CYBER MAGAZINE

CYBER Think Tank ASSINTEL

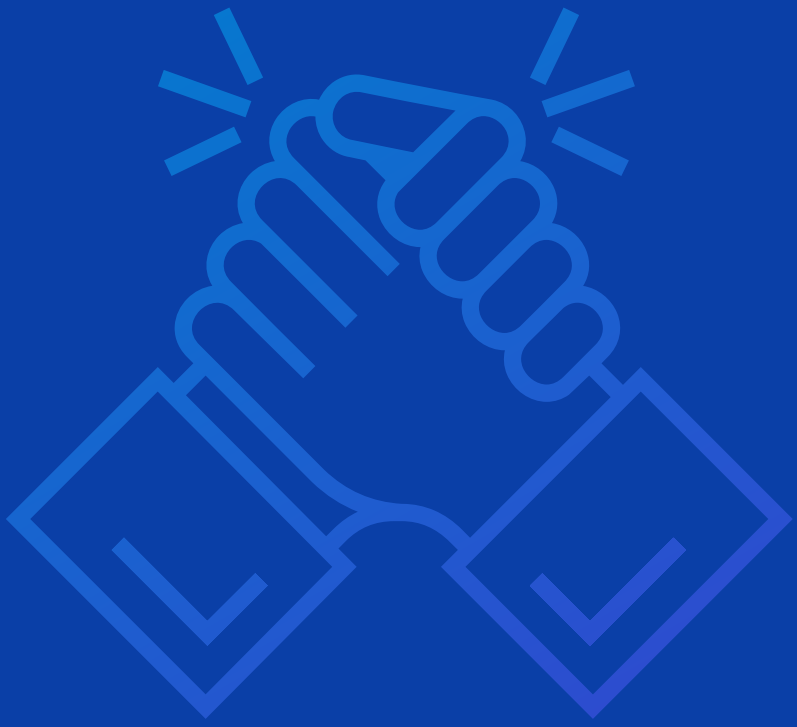
ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

Marzo 2025

Cyber Think Tank Assintel

Unisciti alla rete delle menti che proteggono il futuro digitale!

CYBER Think Tank ASSINTEL



Per Info:
segreteria@assintel.it

Prossimo Incontro

02 Aprile

14:00 - 15:30

CYBER THINK TANK ASSINTEL

INDICE

WEBINAR

PMI e Cybersecurity: la formazione è la miglior difesa

CYBER Think Tank ASSINTEL

Per info scrivi a:
segreteria@assintel.it

Relatori:

Fabio Zanoli

Enzo Veiluva

Paolo Montali

26 Marzo 2025

12:00 - 13:00

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

Marzo 2025

Carissimi lettori,

Benvenuti in questa nuova edizione del Cyber Magazine!

La sicurezza informatica è ormai una delle variabili decisive per la stabilità economica, politica e sociale. Il panorama globale ci impone di affrontare minacce sempre più sofisticate, in un contesto in cui l’intelligenza artificiale, la regolamentazione europea e le tensioni geopolitiche ridefiniscono costantemente il nostro perimetro di azione.

La direttiva NIS2, il DORA e l’AI Act segnano un cambio di passo nella governance del rischio digitale, richiedendo alle imprese e alle istituzioni non solo conformità, ma un ripensamento strategico delle proprie difese.

Al tempo stesso, l’evoluzione delle minacce cyber dimostra quanto sia necessario un approccio resiliente: non basta proteggersi, occorre costruire sistemi capaci di adattarsi e reagire. In questo numero affrontiamo questi temi con la consapevolezza che la cybersecurity non è solo un ambito tecnico, ma una questione di interesse nazionale e globale.

Comprendere e anticipare i trend significa garantire non solo la protezione delle infrastrutture critiche, ma anche la competitività e la sovranità digitale del nostro Paese.

Le sfide sono chiare. Le risposte non possono attendere.

Buona lettura!

Pierguido Iezzi

CYBER Think Tank ASSINTEL

WEBINAR

La direttiva NIS2

CYBER Think Tank ASSINTEL

Relatori:

Federico Brenzone

Enzo Veiluva

Riccardo Modena

Per info scrivi a:

segreteria@assintel.it

14 Aprile 2025

12:00 - 13:00

Intervista a Lorenzo Guerini

Membro della Camera dei deputati della Repubblica Italiana

Guerini, Lorenzo. – Uomo politico italiano (n. Lodi 1966). Laureato in Scienze politiche e di professione consulente assicurativo, ha iniziato la sua carriera politica all'inizio degli anni Novanta militando nella Democrazia cristiana e venendo eletto per due volte consigliere comunale a Lodi. Dal 1995 al 2004 è stato presidente della Provincia di Lodi e dal 2005 al 2012 sindaco di Lodi, eletto in rappresentanza di una coalizione di centro-sinistra. Nel 2013 è stato eletto alla Camera dei Deputati nelle fila del Partito democratico, di cui nello stesso anno è stato nominato membro della segreteria nazionale. Dal 2014 al 2017 è stato vicesegretario del PD. Alle elezioni politiche del 2018 è stato rieletto alla Camera e nello stesso anno è stato eletto presidente del Comitato parlamentare per la sicurezza della Repubblica (Copasir), carica ricoperta fino al 2019. Dal 5 settembre 2019 al 22 ottobre 2022 è stato ministro della Difesa, prima del secondo governo Conte e poi del governo Draghi. Alle elezioni politiche del 2022 è stato rieletto alla Camera nelle fila del PD e nello stesso anno presidente del Copasir.

L'intelligenza artificiale sta diventando sempre più centrale nelle strategie di difesa. Come possiamo assicurarci che l'Europa non diventi dipendente da tecnologie sviluppate al di fuori dei suoi confini, mantenendo così la nostra sovranità digitale?

Lo sviluppo dell'intelligenza artificiale, peraltro ancora nelle fasi iniziali ma che presenta già tutte le sue potenzialità, è senza dubbio un passaggio tecnologico che è possibile definire epocale, termine abusato ma che in questo caso credo sia adatto a descrivere l'influenza che l'AI avrà su tutti gli ambiti della vita individuale, sociale, economica, culturale e politica. È evidente che anche per ciò che riguarda il settore della difesa questo impatto comincia già a influire sui processi e sull'operatività dei sistemi, anzi sulla logica stessa con cui si "pensano" tali sistemi. Direi, anzi, che la difesa è uno degli ambiti dove la ricerca e l'applicazione dell'AI trovano un terreno fertile e produttivo di sviluppi significativi. Ciò detto non a caso ho utilizzato il termine "potenzialità", che incorpora sia le straordinarie opportunità sia i possibili alti rischi, e questo in molteplici direzioni, compreso l'equilibrio geo strategico (che investe ovviamente anche gli ambiti economici). In questo senso il ruolo dell'Europa è certamente rilevante e chiama l'Unione a occuparsi

con puntualità degli impatti dell'AI e anche dell'implementazione delle proprie capacità di ricerca e industriali perché ne facciano un attore importante a livello globale in questo settore. L'approvazione lo scorso marzo da parte del Parlamento europeo di una legge dedicata è sicuramente il segnale che il tema AI è cominciato ad entrare nell'agenda europea. Indubbiamente però, se questa legge affronta innanzitutto i diritti delle persone e la loro protezione, l'Europa non può non continuare ad affrontare la questione della sua sovranità tecnologica e digitale. Ne va della sua capacità di essere protagonista nei nuovi scenari globali che anche con l'avvento dell'AI subiranno, se già non subiscono, rilevanti mutazioni. E siamo di fronte a scelte non solo tecniche ma primariamente politiche. Occorre mettere in comune le capacità tecnologiche e industriali già presenti, stabilire le priorità e le linee strategiche e prevedere corposi e a lungo termine investimenti in capo all'Unione. Il pacchetto che la Commissione ha presentato nel 2021, sulla base della Comunicazione del 2018, ha bisogno di essere implementato e anche con velocità. La straordinaria rapidità dell'avanzamento tecnologico rischia di travolgere i processi decisionali che a livello europeo sono necessariamente elaborati. Una cosa è certa, solo l'Unione europea nel suo complesso può essere in grado di evitare una dipendenza da altri attori, sapendo bene che i singoli Stati non hanno le forze e le capacità per essere competitivi. Questo incide ovviamente anche sul livello di sicurezza interna e sulla capacità di essere "resistenti" a possibili influssi esterni non benevoli. In sostanza quella dell'AI è una sfida tra le più decisive e urgenti per una Unione europea che voglia tutelare i suoi cittadini e rendersi capace di influire a livello globale.

La sovranità digitale europea è sempre più minacciata da giganti tecnologici extraeuropei. La NIS2 punta a rafforzare la nostra resilienza cibernetica, ma siamo davvero pronti a fronteggiare minacce sempre più sofisticate? Quali sono le lacune più urgenti che dobbiamo colmare per proteggere le nostre infrastrutture strategiche? Crede che le recenti iniziative dell'UE, come il Digital Services Act e il NIS2, siano sufficienti? Oppure serve un approccio più aggressivo per difendere le nostre PMI e il nostro patrimonio tecnologico?

Che attori esterni siano interessati a influire sul flusso di informazioni e dati che riguardano i singoli Stati e la UE nel suo complesso mi pare sia un fatto assodato, dimostrato da diverse prove. D'altra parte alcuni di essi lo dichiarano con una certa schiettezza. Questo implica prima di tutto una presa di consapevolezza comune che si deve tradurre in una condivisione di strumenti affinché la tutela della sicurezza cibernetica sia sempre più raffinata ed efficace. Le iniziative finora adottate segnalano una presa di coscienza e possono produrre i risultati sperati ma siamo in un ambito in cui l'evoluzione dello scenario, velocissima, richiede un loro costante aggiornamento. Accanto a questo è evidente che, come detto sopra per quanto riguarda l'AI, la ricerca e lo sviluppo in ambito extra europeo chiamano l'Europa a trovare le forme e i modi più efficaci per essere in grado di essere competitiva in questi settori. Anche in questo caso occorre saper comporre specifici interessi nazionali con una visione unitaria a livello europeo.

> ***"L'Europa non può non continuare ad affrontare la questione della sua sovranità tecnologica e digitale".***

Con l'istituzione di un Commissario alla difesa, si apre una nuova fase per la cooperazione europea…

La scelta di nominare un Commissario alla difesa è una buona notizia. Finalmente, verrebbe da dire. Naturalmente si tratta ancora solo di un passo verso l'obiettivo, non più differibile, della costruzione di una difesa europea compiuta. È una necessità per l'Europa, per diverse ragioni e su diversi fronti. Se pensiamo che già De Gasperi individuava nella difesa europea un elemento che avrebbe dovuto caratterizzare una Europa davvero unita, capiamo il ritardo col quale si è affrontato un tema che invece era e rimane cruciale. In questi ultimi anni si è presa consapevolezza che la difesa comune è un settore dove si gioca la capacità dell'Europa di essere protagonista nell'evoluzione, anche drammatica, degli scenari mondiali. Ma occorre essere chiari: anche in questo caso la scelta è eminentemente politica e non solo tecnica. Significa che non è possibile limitarsi a quello che, con una definizione parziale e fuorviante, viene definito un "esercito europeo". È necessario invece che l'Europa sia in grado di individuare le priorità comuni, gli strumenti per perseguirle e la volontà di utilizzarli per raggiungere i risultati previsti. A partire da una base tecnologica ed industriale condivisa, fino ad arrivare alla costruzione di capacità militari comuni.

Un'attività tutta politica come si capisce che non credo possa aspettare ancora a lungo per essere praticata con convinzione e determinazione.

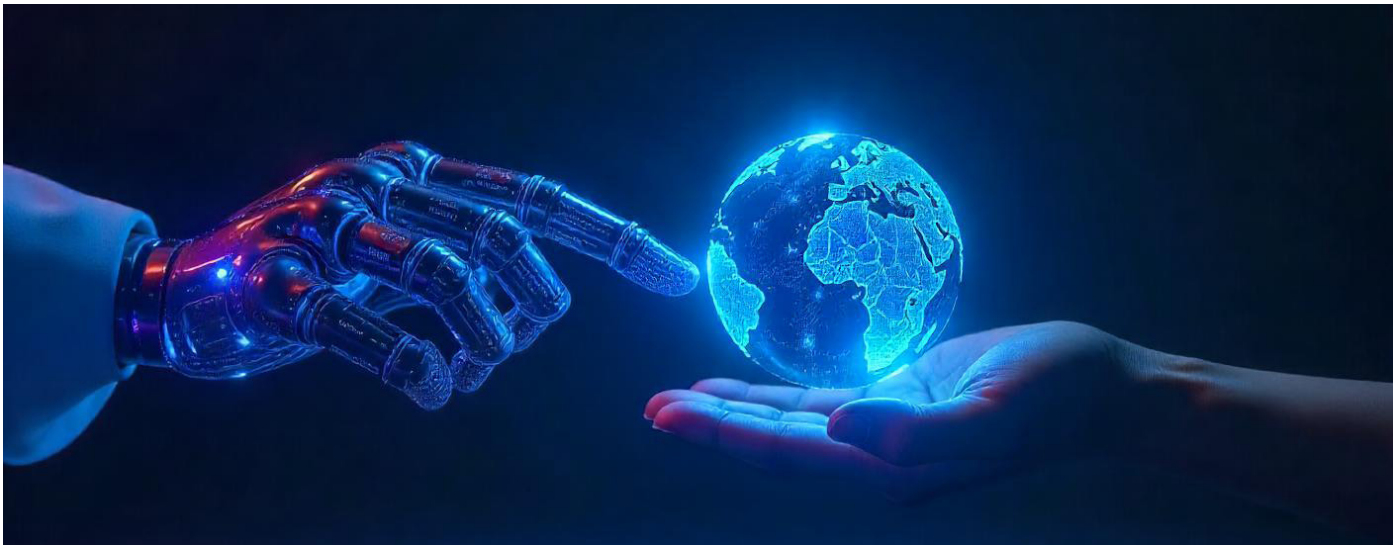
Nell'ambito della difesa europea, come può l'Italia giocare un ruolo da protagonista senza sacrificare le sue specificità industriali e tecnologiche? È possibile conciliare integrazione europea e protezione del nostro patrimonio nazionale? Come evitare che l'Italia rimanga ai margini di questo processo, specialmente nella difesa del nostro know-how tecnologico e industriale?

L'Italia è un Paese fondatore dell'Unione europea e con eccellenze industriali in ambito difesa riconosciute a livello continentale e mondiale. Un fatto che richiede ovviamente la responsabilità e la capacità di mantenere alto il proprio protagonismo nel processo di integrazione europea. Questo sta già accadendo, basti guardare la partecipazione dell'industria italiana ai programmi europei non di rado con ruolo di guida. Naturalmente la sfida è importante: l'approccio che ancora i diversi Stati europei rischiano di adottare è, per certi versi comprensibilmente, solo la difesa della propria industria nazionale, magari a scapito di concorrenti "interni". Con questo non voglio dire che non sia utile e opportuno garantire e incentivare a livello nazionale lo sviluppo dell'industria di settore. Da Ministro della difesa ho emanato a suo tempo una direttiva sulla politica industriale proprio con l'obiettivo di fissare i contorni della collaborazione, nei rispettivi ambiti di responsabilità, tra lo Stato e l'industria. Credo però che, come già detto, questo si debba inserire all'interno di una visione della difesa europea che sistematizzi le capacità dell'industria in rapporto alle scelte politiche che ne caratterizzano gli obiettivi. La capacità dell'industria di muoversi all'interno dei mercati è possibile che vada più veloce delle scelte politiche e questa possibilità, che è dettata dalle esigenze industriali, chiama la politica ad avere maggior coraggio e una prospettiva chiara, in particolare nello stanziamento di risorse adeguate e nella elaborazione di procedure comuni sui programmi. Detto questo l'integrazione europea non può che portare vantaggi anche all'Italia e alla sua industria se gestita e governata secondo linee strategiche tanto chiare e condivise quanto necessarie.

L'Europa sta aumentando il suo sostegno all'Ucraina, ma a che prezzo per la nostra sicurezza interna? Siamo davvero preparati a fronteggiare le possibili ripercussioni, anche in termini di attacchi cibernetici o destabilizzazione economica?

Il sostegno europeo all'Ucraina è indispensabile per la stessa Europa. Sono in gioco i principi e i valori alla base della democrazia e del diritto internazionale. E l'Europa, e in essa l'Italia, hanno opportunamente scelto di stare dalla parte della libertà e del diritto di fronte alla criminale invasione dell'Ucraina da parte di Putin. Che questo comporti delle conseguenze è un rischio possibile e che sta nelle cose, ma in Ucraina sono messi in discussioni i fondamenti della convivenza civile. Il che non significa che non si debbano adottare tutte le misure necessarie per una puntuale prevenzione e un efficace contrasto a possibili azioni che incidono sulla sicurezza. Ma questi rischi non possono e non devono mettere in dubbio la scelta da che parte stare: cioè dalla parte del diritto internazionale e della garanzia della sovranità e della libertà dei popoli.

"La straordinaria rapidità dell'avanzamento tecnologico richiede che l'Unione Europea acceleri nella ricerca e nello sviluppo per garantire resilienza e competitività".



Proteggere il futuro

A colloquio con Serafino Sorrenti

Serafino Sorrenti, Chief Information Security Officer (CISO) presso il dipartimento per la trasformazione digitale della presidenza del consiglio dei ministri e membro permanente del nucleo per la cybersicurezza (NCS) presso ACN.

La trasformazione digitale ha reso il concetto di sicurezza informatica sempre più centrale per la resilienza del sistema Paese. Quali sono oggi le principali sfide per garantire una protezione efficace delle infrastrutture critiche?

La trasformazione digitale non è soltanto un'opportunità straordinaria per il progresso economico e sociale, ma rappresenta anche un terreno di scontro su cui si giocano le più sofisticate strategie di attacco cibernetico. La crescente interconnessione tra settori, l'adozione di soluzioni cloud e l'esplosione dell'Internet of Things amplificano la superficie d'attacco, rendendo sempre più sfumato il confine tra il dominio fisico e quello digitale. Le infrastrutture critiche – che includono settori come energia, trasporti, sanità e telecomunicazioni – non possono più essere difese con un approccio tradizionale basato sulla mera reattività. Oggi la resilienza deve essere il principio cardine, che implica un cambio di paradigma: dalla protezione alla capacità di adattamento. È in questa logica che la direttiva europea NIS2 impone standard più elevati per la gestione del rischio, enfatizzando l'importanza di misure preventive e di un approccio integrato alla sicurezza. Dobbiamo garantire che gli operatori di servizi essenziali adottino una strategia proattiva, che preveda una solida governance del rischio e una gestione tempestiva degli incidenti.

In un contesto globale in cui le minacce cyber sono sempre più sofisticate, quali competenze devono essere sviluppate per garantire una risposta efficace a questi nuovi scenari?

Le minacce cibernetiche si evolvono con una rapidità impressionante, rendendo necessaria una costante innovazione nelle competenze e nelle metodologie di difesa. Non si tratta più soltanto di saper gestire un'infrastruttura IT sicura, ma di sviluppare una visione strategica capace di anticipare gli attacchi. Le figure chiave di oggi devono possedere una combinazione di conoscenze tecniche avanzate e capacità di analisi sistemica. Pensiamo, ad esempio, alla necessità di comprendere i modelli di attacco basati sull'intelligenza artificiale o alle tecniche di penetration testing avanzato. Tuttavia, la mera competenza tecnica non è sufficiente: la cybersicurezza è una disciplina che coinvolge processi, persone e tecnologia. Abbiamo bisogno di esperti che sappiano dialogare con i vertici aziendali, traducendo i rischi cyber in implicazioni economiche e strategiche. La formazione deve quindi

includere anche soft skills, come il crisis management, la comunicazione e la capacità di lavorare in team interdisciplinari. Ecco perché è cruciale investire nella crescita di una nuova generazione di professionisti della sicurezza, capaci di muoversi con agilità in un contesto in continua trasformazione.

> ***"La resilienza deve essere il principio cardine, che implica un cambio di paradigma: dalla protezione alla capacità di adattamento".***

Il contesto normativo europeo sta spingendo sempre più verso una maggiore armonizzazione e standardizzazione della cybersicurezza. Qual è l'impatto della direttiva NIS2 sul tessuto industriale italiano?

La direttiva NIS2 rappresenta una svolta fondamentale nel rafforzamento della resilienza cyber dell'Unione Europea. Il suo impatto sul tessuto industriale italiano è duplice: da un lato, impone un innalzamento del livello di sicurezza per un numero più ampio di soggetti, includendo non solo le infrastrutture critiche tradizionali ma anche aziende private operanti in settori strategici; dall'altro, crea un'occasione straordinaria per colmare il gap di maturità nella gestione del rischio cyber. Uno degli aspetti più significativi di questa direttiva è l'introduzione di obblighi più stringenti in termini di governance e reporting. Le aziende saranno chiamate a implementare piani di gestione del rischio più rigorosi, a garantire una maggiore trasparenza sugli incidenti e a rafforzare la cooperazione con le autorità nazionali. Questo obbligo di compliance, però, non deve essere visto come un mero adempimento burocratico, ma come un'opportunità per elevare la sicurezza aziendale a un asset strategico. In questo scenario, le piccole e medie imprese italiane – che spesso mancano delle risorse necessarie per affrontare il tema della sicurezza in modo strutturato – dovranno essere supportate in un processo di adeguamento che le renda più resilienti. Serviranno incentivi, formazione e una maggiore consapevolezza del rischio cyber come elemento integrante del business.

