamentale nel favorire la transizione digitale e al

tempo stesso contrastare l'emergere di divari che possano compromettere l'equità e l'inclusione sociale. Il programma strategico UE per il decennio digitale13 ha tra l'altro l'obiettivo, da raggiungere entro il 2030, di portare all'80 per cento la quota della popolazione di età compresa tra 16 e 74 anni con almeno competenze digitali di base14. Nel 2023, tale quota si attesta a poco più della metà (55,5 per cento nella media UE27) e l'Italia con il 45,8 per cento si colloca al ventiduesimo posto della graduatoria, con una distanza di 20 punti percentuali dalla Spagna (66,2 per cento) e di 14 punti percentuali dalla Francia (59,7 per cento)".

Non sono opinioni, sensazioni, percezioni soggettive.

Lo dicono i numeri.

Siamo il fanalino di coda di un'Europa che già di suo è indietro rispetto al resto del mondo.

Onestamente davanti a dati di questo genere – che nessuno si offenda – ma ogni altro discorso sul governo dell'intelligenza artificiale, sulle regole, sull'impatto dei nuovi prodigi artificiali sulla società, sulle opportunità che non dobbiamo lasciarci sfuggire, a me sembra da una parte vuoto e superficiale e dall'altra poco consapevole e, forse, persino incosciente.

Prendi la più potente e disruptive tecnologia che l'ingegno umano abbia mai progettato e sviluppato e mettila nelle mani di oltre trenta milioni di persone, la metà della popolazione italiana, completamente a digiuno di qualsiasi competenza digitale di base e il migliore degli scenari possibile sarà quello che si avrebbe se trenta milioni di italiani tutti insieme, senza mai essere saliti su un mono pattino elettrico decidessero di farlo esattamente nello stesso momento nelle vie trafficate della stessa città.

Niente di più pericoloso.

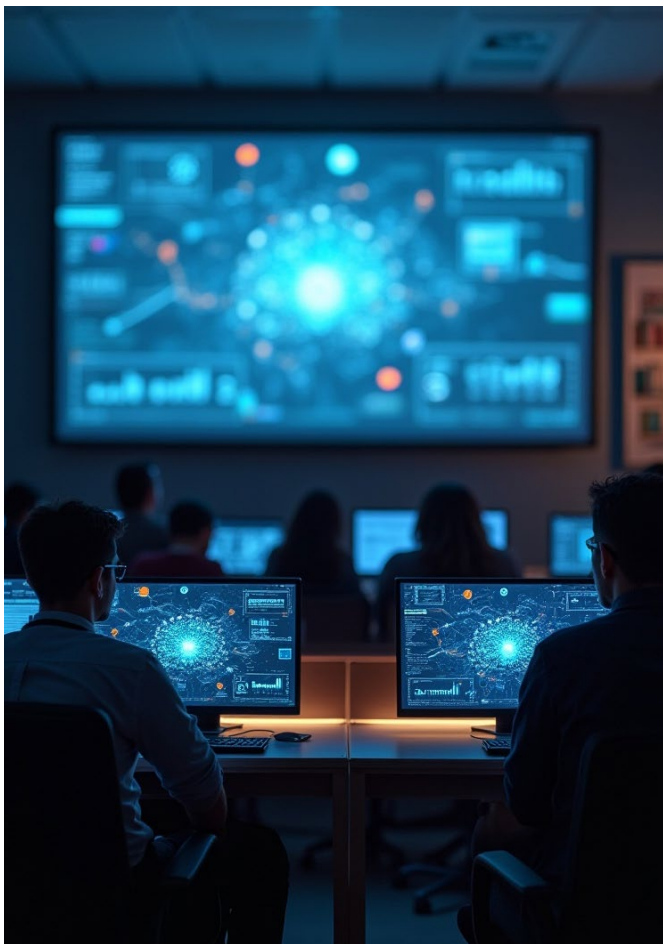
E non basta.

Perché mentre i primi trenta milioni, quelli mai saliti sul monopattino, starebbero a terra a contare le ferite, altri trenta milioni, quelli che hanno avuto la fortuna di imparare a portare il monopattino, sarebbero i primi a arrivare a scuola al mattino, a entrare al lavoro, a mettersi in fila negli uffici pubblici e negli ospedali per esercitare i loro diritti civili e garantirsi una salute migliore.

Questo è, oggi, il Paese nel quale viviamo.

Prima lo capiamo, prima, forse, facciamo un'inversione a "U" e accettiamo l'idea che ciò di cui abbiamo veramente e drammaticamente bisogno – ma domani mattina – è dichiarare guerra all'analfabetismo digitale come nel secondo dopoguerra si fece con quello funzionale.

La migliore delle tecnologie nelle mani di chi non sa usarla è pericolosa per sé e per gli altri e se metà del tuo Paese non sa usarla e quella tecnologia diventa parte integrante dell'infrastruttura di base di quel Paese, il Paese in questione non ha nessuna chance di essere democratico, di essere giusto, di essere equo, né di competere per davvero nella società globale.



Chi non ha un livello di adeguate competenze digitali è un cittadino di serie B, anzi, peggio, è una persona di serie B, perché l'impatto di questo deficit di competenze si abbatte senza pietà in ogni ambito della nostra vita.

Conflitto Israele – Iran: i riflessi sul panorama delle minacce cibernetiche

A cura di Pierluigi Paganini

Mentre il mondo assiste con il fiato sospeso ad un'escalation delle operazioni militari parte del conflitto tra Israele ed Iran, ci si interroga sui possibili riflessi sul panorama delle minacce cibernetiche ed i rischi connessi per le organizzazioni in tutto il mondo.

Da oltre un decennio, il conflitto fra i due paesi non si combatte soltanto sul terreno fisico, lo spazio cibernetico è diventato un campo di battaglia strategico, dove si intrecciano operazioni di intelligence, sabotaggi e guerra psicologica.

La dimensione digitale è oggi parte integrante delle strategie di sicurezza nazionale di entrambi i Paesi, che hanno investito risorse e competenze per sviluppare capacità offensive e difensive all'avanguardia. Questa evoluzione ha conseguenze che travalicano i confini regionali, coinvolgendo aziende, infrastrutture e governi di tutto il mondo, in un contesto in cui la natura senza frontiere del cyberspazio rende potenzialmente vulnerabile chiunque.

Da un lato, c'è Israele che ha costruito, nel tempo, una struttura sofisticata per difendersi e attaccare. Il National Cyber Directorate, insieme all'Unità 8200 delle Forze di Difesa Israeliane, integra capacità difensive, come il progetto "Cyber-Dome", che protegge infrastrutture critiche sfruttando sofisticate soluzioni oggi integrate da sistemi basati sull'intelligenza artificiale. Si riconosce ad Israele un arsenale offensivo di élite e il risultato sono operazioni altamente mirate e precise, che spesso coadiuvano raid aerei o attacchi da parte di droni.

Israele è quindi riconosciuto a livello globale come uno degli Stati più avanzati in materia di sicurezza informatica. Il governo di Tel Aviv destina circa il 7% del budget militare alle attività di cyber difesa e cyber attacco, puntando su tecnologie di intelligenza artificiale, machine learning e sistemi di signal intelligence per monitorare e neutralizzare minacce in tempo reale. Il settore privato gioca un ruolo fondamentale, numerose aziende nazionali collaborano direttamente con le forze armate, testando e implementando soluzioni innovative che ven-

gono poi esportate a livello internazionale.

L'episodio più emblematico della postura cibernetica israeliana resta l'operazione Stuxnet del 2010, condotta insieme agli Stati Uniti, che ha dimostrato come un malware possa sabotare fisicamente infrastrutture strategiche, in questo caso le centrifughe nucleari iraniane nell'impianto di Natanz, senza la necessità di un intervento militare diretto. Questo attacco ha segnato una svolta nella storia della guerra digitale, mostrando al mondo il potenziale distruttivo delle armi informatiche.

Va detto tuttavia che a causa dei conflitti in corso il numero di attacchi contro Israele è in costante aumento. Secondo il rapporto annuale del National Cyber Directorate israeliano, nel 2023 gli attacchi informatici nel Paese sono aumentati del 43 %, passando dai 9.100 del 2022 ai 13.040 nel 2023. Più della metà degli attacchi (68 %) sono avvenuti durante la guerra di Gaza, tra ottobre e dicembre.

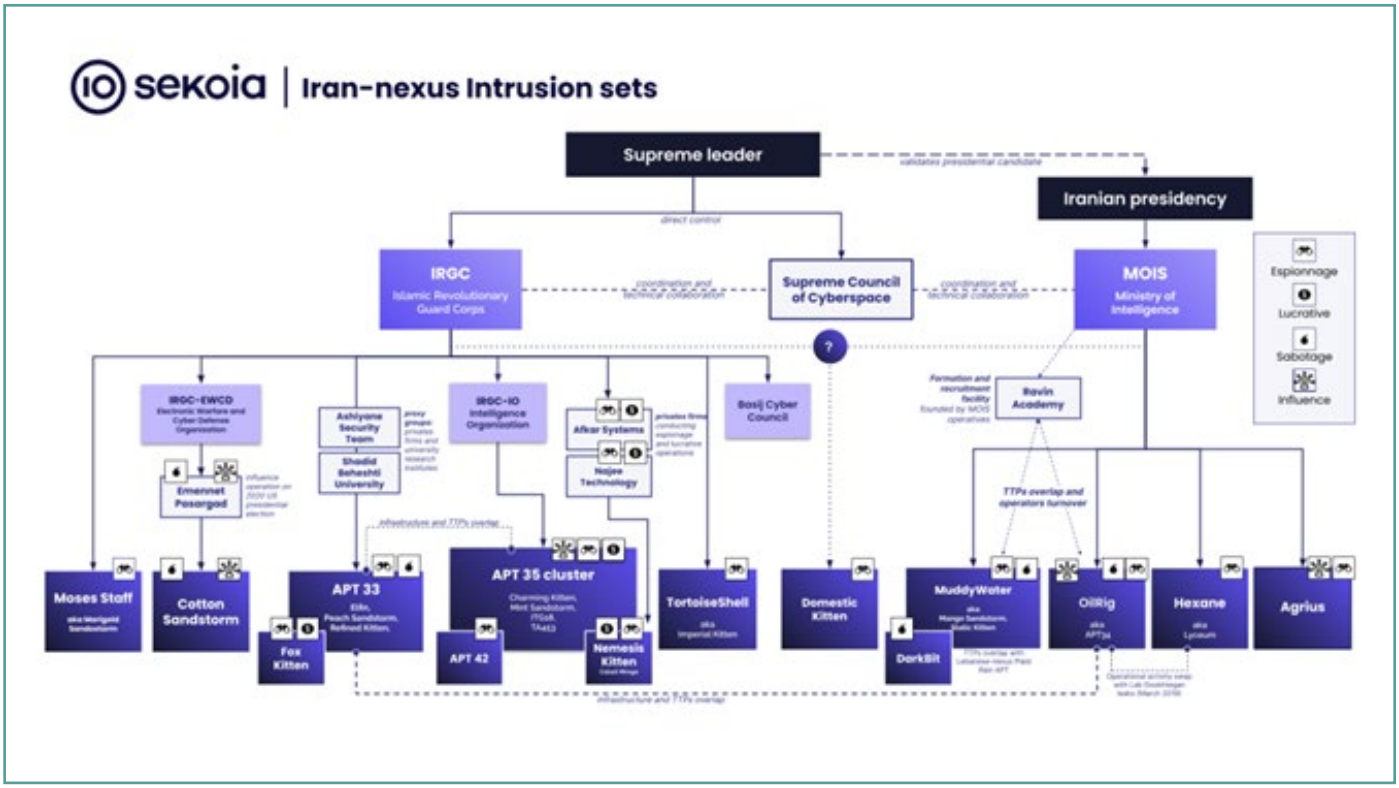
L'ex direttore generale della Cyber Directorate, Gaby Portnoy, lo scorso anno ha affermato che gli attacchi iraniani, non solo contro Israele ma anche contro alleati occidentali, si sono triplicati dopo l'8 ottobre 2023. L'intensità dell'offensiva è cresciuta non solo in quantità, ma anche in sofisticazione e dannosità.

Durante lo stesso arco temporale, ben 3.380 eventi significativi sono stati registrati, di cui 800 avevano un potenziale di danno elevato e sono stati intercettati prima di causare conseguenze rilevanti.

Dall'altro lato, l'Iran ha sviluppato una strategia cibernetica articolata e ramificata. Il suo Cyber Defense Command, insieme ai gruppi legati all'IRGC e al Ministero dell'Intelligence, si avvale di hacker statali e proxy non statali come Hezbollah.

Un esempio eclatante della capacità offensiva iraniana è l'attacco del 2012 a Saudi Aramco, in cui il malware Shamoon ha cancellato dati da 30.000 computer dell'azienda petrolifera saudita, interrompendo per giorni una parte significativa della produzione mondiale di petrolio. L'operazione, oltre a causare danni economici ingenti, ha lanciato un messaggio politico chiaro e ha evidenziato la vulnerabilità delle infrastrutture energetiche globali.

Negli ultimi anni abbiamo assistito a numerose offensive condotte da gruppi coordinati dal governo di Teheran, ivi compresi campagne di cyberspionaggio, attacchi di spear-phishing, attacchi di DDoS, e campagne malware volte a diffondere ransomware e wiper. Obiettivo degli attori nation state sono state le infrastrutture energetiche in Medio Oriente. Gruppi APT (Advanced Persisten Threat) come APT33, APT34, APT35, MuddyWater, e CyberAv3ngers si sono resi responsabili di numerosi attacchi su larga scala che han preso di mira anche obiettivi in Europa e negli Stati Uniti.



Negli scorsi mesi sono stati segnalati blackout temporanei in alcune centrali elettriche israeliane, attribuiti a cyberattacchi iraniani, mentre bot e account social legati a Teheran e Mosca hanno diffuso video e notizie false per minare il morale della popolazione israeliana e influenzare la percezione internazionale del conflitto.

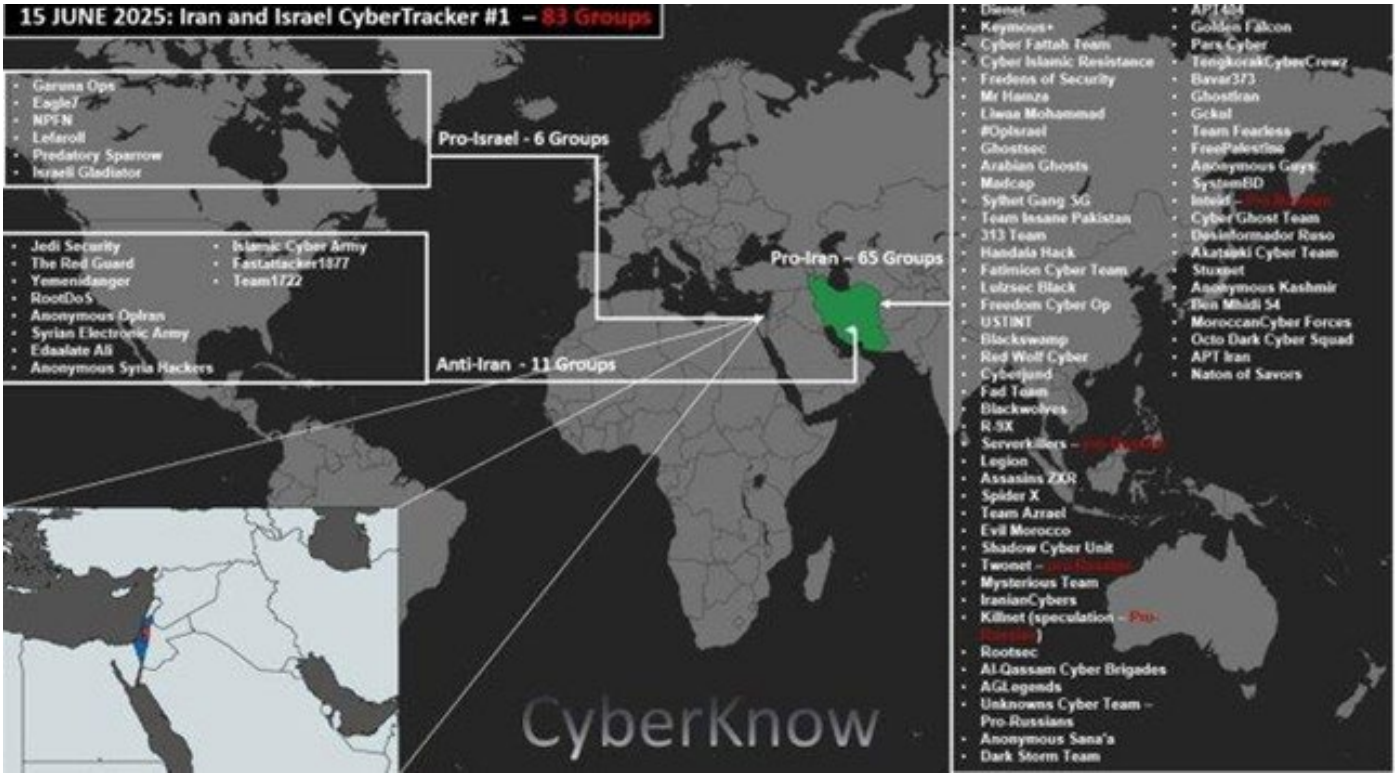
Le operazioni cyber non restano isolate; spesso precedono un attacco convenzionale. Sono utilizzate in operazioni militari per paralizzare e disabilitare i sistemi di difesa avversari, interferire con le comunicazioni lasciando vulnerabili le parti colpite. In diverse occasioni, Israele ha sfruttato attacchi cibernetici per paralizzare i sistemi di difesa iraniani prima dell'esecuzione di raid mirati.