Nel contesto della cybersecurity, quanto è importante la collaborazione tra pubblico e privato per la resilienza del sistema Paese?

La cybersicurezza è, per definizione, un problema che nessun attore può affrontare da solo. Le minacce cyber non hanno confini, e un attacco a un'azienda privata può avere conseguenze dirette sulla sicurezza nazionale. Ecco perché la collaborazione tra pubblico e privato non è solo auspicabile, ma necessaria per garantire la resilienza del sistema Paese. Nel corso degli ultimi anni, abbiamo assistito a un significativo rafforzamento del dialogo tra le istituzioni e il mondo dell'impresa. Iniziative come il Perimetro di Sicurezza Nazionale Cibernetica hanno creato un framework di protezione che integra operatori pubblici e privati in un unico ecosistema difensivo. Tuttavia, c'è ancora molta strada da fare per costruire un modello di scambio informativo rapido ed efficace. Dobbiamo superare la logica della competizione per abbracciare un approccio collaborativo, in cui le informazioni su minacce e vulnerabilità siano condivise in modo tempestivo e strutturato. Le piattaforme di threat intelligence giocano un ruolo cruciale in questo contesto, così come la creazione di laboratori congiunti tra istituzioni e aziende per testare nuovi modelli di difesa. Il vero salto di qualità, però, arriverà quando la cultura della cybersicurezza diventerà parte integrante del tessuto imprenditoriale italiano, con una maggiore consapevolezza da parte dei consigli di amministrazione e dei decisori strategici. Solo così potremo costruire una difesa resiliente e dinamica, capace di adattarsi alle sfide di un mondo sempre più interconnesso e, purtroppo, sempre più vulnerabile.

La sicurezza informatica non è più un tema relegato agli specialisti IT, ma una priorità strategica per la sicurezza nazionale ed economica dell'intero Paese. La resilienza del sistema Italia dipende dalla nostra capacità di anticipare, adattarci e rispondere in modo coordinato alle sfide del cyberspazio. La direttiva NIS2, la crescita delle competenze e una più stretta collaborazione tra pubblico e privato rappresentano gli strumenti con cui possiamo costruire un futuro digitale sicuro, innovativo e sostenibile.

LA CYBER PER TUTTI

ISTRUZIONI SEMPLICI PER QUESTIONI COMPLESSE

CYBER Think Tank ASSINTEL

ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT

Consigli per creare una password "inviolabile"

Con l'accrescersi delle violazioni dei dati e degli attacchi di ingegneria sociale, una ***password sicura*** è la prima linea di difesa.

1. Non usare informazioni personali

2. Usare caratteri speciali

3. Usare almeno 12 caratteri

4. Usare password differenti per differenti account

5. Cambiare password regolarmente (almeno ogni 90 giorni)

6. Non condividere le password e non scriverle su POST-IT

7. Abilitare, se possibile, l'autenticazione a due fattori

8. Disabilitare "Ricordare Password?" sui motori di ricerca

9. Evitare frasi di senso compiuto o ad uso comune

10. Non memorizzare password nel browser

Crosetto clonato e Zavoli “resuscitato”: la nuova frontiera dei gemelli digitali

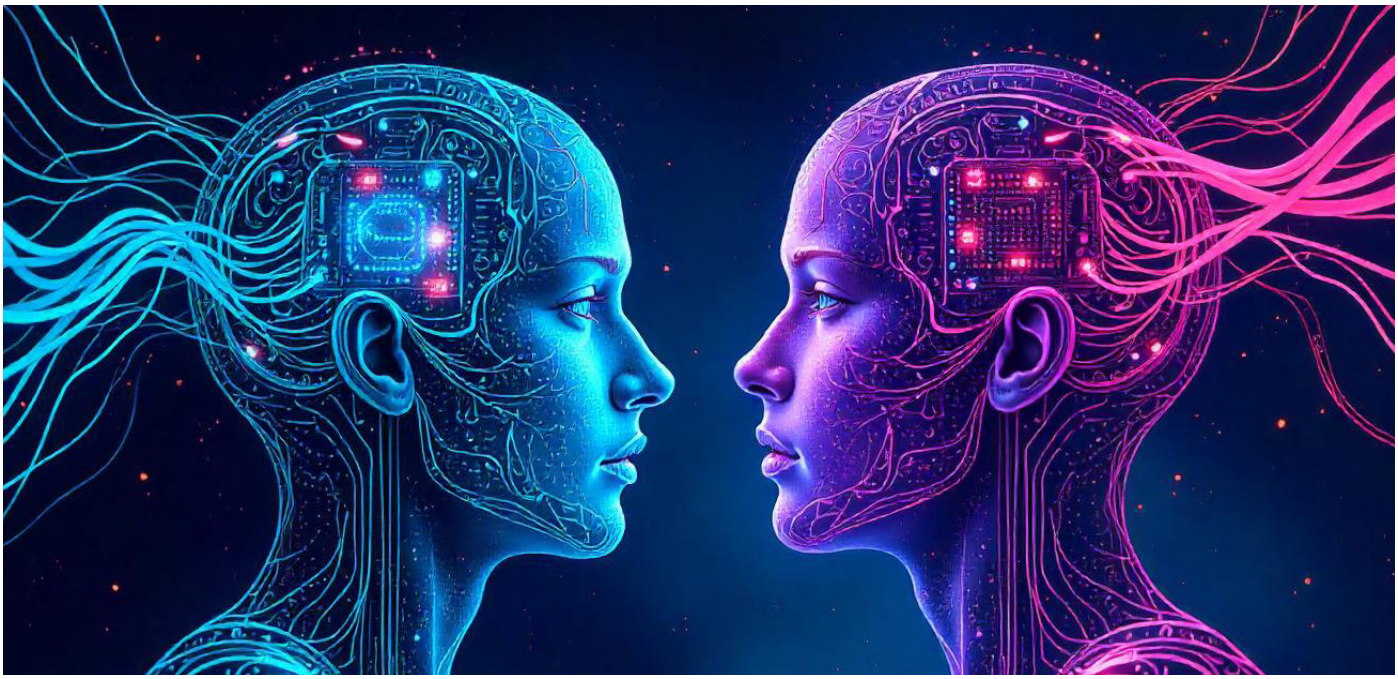
A cura di Pierguido Iezzi

Come i Dioscuri, Castore e Polluce, generati insieme a Elena dall’uovo di Leda congiuntasi con Zeus trasformato in cigno, uno è immortale e l’altro è mortale. Il primo è destinato a vivere per sempre nell’ecosistema digitale, attraverso la sua voce riprodotta in modo così realistico da apparire autentica, mentre il secondo è confinato nel mondo fino al compimento della sua vita terrena. Questo fenomeno, noto come digital twin o gemello digitale, è ciò che sta accadendo grazie ai software di intelligenza artificiale che sono in grado di riprodurre qualsiasi timbro vocale partendo da uno spezzone originale di 15 secondi. Il più noto è Voice Engine di Open AI, mai rilasciato al pubblico per i dubbi della società di Sam Altman riguardo il suo potenziale utilizzo criminale e per le polemiche insorte in seguito alla riproduzione della voce di Scarlett Johannson nel film “Her”, ma ne esistono a decine disponibili sulla rete dove l’imitazione vocale è oggi alla portata di chiunque abbia strumenti adeguati: pochi secondi di registrazione e circa 50$ per consentire all’algoritmo di replicare timbro, intonazione e persino pause di un individuo.

Recenti casi di cronaca e di costume hanno portato alla ribalta il fenomeno anche in Italia. È di questi giorni la notizia che diversi imprenditori hanno versato cifre per milioni di euro in un conto corrente di Hong Kong per adempiere alla richiesta del gemello digitale del Ministro della Difesa Guido Crosetto di provvedere alla raccolta di risorse per pagare la liberazione della giornalista Cecilia Sala. La voce del Ministro, abilmente riprodotta attraverso la IA, ha ingannato persino chi lo conosce di persona, dando vita a una truffa di ingenti proporzioni di cui ancora non si conoscono bene i confini e l’entità e sulla quale la Procura di Milano sta indagando sulla base delle denunce finora pervenute.

La medesima sorte, ma con tutt’altre finalità, è toccata alla voce del celebre giornalista Sergio Zavoli, digitalmente ricostruita per farlo dialogare con la moglie Alessandra in un podcast di cinque episodi, disponibili su Rai Play e realizzati per Radio Due, basati sui taccuini inediti in cui la coppia aveva trascritto le proprie riflessioni su temi tra i più disparati, dalla clausura al ciclismo.

Si tratta di due casi emblematici che riguardano il primo i rischi connessi all’utilizzo criminale dell’intelligenza artificiale, con possibili ripercussioni anche sulla sicurezza nazionale, e il secondo gli interrogativi profondi sull’eticità di tale pratica: il defunto sarebbe stato d’accordo riguardo un simile utilizzo della propria voce? Se per Ser-



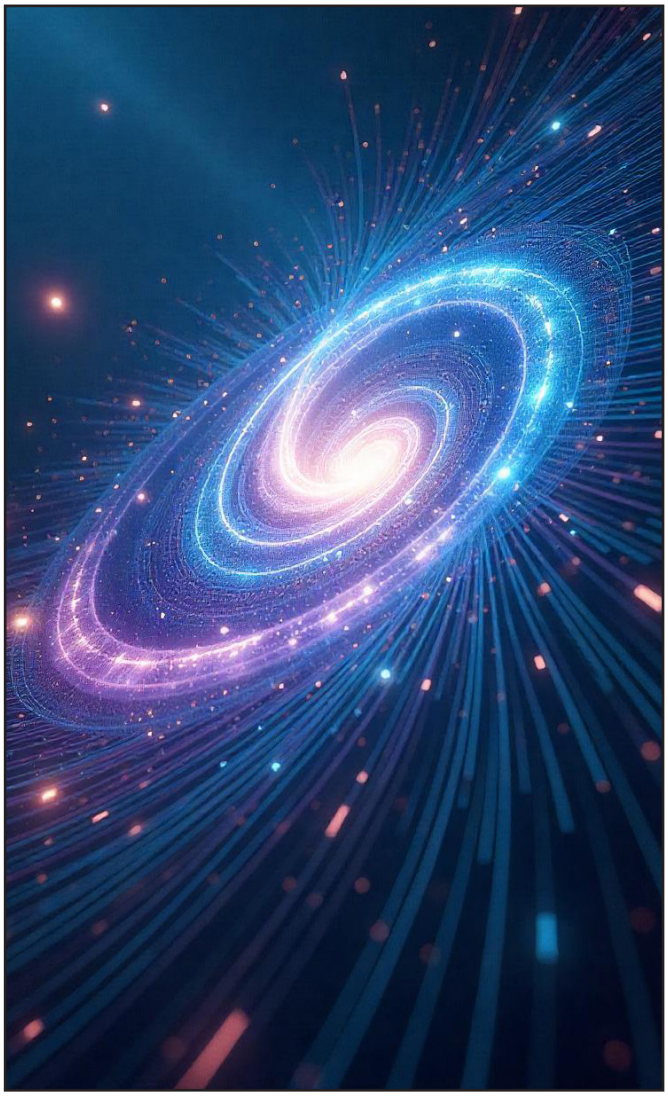
gio Zavoli, giornalista per vocazione votato alla curiosità per l'innovazione, sembrano non esserci dubbi, per altre personalità non tutto è così scontato. Dove si colloca infatti il confine tra l'omaggio alla memoria di un grande personaggio e l'artificiosa manipolazione del ricordo?

La clonazione vocale tuttavia è solo una delle possibili declinazioni del più ampio fenomeno dei gemelli digitali. Nato in ambito industriale per simulare macchinari e processi produttivi, il concetto di Digital Twin si sta estendendo alla sfera umana, generando copie virtuali di individui capaci di parlare, agire e persino prendere decisioni. Ciò ha conseguenze rilevanti in termini di sicurezza e identità: la voce, fino a poco fa considerata un carattere distintivo impossibile da riprodurre, può trasformarsi in un'arma subdola per manipolare o truffare.

Per contro, l'utilizzo responsabile dei gemelli digitali apre a orizzonti di grande speranza. In ambito medico, la possibilità di ricreare digitalmente il corpo umano sta già rivoluzionando la personalizzazione delle cure, con modelli in grado di simulare il funzionamento degli organi, così da tarare terapie ad hoc su ciascun paziente. Nel campo della sicurezza informatica, lo stesso concetto applicato ai sistemi IT sta dando vita ad una sorta di "cyber-twin", copie virtuali delle infrastrutture aziendali da sottoporre a test di vulnerabilità e attacchi simulati per prevenire intrusioni e proteggere l'operatività. Questa tecnologia trova applicazione anche nell'urbanistica, con la creazione di gemelli digitali degli spazi urbani per migliorare la pianificazione, ottimizzare il traffico e ridurre gli sprechi energetici, provando in anticipo gli effetti di nuovi progetti infrastrutturali. Importanti anche gli utilizzi nel campo della tutela dell'ambiente: la Spagna ha sviluppato un gemello digitale dell'ecosistema del Mar Menor nella regione di Murcia, la più grande laguna salata d'Europa minacciata dal turismo di massa: il modello servirà a comprendere gli effetti dell'antropizzazione, permettendo ai ricercatori di studiare in tempo reale possibili soluzioni per tutelare una delle aree più fragili del Mediterraneo.

Come in ogni applicazione di una tecnologia, quindi, tutto è affidato alla responsabilità umana. La macchina non ha etica, è il suo utilizzo che ne determina le finalità. Se da un lato i gemelli digitali possono favorire le truffe, dall'altro possono rappresentare un valore aggiunto per scienza, medicina, ambiente e sicurezza.

L'AI Act segna un primo passo importante per governare lo sviluppo di queste tecnologie, ma non basta: occorrono anche consapevolezza e capacità critica da parte di istituzioni, aziende e cittadini. Il futuro dei gemelli digitali e dell'intelligenza artificiale dipende dalle scelte che ora vengono prese. Il timore dei lati oscuri di queste tecnologie può alimentare uno spirito luddista, oppure può prevalere la fiducia nelle potenzialità positive per migliorare la vita collettiva. La storia del progresso dell'umanità dimostra che ha sempre prevalso il secondo aspetto, a tutto vantaggio della elevazione della condizione umana. Tutto sta nel mantenere viva l'attenzione su chi siamo e su come vogliamo plasmare il domani.



"Il futuro dei gemelli digitali e dell'intelligenza artificiale dipende dalle scelte che ora vengono prese, perché la macchina non ha etica: è l'uomo a determinarne le finalità."

Bilanciare AI e Cybersecurity: i percorsi delle organizzazioni

A cura di Elena Vaciago

L'Intelligenza Artificiale (AI) è l'evoluzione più promettente nel campo della cybersecurity: può incrementare le capacità di difesa di infrastrutture e dati, ottimizzando il rilevamento di attacchi informatici, fornendo una risposta più veloce ed efficace in caso di incidente informatico e aiutando, in sostanza, a prevenire danni considerevoli, come quelli originati dai ransomware. Le opportunità dell'AI applicate alla cybersecurity sono numerose, ma, trattandosi di uno strumento potente e di una tecnologia "dual use", benefica ma potenzialmente malevola, bisogna fare molta attenzione alle sfide che presenta nell'adozione.

Un primo elemento da considerare è che, se da un lato può incrementare l'efficacia della difesa, con infrastrutture più robuste e resilienti e una maggiore velocità nella risposta agli attacchi, dall'altro, gli stessi attaccanti la stanno già utilizzando per realizzare azioni più sofisticate, attacchi più mirati o maggiormente distruttivi. Ad esempio, è stato osservato l'utilizzo malevolo della GenAI per mimare fonti affidabili nelle mail di phishing, nei post social o nelle chat interattive; per migliorare le attività di ricerca di informazioni sui target degli attacchi (Osint, ricerca di dati da fonti pubbliche); per facilitare la creazione di malware sofisticato e specifico per singoli obiettivi oppure per automatizzare i processi di identificazione e sfruttamento delle vulnerabilità nel software e nelle reti delle organizzazioni prese di mira.

È di quest'anno la notizia di specifiche campagne malevole che hanno avuto come obiettivo ChatGPT, con lo scopo di acquisire dati sensibili condivisi con la chat e quindi compromessi. Lo stesso vale per i dati utilizzati per il training dello strumento. Inoltre, esistono siti realizzati ad hoc che "mimano" il funzionamento delle chatbot di GenAI, con nomi molto simili, per frodare gli utenti, indirizzarli verso siti malevoli e indurli a scaricare malware. Un altro esempio riguarda app web che gestiscono in modo non sicuro le chiavi API OpenAI.

I benefici dell'AI nella cybersecurity e i punti di attenzione nell'adozione

È risaputo che le capacità di cybersecurity possono essere ampiamente incrementate con l'ausilio dell'AI in svariati ambiti: dalla gestione degli incidenti alla cyber threat intelligence, dal rilevamento delle minacce all'individuazione e alla risoluzione di vulnerabilità. Anche per quanto riguarda la sensibilizzazione sui temi della sicurezza informatica e l'addestramento delle persone, l'AI generativa è uno strumento di grande ausilio. Tuttavia, l'introduzione dell'AI a fianco delle attività e delle misure di cybersecurity deve avvenire tenendo conto di una serie di limiti e di sfide. In generale, come spesso accade, non basterà dotarsi di queste tecnologie: bisognerà contestualizzare le soluzioni e calarle nel quotidiano e nel contesto specifico.

Le raccomandazioni sono, da un lato, di ordine generale e, dall'altro, molto specifiche. In generale, introdurre tecnologie innovative richiede un ripensamento dei processi operativi e una formazione adeguata delle persone ai nuovi utilizzi. Nello specifico, l'addestramento degli algoritmi AI necessita di grandi quantità di dati, che tipicamente sono già a disposizione di chi si occupa di protezione cyber e deve quotidianamente analizzare molteplici segnali per tenere sotto controllo infrastrutture e applicazioni aziendali: è importante che le diverse tecnologie di cybersecurity siano integrate e collegate all'AI, in sinergia tra loro.

Gli algoritmi AI riescono, una volta ben contestualizzati, a rilevare rapidamente schemi e anomalie che possono indicare la presenza di un attaccante. I dati vanno quindi analizzati in tempo reale e tutte le attività devono essere orchestrate e automatizzate. In aggiunta, le capacità di

machine learning aiutano a realizzare modelli predittivi che, uniti a informazioni di threat intelligence, possono contribuire a prevedere schemi di comportamento tipici dei cyber criminali.

Mettere in sicurezza gli algoritmi AI in azienda

Se l'AI si sta dimostrando un efficace ausilio per la cybersecurity, viceversa, l'utilizzo di sistemi AI in molteplici ambiti aziendali non può prescindere da un'attenta valutazione dei rischi e dall'impiego di specifiche metodologie e misure di sicurezza.

È importante conoscere le vulnerabilità del software AI e GenAI, perché potranno essere sfruttate da attaccanti malevoli (Adversarial AI Attacks). Debolezze a livello di data model aprono alla possibilità che vengano manipolati in modo subdolo gli input (i prompt o anche i dati di addestramento) per rendere questi strumenti inaffidabili e produrre output non corretti, con possibili conseguenze sui processi critici collegati. Accessi non autorizzati alle infrastrutture degli strumenti GenAI potrebbero invece consentire esfiltrazioni o alterazioni dei dati utilizzati nel modello o condivisi dagli utenti.

Un altro rischio è legato alla possibilità che il modello di machine learning o anche il LLM venga duplicato in modo non autorizzato, e che sia quindi utilizzato in modo malevolo dagli hacker per bypassarne la proprietà intellettuale, individuarne vulnerabilità o per altri fini illeciti, come la realizzazione di tool AI specifici per utilizzi fraudolenti.

L'AI, sia sviluppata internamente sia utilizzata as a service (come, ad esempio, i servizi di AI generativa online), sarà sempre più presente in azienda. Servirà quindi identificare un corretto bilanciamento tra le esigenze operative del business e un utilizzo dell'AI che risponda a opportuni requisiti di sicurezza. Fondamentale, dunque, introdurre regole specifiche e puntuali, creando cultura nell'organizzazione per un utilizzo responsabile e corretto delle capacità AI.

Questi percorsi di attenzione verso l'uso dell'AI fanno spesso capo alla cybersecurity. Dove sono iniziati, policy e procedure hanno come punto di riferimento alcune best practice, come le linee guida OWASP (OWASP Machine Learning Security Top Ten).

"Le opportunità dell'AI applicate alla cybersecurity sono numerose, ma, trattandosi di uno strumento potente e di una tecnologia "dual use", benefica ma potenzialmente malevola, bisogna fare molta attenzione alle sfide che presenta nell'adozione".

L'importanza di un framework complessivo di AI Governance

Per tenere il passo con un'innovazione importante, che andrà adottata in modo sicuro, si sta sviluppando un'ampia dottrina su come indirizzare i rischi informatici dell'AI, attraverso misure tecniche e approcci metodologici che in larga parte ricalcano quelli classici della gestione dei rischi cyber. Sarà prioritaria la sensibilizzazione delle persone a questi temi, la formazione dei dipendenti rispetto a rischi come i deepfake e agli utilizzi appropriati delle chatbot di GenAI, oltre all'upgrade delle competenze del team cyber. A livello di contromisure tecniche, si diffonderanno sempre più strumenti AI-based per rilevare attività sospette e rispondere rapidamente. Servirà poi un monitoraggio continuo e aggiornato, atto a rilevare comportamenti insoliti che possono essere legati ad attacchi che utilizzano l'AI. Sempre più importanti saranno anche le partnership e le collaborazioni esterne, per mantenersi aggiornati su tematiche in rapida evoluzione. Esercitazioni specifiche serviranno inoltre a simulare scenari di attacco AI-based.

Non va dimenticato, però, che la Governance dell'AI sarà un tema molto più ampio, di cui la cybersecurity dell'AI è solo una parte.

Le organizzazioni pubbliche e private, in risposta a requisiti normativi più stringenti (es. AI Act), dovranno dotarsi di un ampio framework di AI Governance per garantire un utilizzo sicuro e regolato dell'intelligenza artificiale in molteplici campi.

Smart City e Sicurezza Informatica: la sfida della NIS2 per Roma

A cura dell'Ing. Menichelli e Ing. Righetti

Introduzione

Il concetto di "Smart City" si è rapidamente affermato come paradigma fondamentale per lo sviluppo urbano del XXI secolo. Integrando tecnologie digitali quali l'Internet of Things (IoT), l'Intelligenza Artificiale (AI) e i Big Data, le Smart City promettono di migliorare la qualità della vita dei cittadini, ottimizzare la gestione delle risorse e rendere le città più efficienti e sostenibili. Roma, con la sua storia millenaria e le sue complesse sfide urbane, ha intrapreso un percorso di trasformazione digitale, avviando progetti in ambiti come la mobilità, l'illuminazione pubblica e la gestione dei rifiuti. Tuttavia, la crescente interconnessione e la dipendenza da sistemi informatici espongono le città a rischi informatici sempre più significativi. Un attacco mirato a un'infrastruttura critica, come la rete elettrica o il sistema di trasporto, potrebbe paralizzare la città, causando danni ingenti e mettendo a rischio la sicurezza dei cittadini. In tale contesto, la direttiva europea NIS2 (Network and Information Security 2) riveste un ruolo cruciale per rafforzare la postura di cybersecurity degli Stati membri e garantire la resilienza delle infrastrutture critiche.

Roma tra Smart City e Vulnerabilità

Roma ha avviato diversi progetti volti a migliorare l'efficienza urbana attraverso la digitalizzazione. "Roma Mobilità" rappresenta una piattaforma finalizzata all'ottimizzazione del traffico e del trasporto pubblico, mentre progetti di illuminazione intelligente e raccolta differenziata "smart" puntano a una gestione ottimale delle risorse. Anche la digitalizzazione dei servizi comunali, come l'Anagrafe Digitale, costituisce un progresso rilevante. Tuttavia, tali iniziative si confrontano con vulnerabilità intrinseche alla città. L'estensione territoriale, la complessità amministrativa e la presenza di sistemi di controllo industriale (ICS) obsoleti in settori critici quali i trasporti (ATAC) e l'energia (ACEA) rappresentano sfide considerevoli. Inoltre, l'assenza di una segmentazione efficace delle reti e una formazione carente del personale in materia di cybersecurity incrementano ulteriormente la superficie di attacco.

NIS2, un nuovo quadro normativo per la Cybersecurity

La direttiva NIS2, entrata in vigore a inizio 2023, amplia l'ambito di applicazione della precedente direttiva NIS, includendo nuovi settori strategici e introducendo obblighi più stringenti per gli operatori di servizi essenziali (OSE) e i soggetti importanti. Tra i settori coinvolti, oltre a quelli classici come energia, trasporti e sanità, figurano la pubblica amministrazione, la gestione dei rifiuti e i fornitori di servizi digitali. Gli operatori sono tenuti a effettuare valutazioni regolari dei rischi, adottare misure di sicurezza tecniche e organizzative adeguate (gestione degli incidenti, continuità operativa, sicurezza della catena di approvvigionamento, formazione del personale) e notificare gli incidenti di sicurezza significativi alle autorità competenti, in Italia l'Agenzia per la Cybersicurezza Nazionale (ACN). La NIS2 prevede, inoltre, sanzioni più severe in caso di non conformità, fino a 10 milioni di euro o al 2% del fatturato mondiale annuo.

In Italia, la direttiva NIS2 è stata recepita dal d.lgs. n. 138/2024 (Decreto NIS), in vigore dal 16 ottobre 2024.

L'impatto su Roma e le Sfide Future

La direttiva NIS2 avrà un impatto rilevante su Roma. Enti quali ATAC, ACEA, gli aeroporti di Roma, i principali ospedali e il Comune di Roma stesso (per i servizi digitali) dovranno conformarsi ai nuovi requisiti.

Le implicazioni per i fornitori di servizi sono significative, comprendendo misure quali:

- Gestione degli Accessi e Autenticazione Avanzata: implementazione di sistemi di autenticazione multifattoriale (MFA) e controlli rigorosi per limitare l'accesso ai dati e alle infrastrutture critiche.
- Monitoraggio e Gestione delle Vulnerabilità: obbligo di adottare soluzioni per l'identificazione e la mitigazione tempestiva delle vulnerabilità, con monitoraggio continuo e reportistica periodica.
- Backup e Ripristino: responsabilità di implementare soluzioni di backup affidabili per garantire la continuità operativa dei servizi offerti.

Per garantire il rispetto della direttiva, i fornitori ICT di Roma Capitale e delle sue società dovranno rispettare standard di sicurezza riconosciuti, come ISO 27001, e implementare processi rigorosi per la gestione dei rischi derivanti da terze parti o subappaltatori. Saranno inoltre coinvolti in esercitazioni e simulazioni per garantire la prontezza nella gestione degli incidenti.

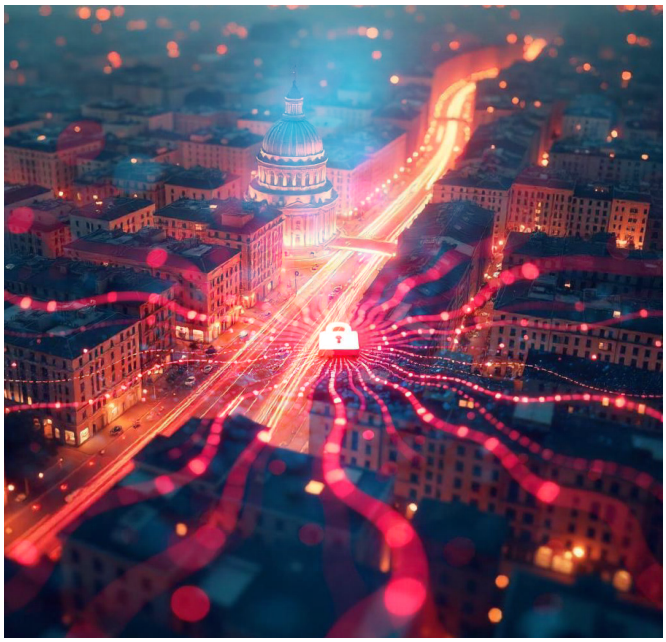
Le sfide principali per la Capitale includeranno il coordinamento tra i numerosi enti coinvolti, gli investimenti necessari per aggiornare le infrastrutture e formare il personale, nonché la complessità burocratica che potrebbe rallentare il processo. Tuttavia, la NIS2 rappresenta anche un'opportunità per migliorare la sicurezza e la resilienza delle infrastrutture critiche romane, stimolare l'innovazione nel campo della cybersecurity e rafforzare la fiducia dei cittadini nei servizi digitali.

Investire nella cybersecurity è un investimento strategico per il futuro di Roma.

Misure di Sicurezza e Collaborazione Pubblico-Privato

Per affrontare le sfide della cybersecurity nelle Smart City, è essenziale adottare un approccio "security by design", integrando la sicurezza sin dalle prime fasi di progettazione dei sistemi. La segmentazione delle reti, il controllo degli accessi, la protezione dei dispositivi IoT, la crittografia, il monitoraggio continuo e la gestione degli incidenti sono elementi fondamentali. La formazione del personale e la sensibilizzazione sui rischi informatici rappresentano ulteriori fattori di successo.

Un altro aspetto cruciale è la collaborazione tra enti pubblici e privati. La condivisione di informazioni su minacce e vulnerabilità, lo sviluppo di standard comuni e l'organizzazione di esercitazioni congiunte sono imprescindibili. A Roma, sarebbe opportuno creare centri di competenza sulla Cybersecurity per le Smart City e promuovere progetti di ricerca congiunti tra università, aziende e amministrazione pubblica. La collaborazione e la condivisione delle informazioni tra i diversi stakeholder (ATAC, ACEA, Comune, ecc.) rappresenteranno fattori determinanti per il successo.



Conclusioni

La trasformazione di Roma in una Smart City è un processo ineludibile che offre grandi opportunità, ma la cybersecurity deve essere considerata una priorità assoluta. La direttiva NIS2 fornisce un quadro normativo significativo per rafforzare la sicurezza delle infrastrutture critiche e dei servizi digitali, ma la sua implementazione efficace richiede un impegno concreto da parte di tutti gli attori coinvolti. Investire nella cybersecurity non rappresenta solo un costo, ma un investimento strategico per il futuro, per garantire la sicurezza dei cittadini, la resilienza delle infrastrutture e la prosperità economica di Roma nell'era digitale. La collaborazione tra pubblico e privato, la promozione di una cultura della cybersecurity e l'adozione di un approccio proattivo e lungimirante saranno determinanti per il successo di Roma come Smart City sicura e resiliente. Solo attraverso un impegno condiviso sarà possibile trasformare la Capitale in una città intelligente, efficiente e, soprattutto, sicura.

NIS2 & DORA
Confronto e Contrasto

A cura di Mark Alan Barlow

Con la trasformazione digitale che continua ad attraversare tutti i settori, diventa sempre più importante sfruttare le tecnologie avanzate per migliorare l'efficienza e la fornitura di servizi. Tuttavia, questo maggiore affidamento ai sistemi digitali comporta una maggiore esposizione ai rischi informatici. L'Unione Europea (UE) ha compiuto passi significativi per mitigare questi rischi con l'introduzione della NIS2 (Network and Information Security Directive), che richiede alle aziende di tutti i settori di valutare la propria posizione di sicurezza e di implementare un piano d'azione correttivo per migliorare le difese di cybersecurity, nonché con il Digital Operational Resilience Act (DORA), una normativa completa volta a rafforzare la cybersecurity e la resilienza operativa delle istituzioni finanziarie e dei loro fornitori di ICT (Information and Communication Technology).

Il NIS2 è entrato in vigore il 17 gennaio 2023 e deve essere implementato da tutti gli Stati membri dell'UE entro il 17 ottobre 2024, mentre il DORA è stato formalmente adottato nel novembre 2022. Le entità finanziarie e i loro fornitori IT terzi hanno avuto tempo per conformarsi al DORA, entro il 17 gennaio 2025.

Un importante punto in comune tra DORA e NIS2 è il potenziamento della resilienza informatica. Mentre la Cyber Security ha l'obiettivo di proteggere da un attacco informatico e di tenere i cattivi attori fuori dall'ambiente, la Cyber Resilience ha l'obiettivo di proteggere da un attacco informatico e di garantire la capacità di continuare le operazioni aziendali dopo che tale attacco si è verificato, e di essere in grado di dimostrare che tali misure sono state adottate e sono in vigore. Questo nuovo approccio genera impatti e risultati diversi, come ad esempio:

- L'azienda deve comprendere il rischio end-to-end, che include le terze parti della catena di fornitura.
- È necessario identificare i diversi livelli di rischio, cui corrispondono varie strategie di mitigazione.
- Le soluzioni, i processi e le procedure non devono solo essere in atto, ma devono essere dimostrate come funzionanti in scenari reali, e queste politiche e procedure devono essere continuamente riviste e valutate e devono essere costantemente adeguate.

Allo stesso tempo, NIS2 e DORA possono essere confrontati e contrapposti, come illustra la seguente tabella:

NIS2	DORA
Misure legali per aumentare il livello generale di sicurezza informatica nell'Unione Europea.	Quadro normativo sulla resilienza operativa digitale.
Una direttiva UE - richiede l'implementazione da parte di ogni Stato - lascia libertà agli Stati di specificare in modo più preciso - viene applicata a livello nazionale.	Un regolamento dell'UE, direttamente vincolante in tutti i Paesi dell'Unione - applicato direttamente dall'UE. DORA ha la precedenza su NIS2.
Una serie più ampia di misure di sicurezza obbligatorie e nuovi requisiti di notifica degli incidenti per le entità essenziali e importanti.	L'obiettivo è armonizzare la legislazione per stabilire un quadro digitale unificato che consenta alle imprese di adattarsi e resistere a tutti i tipi di interruzioni e minacce legate alle ICT.
Enti essenziali come energia, sanità, trasporti, banche, ecc. e nuovi enti importanti come acqua, rifiuti, produzione/trasformazione alimentare, produzione, fornitori digitali, ecc.	Settore finanziario completo. Altre imprese che includeranno risorse cloud, analisi dei dati e revisione contabile. Ampliato, ad esempio Crypto, destinato ad espandersi ulteriormente.
>150.000 aziende colpite	>20.000 aziende impattate

Come nel caso del GDPR, entrambi comportano sanzioni in caso di non conformità:

NIS2:

- Entità essenziali: 10.000.000 di euro o il 2% del fatturato totale annuo a livello mondiale dell'esercizio precedente, se superiore.
- Entità importanti: massimo di almeno 7.000.000 di euro o almeno l'1,4% del fatturato totale annuo a livello mondiale dell'esercizio precedente, a seconda di quale sia il valore più alto.
- Sospensione dell'attività.
- Le persone fisiche che ricoprono posizioni dirigenziali siano responsabili di misure di sicurezza informatica, divieti, multe e procedimenti penali.

DORA:

- Fino a 10.000.000 di euro o al 2% del fatturato totale annuo a livello mondiale o fino all'1% del fatturato medio giornaliero dell'azienda a livello mondiale.
- Le persone fisiche possono incorrere in multe fino a 1.000.000 di euro.
- I fornitori di servizi ICT critici di terze parti, parte integrante di entità finanziarie, potrebbero incorrere in multe ancora più elevate fino a 5.000.000 di euro o 500.000 di euro per i singoli, se non rispettano i severi standard DORA.

È possibile analizzare i due normativi e tracciare una mappa dei vari articoli che li separano:

NIS2	DORA
Identificazione di beni da proteggere e rischi e pericoli	Articolo 21a
Cosa costituisce un'azienda minima vitale e il tempo di ripristino	Articolo 21e
Prevenzione della violazione (End Point) e protezione (crittografia)	Articolo 21h/21g
Rilevamento delle minacce attive e latenti	Articolo 21e
Risposta e recupero	Articolo 21c
Processi interni di monitoraggio, analisi, miglioramento e condivisione delle best practice	Articolo 21a/f

Esiste una notevole sovrapposizione tra NIS2 e DORA (e ISO 27001). Allo stesso modo, la certificazione ISO27001 fornisce una solida base per la gestione della sicurezza delle informazioni, ma non copre completamente gli aspetti di resilienza operativa richiesti. Le istituzioni finanziarie con certificazioni ISO27001 esistenti dovranno eseguire delle analisi delle lacune per assicurarsi di soddisfare i più ampi requisiti di resilienza.

Con l'avvicinarsi della scadenza del 2025, gli istituti finanziari e i fornitori di ICT devono accelerare gli sforzi per raggiungere la conformità al DORA. Non si tratta di un compito da poco. Per molte organizzazioni, in particolare quelle che operano in più giurisdizioni, l'allineamento ai severi requisiti del DORA richiederà cambiamenti significativi nella governance, nella gestione del rischio e nei processi operativi.

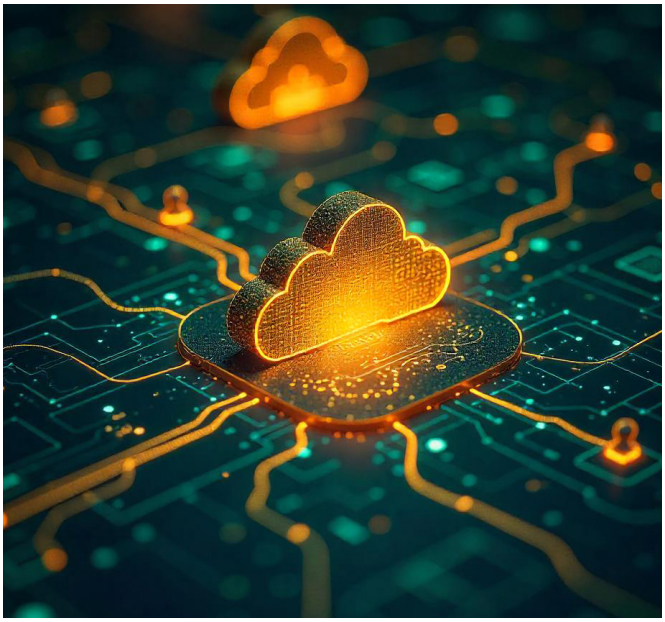
Tuttavia, il raggiungimento della conformità al DORA presenta anche delle opportunità. Le organizzazioni che implementano con successo i requisiti del DORA non solo rafforzeranno la loro posizione di cybersecurity, ma otterranno anche un vantaggio competitivo. La conformità al DORA diventerà un marchio di fiducia e affidabilità nel settore finanziario, in particolare per le istituzioni che si affidano a fornitori terzi.

Inoltre, il passaggio a una maggiore trasparenza e condivisione delle informazioni sulla scia del DORA potrebbe favorire un approccio più collaborativo alla sicurezza informatica nel settore finanziario. Con la continua evoluzione degli attacchi informatici, la capacità di condividere rapidamente le informazioni sulle minacce e di coordinare le risposte sarà essenziale per ridurre al minimo l'impatto delle interruzioni.

In conclusione, NIS2 e DORA rappresentano un coraggioso passo avanti negli sforzi dell'UE per salvaguardare il settore finanziario dalla crescente minaccia di attacchi informatici e di interruzioni dei servizi ICT. Con il suo quadro completo e l'attenzione alla resilienza operativa. Sebbene la strada verso la conformità possa essere impegnativa, coloro che abbracceranno il regolamento non solo garantiranno la loro sopravvivenza in un mondo sempre più digitale, ma si posizioneranno anche come leader nella cybersecurity e nella resilienza operativa.

Con l'avvicinarsi della scadenza del 2025, il settore finanziario deve agire rapidamente per adattarsi a questo nuovo panorama normativo. L'era della resilienza operativa digitale è alle porte e chi non si prepara rischia di rimanere indietro.