Sebbene l'Operazione Rising Lion del giugno 2025 sia stata principalmente un'azione militare tradizionale, il contesto storico e le capacità note di Israele lasciano spazio a un ruolo indiretto ma significativo delle cyber operazioni. Queste, integrate con intelligence e attacchi fisici, hanno probabilmente contribuito a paralizzare le difese iraniane, massimizzando l'impatto strategico. Tuttavia, la mancanza di trasparenza sugli aspetti digitali sottolinea la natura opaca della cyber guerra, dove il confine tra azione militare e criminalità informatica rimane volutamente sfumato.

L'Iran a sua volta risponde con armi cibernetiche, soprattutto per evitare sanzioni internazionali, spostando il conflitto in uno spazio in materiale ma in grado, comunque, di infliggere gravi danni al nemico.

Alle attività di spionaggio e sabotaggio si aggiunge la guerra dell'informazione: leak di documenti sensibili, defacing di siti, campagne di disinformazione e messaggi intimidatori sono parte della dottrina militare di entrambi i paesi. Il fine è destabilizzare l'avversario, influenzare l'opinione pubblica interna ed esterna, e imporre costantemente la propria narrativa sullo scontro in corso.

A questo contesto tumultuoso si aggiunge l'operato di gruppi di hacktivisti a supporto di entrambi i paesi. Negli ultimi giorni, sono stati monitorati i gruppi hacktivisti coinvolti in attività cyber legate alle tensioni tra Iran e Israele. Secondo i ricercatori di CyberKnown al momento risultano attivi 83 gruppi, numero destinato probabilmente ad aumentare. Si registra una presenza maggiore di gruppi anti-Iran rispetto a quelli pro-Israele, riflettendo la tradizionale minore partecipazione hacktivista a favore di Israele. Attualmente, tre gruppi pro-Russia stanno supportando l'Iran. Gli attacchi rivendicati includono DDoS, defacement, furti di dati, doxing, oscuramenti di profili social, ransomware e attacchi a infrastrutture operative. Tra gli attori più rilevanti tornati attivi dopo i recenti attacchi missilistici figura anche Handala Hack, legato all'Iran.



Fonte: Account CyberKnow su X

Il rischio per le imprese e gli asset globali

Il contesto descritto è una fucina di minacce concrete per aziende e organizzazioni di tutto il mondo: il digitale non conosce confini statali, la supply chain è globale e ciò che inizia come azione mirata fra Stati può facilmente sfociare in una minaccia per terzi. Aziende nel settore energetico, manifatturiero, sanitario, nel comparto dei trasporti e della pubblica amministrazione diventano potenziali bersagli: un attacco ben pianificato può arrestare una rete elettrica, compromettere una raffineria, o bloccare sistemi ospedalieri.

Abbiamo imparato dagli attacchi a Saudi Aramco e dalle attività globali parte dell'Operation Cleaver promosse dall'Iran che queste operazioni possono estendersi ben oltre i confini regionali, colpendo infrastrutture critiche in Europa, Nord America, Asia e altrove.

Il quadro italiano: vulnerabilità e difese

L'Italia ha sviluppato una propria architettura di difesa cibernetica negli ultimi anni. Dal 2017 è operativo il Comando Operazioni in Rete (COR) con compiti simili a quelli israeliani. L'istituzione dell'Agenzia per la Cybersicurezza Nazionale nel 2021 ha rappresentato una svolta, centralizzando competenze e responsabilità in materia di policy, protezione e interventi su attacchi informatici.

Secondo i report di TIM e Cyber Security Foundation e i resoconti dell'ACN, l'Italia ha registrato nel 2024 un aumento del numero e della gravità degli attacchi: +36% di DDoS, con frequenze di attacchi giornalieri, +64% di ransomware, e picchi del +111% di attacchi al settore sanitario. Di recente, la PA è stata interessata da circa il 42% dei DDoS, segnando un cambio di scenario: non più bersagli marginali, ma obiettivi in prima linea.

Tutto ciò ci pone di fronte a un bivio: l'Italia, come alleata di Israele e membro NATO, potrebbe diventare obiettivo di rappresaglie cyber. I settori più esposti restano quelli energetico, sanitario, manifatturiero, della difesa e della pubblica amministrazione. Essi sono intrinsecamente connessi con infrastrutture internazionali, gasdotti, centrali, reti IT/OT e quindi esposti a operazioni offensive state-sponsored.

L'Italia è a rischio? E come reagire?

Sì, c'è un rischio concreto, e cresce ogni volta che il conflitto fra Israele e Iran si intensifica. Non possiamo escludere che l'Italia possa diventare teatro di cyber-attacchi indiretti, sia per rappresaglia rispetto al supporto fornito, sia per effetto di procacciamenti di dati, interruzione di servizi o destabilizzazioni sistemiche.

La dipendenza energetica del nostro Paese dal Medio Oriente rende le infrastrutture nazionali vulnerabili a eventuali attacchi o interruzioni. Inoltre, la presenza di multinazionali italiane come Eni e Leonardo in Medio Oriente le espone a rischi di ritorsione o spionaggio industriale. I settori più esposti sono quelli dell'energia, della difesa e dei trasporti.

In risposta, l'Italia ha già implementato misure difensive ed ha innalzato il livello di attenzione. Occorre insistere sulla cooperazione internazionale e sulla condivisione delle informazioni su threat actors e relative tecniche, tattiche e procedure. È cruciale aggiornare normative su obblighi di sicurezza per infrastrutture critiche e investire nella formazione e sensibilizzazione dei settori privati e pubblici.

Conclusione

Il conflitto tra Israele e Iran dimostra ancora una volta che la guerra del futuro si gioca anche nel cyberspazio. Ogni operazione invisibile può trasformarsi in un'aggressione costosa per imprese, servizi e amministrazioni. L'Italia non è immune e deve continuare a rafforzare la propria postura cibernetica, collaborando con partner internazionali e spingendo su deterrenza, legislazione, resilienza e consapevolezza. In uno scenario senza confini, la sicurezza digitale è la prima linea difensiva.

Cybersecurity paradox: la sicurezza informatica più efficace dipende dal “caring” delle risorse umane

A cura di Alessia Valentini

Il Progressivo depauperamento della gestione di risorse umane nelle aziende ha portato diversi fenomeni sistemici: quite quitting, ghostworking addirittura skill shortage dei dipendenti più “datati” e fuga di cercelli. Ma se demotivazione, dequalificazione e destabilizzazione sono deleterie per qualsiasi azienda, nel contesto della sicurezza informatica possono rappresentare un vero e proprio suicidio professionale, una sorta di harakiri sistemico. Ma uscire dal circolo vizioso, non solo si può, si deve. Basta occuparsi per davvero della “ROOT cause”

La forza lavoro in ogni organizzazione è storicamente sempre stata indicata come insieme delle “risorse umane”. Proprio questo termine, “risorse” dovrebbe far riflettere sulla qualità dell’apporto che ogni individuo rappresenta in azienda. Non si parla solo di hard e soft skill, che, come è noto, rispettivamente costituiscono le capacità e competenze principali legate al lavoro svolto e le competenze secondarie da qualche anno rivalutate come altrettanto cruciali. Di fatto, il valore delle persone in azienda è spesso un valore intangibile, legato alle idee, alla capacità di pensare a delle soluzioni innovative, all’entusiasmo, al contributo di passione per il proprio lavoro, alla genuina emozione che si prova nel contribuire insieme ad un progetto ed alla soddisfazione di vederlo svolto bene e riceverne un riconoscimento. Come è facile vedere sono tutti elementi fortemente legati alle emozioni, al nostro “essere umani”. Quelle emozioni che da qualche anno le aziende di ogni ordine e grado vorrebbero suscitare nei propri dipendenti, per “consacrarli” all’azienda, per vederli “mettere anima e cuore” nel lavoro, senza valutare davvero cosa stiano dando in cambio. Purtroppo, sebbene il corrispettivo salariale sia doveroso (anche se dovrebbe essere maggiormente commisurato al ruolo, esperienza e competenze), non basta da solo, a “ingaggiare” davvero le risorse. Sembrano infatti mancare elementi valoriali condivisi, cura delle risorse fatto da formazione e benefit, rispetto vero e proprio delle persone; tutte aspettative mancate in generale, che stanno trasformando il mondo del lavoro in modo sempre più asettico e distaccato con conseguenze di allontanamento emotivo e a seguire anche professionale. Il culmine di tale fenomenologia è lato dipendenti, un abbandono progressivo e un disamoramento del luogo di lavoro, lato azienda, l’adozione di strumenti e agenti automatizzati, che forse possono occuparsi di parte delle attività più a basso livello, ma che certamente non si “sperticano” più del dovuto nei momenti topici e nei casi di crisi. Non si vuole qui sostenere che il lavoro debba diventare una “questione personale”, ma certo un apporto professionale arricchito da motivazione e coinvolgimento come normale bilanciamento è oggi in uno stato di crisi.

Tutta questa dinamica investe il mondo della Cybersecurity in modo ancora più decisivo: le persone sono considerate una prima linea di difesa e il primo motore di reazione e contenimento di incidenti di sicurezza; quindi, i fenomeni depressivi e demotivanti, aggiunti alla cronica pressione e burnout possono concorrere a generare crisi di sicurezza anche del tutto involontarie, ma con effetti domino in termini di danni e reputazione dell’organizzazione.

La soluzione per uscire dall’empasse esiste, ma richiede un profondo esame di coscienza, una riflessione del board e una altrettanto seria e rinnovata cultura delle risorse.

La fotografia attuale

Sono molte le aziende soprattutto in America che dopo la pandemia stanno lanciando un pericoloso monito ai loro lavoratori con effetti anche in Italia. Ne parla Alessandro Lubello per l'Internazionale ma anche il Wall Street Journal sottolineando la regola del "tutti sono rimpiazzabili" che, perlomeno qui in Italia, si conosce da anni nella forma "tutti sono utili, nessuno è indispensabile". Non che saperlo avvantaggi le organizzazioni italiane che sembrano soffrire delle stesse logiche americane, secondo cui, scrive Lubello, si verifica "una vera e propria 'guerra contro il talento', con dirigenti che se fino a qualche tempo fa non mancavano mai di lodare i dipendenti come 'il loro bene più prezioso', oggi non si fanno problemi dichiarare 'lavora di più, lamentati di meno e sii contento se hai ancora un lavoro".

La sicurezza informatica più efficace dipende dal 'caring' delle risorse umane.

D'altra parte, l'indagine European workforce study 2025 di Great place to work sembra certificare per l'Italia proprio questa incapacità di trattenere i talenti: il 40% dei lavoratori su base nazionale ha dichiarato l'intento di cambiare impiego, contro una media europea del 31% e con il picco tra le fasce più giovani, tra i 18 e i 24 anni. Cause scatenanti sono stipendi fermi e scarsa formazione e su tutto l'incapacità dei leader, che non sanno ascoltare i dipendenti. I giovani lamentano la scarsa capacità da parte degli imprenditori di fidelizzarli. Il presidente di Great place to work Italia Beniamino Bedusa, spiega che "ai manager italiani non mancano le competenze ma il loro rapporto con i dipendenti non funziona, non sanno valorizzarli". Dal rapporto emerge come solo il 44% degli impiegati si fidi del proprio capo contro un tasso di stima del 64% nel Nord Europa. Questo perché sottolinea Bedusa "i manager devono prendersi cura dei collaboratori, evitare di controllarli di continuo, dare loro fiducia e far capire come si raggiungono gli obiettivi". Nel campo della Cybersecurity questa disattenzione si concretizza anche con un imponente voragine di skill shortage (giunto allo strabiliante valore di 3,5 posizioni mancanti su base mondiale – secondo Cybercrime magazines, cioè mancanza di competenze, che se in parte è dovuta a scarsità di nuovo personale con le appropriate competenze di sicurezza, in parte è anche causato dalla cronica assenza di formazione specialistica nelle aziende, che lasciano invecchiare le capacità e competenze dei loro dipendenti, senza formarli continuamente in modo allineato alle esigenze del business in trasformazione digitale e ai temi di sicurezza informatica correlati. La linea spesso tenuta dalle aziende è "invitare all'uscita" i dipendenti "datati" con scivoli e accordi conciliativi di licenziamento, per poi assumere nuove leve, a costi bassi, dimenticando come nel frattempo perdano una importante bagaglio di conoscenze specifiche e specialistiche, che non potranno essere oggetto e soggetto di passaggio di consegne.

Istantanea a livello italiano

Per capire il fenomeno dello skill shortage e del conseguente fenomeno di fuga dei talenti verso l'estero (arrivato a oltre 97 mila unità) ne abbiamo parlato con Roberto Susanna Comunicazione e Ufficio Stampa di infocamere che di recente si è speso su questi temi su linkedin e a cui abbiamo chiesto quali possano essere le aspettative mancate e le retoriche che qui in Italia possono caratterizzare il mondo del lavoro: "Le aspettative disattese nel mercato del lavoro italiano, in particolare nei settori STEM e nella cybersecurity, sono uno degli elementi chiave per comprendere la crescente difficoltà nel trattenere talenti e nel contrastare fenomeni come lo skill shortage e il quiet quitting. Le nuove generazioni di professionisti entrano nel mondo del lavoro con un patrimonio di competenze tecnico-scientifiche solido e una visione chiara di cosa dovrebbe offrire un ambiente lavorativo moderno: percorsi di crescita strutturati, cultura del merito, aggiornamento costante e retribuzioni proporzionate alla complessità del ruolo. Queste aspettative, però, si scontrano spesso con contesti organizzativi rigidi, percorsi professionali poco trasparenti e un utilizzo parziale o distorto delle competenze acquisite. In molti casi, a mancare è una reale capacità di investimento nelle persone e nel loro sviluppo. Il risultato è un disallineamento tra ciò che il lavoratore è formato a fare e ciò che viene effettivamente chiamato a svolgere. Da qui, l'insoddisfazione che può spingere verso l'estero o verso forme di disimpegno interno, sempre più diffuse

anche in Italia".

Ma se sono visibili le conseguenze, la causa scatenante è da ricercarsi con doveroso scrupolo e proprio per questo chiediamo a Roberto Susanna di fornire una possibile motivazione su cosa manchi davvero nel mondo del lavoro oggi: "La retorica del cambiamento e dell'innovazione, da anni presente nel dibattito pubblico e privato, rappresenta oggi una delle principali ambiguità del sistema. Si parla con insistenza di "valorizzazione del talento", di "centralità delle persone" e di "trasformazione digitale", ma queste parole faticano a concretizzarsi in politiche aziendali efficaci. In molti casi, le imprese utilizzano un linguaggio orientato al futuro senza che questo si traduca in azioni coerenti: i giovani sono attratti con promesse di flessibilità e formazione continua, ma poi si ritrovano a operare in strutture ancora gerarchiche e lente, dove la vera innovazione è sporadica, e spesso solo di facciata. Il risultato è una perdita di credibilità del sistema: se il linguaggio aziendale promette evoluzione, ma l'esperienza quotidiana restituisce routine e scarsa valorizzazione, il rischio è che le parole diventino un guscio vuoto. Questa distanza alimenta la disillusione e contribuisce al calo dell'engagement, soprattutto tra i profili più preparati, quelli su cui oggi si fondano le sfide della competitività digitale".