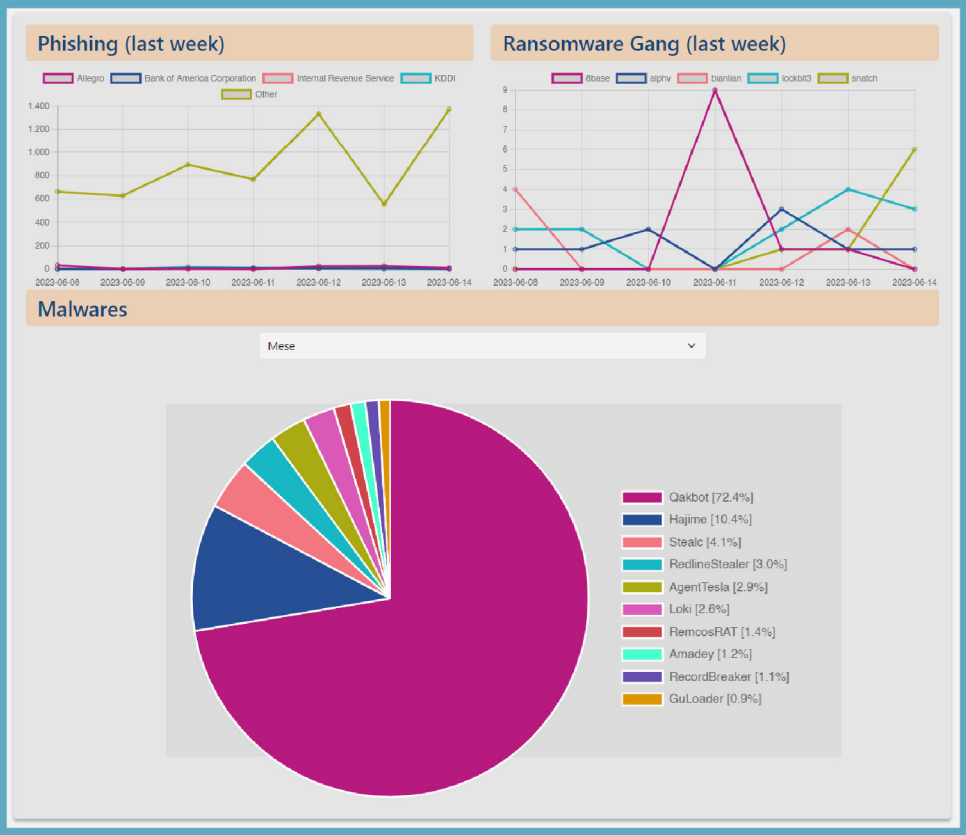
CYBER
Think Tank
ASSINTEL



Threat Infosharing

CYBER Think Tank ASSINTEL

Garantire agli Associati Assintel un servizio di early warning sulle minacce e rischi cyber giornalieri.



Per info scrivi a:

segreteria@assintel.it

Intelligenza Integrata
Quando l'AI incontra il genio della biologia

A cura di Silvia Felici

Con il rapido evolversi delle minacce informatiche, la cybersecurity deve sviluppare soluzioni sempre più avanzate e resilienti. Un approccio innovativo consiste nella trasformazione e nell'evoluzione dell'intelligenza artificiale verso un'intelligenza ispirata a quella biologica, un modello che applica i principi e i processi della biologia alla sicurezza informatica. Questo approccio si ispira a meccanismi naturali, come l'adattamento degli organismi viventi, il sistema immunitario e le reti neurali biologiche.

Queste ultime, costituite da interconnessioni interneuronali nel cervello e nel sistema nervoso periferico, sono in grado elaborare informazioni, anche sofisticate, attraverso segnali elettrici e neurochimici supportando funzioni fondamentali come apprendimento, memoria ed adattamento.

L'intelligenza biologica utilizza l'osservazione e l'imitazione di questi processi per progettare sistemi di difesa informatica più robusti ed efficaci. Grazie alla capacità di adattamento, resilienza e risposta rapida dei meccanismi biologici, è possibile integrare queste dinamiche con le tecnologie avanzate per creare soluzioni capaci di identificare, prevenire e contrastare le minacce emergenti nel cyberspazio, garantendo flessibilità ed efficienza in un contesto in costante evoluzione.

Concetto di Intelligenza Biologica

L'intelligenza biologica è la capacità degli organismi viventi di adattarsi, apprendere e rispondere agli stimoli esterni in modo efficace e resiliente.

Applicata alla cybersecurity, questa idea ispira la creazione di sistemi informatici avanzati, in grado di:

- **Adattamento Dinamico**

  Proprio come gli organismi viventi si adattano ai cambiamenti ambientali, i sistemi di sicurezza informatica necessitano di una evoluzione continua per fronteggiare costantemente le nuove minacce in modo fattivo.

- **Apprendimento Continuo**

  Proprio come il cervello umano che utilizza i suoi sistemi corticali, sottocorticali e limbici per fronteggiare al meglio le quotidiane esperienze emozionali, così la cybersecurity analizza a velocità fantascientifica sia dati che esperienze negative/positive per evolvere le proprie difese.

- **Resilienza alle Minacce**

  Seguendo l'esempio dei sistemi biologici, noti per la loro capacità di resistere, aggiornando la produzione di nuovi anticorpi e rirendersi rapidamente più efficaci di prima, così le infrastrutture informatiche devono essere progettate per garantire continuità operativa anche in caso di attacchi o malfunzionamenti.

Applicazioni dell'Intelligenza Biologica nella Cybersecurity

1. **I Sistemi Immunitari Artificiali (AIS)**

Sono modelli ispirati al sistema immunitario umano, creati per rilevare e fermare le minacce informatiche. Un esempio importante è l'algoritmo delle cellule dendritiche (DCA), rilevando e reagendo agli agenti patogeni attivano la risposta immunitaria contro le infezioni. Analogamente il DCA nella cybersecurity offre una protezione attiva e dinamica, individuando e analizzando le anomalie in tempo reale per contrastare intrusioni e attacchi.

2. **Gli Algoritmi Evolutivi**

Ispirati alla selezione naturale ed all'evoluzione, sono utilizzati per risolvere problemi complessi attraverso un processo di ottimizzazione. In cybersecurity, questi algoritmi vengono impiegati per creare chiavi crittografiche sicure e firewall adattivi che evolvendosi autonomamente rispondono alle nuove minacce ed agli attacchi.

3. **Biometria Comportamentale**

Attraverso l'analisi dei comportamenti distintivi degli utenti, come la velocità di digitazione e i movimenti del mouse, è possibile sviluppare sistemi di autenticazione continua in grado di rilevare accessi non autorizzati. Questi sistemi identificano anomalie confrontando i comportamenti rilevati con i modelli abituali degli utenti, garantendo in tempo reale un avanzato livello di sicurezza.

Vantaggi dell'Approccio Biologico

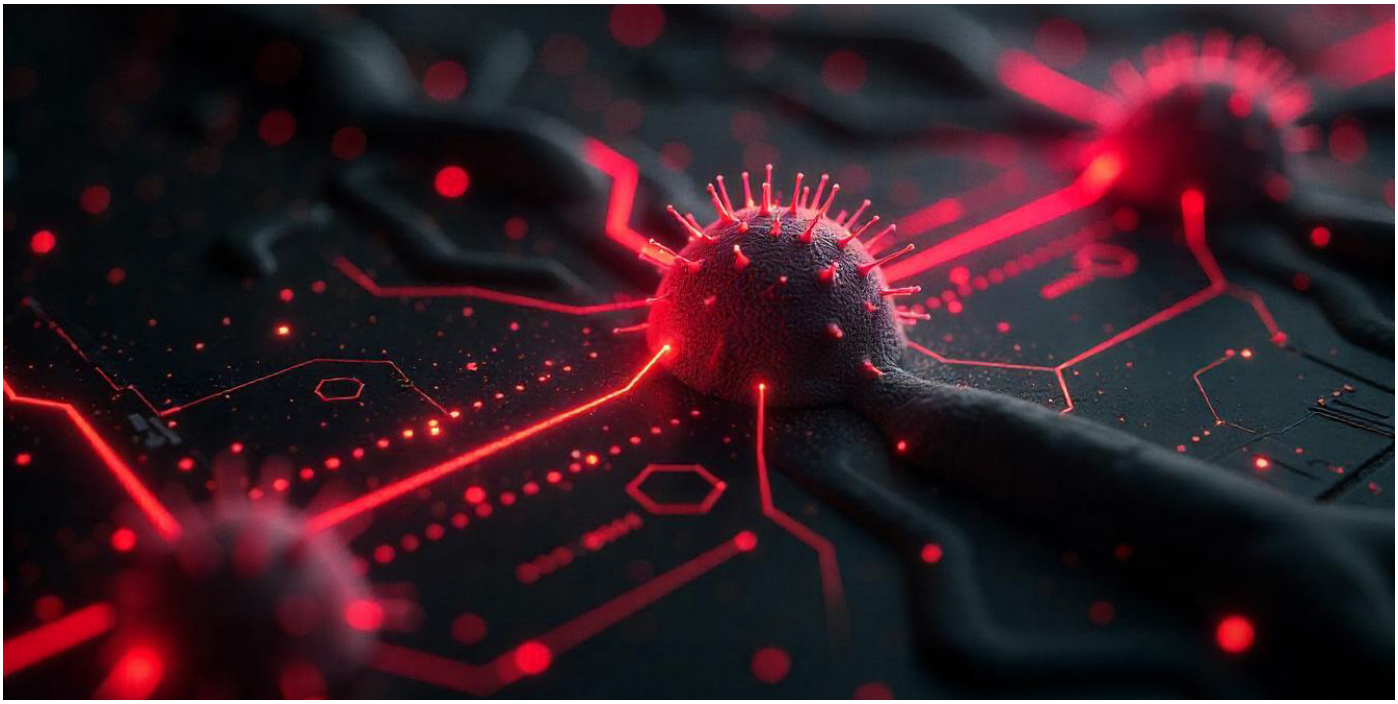
- **Adattabilità:** i sistemi ispirati alla biologia possono modificare le proprie difese in tempo reale, affrontando efficacemente minacce sconosciute o inaspettate.
- **Scalabilità:** come gli ecosistemi naturali, queste soluzioni possono essere implementate su larga scala senza perdere efficacia, adattandosi a infrastrutture di diverse dimensioni e complessità.
- **Resilienza:** ispirandosi alla capacità degli organismi viventi di sopravvivere e prosperare in ambienti ostili, i sistemi di cybersecurity biologicamente ispirati sono progettati per resistere a guasti e attacchi, garantendo una continuità operativa anche in condizioni avverse.

Sfide e Considerazioni

Nonostante i notevoli vantaggi, l'integrazione dell'intelligenza biologica nella cybersecurity solleva alcune problematiche significative che meritano attenzione:

- **Complessità:** la strutturazione dei processi biologici richiede una competenza avanzata in molteplici discipline, tra cui biologia, informatica e ingegneria. L'approccio interdisciplinare necessario può risultare difficile da implementare e, talvolta, difficile da coordinare.
- **Risorse Computazionali:** alcuni algoritmi ispirati ai processi biologici possono essere estremamente esigenti in termini di risorse, necessitando di hardware avanzato e comportando tempi di elaborazione lunghi, il che può limitare la loro applicabilità pratica in scenari ad alta richiesta.
- **Privacy e Sicurezza dei Dati:** l'uso di dati biometrici e comportamentali solleva legittime preoccupazioni in merito alla protezione delle informazioni personali. La gestione di tali dati impone sfide relative alla conformità con le normative sulla privacy e alla garanzia che le informazioni sensibili siano adeguatamente protette contro l'accesso non autorizzato.

"L'intelligenza biologica utilizza l'osservazione e l'imitazione di questi processi per progettare sistemi di difesa informatica più robusti ed efficaci".



Prospettive Future

L'integrazione dell'intelligenza biologica nella cybersecurity sembra destinata a crescere, con sviluppi che potrebbero aprire nuove frontiere, sebbene non senza sollevare alcune perplessità.

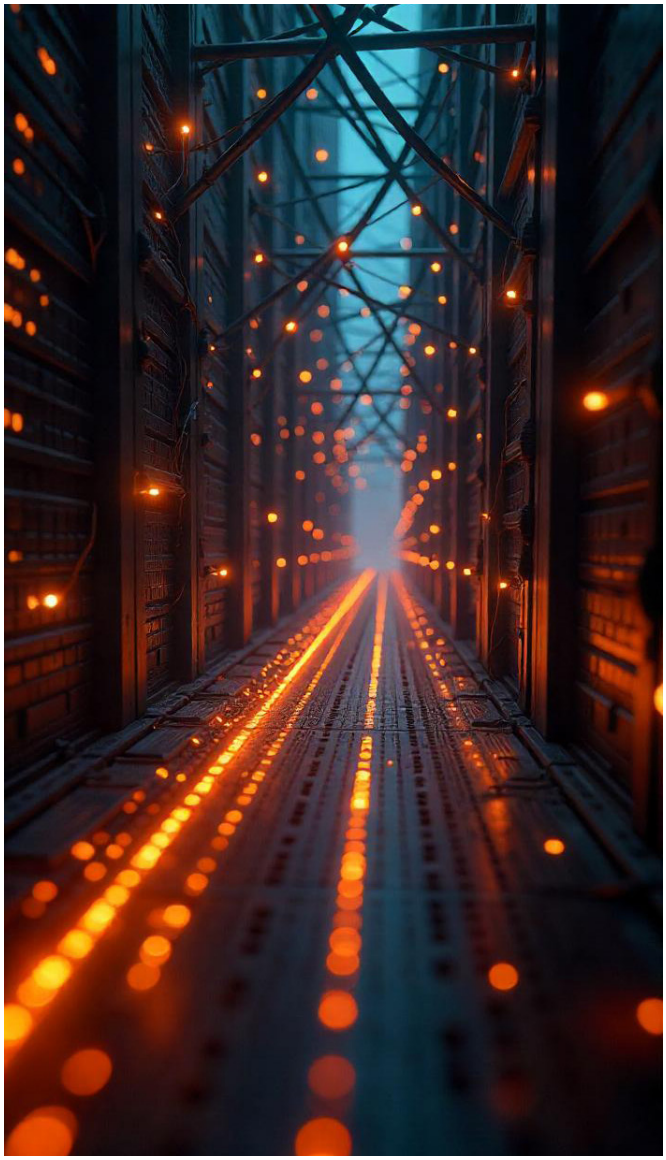
- **Sistemi di Auto-Guarigione:** si prevede la creazione di reti informatiche in grado di identificare e correggere autonomamente le proprie vulnerabilità, ispirandosi ai processi di rigenerazione biologica. Resta da valutare se questi sistemi possano davvero gestire in modo efficace e sicuro le complessità e le variabili delle minacce in continua evoluzione.
- **Ecosistemi Digitali Resilienti:** la costruzione di infrastrutture che imitano la biodiversità degli ecosistemi naturali per migliorare la resistenza alle minacce cibernetiche potrebbe rappresentare una soluzione interessante. Tuttavia, la realizzazione di tali ecosistemi digitali comporta rischi legati alla loro complessità e alla difficoltà di prevedere tutte le possibili interazioni tra i diversi elementi.
- **Interfacce Uomo-Macchina Evolute:** lo sviluppo di interazioni più naturali ed efficienti tra esseri umani e sistemi informatici, basate sulla comprensione dei processi cognitivi e comportamentali, offre indubbi vantaggi. Tuttavia, la sfida risiede nell'assicurarsi che queste interfacce siano veramente sicure e in grado di rispondere in modo adeguato alla varietà dei comportamenti umani, senza compromettere la privacy o la sicurezza.

Conclusione

L'approccio biologico alla cybersecurity rappresenta un'interessante prospettiva innovativa per rispondere alle sfide delle minacce informatiche moderne. Ispirandosi ai processi naturali, offre il potenziale per sviluppare sistemi più adattivi, resilienti ed efficaci, capaci di rispondere in modo dinamico alle nuove vulnerabilità.

Tuttavia, vista la complessità delle interazioni tra biologia ed informatica, emergono numerosi interrogativi su come tradurre i principi biologici in soluzioni tecnologiche applicabili.

Inoltre, non possiamo ignorare le difficoltà legate alla creazione di modelli che possano realmente replicare le capacità del sistema biologico, né le sfide etiche e pratiche che una simile integrazione comporta. Pertanto, è essenziale un continuo impegno nella ricerca interdisciplinare, che coinvolga esperti di etica, biologia, informatica e sicurezza per affrontare queste problematiche ed ottimizzare l'efficacia di tali soluzioni nel lungo periodo.



"Ispirandosi alla capacità degli organismi viventi di sopravvivere e prosperare in ambienti ostili, i sistemi di cybersecurity biologicamente ispirati sono progettati per resistere a guasti e attacchi, garantendo una continuità operativa anche in condizioni avverse".

Il political listening: questo sconosciuto

A cura di Domenico Giordano

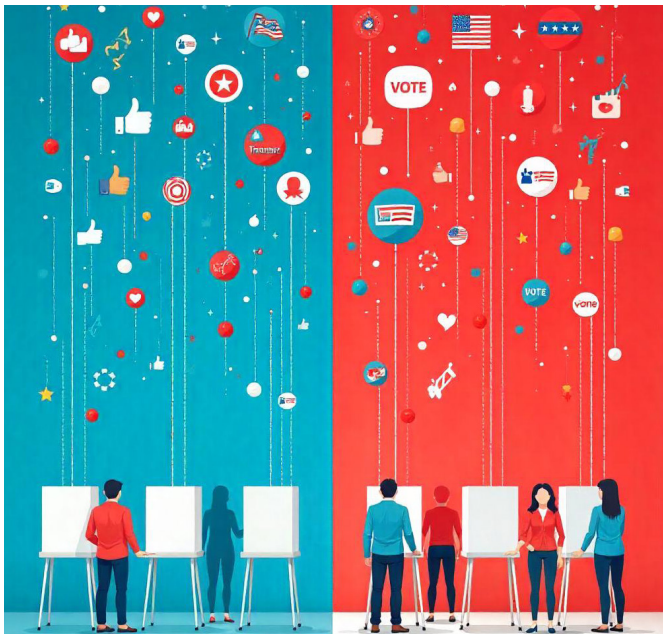
Domenica 25 settembre 2022 alle ore 12.00, nella prima rilevazione del Ministero dell'Interno, la percentuale degli italiani che si erano già recati alle urne era del 19,21%, in linea con quella registrata cinque anni prima nel 2018, quando ai seggi erano andati invece il 19.43% degli aventi diritto.

Qualche minuto dopo, esattamente alle 12.35, l'allora leader di Fratelli d'Italia pubblicava sull'account TikTok un clip di soli 5 secondi, accompagnandola con un testo altrettanto sintetico che riprendeva le parole pronunciate in video, nel quale Giorgia Meloni scegliendo una espressione volutamente ammiccante e sorridente, affermava: "25 settembre, ho detto tutto".

Una clip in cui sorregge nei palmi delle mani due meloni e pubblicata per incunearsi furbescamente, senza pagar pegno, nelle crepe della attuale legge che disciplina tempi e modi della propaganda elettorale, una normativa che da almeno due decenni rimane paurosamente anacronistica, rispetto alle dinamiche e alle opportunità che la società "piattaformizzata" mette a disposizione dei leader politici e dei candidati a qualsiasi competizione.

Quel post all'apparenza innocente, costruito in modo volutamente goliardico e privo di una esplicita cornice politico-elettorale, ha iniziato a generare una valanga di interazioni, diventando già al termine di quella giornata e prima della chiusura delle urne, la clip video con il maggior numero di visualizzazioni tra tutte quelle pubblicate dai leader nel corso della campagna elettorale del 2022. Numeri impressionanti a rivederli a distanza di tempo: 11.200.000 visualizzazioni, a cui si accompagnano, giusto per chiarire, la voluminosità del bottino complessivo che ci svelano la pervasività del messaggio, altri 392.500 like, 27.000 commenti e 63.900 condivisioni. Non male, verrebbe da dire. Anzi, molto bene, eppure il punto sul quale vale la pena porsi una domanda pur se priva di una risposta verificabile è decisamente un'altra: quanto quel singolo post abbia influito sulla scelta dei follower di trasformarsi in elettori votanti? O meglio, quanto la clip postata nella tarda mattinata sia riuscita a incidere sui consensi finali ottenuti dal partito guidato da Giorgia Meloni?

È ovvio che a questi due quesiti non ci possono essere risposte precise e verificate, che rivelino la fondatezza eventuale di un rapporto di causalità diretta tra le visualizzazioni e le interazioni e la successiva presenza ai seggi. Rimane inconfutabile la capacità di quel contenuto di generare una pre-condizione fondamentale per chi mediante il presidio delle piattaforme punta a convertire i cittadini in elettori: ottenere la quota più ampia e profonda di attenzione digitale rispetto alla platea dei competitor. Quindi, invece di perdersi nel buco nero di ciò che non è certificabile, ovvero che un like corrisponde a un voto, è opportuno provare a comprendere quanto una qualunque messe di interazioni, termometro dell'attenzione digitale ottenuta, abbia funzionato da innesco per la conversione degli utenti-follower in elettori-consumatori.



L'attenzione digitale, prima ancora degli applausi delle piazze, dello share dei talk televisivi, dell'intervista al quotidiano, online o cartaceo poco importa, e dei consensi reali depositati nelle urne, è la sola moneta che ha corso legale nel mercato concorrenziale delle leadership politiche. Una moneta che i leader, e i loro staff, si contendono a suon di post, di reel e di live e che ci restituisce il modo in cui questi hanno scelto di presidiare l'in-

fosfera digitale. L'attenzione digitale è la materia prima che sostanzia l'efficacia della narrazione del leader e, al contempo, la legittima in quanto credibile agli occhi degli internauti. Qualsiasi politico senza una dote sufficiente di attenzione digitale rimane un leader azzoppato, poco attrattivo, prigioniero nella sua micro-bolla cognitiva, ma soprattutto rischia di essere un leader con minor probabilità di crescere nelle urne. Il consenso fisico, il voto, oggi si costruisce principalmente online e si ottiene precipuamente a partire dal presidio strategico delle piattaforme. Un presidio che postula credibilità e audience.

"Si preferisce stordirsi con una scarica di dopamina, utile alle leadership quanto alla followership, piuttosto che provare a costruire una community valoriale".