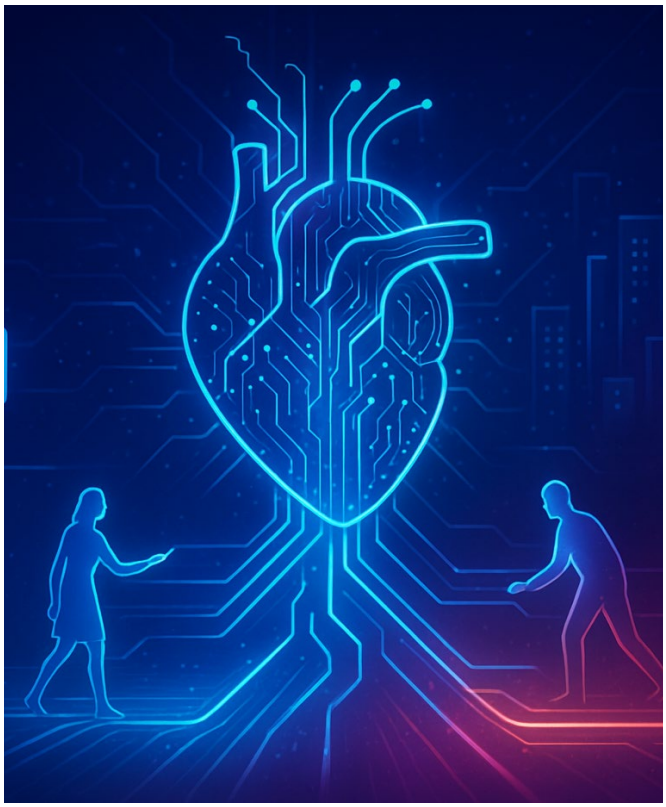
Conseguenze della mancata cura delle risorse

La distanza fra aspettative e realtà aziendale come scarsa attenzione alle risorse comporta diverse conseguenze, prima fra tutte il "quite quitting", quel fenomeno per cui si resta al lavoro da insoddisfatti senza cercare miglioramento in altri luoghi di lavoro, "spegnendo" e riducendo le attività allo stretto indispensabile nell'organizzazione in cui si è occupati. Un 'grande distacco' che secondo il rapporto dell'Osservatorio HR Innovation practice interessa il l 12% dei lavoratori italiani (circa 2,3 milioni di lavoratori) che non si sente valorizzato nei propri talenti. Di contro esiste anche un 6% circa 1,1 milioni di lavoratori, cosiddetti Job Creeper, che non riescono a smettere di lavorare, anche sacrificando la propria vita privata. Fenomeni agli opposti, ma che evidenziano un malessere diffuso di insoddisfazione lavorativa. Fa pensare come secondo il rapporto dell'osservatorio solo l'11% sta bene su tutte e tre le dimensioni del benessere lavorativo: psicologica, relazionale e fisica. E gli altri? È possibile che nella percentuale rimanente sia ricompreso anche il ghostworking un fenomeno evidenziato dallo studio Resume now pubblicato dal New York Post che caratterizza i lavoratori che stressati fino al burn out, si rifugiano in attività simulate: fingono di essere indaffarati al lavoro per non essere ulteriormente caricati di task e attività.

Rinnovare la cultura verso le risorse

La ricetta per un vero cambio di passo deve necessariamente rimettere la risorsa al centro dei processi organizzativi, dei ruoli, delle mansioni e delle deleghe. L'improvvisazione su base emergenza per qualsiasi ruolo aziendale, ma in particolar modo per la Sicurezza informatica non può più essere una regola. Il progressivo impoverimento organizzativo, la semplificazione progressiva dei ruoli senza più sfumatura e appiattiti a tre livelli basici di tecnico, manager e venditore, non ha senso. È necessario ripensare a strutture organizzative che tengano conto di attività specialistiche ed in particolare se si guarda alla sicurezza informatica a tutti gli ambiti specialistici di cui è composta (defence, intelligence, GRC, VA/PT, operations, solo per citare le principali), fornendo ai diversi professionisti ruoli chiari e definiti, deleghe appropriate e budget commisurati, rinunciando al vetusto "on-man-band", ovvero, un professionista caricato di tanti ruoli e mansioni di security come un unico parafulmine per tutte le stagioni, senza budget e senza deleghe e virare con decisione verso un sistema organizzativo che possa permettere al singolo dipendente un reale apporto all'organizzazione, una responsabile contribuzione su base delega per agire e decidere, un progressivo contributo formativo per mantenerlo aggiornato alla trasformazione del business e un opportuno riconoscimento a raggiungimento degli obiettivi.

Il solo rifugiandosi nella sostituzione di risorse umane con agenti di AI come automi automatizzati, non potrà che ulteriormente inaridire i luoghi di lavoro perdendo quello spunto alla creatività e innovazione che da sempre è patrimonio degli esseri umani e non dei suoi strumenti. Ai posteri…..



AI – domande e risposte facili facili – chi siamo noi per l'AI

A cura di Gianpiero Cozzolino

Il riconoscimento facciale e gli altri sensori

Una delle prime forme di "intelligenza artificiale" di cui si è sentito parlare, già qualche anno fa, è il riconoscimento facciale, ossia la capacità di riconoscere una persona dall'immagine del viso. Tale capacità ha moltissimi possibili utilizzi: da una parte utili, come le misure di sicurezza avanzate (per il controllo delle autorizzazioni per dati o azioni critiche; come, per esempio, lo sblocco degli smartphone); dall'altre pericolose, come la sorveglianza di massa (per esempio la schedatura delle persone che frequentano luoghi a carattere sensibile).

Analogamente al riconoscimento facciale, che utilizza videocamere, esistono moltissimi tipi diversi di sensori che raccolgono i dati più disparati (voce, postura, abitudini, preferenze, opinioni, debolezze, etc.), e dai cui è possibile desumere una sorta di identikit "logico" di ognuno di noi. La quantità di dati è così grande che per trattarli non è possibile usare algoritmi tradizionali, ma è necessario ricorrere alle tecnologie di machine/deep learning, che sono alla base dell'intelligenza artificiale, per estrarre dei modelli che descrivono certi nostri aspetti, e che a loro volta possono essere utilizzati per "riconoscerci" -PROFILARCI- confrontandoli con analoghi modelli elaborati in un dato momento con i dati appena raccolti.

Social engineering

Anche il social engineering, cioè la raccolta di informazioni pubbliche (o meno) di un individuo a scopo di riutilizzo fraudolento, non è certo una novità: nasce in tempi in cui non esisteva internet, ha avuto un primo grande salto con l'avvento dei social network (utilizzando quindi informazioni divulgate direttamente da noi) e sta avendo un secondo grande salto con le capacità elaborative dell'intelligenza artificiale, grazie alla capacità di correlare con efficienza sbalorditiva dati provenienti da fonti diverse, fornendo profili estremamente precisi.

Con tale precisione, il furto d'identità o il ricatto diventa

un gioco da ragazzi. Infatti, grazia appunto ai dati disponibili ed alle tecnologie, ogni attività svolta non in presenza è a rischio, poiché i processi di riconoscimento comunemente utilizzati possono essere facilmente aggirati tramite dati falsi (immagini, audio, documenti d'identità) appositamente generati (per questo motivo le famigerate password, purché ben protette ed accompagnate da sistemi ulteriori, cosiddetti "multi fattori", continuano ad essere fondamentali); così come è facile reperire, o persino generare, informazioni "imbarazzanti" che possono essere utilizzate come oggetto di minaccia e ritorsione.

Ma non solo: oltre all'utilizzo di informazioni estremamente precise, c'è la possibilità di effettuare previsioni di comportamenti in determinati contesti, sia a livello di gruppi di persone ma anche a livello individuale, il che comporta il grande rischio di esclusioni o discriminazioni.

Cosa ne penso?

Le tecnologie e applicazioni appena descritte presentano forse i maggiori rischi in assoluto. A causa della varietà di fonti di dati e della pervasività di sensori (ricordiamo che molti di essi li portiamo noi stessi addosso, oppure entrano nelle nostre case con gli oggetti "smart"), ormai non c'è nessuno che possa dirsi al sicuro, ma contemporaneamente non ci si rende conto di quali e quanti dati che ci riguardano vengono raccolti, e soprattutto come possono essere utilizzati a nostra insaputa; il risultato è una grave mancanza di consapevolezza e, di conseguenza, di autodifesa. Non dimentichiamo che i fatti di cronaca più o meno specialistica raccontano spesso di soggetti (pubblici e privati, noti e meno noti) che eludono costantemente ogni normativa o principio etico in nome dei propri interessi.

Rimane sempre in sottofondo il problema di ogni sistema di intelligenza artificiale: i possibili errori (falsi positivi, falsi negativi, "allucinazioni", previsioni sbagliate), la sfida che abbiamo di fronte sarà di capirne l'origine, vera falsa generata ricreata sviluppata integrata dedotta, e quindi di analizzarla su una base etica globale, che richiederà l'impegno globale di ogni testa e macchina pensante.

Non c'è più nessuno al sicuro: i nostri dati ci seguono ovunque, spesso senza che ce ne accorgiamo.

L’illusione della sicurezza: quando la formazione arriva post-mortem

La falsa competenza uccide la sicurezza, un errore alla volta

A cura di Silvia Felici

Nel panorama attuale della sicurezza informatica, è sempre più diffusa una forma di competenza posticcia, acquisita in risposta a eventi critici piuttosto che tramite un percorso strutturato. Si tratta di una conoscenza reattiva, spesso elevata impropriamente a “esperienza”, nata non dalla preparazione ma dall’urto con un incidente di sicurezza.

Molte organizzazioni assimilano la cybersecurity alla gestione delle conseguenze, trascurando la preparazione preventiva. In questo contesto, la formazione viene spesso relegata a voce secondaria nei budget, percepita come un onere piuttosto che come un pilastro essenziale della resilienza digitale.

Tale atteggiamento ha implicazioni tangibili. L’assenza di una cultura formativa diffusa e continuativa si traduce in vulnerabilità operative sistemiche, alimentate da una fiducia mal riposta nella sola tecnologia o nella reattività dei sistemi.

Due casi importanti

Alcuni eventi del 2025 rendono evidente il gap tra percezione di competenza e preparazione reale.

- **Marks & Spencer (UK):**

  Ad aprile, un attacco di social engineering ha colpito i sistemi tramite un accesso indiretto a un fornitore. La risposta ha rivelato carenze nel riconoscimento delle minacce, nella gestione delle credenziali e nelle procedure di verifica. Il danno stimato supera i 300 milioni di sterline. Dopo l’incidente, l’azienda ha riconosciuto che la formazione era stata considerata “sufficiente” fino a quel momento

- **Bank Sepah (Iran):**

  A marzo, un gruppo noto come “Codebreakers” ha ottenuto accesso prolungato ai sistemi centrali della banca, esfiltrando dati di oltre 40 milioni di clienti. L’analisi forense ha identificato una debolezza nei controlli dei privilegi, ma anche una scarsa consapevolezza interna del personale sugli indicatori di compromissione. Nessun training interno era stato condotto nell’anno precedente.

Questi eventi non sono anomalie, ma rappresentazioni di una tendenza generalizzata: la cybersecurity viene trattata come un’attività tecnica e isolata, non come una responsabilità distribuita all’interno dell’organizzazione.

Il ruolo critico della formazione continua

La sicurezza informatica è un dominio a evoluzione rapida, caratterizzato da vettori d’attacco in costante trasformazione. In questo contesto, l’aggiornamento professionale non può essere considerato accessorio.

Molti incidenti gravi degli ultimi anni non sono stati causati da sofisticate vulnerabilità zero-day, ma da errori umani spesso legati ad una formazione insufficiente, come ad esempio: clic su link malevoli, uso reiterato di password deboli, mancata segnalazione di comportamenti anomali.

L’approccio “una tantum” alla formazione (tipicamente una sessione all’anno, spesso in modalità e-learning passiva) è del tutto inadeguato. L’efficacia formativa dipende da frequenza, rilevanza e aderenza al contesto lavorativo. In assenza di queste condizioni, la conoscenza degrada rapidamente, lasciando spazio a comportamenti inconsapevoli.

Un altro elemento spesso trascurato è la diversificazione della formazione per profilo. Un amministratore di sistema, un analista di dati, un commerciale o un manager devono ricevere contenuti differenti, calibrati sul proprio ruolo, livello di esposizione e grado di autonomia operativa. Tuttavia, in molte realtà aziendali, la formazione viene proposta come pacchetto standard per tutti, con impatto formativo minimo.

La falsa sicurezza dell’infrastruttura

Investire in soluzioni tecnologiche avanzate senza formare chi le utilizza rappresenta un paradosso ricorrente. L’illusione che la sicurezza derivi esclusivamente dall’adozione di strumenti di protezione ignora il fatto che la maggior parte delle tecnologie dipende da configurazioni corrette, aggiornamenti puntuali e comportamenti informati da parte degli operatori.

L’assenza di una componente formativa produce quello che in ambito accademico è stato definito “tecnocentrismo cieco”: una fiducia eccessiva nella componen-

te tecnologica a discapito del fattore umano. Questo approccio porta inevitabilmente a un disallineamento tra capacità nominale dei sistemi e resilienza effettiva dell'organizzazione.

Una questione culturale prima che tecnica

Attribuire i fallimenti alla "disattenzione dei dipendenti" è una semplificazione che elude il nodo centrale: l'errore umano, in ambito cyber, è quasi sempre il risultato di un contesto inadeguato. Dove non c'è cultura della sicurezza, l'errore è un prodotto sistemico, non individuale.

Non è sufficiente comunicare regole. Serve costruire comprensione. La security awareness non è un documento firmato all'ingresso, ma un processo continuo. Le organizzazioni che hanno integrato programmi formativi strutturati riportano una maggiore capacità di rilevamento precoce degli attacchi e una minore esposizione a rischi operativi.

La sicurezza informatica non può essere affidata esclusivamente a prodotti e strumenti: senza formazione diffusa, ogni sistema rimane fragile.

Dimensione non è protezione

Le PMI spesso si considerano "troppo piccole per essere un bersaglio", dimenticando che gli attacchi odierni sono in larga parte opportunistici. Gli strumenti di attacco si sono automatizzati, e gli attori malevoli colpiscono vulnerabilità note, indipendentemente dalla rilevanza mediatica della vittima.

In questo contesto, la mancanza di formazione e di consapevolezza rappresenta una superficie d'attacco più ampia della dimensione dell'infrastruttura stessa.

Formazione come strategia

Per affrontare efficacemente la minaccia, la formazione deve essere inquadrata come elemento strategico. Non solo come risposta alle normative o come iniziativa di compliance, ma come strumento di prevenzione.

Tra le buone pratiche documentate troviamo:

- programmi di micro-learning ciclici;
- esercitazioni di phishing simulato;
- tabletop exercises per manager e C-level;
- percorsi di aggiornamento specifici per ruoli tecnici;
- integrazione della formazione nei piani di onboarding.

Le organizzazioni che hanno investito in questi modelli riportano, secondo i dati di SANS e CISA, una riduzione significativa dell'impatto medio per incidente, nonché tempi di risposta più rapidi.

Considerazioni conclusive

La sicurezza informatica non può essere affidata esclusivamente a prodotti e strumenti. Senza una base formativa diffusa, il sistema rimane fragile, indipendentemente dalla tecnologia implementata.

Rinviare o ridurre la formazione equivale, in molti casi, a esternalizzare il rischio all'intera organizzazione. Una strategia sostenibile richiede invece una visione a lungo termine, in cui la competenza sia distribuita e continuamente rinnovata.

In un ecosistema digitale dove la superficie d'attacco si espande, il vero elemento differenziante non sarà tanto l'adozione dell'ultima tecnologia, quanto la qualità della preparazione delle persone che ne gestiscono l'uso quotidiano.

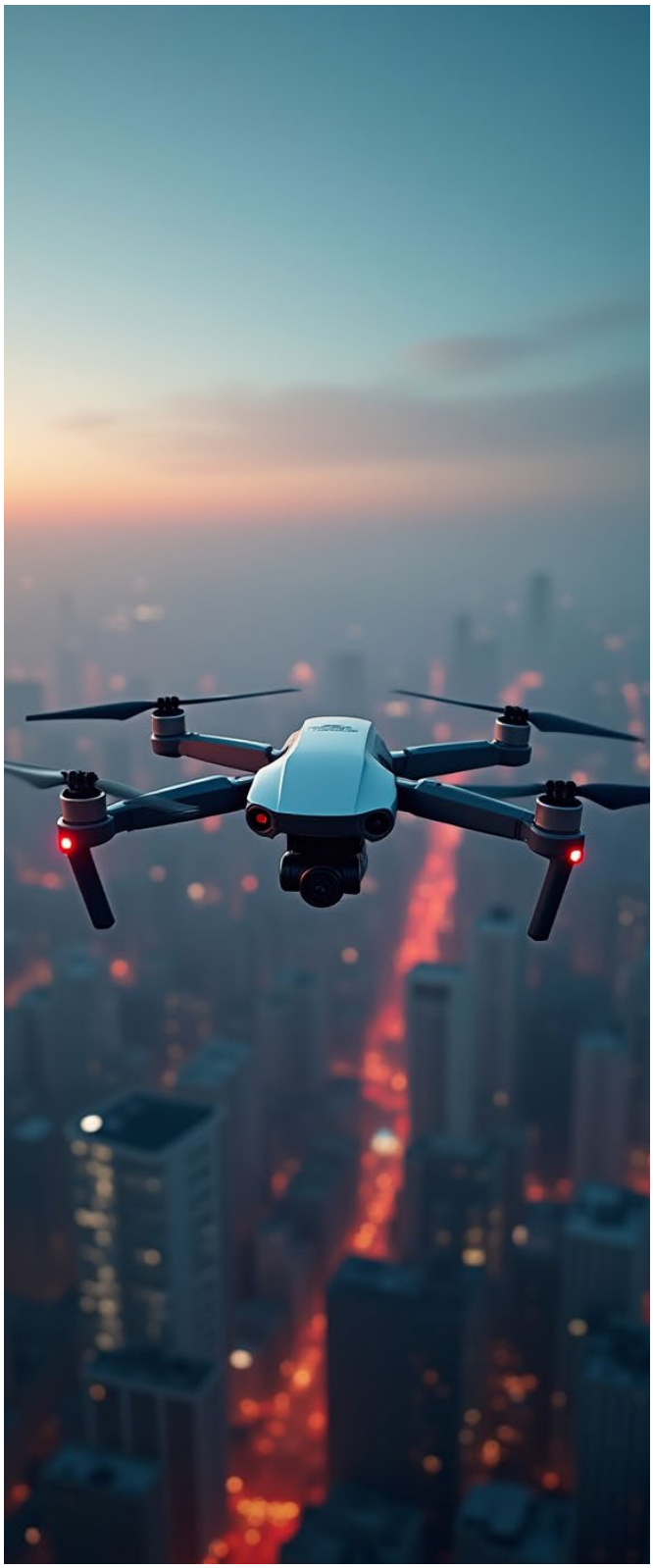
Cybersecurity dei droni: proteggere il cielo digitale tra minacce emergenti e soluzioni

A cura di Francesco Iezzi

L'utilizzo dei droni, noti come UAV (Unmanned Aerial Vehicles), si è ormai esteso ben oltre il settore militare, conquistando ambiti civili, industriali e infrastrutturali. Tuttavia, con la loro crescente diffusione, si è ampliato anche il potenziale di esposizione a minacce informatiche. La cybersecurity degli UAV rappresenta oggi una frontiera critica nella sicurezza digitale e fisica, con rischi concreti che spaziano dallo spionaggio industriale al sabotaggio infrastrutturale.

Tra le vulnerabilità più note vi è il GPS spoofing, una tecnica che consente di ingannare il sistema di navigazione del drone, dirottandolo su rotte non previste. Studi pubblicati su PMC nel 2021 hanno dimostrato come sia possibile, anche con hardware commerciale, alterare la posizione percepita da UAV civili, portandoli a schiantarsi o a varcare spazi aerei protetti. A queste minacce si aggiungono gli attacchi Wi-Fi, in particolare quelli basati su deauthentication (De-Auth) e Denial of Service (DoS). Un'analisi condotta dall'IEEE ha evidenziato come droni commerciali, utilizzando dispositivi semplici come il WiFi Pineapple, possano essere espulsi dalla rete del controller o addirittura "hijackati" durante il volo. Il caso del Raspberry Pi impiegato per attacchi Man-in-the-Middle (MITM) in volo rappresenta un precedente inquietante. Particolare attenzione merita inoltre il sistema DroneID dei droni DJI, largamente diffusi. Questo protocollo, utilizzato per identificare il drone e il suo operatore, è stato reverse-engineerizzato da diversi ricercatori, mettendo in luce la mancanza di crittografia e la conseguente esposizione alla localizzazione dell'operatore, anche in contesti sensibili come zone di guerra.

Queste minacce non sono solo teoriche. La CISA statunitense ha pubblicato alert specifici sull'uso di UAV per il sabotaggio di infrastrutture critiche, come centrali elettriche e impianti industriali. In tali scenari, i droni sono stati utilizzati per sorvolare impianti, catturare informazioni riservate o tentare attacchi diretti. Un altro caso documentato riguarda l'impiego di attacchi MITM durante il volo, in cui l'aggressore ha preso il controllo del flusso dati tra drone e operatore. Inoltre, come riportato da Wired, il sistema DroneID è stato utilizzato attivamente in contesti bellici per identificare e colpire i piloti di droni, sollevando seri problemi di sicurezza personale e militare.



Per contrastare queste minacce, la comunità scientifica sta sviluppando soluzioni architetturali innovative. Tra le più promettenti vi è l'integrazione tra blockchain, SDN (Software Defined Networking) e edge computing, come illustrato nel paper "Fast, Reliable, and Secure Drone Communication". Queste tecnologie consentono una maggiore resilienza delle comunicazioni UAV, riducendo i rischi di spoofing e MITM. Il framework SDNES (Secure Drone Network Edge Service) propone un modello decentralizzato in grado di garantire l'integrità delle comunicazioni tra droni e stazioni di controllo. Parallelamente, sistemi come D3S offrono una valutazione dinamica del livello di sicurezza del drone, attraverso punteggi derivati da test di attacco quali flooding, replay e deauthentication. Sul fronte normativo, la direttiva europea NIS2 ha introdotto obblighi specifici per i droni utilizzati in ambito critico, imponendo piani di gestione del rischio, sistemi di incident response e audit periodici.

Negli Stati Uniti, la Federal Aviation Administration ha reso obbligatorio il sistema Remote ID, con l'obiettivo di identificare e monitorare i droni in tempo reale. Tuttavia, queste misure hanno sollevato preoccupazioni riguardo alla privacy e alla sorveglianza, soprattutto quando sono combinate con tecnologie biometriche o telecamere ad alta risoluzione. Organizzazioni come EPIC e AZoRobotics hanno espresso dubbi sull'uso dei droni in contesti urbani, in particolare per quanto riguarda la raccolta non trasparente di dati personali, l'uso non consensuale di riconoscimento facciale e l'assenza di linee guida etiche chiare.

I droni rappresentano oggi una sfida cruciale per la sicurezza informatica. Non sono più soltanto strumenti aerei, ma nodi mobili di una rete digitale sempre più vulnerabile. Proteggerli significa tutelare infrastrutture, persone e dati. È quindi essenziale che aziende, enti regolatori e operatori sviluppino una strategia di sicurezza by design, che consideri non solo le minacce tecniche, ma anche le implicazioni etiche e legali connesse all'uso di queste tecnologie.

I droni non sono più soltanto strumenti aerei, ma nodi mobili di una rete digitale sempre più vulnerabile.

Restare umani nell'era dell'IA: la complessa sfida delle professionalità digitali

A cura di Andrea Lisi e Chiara Ramirez

Nell'attuale panorama digitale europeo, caratterizzato da normative che spesso si accavallano o sembrano contraddirsi tra loro, si avverte l'impellente necessità di una via interpretativa chiara, un metodo che aiuti a non sentirsi smarriti all'interno del dedalo di disposizioni e che riesca a far rinsavire da quel senso di vertigine che accompagna ormai da tempo l'innovazione tecnologica.

Un metodo che può essere adottato solo da chi interpreta la digital compliance come quell'unico faro strategico in grado di guidare le organizzazioni (pubbliche e private) che si ritrovano a dover navigare il burrascoso mare normativo che contraddistingue il diritto applicato all'informatica. Parliamo di professionalità cruciali, di natura intrinsecamente multidisciplinare, vocate alla compliance e, quindi, sempre più determinanti per il nostro futuro digitale: Data Protection Officer (DPO), Responsabili della conservazione (RDC) e Archivisti digitali, Manager della trasformazione digitale, Referenti della cybersicurezza, fino ai più recenti Eticisti dell'IA. Tutte figure chiamate a governare il complesso contesto digitale con spirito critico e visione interdisciplinare, con l'obiettivo non solo di applicare le singole norme, ma di interpretarle con consapevolezza, autorevolezza e attenzione antropocentrica, mantenendo come solidi punti fermi i nostri diritti fondamentali e la dignità dell'uomo.

È questa, dunque, la vera sfida dell'attuale universo digitale: non inseguire la tecnologia come fine, ma come mezzo, non abbandonarsi al suo fascino, ma attraversarla e governarla da esseri umani. Perché l'innovazione, se non guidata da competenza e consapevolezza, può trasformarsi in un disarmante processo di disumanizzazione, tanto moderno quanto pericoloso.

Nel mondo dei bit non è più un mistero il fatto di essere costantemente "datificati". Le nostre identità si frammentano in granelli di informazione virtuali, spesso aggregati e profilati in modo opaco all'interno degli innumerevoli multiversi social nei quali abbiamo trasferito le nostre vite. A questa semplificazione del sé non può che corrispondere una perdita di controllo e della capacità di riconoscerci nelle nostre stesse tracce digitali; e così l'agognata trasparenza, così tanto proclamata, finisce per diventare una burocrazia svogliata che non illumina, ma confonde.

In questo scenario, il professionista della digital compliance ha il compito, ma soprattutto la responsabilità, di recuperare il senso critico, di riportare logica e interpretazione in un contesto sempre più algoritmico e alienante. E per farlo deve ancorarsi a una cultura solida, non solo giuridica, ma anche etica e umanistica.

In un contesto normativo in così rapida evoluzione, dove la pluralità delle fonti spesso genera incertezza, ciò che può fare la differenza è un metodo di lavoro chiaro, rigoroso, orientato alla persona, nelle mani delle persone. Non un modello astratto o tecnicistico, ma un percorso di coscienza (e conoscenza) normativa, capace di restituire equilibrio tra controllo e fiducia, tra innovazione e umanità.

Per tali motivi, le professionalità digitali, oggi, si misurano non solo nella padronanza di strumenti e competenze, ma anche nella capacità di restare vigili, di riconoscere che nessuno può davvero dirsi arrivato nell'interpretazione dell'IA o degli algoritmi. L'unica vera competenza distintiva del professionista è la consapevolezza, saper restare umani in un mondo che spinge sempre di più verso l'automazione e la disgregazione del sé, è recuperare la lentezza dell'interprete, la pazienza dell'artigiano, la percezione di chi sa che il processo di trasformazione digitale, se non parte dalla persona, è destinato, nel tempo, a fallire.

La vera sfida non è inseguire la tecnologia, ma governarla restando umani.

Nel futuro della digital compliance non può esserci esclusivamente la macchina, ma l'uomo, e per quanto possa sembrare un'ovvietà, ad oggi non lo è affatto. Adesso spetta a noi professionisti riabilitare le coscienze, guidare le organizzazioni e impedire pericolose prese di potere che rischiano di incrinare principi, diritti e dignità sui quali abbiamo costruite le nostre democrazie. Un compito non facile, ma necessario per continuare a tenere ben salda quella bussola orientativa e non lasciarsi trasportare da correnti sempre più impetuose che ormai caratterizzano la nostra realtà digitale.

Analizziamo allora più da vicino le professionalità dedite alla digital compliance che devono avere un ruolo sempre più strategico all'interno delle organizzazioni per presidiare con attenzione questi fondamentali temi.

Il Data Protection Officer e il Responsabile della conservazione: i custodi del nostro patrimonio informativo

Le realtà pubbliche e private che si occupano della gestione di dati personali hanno l'obbligo di designare, così come stabilito dal Regolamento UE 2016/679 (GDPR), il Data Protection Officer (DPO), o Responsabile della protezione dei dati. Si tratta di una figura indispensabile per la corretta governance di dati e informazioni la cui funzione strategica risiede nel monitoraggio di processi e procedure legati all'ambito della data protection.

Accanto al DPO c'è un'altra figura obbligatoria per chi gestisce e conserva documenti informatici, in ambito pubblico e privato: si tratta del Responsabile della conservazione (RDC) o anche definibile come Document Preservation Officer (condividendo così l'acronimo con il più noto Data Protection Officer). Chi sviluppa fatturazione elettronica, riceve PEC e usa firme digitali o sigilli elettronici, ha l'obbligo ex lege di dotarsi di un sistema affidabile di conservazione e affidarne il coordinamento a questa figura prevista dal Codice dell'amministrazione digitale, ribadita in ultimo dalle Linee Guida AgID.

Guidare la trasformazione digitale grazie al Chief Digital Officer (CDO)

Le organizzazioni pubbliche e private devono designare un Chief Digital Officer (CDO), conosciuto anche nelle PA come Responsabile per la transizione digitale (RTD), introdotto dal Codice dell'Amministrazione digitale. Si tratta di un professionista con competenze trasversali in ambito informatico, giuridico e manageriale il cui compito è garantire che la transizione digitale, in quanto processo in continua evoluzione, risponda adeguatamente alle nuove esigenze giuridiche ed etiche.

Il Chief Information Security Officer (CISO): il garante della sicurezza delle nostre identità e dei nostri dati

Il Chief Information Security Officer (CISO), o Responsabile della Cybersicurezza è il professionista che sia in grado di affrontare le nuove sfide poste dalle evoluzioni in ambito di cybersicurezza, con un approccio multidisciplinare, pratico e orientato alle reali esigenze della digitalità, secondo quanto previsto dalla Legge n. 90/2024 e dagli adempimenti della Direttiva NIS 2 (2022/2555/UE), del D.Lgs. n. 138/2024 e dello stesso GDPR.

AI and Data Ethics Compliance Manager (AIDEC) per una visione etica e globale del moderno contesto digitale

Parlare di nuove tecnologie e, nello specifico, di intelligenza artificiale, significa avere non soltanto solide competenze in ambito tecnico e giuridico, ma saper approcciare l'innovazione in maniera etica, così da integrare l'osservanza delle normative a una visione globale della realtà che ci circonda. In uno scenario orientato alla perfetta armonia tra etica e diritto, infatti, i principi di accountability e trasparenza rappresentano le colonne portanti per le organizzazioni pubbliche e private orientate alla digitalizzazione che dovranno, pertanto, introdurre l'etica all'interno della propria compliance digitale, prevedendo l'adozione di nuove procedure e la nomina di figure strategiche preposte a tale scopo. Tra queste, emerge una nuova professionalità destinata a distinguersi nel panorama digitale odierno: l'AI and Data Ethics Compliance Manager (AIDEC) o Esperto di Etica Digitale.

Queste cinque figure professionali, caratterizzate da solide competenze tecniche, giuridiche ed etiche sono ormai essenziali per guidare la trasformazione digitale di ogni organizzazione pubblica e privata.

La Digitalaw Academy, anche attraverso il DigitaLaw Department recentemente costituito presso il CUIRIF, e con la collaborazione scientifica dello Studio Legale Lisi, svilupperà percorsi di ricerca e formazione per garantire un solido e consapevole sviluppo di queste nuove professionalità indispensabili per presidiare con successo i nuovi mercati digitali.

AI e Cybersicurezza

A cura di Graziella Soluri

Per un ambiente digitale sicuro è fondamentale la sinergia tra esperti umani e algoritmi di AI.

Preambolo

Negli ultimi anni, l'intelligenza artificiale ha rivoluzionato molti settori, inclusa la cybersecurity; stiamo assistendo infatti a una vera e propria rivoluzione tecnologica legata allo sviluppo e all'utilizzo dell'AI, con sistemi automatizzati che hanno raggiunto un livello di maturità tale da poter svolgere compiti sempre più raffinati e complessi, che fino a poco tempo fa sembravano essere esclusivamente alla portata di tecnici specializzati umani.

Questa capacità dell'AI di "industrializzare" molte attività dell'intelletto umano ha posto un legittimo quesito ovvero se non sia possibile delegare ad essa la gestione, anche parziale, della sicurezza di un sistema informatico a fronte della capacità degli algoritmi di AI di rendere veloci ed efficaci le risposte alle minacce digitali sempre più complesse; tuttavia, l'adozione non supervisionata degli algoritmi comporta rischi significativi connessi alla loro vulnerabilità intrinseca a causa della sofisticatezza degli attacchi avversari e delle difficoltà nel comprendere la semantica delle minacce che spinge gli attaccanti a sfruttare le debolezze di questi sistemi.

In questo contesto, l'integrazione tra AI e cybersecurity non è più solo una strategia opzionale, ma una necessità per contrastare la crescente complessità ed efficacia degli attacchi informatici; tuttavia, la carenza globale di professionisti qualificati nel settore rende l'impiego di algoritmi per difendere aziende e professionisti da attacchi malevoli un alleato prezioso, ma non un sostituto del lavoro umano; pertanto, questo breve scritto ha come scopo quello di evidenziare la necessità di integrare le grandi capacità dell'AI in materia di sicurezza digitale con le competenze critiche e creative degli esperti umani.

Ebbene, a parere di chi scrive, per un futuro digitale resiliente, è fondamentale bilanciare l'innovazione tecnologica con una gestione proattiva del rischio e investire nella formazione continua, promuovendo una sinergia strategica tra AI e intelletto umano.

Il rapporto tra AI e Cybersecurity: benefici e sfide

Prendiamo in esame i vantaggi dell'uso dell'AI nell'ambito della sicurezza delle infrastrutture digitali delle organizzazioni pubblico o private.

L'intelligenza artificiale e gli algoritmi di Machine Learning (ML) sono strumenti utili al potenziamento delle misure difensive del perimetro di sicurezza di organizzazioni pubbliche e private perché forniscono mezzi avanzati per identificare, prevenire e rispondere alle minacce malevole in modo più efficiente. L'AI ottimizza la velocità e l'efficacia delle risposte agli attacchi, accelerando processi di analisi dei dati che un essere umano non potrebbe mai raggiungere con le proprie facoltà.

In particolare, la sua capacità di elaborare e correlare enormi volumi di dati provenienti da diverse fonti, anche quelle isolate, permette di identificare minacce nascoste e schemi ripetitivi che rivelano la presenza di attacchi informatici in corso per contrastarli efficacemente e proteggere il patrimonio informativo dell'attaccato.

Tra le varie applicazioni, ad esempio, l'AI migliora il rilevamento dei malware, estendendo il raggio d'azione degli antivirus per individuare varianti complesse; permette un rilevamento avanzato delle minacce e l'identificazione proattiva di vulnerabilità, come dimostrato dalla capacità di identificare attacchi non ancora noti basandosi

su comportamenti e framework di attacchi passati. Gli algoritmi di AI possono, ad esempio, analizzare il comportamento degli utenti e il traffico di rete per identificare anomalie e attività sospette e, svolgere analisi utili nel prevenire minacce interne e rilevare tentativi di takeover degli account, inoltre gli algoritmi intelligenti consentono risposte automatizzate e la mitigazione degli incidenti di cybersecurity mediante blocco degli indirizzi IP sospetti e messa in quarantena di richieste infette provenienti da dispositivi non noti o prevedere l'avvio di procedure di risposta automatizzate.