Tra il 24 e il 25 settembre, per provare a codificare un metro di misurazione dell'attenzione digitale generate dalla clip video di Meloni, i follower TikTok del suo account passano da 226.600 a 264.200, per raggiungere il giorno successivo, siamo al 26 settembre ed è ancora in corso lo spoglio delle schede elettorali, a 416.300. Una crescita di nuovi follower che raggiunge in poche ore la percentuale dell'83,72% e che testimonia, se non ci soffermiamo a una sterile aritmetica del fandom, il salto qualitativo prodotto dall'attenzione digitale insita nelle visualizzazioni e nelle interazioni. Senza soluzione di continuità l'utente di una piattaforma che entra in relazione con un contenuto, valuta, in una frazione di secondo, se lo stesso, in qualche misura, è coerente con il tessuto digitale dei suoi interessi e della sua visione del mondo per poi scegliere di iniziare a seguire quell'account. Alla base di quest'ultima decisione c'è anche una motivazione che potremmo definire di riconoscimento dell'autenticità, di una credibilità e della tacita accettazione della narrazione del mittente, leader politico o candidato. Inoltre, nessun altro medium oggi può garantire ai leader politici la stessa visibilità che ottengono dalle piattaforme. Così come, non c'è medium che può costruire dopo pochi secondi di attenzione lo stesso legame tra follower e leader grazie alla dinamica della performance algoritmica, che ha indicizzato il mio tempo o la mia possibile reaction come un valore di interesse e di conseguenza ha scelto autonomamente di classificarmi come utente potenzialmente attrattivo riversando nel mio feed altri contenuti dello stesso mittente e della stessa matrice.

Questa quantità di dati, quantitativi e qualitativi, finisce molto spesso in un angolo buio e impolverato della war room, lasciata marcire nell'indifferenza generale perché considerata priva di un qualsiasi valore, per nulla utili allo scopo e considerati degli scarti comportamentali di cui non importa niente a nessuno. Nonostante in tanti parlino dell'importanza delle campagne data driven, della necessità strategica dei dati per costruire dei posizionamenti cognitivi, c'è invece una sottovalutazione del social e web listening. Tra gli staff dei leader e ciò che riguarda il listening c'è un muro invalicabile, sono due innamorati che non si parlano, che non si incontrano e che fanno solo finta di conoscersi. Questa è la triste metafora che sintetizza lo stato dell'arte del political listening in Italia segnato da tre diverse visioni del dato: c'è curiosità ma manca una metodologia, ci si ferma alla libidine del like e in pochi lo utilizzano per costruire una strategia di lungo periodo.

Attualmente, dall'analisi delle matrici di pubblicazioni dei social dei principali leader politici emergono due diversi approcci che marcano il modo in cui vengono presidiate le piattaforme: da un lato, troviamo l'hype driven approach e dall'altro quello che invece potremmo classificare come il reputation driven approach. Nel primo caso, la ricerca dell'audience detta la linea, impone la scelta degli argomenti che vanno nel feed delle pubblicazioni. Insomma, a determinare cosa e perché pubblicare è la dipendenza dal like e dalle visualizzazioni: si preferisce stordirsi con una scarica di dopamina, utile alle leadership quanto alla followership, piuttosto che provare a costruire una community valoriale.

Al contrario, nel caso di una strategia fondata sulla reputazione piuttosto che sull'audience, quindi comprensibilmente meno eccitante ma anche più redditizia nel lungo periodo, l'agenda delle pubblicazioni non è costruita solo o principalmente sull'emotività dell'hype, ma cerca di valorizzare argomenti e contenuti che seppur riscuotono un'attenzione più bassa riescono maggiormente a creare un legame di fedeltà e di fiducia con il leader.

LA CYBER PER TUTTI
ISTRUZIONI SEMPLICI PER QUESTIONI COMPLESSE

Le società nascono dal connubio fra burocrazie e mitologie

A cura di Michele Mezza

Cybersecurity è innanzitutto potere di iscrizione. Linguaggi e competenze di una tutela digitale adeguata alla guerra ibrida

Uno degli strateghi più sensibili alle opportunità che offriva la storia come Wladimir Illic Lenin, diceva che “ci sono decenni in cui non accade nulla e invece settimane in cui accadono decenni”.

Oggi possiamo dire che da anni viviamo in un tempo in cui ogni giorno sembra resettarsi lo scenario su cui stiamo elaborando le nostre decisioni. Frose proprio la velocità del cambiamento è una di quelle forma di militarizzazione della nostra vita che rendono sempre più complessa e stressante garantirne la sicurezza.

L’irruzione di DeepSeek, l’ormai celeberrima tecnologia generativa cinese a bassissimo costo e in modalità opensource, come il collasso degli indici finanziari ci hanno spiegato con il linguaggio più persuasivo e pragmatico,rende quanto mai precarie certezze che sembravano inviolabili fino a qualche settimana prima.

Il carattere decentrato di questa nuova soluzione, con la riduzione drastica dei costi per quei processi di addestramento che sembravano proibitivi, oltre che la sostituzione dei ricercatissimi microchip di Nvidia che erano contingentati dal nuovo governo americano, che sembravano insostituibili, muta radicalmente il campo della sicurezza digitale, aumentando a dismisura sia il numero dei soggetti che possono operare e sia l’intensità di queste operazioni.

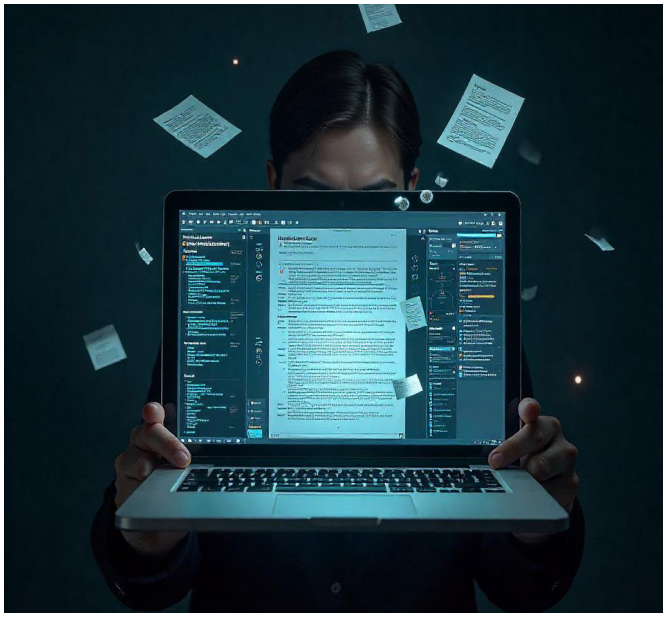
Il tutto per altro all’interno di un contesto in cui un eventuale adozione in massa di questa tecnicalità cinese comporterebbe, inevitabilmente lo spostamento ad oriente di flussi massicci di dati che verrebbero incamerati dai dataserver di quella potenza.

Lo scenario è davvero in grande subbuglio e accelera la trasformazione della cybersecurity da capacità ingegneristica di preservare i depositi, a competenza semantica per salvaguardare l’autonomia di quanto depositato.

Infatti se ha ragione il socio antropologo dell’Università di Gerusalemme Yuval Harary a dirci, nel suo ultimo topo Nexus (Bompiani editore) che “Le società nascono dal connubio fra burocrazie e mitologie”, allora dovremmo ben comprendere la tendenza della seconda, la mitologia intesa come senso comune dei saperi e delle relazioni sociali,oggi sia dominante sulle burocrazie, considerate i sistemi di governance di imprese e istituzioni. Diciamo più sinteticamente ormai si decide in base a cosa ci raccontiamo, ed è proprio la nostra narrazione il vero bersaglio della nuova cybersecurity decentrata.

Questo “connubio” di istituzioni e narrazioni, assume una specifica, e per molti versi totalizzante rilevanza, in virtù del fatto che nell’infosfera digitale, tutta la nostra vita si svolge producendo, tracciando ed elaborando documenti che vengono registrati nel web, come afferma il filosofo Maurizio Ferraris (Documanità, Laterza). Noi oggi siamo i documenti che registriamo.Dunque viviamo in base a quello che registriamo.

“Senza documenti - scrive ancora Maurizio Ferraris - non ci sarebbero neppure intenzioni, azioni sociali aspirazioni”.



Riuscire a interferire nell'elaborazione dei documenti significa condizionare l'intenzionalità operativa di un paese. Per questo, sia gli apparati di governance che le culture di relazione - appunto burocrazie e mitologie - oggi si compongono esclusivamente di documenti che determinano l'intenzionalità di quella comunità.

Possiamo dire, di conseguenza, che, in quella che viene definita come Guerra Ibrida – ossia la manipolazione delle deliberazioni mediante inquinamento del senso comune di uno stato - entrambe le categorie siano messe sotto tiro.

La guerra ibrida si conduce controllando i mezzi di iscrizione che sono la fonte dei documenti. E se il numero di soggetti in grado di interferire con le iscrizioni aumenta, proprozionalmente aumenta il pericolo e la complessità per la cybersecurity.

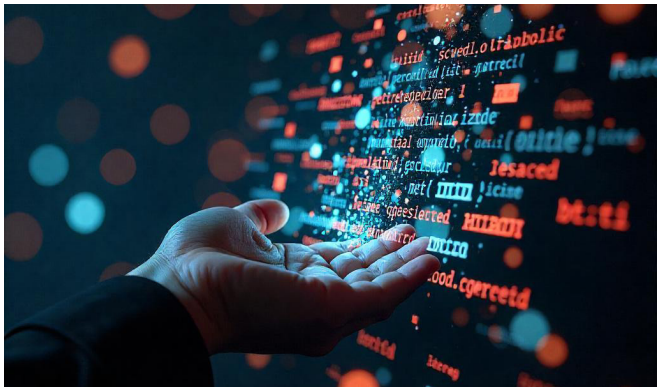
La cybersecurity contemporanea è esattamente quella scienza che analizza ed elabora, per neutralizzarle, le procedure di minaccia e alterazione della nostra autonomia di iscrizione.

Certo che la burocrazia- gli apparati gestionali pubblici o privati- rimang un bersaglio prioritario delle forme tradizionale di hackeraggio, che mira a intromettersi negli ambienti in cui depositiamo i documenti. Possiamo definire questa prima forma la cybersecurtity "immobiliare", in qualche modo residente in luoghi e spazi finiti e identificabili- i data center o i singoli computer- dove depositiamo la massa di documenti che produciamo. Ma rapidamente viviamo la transizione verso un nuovo mercato, in cui al centro della contesa sono i documenti, il flusso e l'interattività sociale che inducono. Oltre che testimoniare la nostra intenzionalità i documenti sono anche strumenti di addestramento dei dispositivi di intelligenza artificiale che orientano l'automatizzazione delle nostre decisioni e come tale individuano un nuovo campo di battaglia per la sicurezza cyber.

Per questo è proprio questa seconda forma di sicurezza digitale, che potremmo definire "mobiliare ", sia per la sua immaterialità che per la sua volatilità, sta ricodificando l'intero settore. Ci riferiamo quella coltre di linguaggi e valori in base ai quali una comunità, condividendo i propri documenti, si riconosce come affine e solidale.

Infatti se la guerra ibrida sta sostituendo in tutto e per tutto la pace come intervallo fra i conflitti combattenti, è evidente come diventi centrale una nuova modalità di tutela della sicurezza cyber di carattere mobiliare, che abbia come oggetto il flusso dei documenti, la struttura della narrazione, il senso comune della comunità nazionale, il potere di iscrizione.

"La guerra ibrida si conduce controllando i mezzi di iscrizione che sono la fonte dei documenti".



Proprio la contemporaneità di due conflitti, quali quelli in Ucraina e nel medio oriente, ci permette di cogliere l'aspetto più concreto e innovativo di questa nuova forma di guerra ibrida. In entrambi gli scacchieri infatti i combattimenti materiali sono organizzati, condotti e pianificati da un fuoco di sbarramento narrativo che mira proprio a manipolare le mitologie sia dell'avversario diretto che di quella platea di osservatori che costituiscono l'opinione pubblica globale. E in questa spirale un ulteriore decentramento delle potenze operastive, come indubbiamente DeepSeek annuncia, impone un upgrading di tutti i comportamenti del settore.

Del resto sono stati proprio gli alti comandi militari, a cavallo del primo decennio del nuovo secolo, ad avvertire il pericolo per il loro primato delle forme di distribuzione delle capacità tecnologiche, in cui l'accessibilità diventa minaccia. Infatti, siamo a cavallo del 2010, dopo la lezione delle primavere arabe e della sobillazioni arancioni indotte da una manipolazione della comunicazione di quei paesi, che si elaborano visioni più moderna del conflitto armato e in cui la cybersecurity è una forma centrale di logistica, che prolunga la guerra nella vita civile.

Dalle teoria dell'ex consigliere militare di Obama, John Arquilla- per battere un network ci vuole un network- a quelle del generale cinese Quiao Liang - la guerra è sempre cospirazione- fino al saggio del capo di stato maggiore Russo Gerasimov - si combatte interferendo nel senso comune dell'avversario- la guerra si è impossessata di quei comportamenti e linguaggi affilati nella pace.

Oggi ci troviamo con un unico apparato concettuale, che congiunge militare e civile, dove la coppia amico-nemico, la cospirazione sulle decisioni, la manipolazione delle certezze dell'informazione, sono un comune arsenale in cui le competenze professionali delle imprese di cybersecurity devono adeguarsi ad essere centri di eccellenza e di formazione per la tutela dell'autonomia del proprio potere di iscrizione.

Holistic Knowledge

Cyber Sicurezza e Project Management (per esempio)

A cura di Rita Takaks

Sono sempre felice di raccontare questa storia (la mia storia), nella speranza che possa rappresentare per un mio alter ego più giovane quella luce che illumina le proiezioni delle ombre gettate da quella saccente coscienza sociale, noiosa e irritante nell'ostentare la propria erudizione su ciò che è giusto e ciò che è sbagliato.

Amare molte scienze, e vedere continuamente il fil rouge che le lega, in un passato non troppo remoto era… sbagliato.

"Ami l'informatica, ma studi psicologia?! Ti affascina la statistica, la logica, la programmazione, ma scrivi poesie?! Devi scegliere e mantenere una coerenza di percorso, non puoi essere <qualsiasi cosa>!"

Avvilente monito per uno spirito sfaccettato.

Invano intuizioni facevano capolino (non sorrette da un opportuno framework) sull'esistenza di una diretta proporzionalità tra un'estensione orizzontale del sapere e l'agilità della verticalizzazione <on demand>. Mi spiego meglio: una conoscenza trasversale (l'essere <T-shaped>) si rivela sempre un prezioso humus per i momenti in cui si decide invece di approfondire (o addirittura eccellere) in un argomento (l'essere <I-shaped>). Non sono come Yin e Yang in rapporto di antitesi o vicendevole esclusione, ma due concetti complementari che traggono reciproco vantaggio dal loro connubio.

"Ehhh… sì! E poi? Che altro?"

L'eco di ritorno era sempre lo stesso: una sfiducia mescolata a un leggero dileggio.

La conoscenza, in tutte e sue forme, primarie e combinatorie, è meritevole di soprastare ai pregiudizi, all'ottusità, ai retaggi e a quei particolari ingranaggi, non oleati da tempi dimenticati, delle arti e dei mestieri.

Qualcuno ci avrà già pensato (ne ero sicura) e avrà coniato una chiave di lettura così diversa, da aprire un universo parallelo, e non solo metaforicamente una porta! Basterà solo trovarla, no?!

Tra un corso di… <gestione delle reti> e uno di… <gestione del magazzino> (eh, sì, volevo davvero essere "La Cosa" dei fantastici 4, per la precisione "Qualsiasi Cosa"), avevo trent'anni quando mi sono iscritta ad un corso universitario serale, compatibile con il lavoro (il classico corso post laurea), di <Project Management>.

BANG! La chiave master che apre tutte le serrature!

Mi è sembrata straordinariamente preziosa, come un oggetto dorato con brillanti incastonati, simbolo di una scoperta che avrebbe cambiato il mio percorso.

L'ho capito fin dalla prima lezione con Giorgio Bensa (monumentale nella sua passione genuina!), oggi non più tra noi purtroppo…

Lo <Sbagliato> diventò <Giusto>, così come <Mea culpa> si tramutò in <Meritum meum>. Oggi argomento oserei dire arcinoto, sebbene una sintesi di alto livello è sempre doverosa.

Un progetto è un'impresa temporanea intrapresa per creare un unico prodotto, servizio o risultato (elemento chiave del progetto è, di fatti, l'unicità della sua risultanza, caratteristica applicabile anche, eventualmente, al contesto e/o al team costituito ad hoc per la sua gestione)

Così come il <project management> è l'applicazione di conoscenze, attitudini, strumenti e tecniche alle attività di un progetto, al fine di conseguirne gli obiettivi»

(definizioni tratte dal PMBOK Guide - Project Management Body of Knowledge – Project Management Institute).

Ma quali conoscenze, attitudini, strumenti e tecniche?

Un corpus multi-disciplinare di conoscenze, che opportunamente integrate (la prima area di conoscenza, quella che il Project Manager non può delegare a altri membri del team, è, appunto, la Getione dell'INTEGRAZIONE), consentono:

• una gestione efficace del contenuto (Gestione dell'AMBITO, più comunemente indicato anche in italiano con il termine inglese SCOPE), • nel rispetto delle tempistiche (Gestione della SCHEDULAZIONE), • dei COSTI (Gestione dei Cosv) e • della QUALITÀ (Gestione della Qualità), ponendo attenzione • all'impiego delle RISORSE (Gestione delle Risorse, intese come risorse umane, ma anche materiali), • alla cura delle COMUNICAZIONI (Gestione delle Comunicazioni), • al controllo dei RISCHI (Gestione dei Rischi) e • delle fonti di APPROVVIGIONAMENTO (Gestione dell'approvvigionamento, ovvero della Supply Chain e dei processi di procurement), • delle persone/enti interessate al progetto o che possono essere da esso impattate (Gestione degli stakeholder, un altro anglicismo entrato ormai in pianta stabile nel vocabolario italiano).

Tutto, ma proprio tutto quello che avevo studiato nel mio pellegrinaggio apparentemente caotico tra scienze, pseudoscienze e valutazioni prodromiche, aveva una sua casellina e si incastrava a meraviglia.

Oltre alla gestione operativa del progetto, il project manager deve possedere un ampio spettro di soft skills che gli permettano di navigare tra le complessità del lavoro quotidiano (per le quali c'è un'offerta gigantesca di approfondimento e affinamento): problem solving, flessibilità, creazione e perfezionamento del lavoro di squadra (Team building), pensiero laterale, leadership, creatività, capacità di creare fiducia (Trust building)

Psicologia e comunicazione: 90% del lavoro di un project manager è comunicazione e soft skills, empatia e, in generale, capacità interpersonali. Comunichiamo con il linguaggio verbale, paraverbale (tono, inflessioni della voce), non verbale (linguaggio del corpo), con una buona presentazione Powerpoint o con un Diagramma di Gantt, con un diagramma di processo, un report o una email. Un conflitto si previene e si cura con la comunicazione, una negoziazione vincente diventa win-win se ad altri necessari fattori possiamo aggiungere una comunicazione assertiva ed efficace.

E ancora: non possiamo prescindere in questo mestiere dalla conoscenza dei principi contabili e finanziari, di modelli, teorie e framework di qualità, dei principi del marketing e delle strategie di vendita, del ciclo di vita dei prodotti, della statistica (per esempio le tecniche di Earned Value Management per determinare la varianza di tempo o di costo rispetto al pianificato), della gestione dei processi di procurement, che spesso iniziano con la gestione di una gara d'appalto.

E quando si tratta di contratti, oltre alle clausole legali, si deve considerare una domanda che non ha risposta univoca e che cambia a seconda del caso: cosa potrebbe andare storto e come ci si dovrebbe comportare in quel caso? Con la consapevolezza che <i contratti sono fatti per litigare bene> e non per assolvere un fastidioso compito burocratico.

"La conoscenza è potere, ma solo se usata con saggezza".

Il compliance management, o gestione della conformità aziendale, come insieme di processi e procedure atti a garantire che un'azienda rispetti leggi, regolamenti e norme (interne o esterne) applicabili al suo settore.

Che si tratti di normative europee (GDPR, la recente NIS2) o nazionali (leggi sul lavoro, leggi antitrust, leggi ambientali…).

L'informatica? La più trasversale delle scienze. "Slice and dice your data", organizza, riassumi, archivia correttamente, ritrova sempre tutto, genera velocemente contenuti (oggi l'AI ci supporta, ma dobbiamo usarla cum grano salis).