Questo riduce i tempi di inattività e minimizza i danni grazie alla tempestiva reattività all'attacco. Inoltre, con gli algoritmi di Ai si possono automatizzare attività di sicurezza ripetitive come la gestione delle identità, l'analisi dei log e la correzione delle vulnerabilità, riducendo la dipendenza dal lavoro manuale e migliorando l'efficienza dei controlli di sicurezza al fine di liberare risorse umane da destinare a compiti più complessi e strategici.

Algoritmi di AI che auto-apprendono offrono anche la capacità di mantenere le difese sempre aggiornate, poiché gli algoritmi di ML possono essere addestrati continuamente, anche in modo autonomo predisponendo, in ogni caso, una verifica periodica umana del dataset implementato, con nuovi dati per meglio adattarli alle minacce emergenti, riducendo al contempo i falsi positivi e gli errori.

In sintesi, un ottimo sistema di sicurezza correttamente implementato e integrato con algoritmi di AI addestrati sulle minacce passate e potenziali, supervisionato e aggiornato, accanto a personale umano altamente specializzato sono la soluzione sinergica più idonea a contrastare attacchi informatici sempre più frequenti, precisi, efficaci e dannosi.

L'evoluzione delle minacce mediante algoritmi di AI

Nonostante i vantaggi, affidarsi completamente a sistemi di AI per la sicurezza informatica comporta rischi significativi per i limiti intrinseci insiti nei sistemi e per la facilità con cui gli attacchi possono essere realizzati con l'uso di sistemi di Aia scopo malevolo parimenti potenti e pervasivi.

Solo la sinergia tra AI e intelletto umano può garantire un futuro digitale sicuro.

Pertanto, un problema fondamentale dell'impiego di sistemi di ML nella cybersecurity è la presenza di un avversario non più solo umano e molto abile, ma o potenziato dagli algoritmi di AI o come autonomo agente razionale, in grado di elaborare strategie efficaci finalizzate a sfruttare le debolezze dei sistemi di riconoscimento delle minacce e penetrare le difese.

Le AI hanno infatti problemi di sicurezza intrinseci che sono spesso trascurati e solo il 40% delle aziende che utilizzano questi algoritmi hanno introdotto pratiche di sicurezza specifiche per irrobustire la difesa predisposta con questa tecnologia; purtroppo, infatti, molte delle soluzioni adottate non proteggono contro attacchi specifici alle AI, come, ad esempio, le backdoor nei modelli di machine learning.

C'è il rischio quindi che l'uso dell'AI come strumento di sicurezza si trasformi in un boomerang; in particolare, gli algoritmi di ML, pur essendo accuratissimi, non sono infallibili.

Essi sono agenti puramente sintattici, che non possono fare riferimento alle proprietà semantiche delle informazioni e, questo difetto intrinseco, rende gli algoritmi classificatori aggirabili, come dimostrato dagli attacchi che bypassano i Web Application Firewall (WAF) tramite trasformazioni sintattiche che preservano la semantica malevola.

La cybersecurity richiede tecnologia avanzata, ma soprattutto competenze umane critiche.

Le minacce AI-driven includono, ad esempio, campagne di disinformazione e manipolazione dell'AI generativa capaci di incidere significativamente sui diritti e le libertà fondamentali degli utenti finali. Attacchi come il data poisoning e il data slow poisoning possono distorcere la capacità di riconoscimento di un sistema con minime perturbazioni nel modello di apprendimento.

I cyber criminali stanno anch'essi implementando l'AI per creare nuove minacce, come gli attacchi "AI driven dumpster diving" per estrarre informazioni personali, i "credential stuffing" per accedere a un grande numero di account e rubare dati sensibili, e le "spear phishing email" generate dall'AI per aumentare il successo degli attacchi.

Inoltre, l'AI, essendo una tecnologia relativamente nuova, non è ancora sufficientemente affidabile per operare in modo completamente indipendente e potrebbe non essere altrettanto efficace nel rilevare minacce nuove ed emergenti, basandosi, il suo funzionamento, su dati storici, seppur periodicamente aggiornati.

I sistemi di AI che auto-apprendono presentano molte vulnerabilità e sono esposte a corruzione o manipolazione dei dataset di input, inoltre, la mancanza di trasparenza nei loro modelli decisionali rende difficile ricostruire ciò e in che modo si è diffusa la violazione di sicurezza che ha alterato il sistema e complessa l'analisi forense post-attacco, impedendo una piena comprensione di come e perché una violazione sia avvenuta. Pertanto, è essenziale combinare l'impiego di sistemi di sicurezza gestiti con l'AI con controlli umani e strategie di sicurezza multilivello per prevenire o mitigare rischi futuri.

La carenza di competenze nel settore

Ulteriore problema da gestire in materia di sicurezza informatica è la formazione del personale che viene descritto come l'anello debole delle misure preventive adottate dall'organizzazione per far fronte ad attacchi malevoli.

La disponibilità di personale qualificato è un problema significativo a livello globale nel settore della cybersecurity; l'Europa, ad esempio, soffre di una carenza di talenti stimata in 500.000 professionisti. Assumere personale qualificato può essere costoso, e la necessità di formazione e certificazione continua è un impegno gravoso per le aziende ma remunerativo sul lungo periodo.

Infatti, sebbene gli strumenti di sicurezza basati sull'AI possano ridurre la necessità di personale specializzato e i costi associati, è essenziale riconoscere il fatto che a livello globale gruppi di esperti di cybersecurity in grado di implementare e supervisionare strumenti di AI impiegati per la sicurezza informatica anche basati sul ML è ancora troppo ridotto rispetto all'immensa domanda che si sta generando.

Tutto questo evidenzia come l'investimento in misure di sicurezza gestite anche in modo automatizzato rimane uno degli asset strategici da adottare in azienda per proteggere il patrimonio informativo delle organizzazioni mentre l'investimento nella formazione del personale umano sarà una delle misure necessarie ed imprescindibili da adottare per soddisfare le migliori esigenze di difesa.

Bilanciare l'innovazione con la gestione del rischio attraverso strategie proattive

Ebbene, per sfruttare appieno il potenziale dell'AI nella cybersecurity, le organizzazioni devono trovare un equilibrio tra l'adozione dell'innovazione e la gestione dei rischi. È fondamentale adottare una strategia di sicurezza basata sul rischio, che identifichi le aree più vulnerabili e si concentri sulla loro mitigazione. Questo include l'implementazione di piani di intervento che armonizzino la segmentazione delle reti OT, l'adozione della gestione dell'IoT nel cloud e l'impiego di tecnologie difensive potenziate dall'AI/ML per il monitoraggio attivo dei sistemi implementati.

È consigliabile investire in soluzioni di sicurezza basate sull'AI che siano in grado di rilevare e rispondere alle minacce in modo più efficace rispetto ai metodi tradizionali, ma, lo ribadiamo, per fare ciò è necessaria una preventiva analisi dei rischi cui l'organizzazione può essere esposta in ragione dell'attività svolta e del patrimonio da proteggere.

Tuttavia, l'AI deve essere impiegata in modo razionale e ponderato, riconoscendo che la decisione ultima in materia di misure di sicurezza, interventi di prevenzione

e di contenimento del rischio da implementare anche in modo automatizzato, spetta sempre all'essere umano.

L'AI fornisce dati, analisi e raccomandazioni, ma è il professionista della sicurezza che deve valutare la situazione nel contesto specifico in cui la misura deve operare e prendere le decisioni finali assumendosi la responsabilità dell'uso di questi sistemi. Le informazioni fornite dall'AI, per quanto possibile, vanno sempre verificate e valutate e soprattutto conservate e analizzate come strumento informativo utile per la scelta di misure eventuali aggiuntive atte a prevenire il rischio di ulteriori tipologie di attacchi.

Le strategie proattive devono includere una formazione regolare del personale sulla consapevolezza della sicurezza per tutti i dipendenti, in quanto essi svolgono un ruolo strategico fondamentale nel mantenimento della postura di cybersecurity di un'organizzazione.

Per garantire l'efficacia delle misure adottate è necessario l'aggiornamento specifico del personale addetto alla gestione dei sistemi di sicurezza informatica basati sull'Ai, il monitoraggio dei sistemi e la valutazione continua delle soluzioni di cybersecurity adottate dagli esperti, la revisione periodica e la validazione delle prestazioni degli algoritmi.

Inoltre, è necessario aggiornare regolarmente le policy sui dati per conformarsi alla legislazione in continua evoluzione, specialmente per quanto riguarda la riservatezza e sicurezza dei dati trattati, dato che i sistemi di ML richiedono l'elaborazione di grandi quantità di dati aggregati per il training ed il corretto funzionamento.

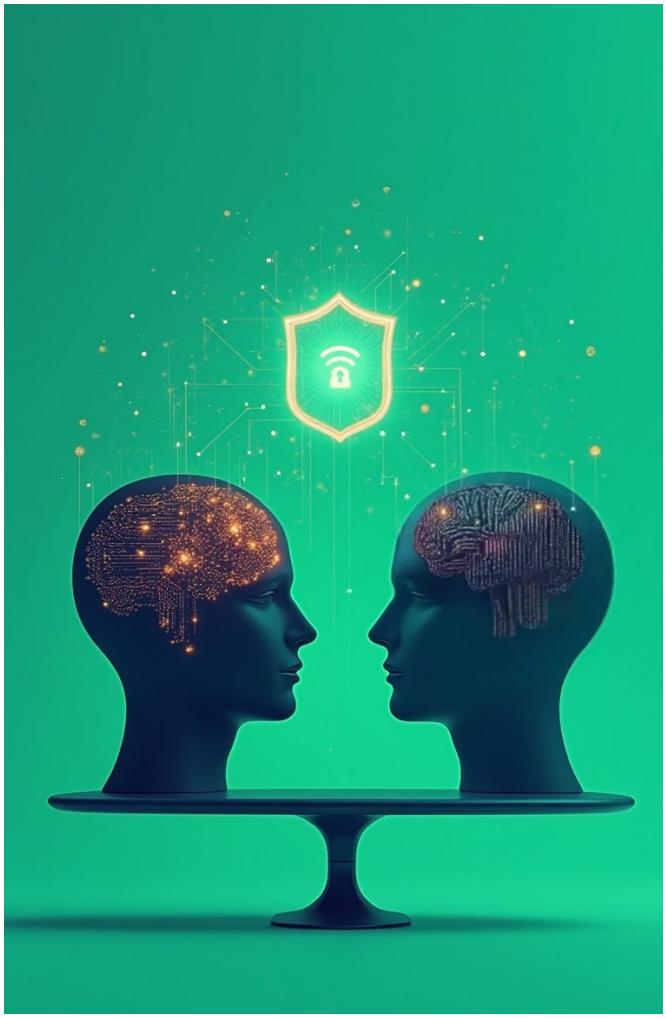
La collaborazione con partner del settore, la condivisione di informazioni sulle minacce e la cooperazione sulle soluzioni possono aiutare le organizzazioni a rimanere al passo con le minacce informatiche comuni e più gravi. L'Unione Europea, ad esempio, sta rafforzando la cybersecurity attraverso strategie legislative come il Cyber Resilience Act (CRA) per i prodotti IoT, e partnership con aziende tech come Google e Amazon per la formazione e la condivisione di best practice.

In sostanza si possono trarre concreti benefici da sistemi di cybersicurezza basati sull'AI solo se le scelte dell'organizzazione che se ne avvale sono prese in modo consapevole, strategico e proattivo sulla base del corretto bilanciamento tra l'aggiornamento del sistema e l'uso del medesimo da parte di personale competente e altamente formato nonché la conoscenza diffusa di tutti i dipendenti dell'organizzazione delle misure necessarie da attuare per il suo corretto funzionamento.

Integrazione di algoritmi di AI e competenze umane: una sinergia imprescindibile

Da quanto sin qui evidenziato possiamo dedurre che l'AI non sostituirà completamente i lavori nell'ambito della sicurezza informatica, ma sta portando a una ridefinizione delle mansioni degli esperti di sicurezza umani. Molti dei compiti ripetitivi e banali possono essere svolti dall'AI, permettendo ai gruppi di esperti di sicurezza informatica di concentrarsi su aree a maggiore valore aggiunto. Gli esseri umani saranno sempre chiamati a gestire e supervisionare gli strumenti di AI, assicurandosi che funzionino correttamente, siano privi di pregiudizi e forniscano le giuste informazioni e risposte e siano reattivi nel contrastare attacchi indesiderati.

Potremmo quindi definire l'AI un "acceleratore di reazione" e un "abilitatore tecnologico" che supporta l'operatore umano, ma non è in grado di replicare il pensiero critico e la creatività umana; l'integrazione dell'AI nella cybersecurity, quindi, non è una soluzione miracolosa, ma un approccio multilivello che combina competenze umane e tecnologie all'avanguardia necessarie a contrastare pericoli sempre più numerosi con modalità sempre più complesse; pertanto solo un impegno costante e condiviso tra organizzazioni, governi e professionisti del settore, che bilanci attentamente l'innovazione con la gestione del rischio e investa nella ricerca e sviluppo, può garantire un ambiente digitale sicuro e resiliente di fronte alle numerose minacce in costante evoluzione.



Implementare il Third-Party Risk Management

Passo dopo passo

A cura di Mark Barlow

Nel panorama normativo europeo della sicurezza informatica, le nuove direttive NIS2 e DORA hanno introdotto un cambiamento importante nel modo in cui le organizzazioni devono affrontare la gestione del rischio. Una delle aree più critiche è la gestione del rischio delle terze parti — meglio nota come Third-Party Risk Management (TPRM).

La digitalizzazione dei servizi, l'esternalizzazione crescente e l'interconnessione delle supply chain ICT hanno esposto le aziende a vulnerabilità indirette: una falla in un fornitore può equivalere a un varco aperto nei sistemi più protetti. NIS2 e DORA non solo riconoscono questo rischio, ma lo mettono al centro della strategia di resilienza.

NIS2 e DORA: due pilastri complementari

La Direttiva NIS2 (UE 2022/2555), applicabile pienamente nel 2025, amplia il perimetro dei "servizi essenziali e importanti" includendo infrastrutture critiche e fornitori digitali. Introduce obblighi stringenti in materia di gestione degli incidenti e responsabilità diretta dei vertici aziendali.

Il Regolamento DORA (UE 2022/2554), specifico per il settore finanziario, è entrato in vigore nel gennaio 2023 con piena applicazione dal gennaio 2025. A differenza della direttiva, ha natura regolamentare e quindi obbligatoria senza necessità di recepimento.

DORA e NIS2: due strade, un obiettivo comune

Il quarto pilastro di DORA, dedicato alla gestione del rischio ICT delle terze parti, impone obblighi stringenti sia per le entità finanziarie che per i loro fornitori critici. NIS2, parallelamente, dedica l'articolo 21(d) alla sicurezza della supply chain, responsabilizzando le organizzazioni sulla solidità dell'intero ecosistema digitale.

Questo significa, in concreto, che non è più sufficiente proteggere i propri server e processi interni. Le aziende devono mappare tutte le dipendenze ICT esterne, valutare la postura di sicurezza dei fornitori, formalizzare obblighi contrattuali precisi e, dove necessario, diversificare le fonti critiche.

Un approccio pragmatico in un contesto normativo in evoluzione

Il Third-Party Risk Management non è un processo statico, ma un sistema complesso e dinamico che si muove all'interno di un quadro normativo europeo ancora in evoluzione. Questo scenario impone alle aziende un approccio proattivo, per anticipare evoluzioni normative ed evitare rischi di non conformità.

In questo scenario di trasformazione, un'azienda italiana certificata ISO 9001 e ISO/IEC 27001, ha scelto un approccio progressivo e concreto. Tale azienda ha pensato a come rispondere efficacemente alle sfide normative e ha adottato una strategia step-by-step, "passo dopo passo", basata su azioni misurabili e un sistema di monitoraggio continuo.

Il TPRM non viene interpretato solo come obbligo, ma come occasione di evoluzione organizzativa, costruendo un sistema capace di apprendere e adattarsi in tempo reale.

Tale strategia si articola su diversi assi operativi:

1. Inventario dei Fornitori: ogni terza parte, incluso il personale freelance ("Professionals") con partita IVA, è tracciata e categorizzata secondo accesso ai dati e tipologia di rischio. Tali classificazioni includono:

- "Nessun accesso": nessuna azione
- "Inattivo": nessuna azione

- “Interni”: questi fornitori hanno accesso ai dati aziendali interni e devono compilare il modulo del trattamento dati come titolare
- “Clienti”: questi Fornitori hanno accesso ai dati dei Clienti della Compagnia e quindi devono (1) compilare un assessment, (2) comunicare i loro sub-fornitori che possono impattare la catena, (3) sottoporsi a un Risk Assessment sulla fornitura
- “Entrambi”: hanno accesso sia ai dati Aziendali sia ai dati dei Clienti e, quindi, devono essere effettuate le azioni dei due punti sopra
- “Professional”: Devono partecipare alle formazioni sugli standard di sicurezza aziendali oppure dimostrare di possedere competenze equivalenti.