E... già! Ricorda di suddividere i progetti in fasi (li renderà più gestibili), non essere troppo parsimonioso con le milestone (pietre miliari che indicano un traguardo, una data importante, fermati un attimo e festeggia, arriverai prima!). Il tutto per non cadere nella trappola del proverbiale "elefante" nella lista delle cose da fare (una delle metafore più conosciute nel mondo del project management decreta un assioma solo in apparenza semplicistico: "il modo per mangiare un elefante è un boccone alla volta").

Non è alquanto meraviglioso anche solo sfiorare tutta questa conoscenza? Fare un mestiere che ti chiede proprio questo, di allargare i tuoi orizzonti, di allontanarti e

guardare il quadro da lontano. Perché solo così avrai quella visione olistica che ti permetterà di coglierne il vero significato. Non mi vergogno più di dare libero sfogo alla sete di conoscenza, e oggi sono cosciente (e grata) che è stato un grande privilegio l'aver trovato la mia chiave master.

E le scoperte non sono certamente finite!

Il bello e il brutto della mente sfaccettata è che ogni nuova scoperta ti mostra quanto ancora ci sia da imparare. E seppur per un momento un velo di tristezza può coprirla, è subito seguito da una scintilla di entusiasmo per le avventure che ci attendono. Come direbbero nei manga, mi viene in mente una scintilla di entusiasmo, un 'Kira Kira' che simboleggia la ripartenza.

> ***"Sicurezza e resilienza significano anche business continuity".***

Quando ho intrapreso il mio viaggio nel mondo della cybersecurity circa un anno fa, non avrei mai immaginato quanto questa disciplina avrebbe arricchito la mia visione professionale, colmando lacune nel mio percorso che non sapevo nemmeno di avere.

OSINT: Un Ponte tra Due Mondi

La vera introduzione alla cybersecurity è avvenuta durante un corso di OSINT (Open Source Intelligence) & Social Engineering, che mi ha aperto gli occhi su un universo sommerso di informazioni e tecnologie. Utilizzare l'OSINT ha migliorato la mia capacità di raccogliere e analizzare dati, un'abilità cruciale nel project management per comprendere meglio i rischi e le opportunità.

Dark Web e Deep Web: Nuove Frontiere della Conoscenza

È stato in questo mondo oscuro e affascinante, attraverso "l'instradamento della cipolla", che ho trovato nuovi strumenti e prospettive che hanno arricchito la mia visione professionale.

Ho scoperto due mondi paralleli che operano al di là della superficie visibile di Internet. Un inimmaginabile combinato disposto di fattori che possono influenzare le nostre attività, ma se positivamente o negativamente è spesso una scelta. La conoscenza, ancora una volta, è potere. Per fare un esempio: ho appreso nuovi strumenti per la gestione delle informazioni sensibili e la protezione dei dati.

Arricchimento della Visione Professionale

Il project management e la cybersecurity condividono un comune denominatore: la necessità di una gestione rigorosa e strutturata delle risorse e delle informazioni. Integrando le tecniche di cyber sicurezza nel project management, sono stata in grado di sviluppare strategie più robuste e resilienti per affrontare le sfide moderne.

L'esplorazione del mondo cyber ha arricchito non solo la mia base di conoscenza, ma anche la mia visione professionale. Ho acquisito una consapevolezza maggiore delle minacce globali e delle dinamiche digitali che influenzano il successo dei progetti. Ho aggiunto elementi essenziali alle liste dei requisiti funzionali di un software (crittografia, protocolli, certificati, architetture sicure, gestione degli accessi, VAPT, security by design e by default, least privilege vs need to know, e chi si ferma è perduto, che viaggio emozionante! Questa consapevolezza mi ha permesso di sviluppare un approccio più olistico e informato alla gestione dei progetti, considerando non solo gli aspetti tradizionali, ma anche le nuove sfide e opportunità offerte dal mondo cyber.

In conclusione, l'approfondimento del mondo della cyber sicurezza ha rappresentato per me una fonte inesauribile di nuove competenze e prospettive. Come project manager, ho potuto integrare queste conoscenze per migliorare la gestione dei progetti, ma anche le risultanze progettuali stesse. Sicurezza e resilienza significano anche business continuity, da sempre sulla nostra lista dei desideri.

Il viaggio nel mondo cyber è solo all'inizio. La semplicità segue la complessità e non viceversa. In un mondo in cui, come si dice, 'l'unica cosa che non cambierà mai è il fatto che tutto cambia', la vera meta è il viaggio stesso. E ora, più che mai, sono pronta ad affrontare le nuove sfide che ci attendono. E tu?

Cybercrime: conoscere il valore degli Asset per vincere la battaglia del rischio

A cura di Martina Fonzo

In un mondo sempre più interconnesso, la cybersecurity è diventata una questione strategica che richiede un approccio non solo tecnico, ma anche economico e gestionale. La crescente complessità delle minacce informatiche impone alle organizzazioni di ogni tipo, pubbliche e private, di ripensare il proprio approccio alla gestione del rischio. Spesso, però, il top management fatica a comprendere l'urgenza degli investimenti necessari, se non si traduce il rischio in termini economici.

La necessità del Quantitative Risk Management

"Conosci il tuo nemico e conosci te stesso e in cento battaglie non sarai mai in pericolo". Questo insegnamento di Sun Tzu rimane incredibilmente attuale nel contesto della cybersecurity. Tuttavia, troppo spesso si concentra l'attenzione unicamente sull'analisi delle minacce esterne, trascurando l'importanza di una conoscenza approfondita di sé stessi. Questo significa valutare, con metodi quantitativi, il valore degli asset critici e il potenziale impatto economico di un attacco.

La gestione quantitativa del rischio (Quantitative Risk Management) si distingue dagli approcci tradizionali perché consente di calcolare il rischio in termini numerici e oggettivi. Attraverso analisi basate su dati concreti, le organizzazioni possono stimare non solo la probabilità di un attacco, ma anche il costo associato a una compromissione, rendendo il rischio tangibile per il management.

Simulare per comprendere: il valore degli asset in caso di breach

Un aspetto cruciale del quantitative risk management è la capacità di simulare scenari di attacco per valutare il valore economico degli asset. Questo approccio va oltre l'inventario delle vulnerabilità tecniche, includendo un'analisi dettagliata delle conseguenze finanziarie di un incidente.

Ad esempio, una grande organizzazione che subisce un attacco ransomware potrebbe affrontare costi diretti, come il pagamento del riscatto o il ripristino dei sistemi, ma anche costi indiretti: interruzioni operative, perdita di fiducia da parte dei clienti, sanzioni normative e danni reputazionali. Simulare questi scenari aiuta a identificare i punti critici e a stimare il valore reale degli asset.

Un'azienda manifatturiera, ad esempio, potrebbe scoprire che il blocco della produzione per 48 ore comporterebbe una perdita economica di milioni di euro. Questo dato non solo sensibilizza il management, ma aiuta anche a prioritizzare gli investimenti in sicurezza per proteggere gli asset più critici.

Uno degli ostacoli principali nell'adozione di strategie

di cybersecurity efficaci è la difficoltà di comunicare il rischio in termini comprensibili al top management. I dirigenti, spesso concentrati sugli obiettivi di business, tendono a considerare la cybersecurity come un costo anziché come un investimento strategico.

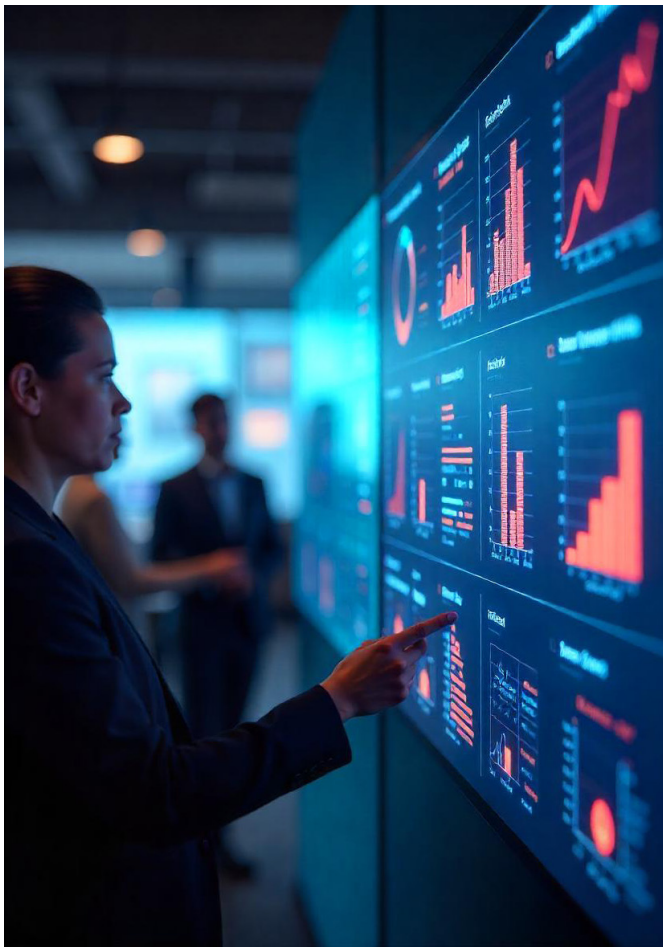
Il rischio, però, diventa molto più chiaro quando tradotto in metriche economiche. Sapere che un attacco potrebbe comportare perdite per decine di milioni di euro è un potente incentivo a investire in misure preventive. Inoltre, un approccio quantitativo consente di confrontare diversi scenari di rischio e identificare le aree in cui gli investimenti possono offrire il massimo ritorno in termini di mitigazione.

"Il rischio, però, diventa molto più chiaro quando tradotto in metriche economiche".

Un approccio integrato alla cybersecurity

Per costruire una strategia efficace, basata sulla gestione quantitativa del rischio, le organizzazioni devono seguire un percorso chiaro:

1. **Inventario degli asset:** identificare e classificare gli asset critici, come dati sensibili, sistemi IT, infrastrutture operative e processi.
2. **Valutazione del rischio economico:** utilizzare strumenti di analisi quantitativa per calcolare il costo potenziale di un attacco su ogni asset.
3. **Simulazioni e scenari:** testare i sistemi attraverso simulazioni realistiche per comprendere l'impatto di un breach.
4. **Coinvolgimento del management:** tradurre i risultati in un linguaggio comprensibile per i decisori, mostrando chiaramente il rapporto tra rischio e investimento.
5. **Formazione e sensibilizzazione:** educare i dipendenti sull'importanza della protezione degli asset critici e sui rischi legati a comportamenti non sicuri.



Nel mondo della cybersecurity, conoscere il nemico è dunque fondamentale, ma conoscere sé stessi è altrettanto, se non più, importante. Valutare il rischio in termini quantitativi consente alle organizzazioni di agire con consapevolezza, proteggendo non solo i propri asset, ma anche la propria reputazione e continuità operativa. Il quantitative risk management rappresenta una svolta necessaria per trasformare la cybersecurity in una priorità strategica, capace di parlare non solo al reparto IT, ma anche al cuore delle decisioni aziendali.

Quantificazione del rischio nel mondo

A cura di Lorenzo Mazzei

Negli ultimi anni, l'evoluzione tecnologica ha trasformato le modalità con cui le aziende operano, introducendo sistemi di Operational Technology (OT) e Internet of Things (IoT) sempre più sofisticati. Tuttavia, questa trasformazione ha anche esposto le imprese a nuove sfide in ambito di cyber security, richiedendo un approccio sistematico per la quantificazione del rischio.

L'importanza e le sfide della quantificazione del rischio – Rischi specifici in OT/IoT

La quantificazione del rischio è un passaggio fondamentale per gestire efficacemente le minacce cyber. Nel contesto OT/IoT, i rischi non riguardano solo la perdita di dati o il furto di informazioni sensibili, ma anche l'interruzione delle operazioni industriali, con conseguenze potenzialmente devastanti in termini di sicurezza fisica, economica e reputazionale.

Le differenze tra i sistemi IT tradizionali e quelli OT/IoT complicano ulteriormente la valutazione del rischio. I sistemi OT, progettati principalmente per garantire continuità e affidabilità operativa, spesso utilizzano tecnologie legacy che non sono state concepite con la cyber security in mente. Dall'altra parte, l'IoT introduce una vasta gamma di dispositivi connessi, spesso difficili da monitorare e proteggere.

In considerazione di quanto premesso sopra, la quantificazione del rischio in ambito OT/IoT richiede l'adozione di metodologie specifiche che combinano strumenti tradizionali di gestione del rischio con approcci innovativi. Altrettanta importanza rivestono il ruolo della Governance e degli standard normativi.

Qui di seguito una valutazione delle principali metodologie e dei framework normativi di riferimento:

1. Analisi qualitativa e quantitativa del rischio

- L'analisi qualitativa si basa sulla valutazione soggettiva delle minacce e delle vulnerabilità. Considerati i range di riferimento di Accettazione e Tolleranza viene spesso utilizzata per identificare i rischi più critici e definire le priorità di intervento.
- L'analisi quantitativa, invece, utilizza dati storici e modelli matematici per stimare la probabilità e l'impatto economico di un attacco.

2. Machine Learning, Artificial Intelligence e Big Data Analythics

- ML ed AI permettono di analizzare grandi volumi di dati storici in tempo reale per identificare pattern e tendenze che potrebbero suggerire la probabilità di un rischio imminente
- Creazione di matrici di rischio e valutazioni probabilistiche.

3. Block Chain

- Integrità e sicurezza dei dati
- Tracciabilità e audit delle transazioni

4. Framework di riferimento

- Standard come ISO 27001 e ISA/IEC 62443, forniscono linee guida per l'identificazione, la valutazione e la gestione dei rischi in ambienti OT/IoT.

Framework specifici per la supply chain, come il NIST Cybersecurity

- Framework, includono strumenti per mappare e proteggere i flussi di dati e materiali.
- Regolamenti e Compliance integrata.

5. Tecniche di simulazione

- L'uso di digital twin e di scenari di simulazione consentono di valutare l'impatto potenziale di un attacco su sistemi OT/IoT senza interrompere le operazioni reali sfruttando le capacità del primo di capire cosa sta accadendo in tempo reale e del secondo invece di cosa potrebbe accadere in caso di introduzione di cambiamenti di processo.

6. Valutazioni di vulnerabilità

- Strumenti di scansione e penetration testing aiutano a identificare le vulnerabilità presenti nei dispositivi IoT e nei sistemi OT, fornendo dati utili per la stima del rischio.

"La quantificazione del rischio è un passaggio fondamentale per gestire efficacemente le minacce cyber".

La connessione con la direttiva NIS2

L'introduzione della direttiva NIS2 rappresenta un punto di svolta nella gestione del rischio per le infrastrutture critiche e le organizzazioni che operano in ambiti essenziali. Questa normativa europea rafforza l'obbligo per le organizzazioni di implementare misure efficaci per la gestione del rischio, con particolare attenzione alla resilienza delle infrastrutture essenziali e alla sicurezza della supply chain.

In particolare, la NIS2 enfatizza:

1. Gestione dei rischi di terza parte

Le organizzazioni devono valutare non solo i rischi interni, ma anche quelli legati ai fornitori e ai partner della supply chain. Questo richiede l'adozione di contratti che includano requisiti di sicurezza e un monitoraggio continuo delle performance dei fornitori.

2. Resilienza delle infrastrutture essenziali

La direttiva richiede che le infrastrutture critiche, come quelle energetiche, di trasporto e sanitarie, siano in grado di resistere e recuperare rapidamente da attacchi cyber. Questo obiettivo è strettamente legato alla capacità di quantificare i rischi e implementare piani di risposta e recovery.

3. Approccio basato sul rischio

La NIS2 promuove l'adozione di un approccio basato sul rischio, integrando valutazioni qualitative e quantitative per prioritizzare le risorse e garantire una protezione efficace.

Sfide nella digital supply chain

La digital supply chain introduce ulteriori complessità nella gestione del rischio. Con la crescente interconnessione tra fornitori, partner e clienti, una vulnerabilità in un punto della catena può avere effetti a cascata su tutto l'ecosistema.

Alcune delle principali sfide includono:

1. Lack of visibility

Monitorare ogni nodo della supply chain è spesso difficile, specialmente quando si utilizzano fornitori terzi che non seguono standard di sicurezza uniformi.

2. Dipendenza da tecnologie eterogenee

La presenza di dispositivi di diverse generazioni e provenienti da produttori differenti, la mancanza di standardizzazione nei processi e dati isolati tra fornitori, rendono complessa l'integrazione e la protezione.

3. Minacce avanzate e persistenti (APT)

Gli attacchi mirati, spesso sponsorizzati da stati nazionali o organizzazioni criminali, possono compromettere intere supply chain.

Strumenti per mitigare il rischio

Per affrontare queste sfide, le organizzazioni devono adottare un mix di strategie tecniche, organizzative e operative:

1. Threat Intelligence

L'uso di servizi di threat intelligence consente di anticipare potenziali attacchi, monitorando attivamente le minacce emergenti e modellando scenari che riflettono possibili eventi.

2. Segmentazione della rete

Isolare i sistemi OT da quelli IT riduce il rischio che un attacco informatico si propaghi tra diverse parti dell'infrastruttura.

3. Formazione del personale

Investire nella consapevolezza e nella formazione dei dipendenti aiuta a ridurre il rischio legato a errori umani.

4. Monitoraggio continuo

Implementare soluzioni di Security Information and Event Management (SIEM) e sistemi di rilevamento delle intrusioni (IDS) specifici per OT/IoT.

Il futuro della quantificazione del rischio in OT/IoT

Con l'evoluzione delle tecnologie, anche gli approcci alla quantificazione del rischio stanno cambiando. L'uso di intelligenza artificiale e machine learning promette di migliorare la capacità di analizzare grandi quantità di dati e prevedere attacchi con maggiore precisione. Allo stesso tempo, l'adozione di standard globali più rigorosi e l'integrazione di metriche di sostenibilità nella valutazione del rischio potrebbero favorire un approccio più olistico.

Conclusioni

La quantificazione del rischio nel mondo OT/IoT e nella digital supply chain è un elemento chiave per garantire la resilienza delle organizzazioni in un panorama di minacce sempre più complesso. Attraverso l'adozione di metodologie innovative, la collaborazione tra stakeholder e l'investimento in tecnologie avanzate come l'AI e l'analisi dei Big Data, le imprese possono non solo mitigare i rischi, ma anche trasformarli in opportunità per rafforzare la propria posizione competitiva.

"Con l'evoluzione delle tecnologie, anche gli approcci alla quantificazione del rischio stanno cambiando".

Comunicazione e condivisione nella risoluzione di un incidente di sicurezza

A cura di Massimo Poletti

"Non è una questione di se, ma una questione di quando": questa è la frase che chi si occupa di cybersecurity sente ripetere sempre più spesso. Gli attacchi informatici, in costante aumento per numero e sofisticazione, richiedono non solo una prevenzione adeguata, ma anche una preparazione dettagliata per affrontare l'inevitabile: la gestione dell'incidente.

Le normative di sicurezza oggi in vigore prevedono che le organizzazioni abbiano un piano di risposta agli incidenti, articolato in rilevamento, contenimento e ripristino. Tuttavia, un elemento spesso trascurato è l'importanza della comunicazione e della condivisione delle informazioni durante tutte le fasi di gestione. Non si tratta solo di soddisfare i requisiti normativi nei rapporti con le Autorità, ma anche di mitigare le conseguenze dell'incidente nel breve e medio periodo.

La comunicazione come pilastro della gestione

Basandomi sull'esperienza del gravissimo incidente informatico che ha colpito il Comune di Ferrara nel luglio 2023, vorrei esplorare i diversi livelli di comunicazione che abbiamo affrontato:

1. **Comunicazione interna:** verso vertici aziendali, colleghi e personale.
2. **Comunicazione esterna:** verso gli organi di stampa.
3. **Comunicazione diretta:** verso i cittadini tramite sito web e social media.
4. **Comunicazione istituzionale:** verso le Autorità competenti e il DPO.

Per motivi di spazio, mi concentrerò sui principi e le modalità operative che hanno guidato queste attività, fornendo spunti pratici.

A tempo zero: come impostare la risposta

Ci sono due elementi essenziali da predisporre per essere pronti a rispondere a un attacco:

- un numero di telefono dedicato per attivare immediatamente il Response Team;
- un coordinatore con funzioni di "comandante in capo" (spesso il CIO o il CISO), supportato da un coordinatore tecnico che isoli il team operativo dal flusso esterno di richieste e informazioni.

Nel nostro caso, l'incidente è stato rilevato intorno alle 8 del mattino. Dopo aver attivato il Response Team, nella mia funzione di dirigente IT e RTD ho avviato rapidamente la comunicazione interna utilizzando tutti i canali disponibili:

1. **Vertici aziendali:** li ho informati immediatamente sulla gravità potenziale della situazione, rassicurandoli che avrei gestito l'intero processo e li avrei tenuti aggiornati.
2. **Colleghi dirigenti:** ho impartito istruzioni tecniche semplici e immediate, come la disconnessione degli apparati di rete.
3. **Personale:** ho inviato comunicazioni chiare e dirette con disposizioni operative.

La priorità iniziale è mantenere la calma: un tono deciso e rassicurante è fondamentale per evitare il panico. La leadership situazionale insegna che un leader determinato può aumentare la coesione e l'efficacia decisionale del gruppo.

Comunicare con l'esterno: stampa e cittadini

La mattina stessa dell'attacco, abbiamo emesso un primo comunicato stampa per mantenere il controllo della narrazione. Il silenzio comunicativo è pericoloso: può essere interpretato come inazione e favorire speculazioni. Anche nei momenti più delicati, come durante la pubblicazione di alcuni dati sensibili, abbiamo garantito una comunicazione trasparente, mantenendo il pallino saldamente nelle nostre mani.

Per i cittadini, è stata creata una sezione dedicata sul sito istituzionale, dove raccogliere comunicati, notizie e aggiornamenti, integrata con i canali social per raggiungere il maggior numero possibile di persone. Questo approccio ha contribuito a mantenere alta la fiducia della cittadinanza, come dimostrato dal basso numero di richieste di accesso agli atti ricevute.

Rapporti con le Autorità e il DPO

La comunicazione verso le Autorità è regolata da normative precise. Nel nostro caso:

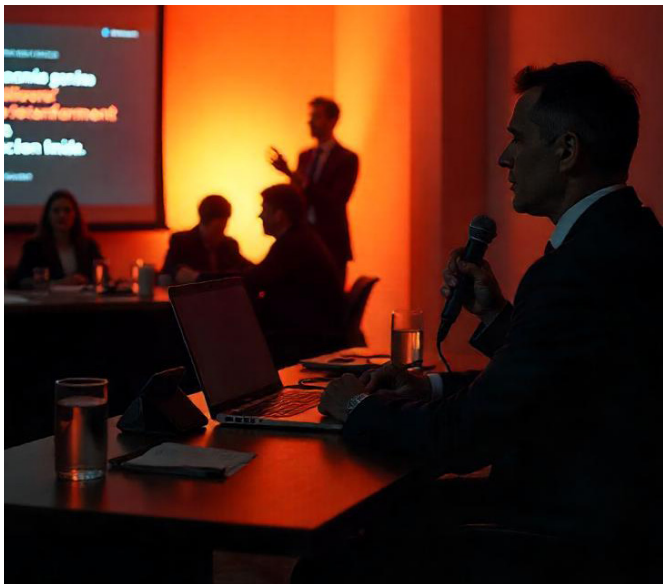
- abbiamo immediatamente effettuato la consultazione con il DPO dell'Ente al fine della tempestiva notifica al Garante per la protezione dei dati personali;
- abbiamo denunciato subito il reato alla Polizia Postale;
- abbiamo effettuato le segnalazioni all'ACN nei tempi previsti.

Un aspetto cruciale è mantenere un rapporto costante con il Garante, soprattutto in caso di incidenti complessi e prolungati. Meglio inviare comunicazioni frequenti con aggiornamenti parziali, piuttosto che lasciare buchi temporali significativi. L'ultima segnalazione deve includere una ricapitolazione completa dell'accaduto e un'analisi esaustiva, utile a dimostrare che tutto il possibile è stato fatto. Il DPO dell'Ente ci ha supportato non solo nella valutazione dei rischi per gli interessati e nelle metodologie da utilizzare per la loro non facile identificazione, ma anche nei rapporti con la parte legale e l'individuazione delle forme più opportune di comunicazione.

La gestione della pubblicazione dei dati

Nel caso di perdita di riservatezza dei dati, la comunicazione si complica ulteriormente:

- **Internamente:** è essenziale valutare rapidamente la qualità dei dati pubblicati e i rischi associati.
- **Esteriormente:** è necessario informare tempestivamente gli interessati e collaborare con il DPO per garantire la massima trasparenza.
- **Verso le Autorità:** segnalare il nuovo reato alla Polizia Postale e aggiornare il Garante con regolarità fino alla chiusura dell'evento.



Condivisione: un dovere verso la comunità

Non tutto può essere condiviso durante e dopo un incidente, ma è fondamentale diffondere le lezioni apprese con la comunità professionale. Nel nostro caso abbiamo scelto un approccio innovativo: una cronaca in tempo reale delle attività tecniche, che è stata molto apprezzata dai colleghi.

Condividere esperienze non solo aiuta gli altri a prepararsi meglio, ma rafforza anche la resilienza collettiva contro le minacce informatiche. In un mondo dove "quando" è l'unica certezza, la comunicazione e la condivisione diventano le nostre armi più potenti.

"In un mondo dove 'quando' è l'unica certezza, la comunicazione e la condivisione diventano le nostre armi più potenti".

L’imprescindibile correlazione tra digitalizzazione, Cybersecurity e protezione dei dati personali

A cura di Paola Casaccino e Adriano Orlando

La digitalizzazione rappresenta un processo di trasformazione che ha rivoluzionato il contesto sociale ed economico, influenzando la gestione delle informazioni e dei dati personali. Questo processo di evoluzione digitale è strettamente legato alla necessità di garantire una cybersecurity solida e una protezione efficace dei dati personali, elementi fondamentali per uno sviluppo sostenibile e sicuro. Tale trasformazione implica l’adozione di tecnologie innovative e la loro integrazione nelle attività quotidiane, nei processi aziendali, nella comunicazione e nella gestione delle informazioni.

Alcuni aspetti chiave dell’evoluzione digitale includono ovviamente:

Intelligenza Artificiale (AI): Lo sviluppo di sistemi in grado di eseguire compiti che normalmente richiedono intelligenza umana, come il riconoscimento vocale, la traduzione automatica e l’analisi dei dati.

Blockchain: Una tecnologia che consente la creazione di registri distribuiti e immutabili, utilizzati principalmente per garantire la sicurezza e la trasparenza delle transazioni digitali.

Machine Learning: Una branca dell’AI che si concentra sullo sviluppo di algoritmi che permettono ai computer di apprendere dai dati e migliorare le loro prestazioni nel tempo senza essere esplicitamente programmati.

Crittografia dei dati: Metodi per proteggere le informazioni digitali rendendole illeggibili a chiunque non possieda le chiavi di decrittazione necessarie.

Internet delle Cose (IoT): La connessione di oggetti fisici a internet, permettendo loro di comunicare tra loro e con altri dispositivi digitali, migliorando l’efficienza e l’automazione.

L’evoluzione digitale sta trasformando ogni aspetto della vita dei cittadini creando nuove sfide, come la necessità di garantire la sicurezza informatica e la protezione dei dati personali, nonché di sviluppare competenze digitali adeguate per affrontare il futuro..

In questo ambito, un parallelismo deve essere effettuato con la recente introduzione della nozione di “Quarta Rivoluzione Industriale”.

In Italia una delle spinte più innovative degli ultimi anni in ambito di digitalizzazione è rappresentata dal Piano Nazionale Ripresa e Resilienza (di seguito “PNRR”), in cui è stata inserita la Missione 1, che si concentra sull’evoluzione digitale e sul favorire ed incrementare le competenze digitali dei cittadini proteggendoli al contempo

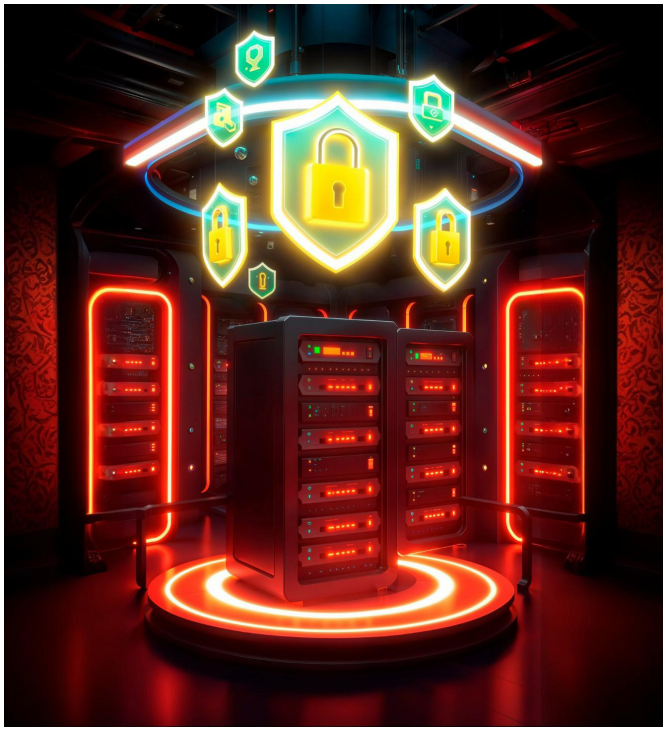
dalle minacce cyber.

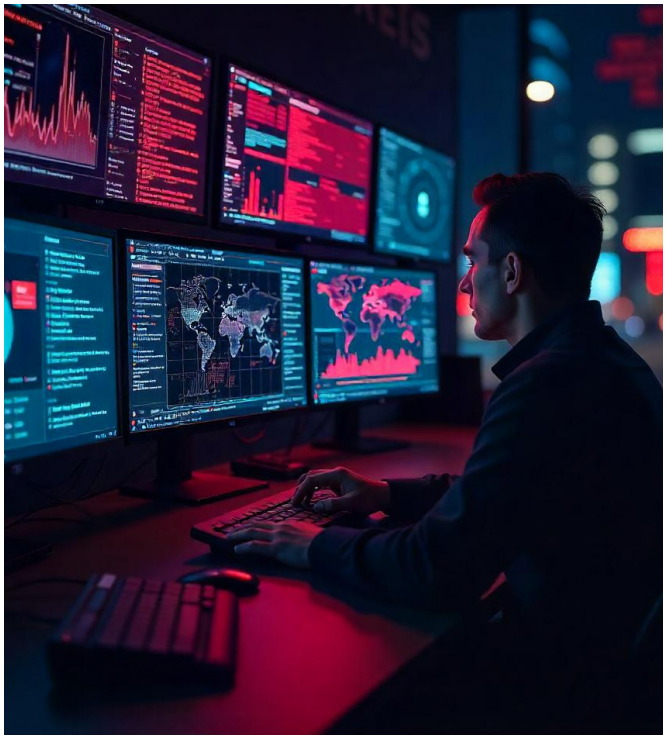
In merito alla protezione dei dati, la cybersecurity rappresenta una delle sfide più importanti e più avvincenti per gli Stati nel XXI secolo, e conseguentemente, per il loro relativo diritto. Questa, richiede che siano presenti misure di sicurezza efficaci che si concentrino su tre elementi fondamentali: le persone, i processi e la tecnologia ed ogni strategia di sicurezza informatica deve essere essenzialmente basata sulla confidenzialità, integrità e disponibilità dei dati.

Nel 2024, le violazioni dei dati hanno rappresentato una sfida significativa per le organizzazioni di tutto il mondo. Secondo il report annuale di IBM, il costo medio di una violazione dei dati è aumentato del 10% rispetto all'anno precedente, raggiungendo i 4,88 milioni di dollari a livello globale. In Italia, il costo medio è stato di 4,37 milioni di euro, con un aumento del 23% rispetto al 2023.

Alcuni dei principali vettori di attacco iniziale nel 2024 sono stati il phishing e il furto o la compromissione delle credenziali, che rappresentavano il 30% delle violazioni in Italia. Tuttavia, l'adozione di tecnologie innovative come l'intelligenza artificiale (AI) e l'automazione ha permesso alle organizzazioni di ridurre i costi delle violazioni di circa 3,24 milioni di euro rispetto a quelle che non le hanno utilizzate.

L'integrazione tra cybersecurity e privacy è quindi essenziale per la protezione dei dati, coinvolgendo la gestione dei rischi e la sicurezza dei sistemi informatici. Saranno necessarie governance efficaci e politiche condivise per contrastare il cyberterrorismo e la criminalità transnazionale. La cybersecurity richiede alleanze forti e strategie cooperative per creare un ambiente digitale sicuro.





"L'integrazione tra cybersecurity e privacy è quindi essenziale per la protezione dei dati, coinvolgendo la gestione dei rischi e la sicurezza dei sistemi informatici".

Trends di Cybesecurity per il 2025

A cura di Corradino Corradi

All'inizio di ogni anno molti CISO ed esperti di sicurezza informatica si cimentano in previsioni su quali saranno i trends più importanti dell'anno. Anche io non mi sottraggo a questo esercizio, ma lo faccio considerando il punto di vista di chi lavora da qualche anno in paesi emergenti e vede l'Europa e l'Italia con la prospettiva dell'Emisfero Sud della Terra.

Al di là dell' esattezza delle previsioni, l'esercizio di analizzare i principali trends della sicurezza informatica per i prossimi dodici mesi è utile per fare una analisi dello "scenario" cyber e consolidare la strategia di cyber-security da presentare a top management e Board.

Ecco la mia top list.

Skill shortage nella cybersecurity

La carenza di competenze in cybersecurity è e resterà un problema significativo sia in Italia che in Europa nel 2025.

In Italia la domanda di esperti in cybersecurity continua a crescere rapidamente, superando l'offerta disponibile. Questo fenomeno è aggravato dalla necessità di competenze avanzate per affrontare le nuove minacce digitali e l'adozione di tecnologie come l'intelligenza artificiale e il cloud computing.

In Europa e nel mondo la carenza di professionisti in cybersecurity è un problema diffuso. Secondo l'European Cyber Security Organisation (ECSO), ci sono milioni di posizioni vacanti nel settore della sicurezza informatica.

La formazione continua e l'aggiornamento delle competenze sono cruciali per colmare questo gap a livello aziendale; è inoltre necessario uno sforzo, sia a livello di scuole superiori che di università, per creare corsi ad hoc dedicati alla sicurezza informatica.

L'intelligenza artificiale generativa adottata da entrambe le parti del "campo di battaglia"

L'intelligenza artificiale generativa ha rivoluzionato il campo della cybersecurity, offrendo strumenti potenti sia per la difesa che per l'attacco.

Da un lato, le tecnologie di AI generativa sono impiegate per identificare e neutralizzare minacce in tempo reale, analizzando grandi volumi di dati e rilevando pattern anomali. Piattaforme di sicurezza informativa "powered by AI" possono prevedere e prevenire potenziali attacchi, migliorando la resilienza delle infrastrutture digitali.

Dall'altro lato, l'AI generativa è utilizzata dagli attaccanti per creare malware sofisticati, capaci di adattarsi e mutare per eludere le difese tradizionali. Gli attacchi possono essere automatizzati e orchestrati con precisione, aumentando l'efficacia e la scala delle operazioni malevole.

Questa doppia faccia dell'AI generativa crea un nuovo "campo di battaglia", dove difensori e attaccanti competono per ottenere un vantaggio tecnologico.

In particolare nel 2025, vanno predisposte contromisure per ridurre i rischi legati ad attacchi informatici e frodi online che sfruttano le capacità avanzate di AI per realizzare "deepfake" ed "advanced phishing"

Cyber Security In The BoardRoom

Il ruolo del CISO è diventato cruciale nell'odierno panorama digitale, dove le minacce informatiche sono in costante evoluzione. Il CISO non solo gestisce la sicurezza delle informazioni, ma riveste anche una funzione strategica all'interno dell'organizzazione.

È fondamentale che il CISO comunichi regolarmente con il Top management ed il Board, utilizzando un linguaggio manageriale e focalizzato sui rischi, piuttosto che esclusivamente tecnico.

Mantenere il Board aggiornato sulle sfide e le vulnerabilità emergenti permette di ottenere il supporto necessario per implementare misure di sicurezza efficaci. Il CISO deve tradurre i rischi tecnici in termini di impatto commerciale e operativo, evidenziando come le minacce possano influire sulla continuità del business, sulla reputazione aziendale e sulla conformità normativa. Una comunicazione chiara e strategica facilita l'allocazione delle risorse e l'approvazione del di sicurezza aziendale.

Nel 2025 mi aspetto che sempre più aziende medie e piccole creino o rafforzino il ruolo del CISO, così come già avviene per le aziende di grandi dimensioni, parte della infrastruttura critica dei paesi dove operano.

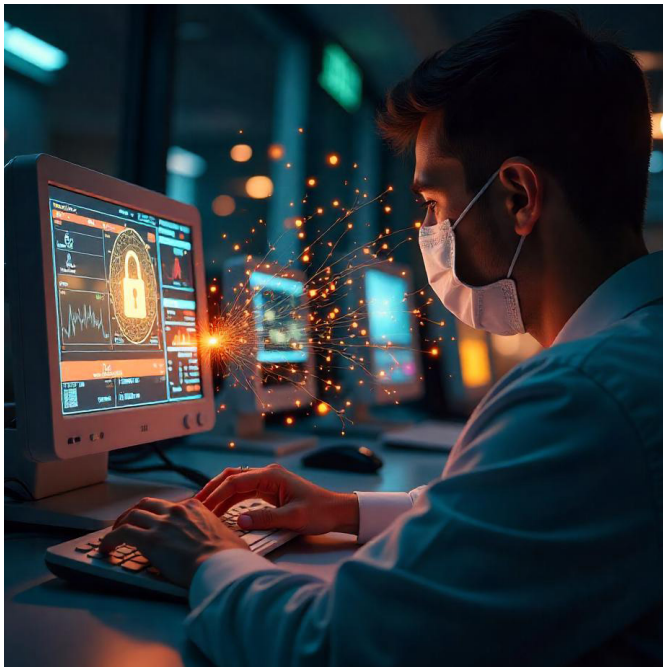
"Il ruolo del CISO è diventato cruciale nell'odierno panorama digitale, dove le minacce informatiche sono in costante evoluzione".

IoT Cyber Attacks, con focus su apparati medicali

Un trend emergente particolarmente preoccupante è l'aumento degli attacchi su dispositivi IoT, con un focus specifico sugli apparati medicali. Questi dispositivi, spesso caratterizzati da una sicurezza limitata e una connettività elevata, sono diventati bersagli privilegiati per i cybercriminali. Gli attacchi ai dispositivi medici IoT possono avere conseguenze importanti, compromettendo la sicurezza dei pazienti (intesa come safety) e la privacy dei loro dati sanitari (informazioni personali e sensibili).

Gli attacchi possono variare da intrusioni mirate che mirano a manipolare i dati dei pazienti o a interrompere il funzionamento dei dispositivi, fino a campagne di ransomware che criptano i dati cruciali e bloccano l'accesso ai sistemi finché non viene pagato un riscatto.

Negli ultimi anni il settore ospedale italiano è stato oggetto di numerosi attacchi di tipo ransomware; anche se la situazione è migliorata, anche nel 2025 l'attenzione deve restare massima e le aziende devono predisporre "contingency plan" e stipulare coperture assicurative cyber.



Cyber Warfare e attacchi informatici sponsorizzati dallo Stato

Gli attacchi informatici sponsorizzati da stati hanno registrato un preoccupante aumento negli ultimi anni, accelerando in modo significativo in seguito a conflitti geopolitici come la guerra tra Russia e Ucraina e tra Israele e Hamas in Palestina. Queste operazioni, spesso sofisticate e ben finanziate, mirano a destabilizzare infrastrutture critiche, rubare informazioni sensibili e influenzare l'opinione pubblica.

Durante il conflitto russo-ucraino, ad esempio, sono stati documentati numerosi attacchi coordinati contro infrastrutture energetiche, reti di comunicazione e sistemi governativi, volti a paralizzare la capacità operativa dell'Ucraina e a diffondere disinformazione.

Allo stesso modo, le tensioni tra Israele e Palestina hanno visto un aumento degli attacchi informatici che prendono di mira sia obiettivi militari che civili, con lo scopo di interrompere servizi essenziali e compromettere la sicurezza nazionale.

Questi attacchi non si limitano ai paesi direttamente coinvolti nei conflitti, ma spesso si estendono anche ad alleati e rivali (digital proxy war), creando una rete globale di cyber guerre e spionaggio digitale.

Il 2025 vedrà un ulteriore aumento delle capacità of-

fensive cibernetiche degli Stati, con un impatto sulla sicurezza internazionale che richiede una cooperazione più stretta tra nazioni e l'adozione di strategie di difesa avanzate per proteggere le infrastrutture critiche e i dati sensibili.

Impatto crescente della regolamentazione, in particolare in Europa

I legislatori di tutto il mondo hanno compreso l'importanza di sviluppare leggi e regolamenti per contrastare in modo efficace la crescente minaccia informatica che impatta sia i cittadini che le aziende. In Europa, in particolare, sono stati introdotti strumenti legislativi avanzati come il Cybersecurity Act europeo, la NIS2 e DORA.

Il Cybersecurity Act europeo ha introdotto un quadro di certificazione comune per i prodotti, i servizi e i processi di cybersecurity. Questo atto legislativo ha l'obiettivo di aumentare la fiducia nel mercato digitale, garantendo che i prodotti certificati rispettino standard di sicurezza elevati. L'European Union Agency for Cybersecurity (ENISA) ha un ruolo chiave nell'implementazione di questo quadro normativo, promuovendo la cooperazione tra gli Stati membri e il settore privato.