2. Mappatura dei Subfornitori: è richiesto ai fornitori di dichiarare chi sono i loro subfornitori e se rappresentano un potenziale punto di rischio per l’Azienda e i Clienti del Business.

3. Clausole contrattuali conformi a DORA: i contratti vengono aggiornati per includere impegni formali sulla sicurezza e la possibilità di audit.

4. Valutazione della postura di sicurezza: l’Azienda ha sviluppato un questionario analitico di autovalutazione da usare internamente e nei confronti dei fornitori. Tale questionario può essere inviato ai Clienti se viene richiesto.

5.Risk Assessment dei fornitori: ogni fornitore viene sottoposto a un’analisi del rischio, per avere una fotografia dinamica e costantemente aggiornata del panorama complessivo dei rischi.

6.Coinvolgimento dei “Professionals”: ii collaboratori esterni devono partecipare alla formazione su privacy e cybersecurity o dimostrare percorsi equivalenti.

Una leva competitiva

In un contesto di mercato sempre più attento alla continuità operativa e alla trasparenza, dimostrare di avere sotto controllo l’intera catena del valore digitale è un vantaggio strategico.

I clienti oggi cercano partner affidabili, resilienti e consapevoli della cultura della sicurezza. Un sistema TPRM ben strutturato permette non solo di ridurre i rischi, ma anche di acquisire fiducia, posizionarsi in modo distintivo, facilitare audit e due diligence, e consente di posizionarsi in modo proattivo rispetto al cambiamento.

Dalla compliance alla cultura della sicurezza

Quello illustrato è un esempio di trasformazione culturale, oltre che di adeguamento normativo. L’adozione di un modello TPRM solido è oggi una necessità operativa per garantire continuità e fiducia nel servizio, soprattutto nei settori ad alta intensità regolatoria come quello finanziario.

La sicurezza non si esaurisce al perimetro aziendale. In un sistema interconnesso, è necessario pensare in rete e gestire i rischi come una catena coesa.

Con l’imminente piena applicabilità della NIS2 e l’entrata in vigore del DORA, il tempo per agire è adesso. La cultura della sicurezza non si impone: si costruisce, giorno dopo giorno, attraverso consapevolezza, controllo e collaborazione.

Guardando avanti

In futuro si prevede l’evoluzione del TPRM verso una piattaforma integrata, capace di dialogare in tempo reale con i sistemi di monitoraggio, le analisi di rischio e i framework internazionali emergenti.

Sarà opportuno progettare l’automazione di parte dei controlli, l’introduzione di strumenti predittivi, e la creazione di un modello di collaborazione attiva con i fornitori, basato su formazione congiunta e condivisione di buone pratiche.

L’obiettivo è trasformare il Third-Party Risk Management in un vero asset strategico di resilienza, governance e vantaggio competitivo.

In un ecosistema digitale, la sicurezza non può più essere un esercizio isolato: deve essere condivisa, distribuita, verificabile.

Per questo non vogliamo inseguire il futuro: vogliamo progettarlo.

Perchè coniugare Cyber Intelligence e Risk Management

A cura di Sofia Scozzari

In uno scenario cyber sempre più complesso e in continua evoluzione, non è più sufficiente limitarsi a reagire agli attacchi, ma è necessario comprenderli, informarsi e anticiparli (per quanto possibile), oltre a valutarne i rischi associati per essere in grado di mitigarne gli impatti.

Peraltro, come ribadito dal World Economic Forum, la cybersecurity non può più essere considerata una mera funzione tecnica isolata, ma deve diventare una priorità strategica e condivisa all'interno dell'azienda, in linea con gli obiettivi di business.

In questo contesto, l'integrazione tra Cyber Threat Intelligence (CTI) e Risk Management rappresenta una combinazione essenziale per evolvere la cybersecurity da mero costo aziendale a strategia di resilienza.

Il valore della Cyber Threat Intelligence

Spesso la Cyber Threat Intelligence viene erroneamente concepita come un accumulo di informazioni grezze su minacce informatiche e attaccanti, spesso con connotazioni eccessivamente tecniche.

In realtà, se utilizzata correttamente, ed in particolare nella sua declinazione di Strategic Threat Intelligence, è piuttosto un processo strutturato che può aiutare il management dell'azienda a comprendere lo scenario delle minacce cyber, sia per quanto riguarda gli attaccanti che le loro motivazioni, le tecniche utilizzate, i settori e le aree geografiche maggiormente a rischio.

Una CTI efficace offre quindi informazioni pratiche e mirate, che consentono alle aziende di identificare preventivamente le minacce specifiche per il proprio settore o area geografica, in modo da focalizzare le proprie risorse sugli scenari di rischio più concreti ed urgenti.

L'aspetto strategico del Risk Management

Il Risk Management è la disciplina che permette di valutare l'impatto potenziale delle minacce sugli asset aziendali.

A seguito di un'adeguata definizione del rischio cyber è inoltre possibile definire le priorità operative per allocare risorse e budget in modo più efficace.

Tuttavia, in assenza di dati contestualizzati ed aggiornati, il Risk Management rischia di basarsi su scenari generici, non realistici e, soprattutto, non specifici per il threat model dell'azienda, diminuendo in maniera esponenziale l'efficacia delle strategie di difesa.

I vantaggi dell'integrazione delle due discipline

L'integrazione di CTI e Risk Management apporta numerosi benefici concreti.

In primo luogo, permette di correlare in modo diretto le minacce reali dello scenario cyber attuale con i rischi effettivi dell'azienda, evitando valutazioni astratte, troppo generiche, o, peggio, inesatte.

Inoltre, permette di stabilire le priorità degli investimenti e degli interventi in modo più efficace, basandosi su una stima concreta degli impatti potenziali, favorendo così un maggiore allineamento tra le strategie di cybersecurity e gli obiettivi aziendali.

Infine, in particolare quando si fa riferimento alla Strategic Threat Intelligence, un ulteriore vantaggio è il supporto più solido alle decisioni del board, grazie a metriche e informazioni comprensibili anche da personale non tecnico.

In definitiva, la sinergia tra le due discipline rafforza in modo significativo le strategie di difesa e preparazione alle minacce cyber, oltre che la resilienza dell'intera organizzazione.

Conclusione

Le minacce informatiche sono sempre più integrate con le sfide geopolitiche, tecnologiche ed economiche, rendendo necessario adottare strategie che uniscano innovazione, sicurezza e resilienza.

In questo contesto, un approccio proattivo che integri la comprensione delle minacce attuali con una valutazione accurata dei rischi rappresenta l'unica strategia efficace per proteggere realmente gli asset aziendali, garantendo sicurezza e continuità operativa.

L'integrazione tra Cyber Threat Intelligence e Risk Management trasforma la cybersecurity da mero costo aziendale a strategia di resilienza.

Phishing 2.0: come l'Intelligenza Artificiale ha aperto una nuova era delle frodi digitali

A cura di Jim Biniyaz

Il phishing è sempre stato uno degli strumenti preferiti dai criminali informatici, ma negli ultimi anni ha cambiato volto in modo significativo e preoccupante. Quello che una volta era un semplice tentativo di inganno via e-mail si è trasformato in una minaccia digitale molto più sofisticata e personalizzata, resa ancora più insidiosa dall'arrivo dell'Intelligenza Artificiale (IA). Siamo nell'era del Phishing 2.0.

L'IA ha rivoluzionato il modo in cui vengono realizzati gli attacchi di phishing, rendendoli più credibili e mirati. Non si parla più di messaggi con errori evidenti o segnali sospetti, ma di contenuti costruiti con grande cura grazie a tecnologie avanzate come deepfake, voice cloning e l'uso approfondito di OSINT (Open Source Intelligence). Video e audio deepfake riescono a replicare in modo sorprendentemente realistico volti e voci di persone conosciute, spingendo le vittime a fidarsi di ciò che vedono e ascoltano. Il voice cloning, in particolare, permette di imitare con precisione la voce di dirigenti, colleghi o familiari, rendendo credibili telefonate o messaggi vocali contraffatti. L'OSINT permette la ricerca di tutte le informazioni che l'utente ha pubblicato, tramite social media come Instagram, Facebook e Linkedin, comprendendo anche passioni, relazioni e lavoro della persona oggetto dell'attacco.

Nel 2024 e nei primi mesi del 2025 abbiamo visto un aumento significativo di toolkit basati su IA utilizzati per scopi malevoli. Questi strumenti non si limitano a generare testi ingannevoli con modelli linguistici avanzati, ma automatizzano anche la raccolta di dati personali, creano profili dettagliati delle vittime e pianificano attacchi estremamente mirati. Il risultato è un phishing "su misura", pensato per ogni singolo bersaglio, con un livello di personalizzazione che mette in difficoltà anche i sistemi di difesa più sofisticati.

I casi concreti sono ormai numerosi: a gennaio 2024, una grande azienda inglese ha perso 25 milioni di dollari dopo una videoconferenza deepfake che ha convinto un dirigente a effettuare un bonifico fraudolento. Nello stesso mese, un attacco audio deepfake ha cercato di influenzare gli elettori durante le primarie nel New Hampshire (USA), con l'obiettivo di indurli a cambiare il proprio voto. Mentre a maggio, una multinazionale come WPP è stata colpita da un tentativo di impersonificazione

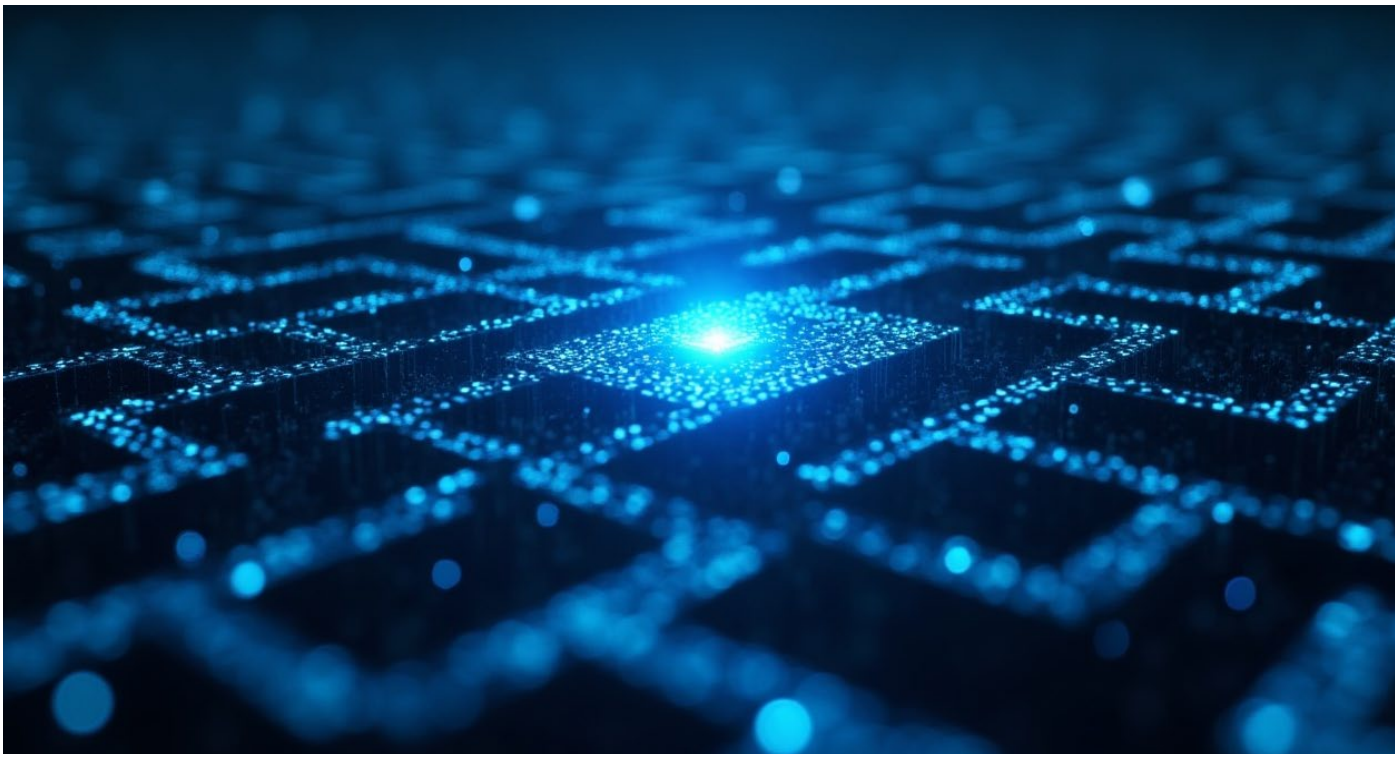
molto sofisticato, fortunatamente senza danni economici.

Questi episodi mostrano chiaramente come l'IA abbia superato il confine tra frodi "artigianali" e ingegneria sociale su scala industriale. Oggi gli attacchi sono più credibili, più difficili da individuare e potenzialmente più dannosi. L'IA è capace di replicare con precisione lo stile comunicativo di una persona, scrivere e-mail indistinguibili da quelle autentiche e produrre contenuti multimediali in grado di ingannare anche esperti. La minaccia non è più solo tecnica, ma anche cognitiva.

Non basta aggiornare filtri antispam o firewall per rispondere a questa sfida. Serve un cambio di paradigma nella cultura della sicurezza informatica. Non possiamo più affidarci solo alla tecnologia: è fondamentale aumentare la consapevolezza delle persone. Gli utenti devono imparare a riconoscere le dinamiche dell'inganno, anche quando sembrano perfettamente plausibili. Dobbiamo tornare a osservare con attenzione, a dubitare e a verificare. Paradossalmente, proprio mentre l'IA imita alla perfezione la comunicazione umana, la nostra capacità di percepire ciò che non va resta la difesa più efficace.

Affrontare il Phishing 2.0 significa adottare un approccio integrato. È necessario investire in tecnologie di rilevamento avanzate, promuovere programmi di formazione continua, monitorare costantemente le nuove minacce e costruire un ecosistema di difesa in cui ogni elemento tecnico, umano e organizzativo svolge un ruolo attivo e proattivo. Ormai non è più una battaglia che si può combattere da soli: coinvolge aziende, istituzioni e privati. Nessuno è escluso.

Per affrontare efficacemente il nuovo panorama di minacce in continua evoluzione del Phishing 2.0, è fondamentale agire in anticipo, adottando una strategia dinamica, proattiva e condivisa. Solo così sarà possibile contenere e identificare gli attacchi più insidiosi della nuova era digitale.



Cybersecurity e Protezione Dati: l'Integrazione Strategica che Garantisce la Resilienza Digitale

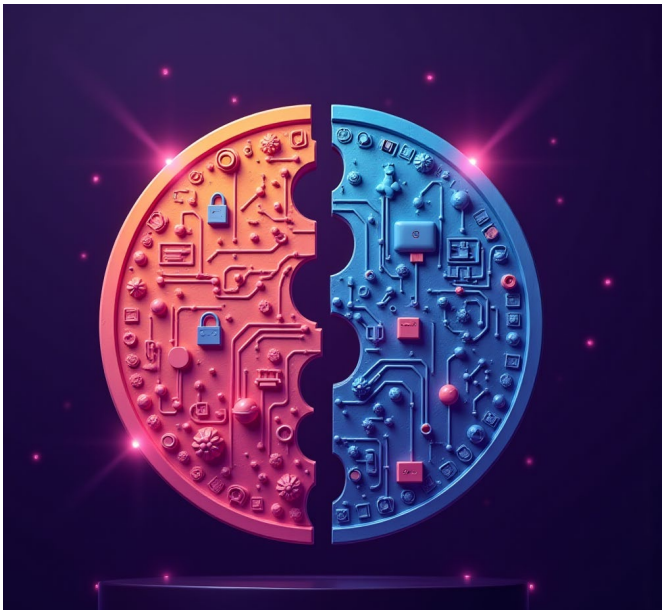
A cura di Fabio Zanoli

La crescente complessità normativa, come il palesarsi di minacce informatiche sempre più sofisticate, fanno sì che l'integrazione tra cybersecurity e protezione dei dati personali non rappresenti più una semplice opportunità, ma una necessità strategica.

L'implementazione di questo ecosistema di sicurezza è fondamentale per ogni organizzazione, non solo per quanto in premessa, ma per rimanere ed evolversi sul mercato. Un'azienda che non sappia garantire la sicurezza dei dati che le vengono consegnati dai propri clienti, fornitori o partner risulterà sempre meno attrattiva in un mondo che si evolve a velocità warp, sia nei contenuti, che nelle minacce.

Questa convergenza è dettata, quindi, tanto dalla natura complementare delle due discipline, quanto dall'urgenza di garantire la resilienza digitale di aziende, enti pubblici e organizzazioni di ogni settore.

Le principali normative europee, tra cui il GDPR (Regolamento Generale sulla Protezione dei Dati), la NIS2 (Direttiva sulla sicurezza delle reti e dei sistemi informativi) e il DORA (Digital Operational Resilience Act), tracciano un quadro che risulta evidente: la sicurezza informatica e la tutela della privacy devono essere affrontate in modalità congiunta, coerente e sinergica.



Due Facce della Stessa Medaglia

Sebbene si concentrino su aspetti distinti, cybersecurity e protezione dei dati personali condividono un obiettivo comune: garantire la riservatezza, l'integrità e la disponibilità delle informazioni. La cybersecurity ha come focus la protezione dell'infrastruttura digitale da attacchi esterni, vulnerabilità e minacce persistenti avanzate. La privacy, al contempo, pone al centro la centralità della persona, tutelando i dati personali da trattamenti illeciti o non proporzionati.

Insomma tutelare le persone e farlo con metodi corretti tecnicamente non è più una cosa da NERD, ma un valore aggiunto anche dal punto di vista del business.

Queste due aree si intersecano in maniera strutturale in molteplici ambiti, come ad esempio:

- **La gestione degli accessi e controllo delle identità (IAM):** definire, e mantenere nel tempo, in modo puntuale e attento chi può accedere a quali informazioni è essenziale per entrambe le funzioni. Un errore in questo ambito può portare sia a violazioni della sicurezza sia a trattamenti illeciti di dati personali.
- **La Crittografia:** se adottata come tecnica fondamentale per proteggere i dati in transito e a riposo, è uno strumento chiave tanto per la compliance privacy quanto per la sicurezza informatica.
- **Audit, tracciamento e logging:** queste attività risultano indispensabili per verificare il rispetto delle policy aziendali, ricostruire eventuali incidenti come per dimostrare la conformità alle normative con cui l'organizzazione deve continuamente confrontarsi.

Il GDPR, non il manuale della paper compliance, ma il cuore della protezione dei Dati

Il Regolamento UE 2016/679 (GDPR) ha rappresentato una vera e propria rivoluzione nella gestione dei dati personali. La sua portata extraterritoriale e l'approccio basato sul rischio lo rendono un pilastro nella costruzione di una cultura della privacy.

I concetti di accountability, privacy by design e privacy by

default hanno imposto – lo stanno tuttora imponendo a dire il vero - un cambiamento strutturale: le modalità con cui proteggere i dati devono essere tenuta in considerazione sin dall'inizio e quindi fin dalla progettazione di un progetto, di una nuova attività aziendale, ci marketing ecc. Non può essere tenuta in considerazione solo alla fine del progetto come "misura di paper compliance". Ne consegue che far sì che questo concetto sia chiaro a tutti i livelli dell'organizzazione migliora le performance e velocizza lo sviluppo delle attività, siano queste rivolte al pubblico che ad al mercato privato.

NIS2, verso la "cybersecurity diffusa"

La Direttiva NIS2, recepita nel nostro Paese con il D.lgs. 138/2024, amplia significativamente l'ambito di applicazione della cybersecurity, includendo anche settori ritenuti "non critici" in passato, come il commercio elettronico, i servizi postali, i fornitori di cloud, ma anche le amministrazioni pubbliche centrali. Inoltre espande la richiesta di sicurezza anche alla catena di fornitura, diffondendo così la necessità di aumentare il proprio perimetro di cybersecurity anche alla PMI, finanche alla micro aziende, in molti casi. Perché se è vero che queste non risultano impattate direttamente dalla norma, è altrettanto vero che queste riceveranno richieste di miglioramento dei loro processi e modalità di cybersecurity dai prte loro clienti.

La norma, come ben sappiamo, introduce inoltre "requisiti minimi di sicurezza" più rigorosi, che comprendono: valutazioni del rischio sistematiche e continuative, politiche di gestione della supply chain anche dal punto di vista della cybersicurezza, obblighi di reporting strutturati e di tenuta documentale degli incidenti, un miglioramento delle misure tecniche e organizzative rispetto agli attacchi informatici.

In questo scenario, le organizzazioni sono chiamate a dimostrare proattività non solo nella risposta agli incidenti, ma anche nella loro prevenzione.

La sfida dell'integrazione. Oltre i "silos organizzativi"

L'integrazione tra cybersecurity e privacy non è sempre semplice. Le due aree, spesso presidiate da team distinti – il CISO da un lato, il DPO dall'altro ad esempio – possono cadere nella trappola dei silos organizzativi, generando incoerenze e ridondanze.

Eppure, proprio la collaborazione tra i componenti di questi due staff può fare la differenza. Una strategia integrata, ovvero la progettazione e l'inserimento nei processi dell'organizzazione di questo ecosistema di sicurezza, permette di: evitare duplicazioni di strumenti e processi, condividere know-how e aggiornamenti normativi. Inoltre rende possibile la compliance a più normative simultaneamente (GDPR, NIS2, DORA, ISO 27001, ecc.), riducendo i costi ed aumenta la capacità di risposta agli incidenti, migliorando la business continuity e mettendo al riparo le organizzazioni da perdite finanziarie. Insomma, parafrasando una vecchia pubblicità: "prevenire è meglio che riemettere on line". Costa molto meno, da qualsiasi punto di vista, sia finanziario, che organizzativo che reputazionale.

Come dirigersi verso una Governance Integrata

Una buona governance dei dati e della sicurezza parte da una visione strategica unitaria. Che implica andare a definire policy comuni, o comunque integrate e non confliggento, tra sicurezza e protezione dati, mappare i flussi di dati e i punti di vulnerabilità comuni Mettere a budget investimenti in strumenti tecnologici interoperabili, come SIEM e DLP, ma anche piattaforme di gestione delle violazioni e dei data breach e degli incidenti informatici e, last but not last, monitorare gli asset digitali

critici con continuità, prevedendo escalation e remediation condivise.

Best Practice per una Strategia Unificata

Per promuovere un approccio davvero efficace, le organizzazioni dovrebbero adottare alcune best practice operative, alcune delle quali potrebbero essere quelle che elenchiamo qui di seguito:

- Formazione continua: lavoratori e collaboratori formati rappresentano la prima linea di difesa contro errori umani e social engineering.
- Piani di continuità integrati: incident response plan e data breach notification plan devono essere coerenti tra loro.
- Automazione e orchestrazione (SOAR): integrare strumenti per ridurre il tempo di rilevamento e reazione agli incidenti.
- Collaborazione multidisciplinare: promuovere tavoli di lavoro congiunti tra IT, legale, compliance e business.
- Coinvolgimento del vertice aziendale: la sicurezza non è solo un tema tecnico, ma un tema di governance e reputazione.

Concludendo, nel contesto normativo e tecnologico attuale ed in quello che si prepara, la separazione tra privacy e cybersecurity è un approccio anacronistico. Le due discipline si alimentano a vicenda, rafforzandosi reciprocamente.

L'adozione di un approccio integrato – l' ecosistema di sicurezza - consente di trasformare, nella pratica e non solo nel libro dei sogni, la compliance da obbligo a opportunità: costruire fiducia con clienti e stakeholder, migliorare l'efficienza operativa, aumentare la resilienza e rafforzare la reputazione aziendale, creare risparmi finanziari, ridurre i costi dei propri servizi e prodotti immessi sul mercato, ecc.

L'oggi della protezione digitale passa inevitabilmente dalla capacità delle organizzazioni di vedere la cybersecurity e la protezione dei dati come due elementi inseparabili, centrali in ogni strategia di innovazione, crescita e sostenibilità.

Cyber-attribuzione: il ruolo cruciale della cooperazione per navigare nella ‘zona grigia’

A cura di Olivia Terragni

Con l’aumento costante delle attività di gruppi criminali e APT sempre più avanzati, che colpiscono infrastrutture critiche e istituzioni governative in un mondo deterritorializzato e costituito da infrastrutture e sistemi interconnessi globalmente come si può garantire una risposta condivisa e affidabile per identificare con certezza i responsabili e prevenire escalation di conflitti digitali?

Un’agenzia di attribuzione internazionale o europea?

Nel dibattito internazionale e accademico si discute ampiamente della creazione di un meccanismo internazionale di attribuzione per superare le difficoltà tecniche, politiche e diplomatiche [22]. Tuttavia, la realizzazione di un organismo super partes si rivela complessa, data la diffidenza tra grandi potenze e la difficoltà di raggiungere consenso su procedure, standard e attribuzioni politiche. Le norme del diritto internazionale sono applicabili alle operazioni informatiche, ma la loro interpretazione è ancora incerta e frammentata e raramente gli Stati fanno riferimento esplicito alle norme violate nelle loro dichiarazioni pubbliche [23].

Le iniziative a sostegno di tale meccanismo non sono mancate - Consiglio Atlantico, Microsoft, RAND Corporation, Cyber Peace Institute [24] - ma non è in corso alcuno sforzo concreto per istituirlo. Le grandi potenze sono poco interessate, preferendo gestire autonomamente la questione grazie a proprie capacità tecniche, politiche e alleanze, ma i paesi con capacità tecnologiche limitate potrebbero trarne vantaggio, l’Unione Europea (UE), potrebbe rafforzare la legittimità delle sanzioni e delle risposte collettive. Un’agenzia europea coordinata, in tal senso, potrebbe rappresentare una strategia più efficace, con il vantaggio di operare all’interno di un quadro già consolidato, come la direttiva NIS 2 e l’azione coordinata di enti quali ENISA, EU-CyCLONe e le autorità nazionali (es. ACN in Italia), con linee guida comuni e best practice condivise. Inoltre ENISA ha già un mandato permanente per coordinare la cooperazione operativa in materia di cybersicurezza tra gli Stati membri [25]. L’obiettivo è quello di rafforzare le collaborazioni esistenti, ossia stabilire standard probatori e promuovere il rispetto del diritto internazionale e una cultura della responsabilità collettiva, riducendo in tal modo l’impunità nel cyberspazio.

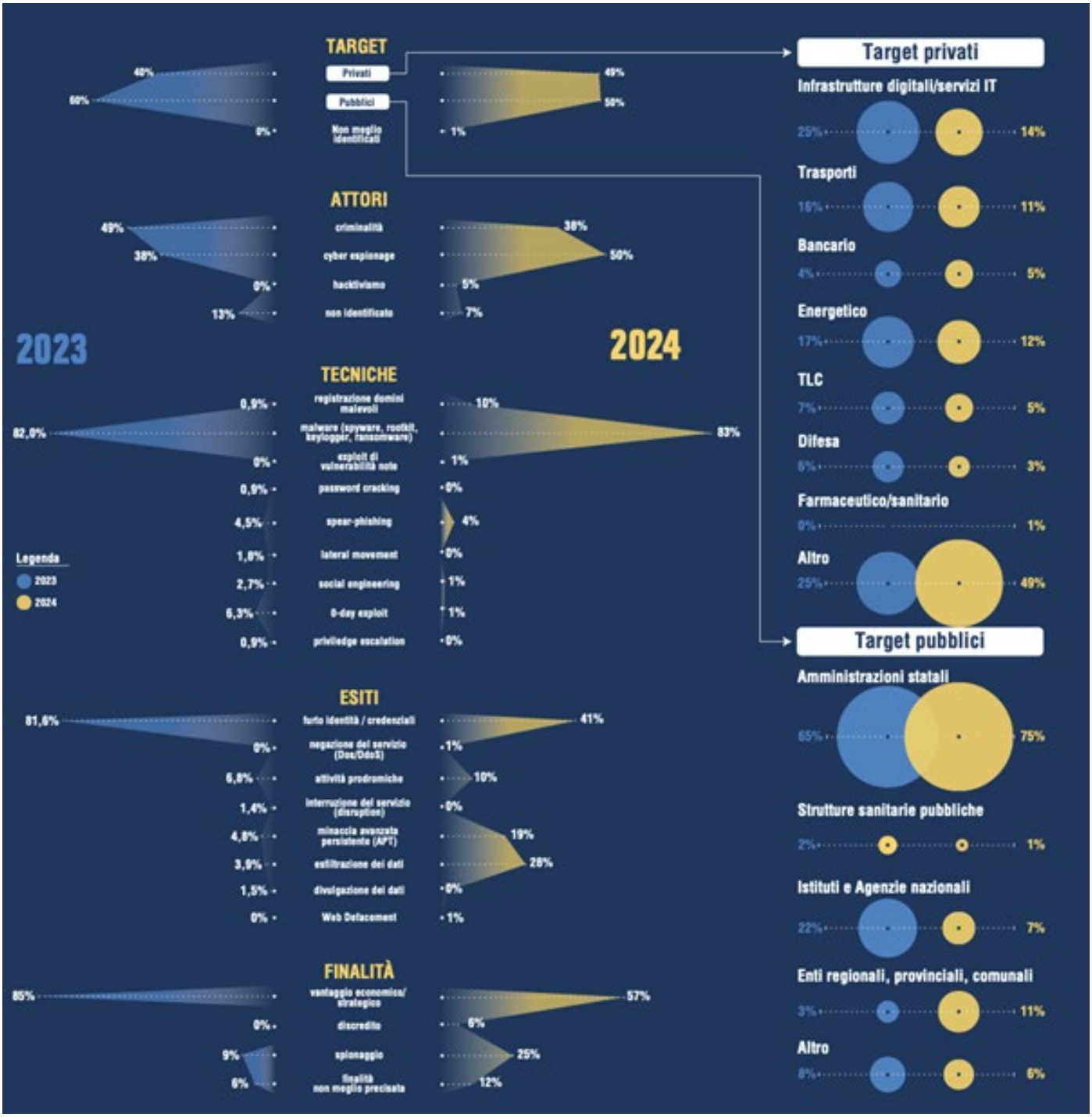
Un’escalation senza precedenti e il contesto geopolitico

Mappando il cyberspazio, la diffusione di malware e attacchi digitali, iniziata nel 2000, ha registrato un’accelerazione esponenziale, con un raddoppio di incidenti sino al 2025 e un tasso di crescita annuo superiore al 25% a livello globale. Gli attacchi APT (Advanced Persistent Threat), hanno avuto un’accelerazione marcata dal 2016, triplicando le operazioni cyber su larga scala, segnando un record nel 2024, che, in Italia [5], ha rappresentato circa il 50% degli attacchi cyber rilevati con un aumento del 12% rispetto all’anno precedente. Gli attacchi globali a scopo di spionaggio, sono passati dal 9% a circa il 25%, secondo le analisi più recenti, riflettendo un uso crescente del cyberspazio per obiettivi strategici statali, con operazioni su larga scala, persistenti e altamente mirate, che oggi rappresentano una delle minacce più critiche per la sicurezza nazionale e le infrastrutture critiche.

A ció si sommano le tensioni geopolitiche, come i conflitti regionali (Russia-Ucraina e Medio Oriente), la rivalità tra grandi potenze (USA-Cina) e una guerra informatica i cui vantaggi strategici sono ottenuti senza oltrepassare la soglia di un conflitto aperto. Ciò alimenta una ‘zona grigia’ in cui l’opacità delle operazioni cyber viene sfruttata per complicare le decisioni strategiche in un terreno di confronto asimmetrico. In questo contesto la gestione dell’incertezza e del disordine del cyberspazio diventa una componente cruciale della sicurezza globale. Ogni forma di intelligence (Osint, Sigint, Masint, Imnit, GeoInt, Cybint, Socint, Humint) si è sviluppata a livelli mai visti prima e si rendono necessarie nuove figure come quella che possiamo chiamare “architetti dei sistemi complessi” in grado di muoversi tra dimensione tecnica, strategica e umana, richiedendo pragmatismo, competenza e resilienza per navigare le sfide internazionali.

Il problema dell’attribuzione: le criticità

L’attribuzione in sé, non è un risultato binario ma graduale e composto da numerosi passaggi - tecnico, politico-pubblico e giuridico - che richiedono livelli crescenti di evidenza e collaborazione, competenze tecniche, capacità di intelligence, tecnologie avanzate, una forte collaborazione, decisioni politiche su quando e come



Fonte immagine: La sicurezza cibernetica in Italia, Relazione annuale Intelligence 2025.

rendere pubblica un'attribuzione e investimenti rilevanti a fronte di risposte lente o controverse [27]. A ciò si aggiunge che gli Stati non sono sempre propensi a pubblicare le proprie prove o la metodologia di attribuzione e considerano l'attribuzione una prerogativa sovrana [23]. 'Attribuiscono quando serve ai loro interessi e nel momento da loro scelto [28]' per non esporre le proprie fonti di intelligence, per limiti tecnici, incertezze, motivazioni politiche o mancanza di vincoli normativi chiari.

Oggi anche in presenza di minacce persistenti avanzate (APT), attribuire con precisione, rigore, imparzialità e tempestività un attacco informatico, permette non solo di adottare misure legali o tecniche per prevenire, reprimere o scoraggiare ulteriori attacchi, ma di ridurre accuse errate o sospetti e quindi ridurre il rischio di conflitti derivanti dagli attacchi stessi.

Ovviamente esistono delle criticità. Anche se "un'agenzia di attribuzione [basata sul consenso] potrebbe svolgere un ruolo chiave [23]", come organismo super partes, offrendo procedure condivise per gestire disac-

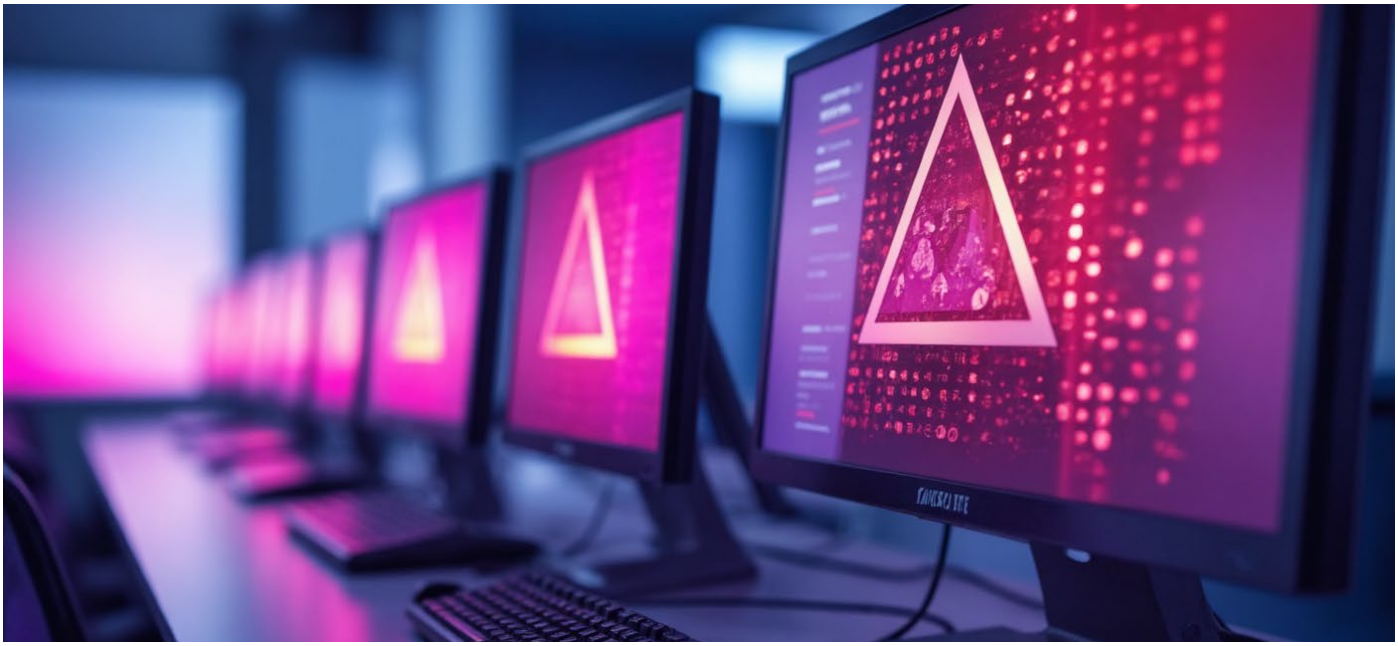
cordi, mettere a disposizione esperti qualificati e fornire supporto amministrativo e finanziario, potrebbe entrare in concorrenza con Stati e aziende private, non sempre disposti a condividere conoscenze e risorse. Basti pensare alll'interconnettività delle reti e delle infrastrutture informatiche: ricerche approfondite potrebbero accedere inavvertitamente a informazioni sensibili o reti critiche di uno Stato. Inoltre se coloro che conducono le indagini abusassero della propria posizione in caso di intrusione, ne seguirebbero "accuse e recriminazioni, e di conseguenza l'agenzia di attribuzione si espanderebbe anziché contenere le controversie sottostanti [23]".

La gestione dell'incertezza e del disordine del cyberspazio diventa una componente cruciale della sicurezza globale.

Una gestione strutturata del disordine: le opportunità

Da un lato, la sicurezza informatica, divenuta elemento strategico, non può più essere considerata a compartimenti stagni e azioni separate ma come il risultato di processi integrati e coordinati. Dall'altro il disordine nel cyberspazio — inteso come complessità, ambiguità, fluidità delle identità — è "inevitabile e persino necessario per la vitalità e l'innovazione del sistema globale digitale così come necessario per stimolare adattamento, creatività e resilienza, evitando rigidità e stagnazione nella società" (Richard Sennett e Serge Moscovici). In questo contesto, un organismo che coordini e standardizzi l'attribuzione degli attacchi non mirerebbe a imporre un ordine rigido o gestire le controversie, ma a gestire strutturalmente il disordine, rendendolo governabile attraverso procedure condivise, trasparenti e affidabili: una diplomazia cyber attiva basata su dialogo, negoziazione e cooperazione, che possono prevenire escalation e costruire fiducia.

La creazione di un'organismo super partes, riconosciuto dagli Stati e a loro supporto, che sviluppi sinergie, potrebbe standardizzare i protocolli per la raccolta di evidenze o l'analisi forense, permettere di 'condividere intelligence' in tempo reale tra paesi e settori privati, sviluppare framework per mappare le connessioni tra attori statali e criminali, elaborare risposte proporzionali e sanzioni economiche mirate, superando le diffidenze geopolitiche ed emettere così rapporti di attribuzione condivisi, basati su criteri trasparenti e verificabili riducendo il rischio di accuse unilaterali ed escalation o stabilire in modo chiaro quali azioni possano innescare risposte collettive automatiche, anche senza attribuzione certa. Fonti di ispirazione si trovano nel modello NATO (Art. 5) e nell'iniziativa UE per una Cyber Unit congiunta, nell'analisi di Bruce Schneier e Adam Segal sulla "deterrenza dinamica" nel cyberspazio basata su un uso combinato di strumenti tecnici, legali, diplomatici ed economici per rispondere in modo proporzionato agli attacchi.



Vulnerabilità nei sistemi di Intelligenza Artificiale: ci siamo! E adesso?

A cura di Giancarlo Calzetta

È inutile fingersi sorpresi: sapevamo benissimo che sarebbe successo. L'avanzata dell'intelligenza artificiale, sebbene rivoluzionaria, sta inesorabilmente portando alla luce nuove sfide nel panorama della sicurezza informatica. Dopo gli allerta generici degli specialisti, i quali sanno bene che ogni nuova tecnologia porta con sé delle vulnerabilità, negli ultimi tempi sono state identificate le prime due significative falle che illustrano perfettamente perché la sicurezza aziendale IT deve evolversi, andando oltre gli strumenti di indagine usati oggi.

EchoLeak: La Prima Vulnerabilità Zero-Click per l'IA in Microsoft 365 Copilot

Nel gennaio 2025, ma se n'è parlato solo ora, i ricercatori di Aim Labs hanno identificato un nuovo tipo di attacco indirizzato ai sistemi AI: EchoLeak. Si tratta della prima vulnerabilità zero-click documentata capace di estrarre informazioni sensibili da Microsoft 365 Copilot senza alcun intervento da parte dell'utente. La sua pericolosità ha indotto Microsoft e gli scopritori a tenerla segreta fino a quando è stata risolta (lato server) a maggio.

Microsoft ha affermato di non aver riscontrato prove di sfruttamenti reali e che nessun utente è stato interessato, il che significa che la vulnerabilità sembra esser stata risolta prima di causare danni effettivi. Ma il concetto è che EchoLeak ha dimostrato come anche sistemi apparentemente protetti da barriere interne possano essere manipolati attraverso le peculiarità dei modelli linguistici. Un campo che, finora, non ha fatto parte dei metodi strutturati di ricerca delle vulnerabilità.

Ovviamente, il problema era nel codice, ma il suo sfruttamento segue una dinamica diversa. Microsoft 365 Copilot integra i modelli GPT con il Graph proprietario per assistere gli utenti nelle applicazioni di Office, dalla redazione di contenuti all'analisi dei dati. Il fulcro della vulnerabilità risiedeva nel modo in cui l'IA gestisce e interpreta il contesto, specialmente quando entra in gioco la Retrieval-Augmented Generation (RAG). In pratica, una frase abilmente strutturata, anche senza codice eseguibile, può indurre il sistema a eseguire delle azioni inattese e malevole. Data la profonda integrazione di Microsoft 365 in applicazioni come Outlook, Word, Excel e PowerPoint, la superficie di attacco era estremamente ampia.

EchoLeak è classificato come una nuova categoria di vulnerabilità, definita LLM Scope Violation, in cui il modello linguistico ottiene e divulga dati riservati pur non

avendo l'autorizzazione. Il modello viene ingannato tramite istruzioni celate all'interno del prompt, aggirando i sistemi di difesa automatica come XPIA. Questo comportamento può essere sfruttato in modo automatico e impercettibile in ambienti aziendali complessi.

Il processo di attacco ha inizio con l'invio di un'e-mail apparentemente innocua, ma che in realtà contiene una "prompt injection" invisibile all'utente, una frase che sembra innocua o addirittura completamente nascosta che viene "digerita" dal sistema. Quando l'utente, anche giorni dopo, pone a Copilot una domanda che è collegata alla mail "infetta", l'e-mail viene recuperata e incorporata nel contesto operativo del modello. A quel punto, il prompt nascosto indirizza il sistema a raccogliere dati interni che vengono poi inviati all'esterno.

Una frase abilmente strutturata, anche senza codice eseguibile, può indurre il sistema a compiere delle azioni inattese e malevole.

La Falla di Asana nel Model Context Protocol (MCP)

E dopo Microsoft, è il turno di Asana. Appena una settimana dopo aver divulgato EchoLeak, Asana ha comunicato di aver affrontato un problema nello stesso ambito, ma con una struttura molto diversa. Questa azienda, nota per il suo software di collaborazione, ha dovuto sospendere per quasi due settimane il suo server sperimentale basato su intelligenza artificiale, il Model Context Protocol (MCP), a seguito della scoperta di una falla che avrebbe potuto rendere visibili i dati di un'organizzazione ad altri utenti sulla piattaforma.

Il problema era nell'implementazione dell'MCP, un protocollo a sorgente aperta lanciato da Anthropic nel 2024 e ideato per connettere agenti AI e modelli linguistici a risorse esterne, come database e sistemi di messaggistica. Asana aveva attivato il proprio server MCP il 1° maggio, permettendo agli utenti di interrogare i dati aziendali usando il linguaggio naturale e di integrarsi con altre applicazioni AI.

Purtroppo, il 4 giugno, Asana ha rilevato un difetto nel server MCP che, come comunicato ai clienti, poteva potenzialmente esporre informazioni specifiche del dominio Asana ad altri utenti MCP. Questo incidente ha causato la disabilitazione del servizio dal 5 al 17 giugno, in attesa di una correzione. I dettagli tecnici completi della vulnerabilità non sono stati resi pubblici, ma sembra che il problema fosse correlato a un malfunzionamento nei meccanismi di isolamento dei tenant, un aspetto cruciale quando si opera con modelli di intelligenza artificiale in contesti multi-tenant. Asana ha dichiarato di non aver rilevato prove di accessi non autorizzati o di sfruttamenti effettivi.

Anche se le due falle sono state risolte, la loro scoperta solleva mostra chiaramente che l'adagio "tecnologia nuova, vulnerabilità nuove" è sempre attuale. Per proteggersi, le organizzazioni devono rafforzare i sistemi di controllo sui prompt in ingresso, applicare filtri di post-elaborazione alle risposte generate e impedire la creazione automatica di link o dati strutturati. Inoltre, è cruciale configurare i motori RAG per prevenire il recupero di contenuti potenzialmente dannosi da e-mail, documenti o repository non verificati.

Ma tutto ciò deve avvenire in seguito a un "arricchimento" della mentalità degli esperti di cybersecurity che devono aggiungere un nuovo modo di pensare al loro bagaglio culturale per riuscire a trovare bug e vulnerabilità che funzionano in maniera molto diversa dai soliti code injection e privilege escalation.

Disclaimer

Gentile lettore,

Ti informiamo che il contenuto pubblicato su questo magazine è fornito a scopo puramente informativo e di intrattenimento. Tutte le opinioni, idee e punti di vista espressi negli articoli sono esclusivamente quelli degli autori e non riflettono necessariamente l'opinione di Assintel o dei suoi redattori.

Tutte le informazioni fornite sono basate sulle conoscenze e le fonti disponibili al momento della pubblicazione. Tuttavia, non possiamo garantire l'accuratezza, l'integralità o l'aggiornamento delle informazioni fornite. Pertanto, l'utilizzo delle informazioni presenti su questo magazine avviene a proprio rischio e discrezione.

Si prega di tenere presente che il contenuto potrebbe evolvere nel tempo e potrebbe non essere più aggiornato o rilevante al momento della lettura. Pertanto, consigliamo di verificare sempre l'attualità delle informazioni fornite e di consultare professionisti qualificati per eventuali questioni specifiche o decisioni importanti.

Inoltre, il Cyber Think Tank di Assintel declina ogni responsabilità per eventuali errori, omissioni o danni derivanti dall'uso delle informazioni contenute nel presente magazine. Non siamo responsabili per qualsiasi rivendicazione, perdita o danno di qualsiasi tipo che possa sorgere direttamente o indirettamente dall'utilizzo delle informazioni qui presentate.

Ti invitiamo a fare affidamento su più fonti di informazione per ottenere una visione più completa e a considerare che i punti di vista espressi possono variare in base all'esperienza e alle opinioni personali degli autori.

Infine, vorremmo sottolineare che il magazine non fornisce consulenza legale, finanziaria, medica o professionale di alcun genere. Si consiglia di consultare sempre un professionista qualificato per risolvere eventuali questioni specifiche che riguardano la tua situazione personale.

Cordialmente

La redazione

CYBER
Think Tank
ASSINTEL

Riferimenti

1. https://attack.mitre.org/
2. https://www.secalliance.com/blog/irans-cyber-strategy-and-the-israel-iran-conflict
3. https://securityaffairs.com/30734/intelligence/operation-cleaver-iranian-hackers.html
4. https://en.wikipedia.org/wiki/Operation_Cleaver
5. https://blog.sekoia.io/iran-cyber-threat-overview/
6. https://www.gruppotim.it/it/archivio-stampa/corporate/2025/CS-Report-TIM-Cybersecurity-Foundation-12-6.html
7. https://www.unitedagainstnucleariran.com/index.php/history-of-iranian-cyber-attacks-and-incidents
8. https://www.timesofisrael.com/cyberattacks-by-iran-hezbollah-have-tripled-during-the-war-says-israel-cyber-czar/
9. https://www.ynetnews.com/business/article/r1e2w6w1a
10. l'Internazionale (https://www.internazionale.it/notizie/alessandro-lubello/2025/05/24/lavora-di-piu-e-lamentati-di-meno)
11. Wall Street Journal (https://www.wsj.com/lifestyle/workplace/corporate-bosses-workers-culture-changing-cbd19c2c?mod=hp_lead_pos8)
12. European workforce study 2025 di Great place to work (https://gptw.greatplacetowork.it/blog/european-workforce-study-2025),
13. Cybercrime magazines (https://cybersecurityventures.com/jobs/),
14. Osservatorio HR Innovation practice (https://www.osservatori.net/hr-innovation-practice/)
15. Studio Resume now pubblicato dal New York Post (https://nypost.com/2025/05/21/lifestyle/what-is-ghostworking-trend-how-burned-out-employees-pretend-to-do-their-jobs-every-day/)
16. Così l'intelligenza artificiale sta rivoluzionando la cyber security – Federica Maria Rivelli - 25 settembre 2025 https://www.cybersecurity360.it/cultura-cyber/cosi-lintelligenza-artificiale-sta-rivoluzionando-la-cyber-security/
17. L'illusione della sicurezza: i pericoli nascosti dell'AI nella cybersecurity – Gabriele Costa – 16 settembre 2024 https://www.agendadigitale.eu/sicurezza/lillusione-della-sicurezza-i-pericoli-nascosti-dellai-nella-cybersecurity/
18. https://blog.cyberoo.com/intelligenza-artificiale-per-la-cyber-security-vantaggi-e-applicazioni
19. https://www.kaspersky.it/resource-center/definitions/ai-cybersecurity
20. https://dirigentindustria.it/fm-triveneto/opinioni/intelligenza-artificiale-e-cybersecurity.-le-nuove-frontiere-della-protezione.html
21. https://www.ictsecuritymagazine.com/articoli/intelligenza-artificiale-cybersecurity/
22. The Prospects for an International Attribution Mechanism for Cyber Operations – An Analysis of Existing Approaches, Isabella Brunner, (2022)
23. Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations, François Delerue (2024), Questions of International Law.
24. An International Attribution Mechanism for Hostile Cyber Operations?', Michael N Schmitt e Yuval Shany, MN Schmitt, Y Shany, (2020)
25. L'attribuzione degli attacchi informatici, Ranieri Razzante, European Journal of Privacy Law and Technologies [2022]
26. La sicurezza cibernetica in Italia, Relazione annuale Intelligence (2025).
27. The six degrees of cyber attribution,International Institute for Strategic Studies (IISS), (2024)
28. Nichola Tsagourias, Questions of Cyber Law, Cyber Attribution Agencies: A Sceptical View (2024)
29. An International Agency for the Attribution of Malicious Cyber Operations?, Introduced by Emanuele Cimiotta, Full Professor of International Law, Department of Political Sciences of the Perugia University, Questions of International Law,
30. Attribution in International Law, Challenges and Evolution, Kristen E. Boon (2024)
31. EU External Action and the Attribution of Conduct under International Law, Pietro Violante, Università Bocconi (2021).

CYBER MAGAZINE

CYBER
Think Tank
ASSINTEL

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Contattaci:

segreteria@assintel.it
www.assintel.it