> ***"La carenza di competenze in cybersecurity è e resterà un problema significativo sia in Italia che in Europa nel 2025".***

NIS2 (Network and Information Systems Directive) rappresenta un potenziamento della direttiva NIS precedente, rafforzando i requisiti di sicurezza per le infrastrutture critiche e ampliando la portata delle entità obbligate a conformarsi alle nuove regole. Questa direttiva mira a migliorare la resilienza dei servizi essenziali in Europa contro gli attacchi informatici, richiedendo misure di sicurezza più robuste e una maggiore cooperazione tra gli Stati membri.

DORA (Digital Operational Resilience Act) è un'altra iniziativa legislativa europea che si concentra specificamente sulla resilienza operativa digitale delle istituzioni finanziarie. DORA mira a garantire che le banche, le assicurazioni e altre entità finanziarie che operano a livello europeo siano preparate a gestire e mitigare i rischi informatici. Questo regolamento richiede l'adozione di misure di gestione del rischio, test di resilienza e una maggiore trasparenza nella comunicazione delle minacce.

In sintesi, le strategie regolamentari europee come i Cybersecurity Act, NIS2 e DORA rappresentano passi significativi verso una maggiore sicurezza informatica; molte aziende saranno impegnate, nel 2025, nel garantire la compliance a questi adempimenti.

Nel contesto italiano, a queste direttive e regolamentazioni europee, va aggiunto il Perimetro di Sicurezza Cibernetica, che prevede la necessità di effettuare la mappatura delle Infrastrutture Critiche, la valutazione dei rischi, l'adozione di misure di sicurezza ad-hoc, la predisposizione di piani di risposta agli incidenti, la formazione e supporto per la cooperazione ed infine la condivisione delle informazioni di sicurezza

Vulnerabilità su dispositivi di sicurezza perimetrali

Nel 2024, il panorama della sicurezza informatica è stato caratterizzato da un aumento significativo delle vulnerabilità riscontrate nei dispositivi di sicurezza perimetrali, quali router e firewall. Tra i maggiori fornitori colpiti si annoverano Fortinet, Cisco e Palo Alto.

I gruppi hacker Salt Typhoon e Volt Typhoon hanno

sfruttato queste vulnerabilità per condurre attacchi mirati agli operatori di telecomunicazioni statunitensi. Salt Typhoon, noto per le sue campagne di cyber spionaggio, ha utilizzato le falle nei dispositivi Fortinet e Cisco per ottenere accesso non autorizzato a reti critiche, esfiltrare dati sensibili e monitorare le comunicazioni interne degli operatori. Volt Typhoon, d'altra parte, ha lanciato attacchi informatici utilizzando le vulnerabilità nei dispositivi Palo Alto. Questi attacchi hanno portato alla compromissione di numerosi sistemi di gestione della rete, causando interruzioni del servizio e perdite finanziarie significative per gli operatori colpiti.

È fondamentale che nel 2025 le organizzazioni adottino misure di sicurezza avanzate (compreso accesso da remoto mandatorio con l'autenticazione multi-fattore -MFA), effettuino aggiornamenti regolari dei propri sistemi perimetrali (hardening e patch management) ed implementino soluzioni di posture management in grado di coprire tutta la superficie degli asset digitali esposti su Internet.

Aumento significativo degli infostealers

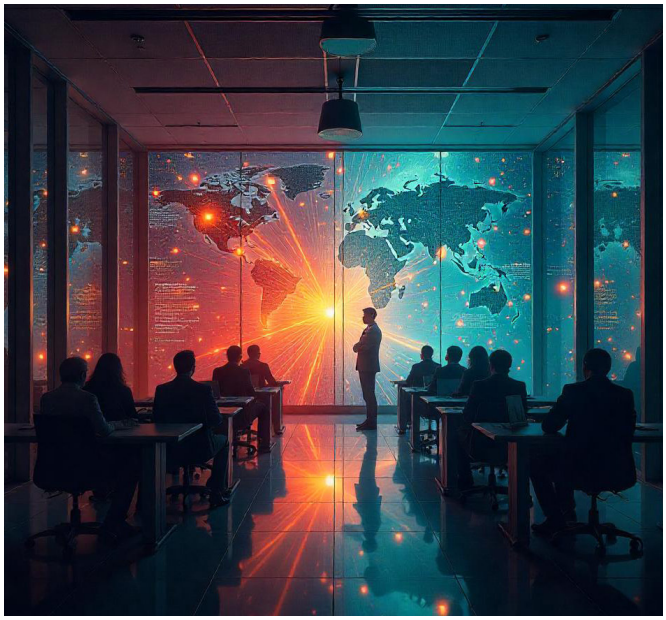
Nel 2024, gli infostealers (malware, progettati per rubare informazioni sensibili come credenziali di accesso, dati finanziari e altre informazioni personali) hanno svolto un ruolo cruciale nel facilitare l'aumento degli attacchi informatici di successo ("andati a segno"). Essi sono diventati sempre più sofisticati e difficili da rilevare. La facilità con cui gli infostealers possono essere distribuiti e utilizzati ha reso le reti aziendali e personali particolarmente vulnerabili, permettendo agli aggressori di ottenere rapidamente l'accesso a sistemi critici e di esfiltrare dati preziosi senza essere rilevati.

Per mitigare questa minaccia, le organizzazioni devono adottare strategie di sicurezza avanzate che includono l'implementazione del modello Zero Trust; inoltre, le organizzazioni dovrebbero investire in soluzioni di monitoraggio continuo e analisi comportamentale per identificare attività sospette e rispondere tempestivamente agli incidenti.

Mi aspetto che anche nel 2025 gli infostealers saranno uno delle tecniche più utilizzate dagli hackers insieme a spear phishing.

In conclusione, spero che questa carrellata di trend di sicurezza informatica sia stata utile e possa rappresentare uno spunto per chi di voi si occupa di strategie di cyber-security e creazione di piani di "cyber risk mitigation". In fin dei conti aveva ragione Winston Churchill quando affermava che "Plans are of little importance, but planning is essential."

CYBER
Think Tank
ASSINTEL



Cyber-Crimine e Supply Chain
Il giallo dello Zero-Day che non c'è

A cura di Luca Mella

Introduzione

Nel corso dell'ultimo biennio, l'ecosistema delle minacce informatiche criminali è diventato il teatro di attacchi sempre più devastanti, in cui i criminal-hacker ricorrono a tattiche "ad ampio spettro" per compromettere le difese delle aziende. Sono in aumento i casi in cui i dispositivi di sicurezza – quali firewall e router – diventano essi stessi la porta d'accesso privilegiata per gli attaccanti, sfruttando talvolta falle appena scoperte o non note al momento dell'attacco, le cosiddette 0-day, oppure sviluppando attacchi mirati contro vulnerabilità note, ma non patchate in un grande numero di installazioni, in gergo note come falle 1-day.

Ma cosa sta succedendo esattamente nel mondo criminale riguardo allo sfruttamento delle vulnerabilità nei dispositivi? E come stanno rispondendo i produttori degli apparati che abbiamo installato all'interno delle nostre aziende? Queste sono le domande cardine su cui, nell'articolo, ragioneremo dati alla mano, lasciandoci con più di una sorpresa.

Lo Scenario 0-day nel Cyber Crime

Per comprendere come si stia evolvendo lo scenario delle minacce informatiche criminali, quelle che rappresentano di gran lunga le maggiori sfide per le PMI – colonna portante del tessuto produttivo nazionale e delle catene del valore di grandi aziende e gruppi – è necessario rivolgere un breve sguardo al passato.

Già nel 2022, in questo periodico, avevamo segnalato le prime avvisaglie di questo fenomeno. Esplorando la fuga di informazioni del defunto gruppo criminale russo Conti, avevamo documentato l'adozione di protocolli di R&D volti a individuare falle interne nei prodotti di sicurezza (es. router e firewall Cisco), per scoprire potenziali 0-day da sfruttare durante le intrusioni. Tali attività venivano spesso supportate dall'acquisto di software, apparati e licenze di questi prodotti tramite società di copertura.

Già allora si prefigurava un aumento del rischio senza precedenti, nel quale attacchi basati su 0-day e 1-day si univano a tecniche avanzate per eludere le difese aziendali. Questo trend trova riscontro anche nei dati delle Known Exploited Vulnerabilities (KEV) tracciate dal CISA americano, che evidenziano un aumento a doppia cifra della porzione di vulnerabilità 0-day registrate negli ultimi anni.

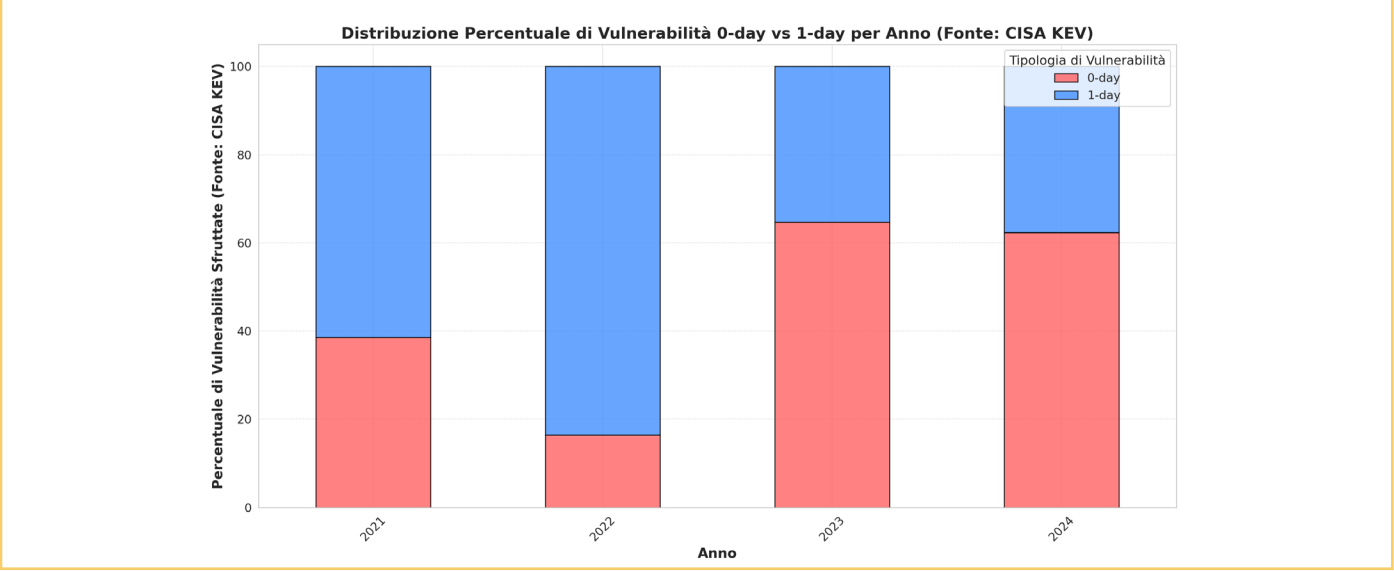


Figura 1. Distribuzione percentuale di vulnerabilità 0day e 1day (Sorgente:KEV)

Ma non è una mera questione di dati. Se, leggendo questi numeri, aveste cominciato a pensare: “Sì, ma il CISA probabilmente traccia gran parte di questi 0-day in contesti di attacchi state-sponsored, dove i livelli di sofisticazione sono ben più alti rispetto a quelli dei criminali”, purtroppo, non ci sono buone notizie.

Questo trend di attacchi 0-day e 1-day si è manifestato più volte, in modo estremamente brutale, per mano di attori criminali. Ad esempio, la gang cybercriminale Cl0p, nota per le sue devastanti campagne di doppia estorsione, ha investito ingenti risorse nello sviluppo di capacità offensive di questo tipo. Nel 2023, ha sfruttato uno 0-day nel software MOVEit Transfer (CVE-2023-34362), accedendo abusivamente ai dati di migliaia di organizzazioni in tutto il mondo e sottraendo informazioni personali di oltre 60 milioni di persone. Devastante. E, nel 2024, hanno replicato l’impresa! Questa volta, sfruttando 0-day nei software di trasferimento file di Cleo, tra cui Cleo Harmony, VLTrader e LexiCom (CVE-2024-50623 e CVE-2024-55956), sono riusciti a compromettere le reti di almeno 66 organizzazioni, sottraendo ulteriori dati sensibili.

Un altro esempio è l’elusiva gang criminale MalasLocker, che nel 2023 ha preso di mira i server di posta Zimbra. Sfruttando falle 1-day come la CVE-2022-24682, è riuscita a trafugare e pubblicare online gli archivi di posta elettronica di centinaia di organizzazioni in tutto il mondo. Anche in questa occasione, l’Italia e le nostre PMI non sono rimaste al di fuori delle cronache: il nostro paese, infatti, è risultato il più colpito. Inoltre, gli indicatori di rischio per le PMI sono estremamente concreti: in quella particolare campagna 1-day, oltre la metà delle aziende colpite aveva meno di 200 dipendenti.

Insomma, lo sfruttamento di vulnerabilità di tipo 0-day rappresenta uno dei maggiori incubi per le aziende e per i vendor di soluzioni di cybersecurity. Il cybercrimine, come osservato negli ultimi anni, si è strutturato per colpire duramente proprio in questo ambito.

Ma il problema non finisce qui. L’incremento di attacchi di questo tipo pone grandi sfide non solo alle organizzazioni, ma anche ai vendor, ai quali vengono richiesti livelli di attenzione, trasparenza e celerità sempre più elevati. In caso contrario, la sicurezza collettiva è seriamente compromessa. Ad esempio, se un vendor non fornisce dettagli specifici sulla falla sfruttata (o lo fa in modo generico), si genera incertezza, che può trasformarsi rapidamente in un problema critico, soprattutto per chi ha basato la protezione del perimetro proprio sui dispositivi coinvolti dalla vulnerabilità.

Per comprendere meglio questo punto, nelle prossime sezioni tratteremo il caso Zyxel, un noto firewall perimetrale estremamente diffuso in ambiente PMI, che nel quarto trimestre del 2024 ha evidenziato in maniera drammatica questa criticità.

Il Caso Zyxel

Questo caso è stato emblematico. Ma, prima di immergerci nel giallo che ha portato con sé, chiariamo cosa è accaduto. A partire da settembre 2024 sono state registrate varie intrusioni in tutta Europa, ed anche in Italia: attacchi ransomware a PMI clienti di Zyxel, notissimo produttore di dispositivi di rete economici. In base alle ricostruzioni effettuate da ricercatori di sicurezza e dagli avvisi emanati dal Vendor stesso, gli attacchi avvenivano tutti in modalità similari:

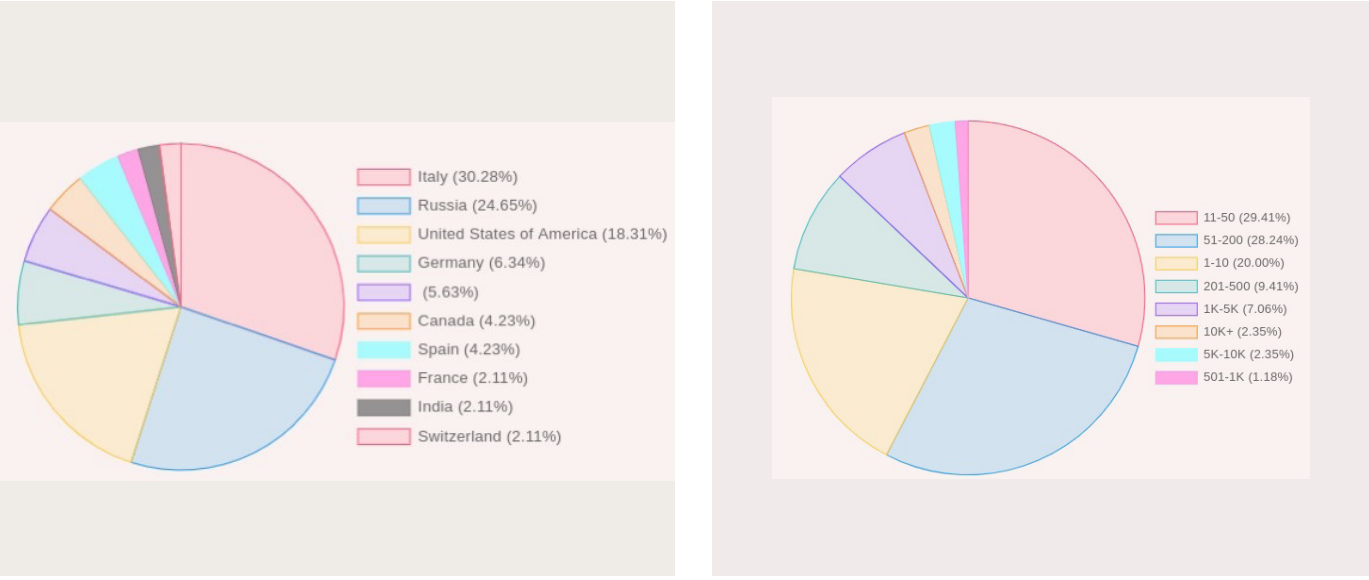


Figura 2. Distribuzione geografica delle organizzazioni con Zimbra violate da Malas (sinistra) e dimensione per numero di impiegati (destra). (Sorgente:doubleextortion.com)

1. L'accesso iniziale veniva effettuato attraverso i firewall Zyxel.
2. I criminali creavano sugli Zyxel account locali con nomi come "SUPPORT<NUMERO>" e configuravano regole ACL che appiattivano la rete (ad esempio, l'inserimento di regole ANY ANY, per chi è più tecnico).
3. L'intero ciclo di intrusione, dalla compromissione iniziale all'esecuzione del ransomware, si concludeva nell'arco di 1-2 ore.
4. I criminali si spostavano rapidamente da un sistema all'altro utilizzando strumenti legittimi, come Remote Desktop, PowerShell e scanner IP freeware. In alcuni casi, ricorrevano anche a strumenti comunemente utilizzati dai penetration tester, come Mimikatz.
5. Infine, venivano inoculati cifratori ransomware sia su sistemi Windows che sui virtualizzatori ESXi, basati su sistemi operativi Unix.

Questi attacchi sono stati attribuiti al gruppo "HellDown", apparso sulla scena intorno alla metà del 2024. Ma su questo torneremo più avanti.

L'aspetto più significativo di questi eventi, almeno ai fini dell'articolo, è la scarsa chiarezza dimostrata dal vendor. Zyxel ha infatti dichiarato che questi attacchi hanno sfruttato "precedenti vulnerabilità" nelle versioni firmware, genericamente indicate come "dalla 4.32 alla 5.38", senza però pubblicare dettagli tecnici né identificativi specifici. Questo livello di opacità ha generato un vero e proprio giallo.

"Proteggere una rete non significa solo bloccare le minacce, ma anche garantire che i dati possano fluire in modo sicuro e controllato".

Il Giallo dello 0day

Zyxel, infatti, ha emesso diversi avvisi di sicurezza tra settembre e novembre 2024, proprio in relazione a queste ondate di attacchi estorsivi. Tuttavia, con una precisione quasi chirurgica, non ha fornito alcun dettaglio tecnico che consentisse di identificare chiaramente il bug sfruttato dai criminali. In particolare:

- Nel bollettino del 9 ottobre 2024, Zyxel dichiarava che i criminali riuscivano a rubare credenziali dai firewall sfruttando "vulnerabilità precedenti", senza però fare riferimento ad alcun altro bollettino, né tantomeno a identificativi CVE. L'unica informazione fornita era una generica indicazione secondo cui "le vulnerabilità hanno interessato le versioni precedenti del firmware ZLD V4.32 fino alla versione ZLD 5.38".
- Poco prima, il 3 settembre 2024, Zyxel aveva rilasciato un bollettino in cui forniva aggiornamenti firmware per una serie di falle (cinque, tutte scoperte nel 2024), specificando che la versione del firmware in grado di risolverle era la ZLD V5.39, indicata anche negli avvisi sugli attacchi come "sicura". Si potrebbe dunque supporre che la "vulnerabilità precedente" menzionata nel bollettino di ottobre sia tra queste? Una domanda legittima, ma, per ora, rimane senza risposta. Approfondiremo la questione più avanti.
- Un ulteriore elemento interessante riguarda il comunicato di rilascio del firmware 5.39, identificato con il numero 25726, che introduceva la patch del firmware v5.39patch-0. Questo comunicato, inizialmente pubblicato a settembre, è stato rimosso poche settimane dopo e riapparso solo a novembre con un nuovo link identificato come 26897. In questo caso, la versione della patch risultava leggermente diversa: v5.39patch-1. Anche qui, però, non è stato fornito alcun riferimento a identificativi di vulnerabilità o agli attacchi in corso, lasciando spazio a ulteriori dubbi e incertezze.

Insomma, la dinamica della comunicazione da parte del vendor è stata alquanto opaca. Persino un controllo incrociato dei dati sulle vulnerabilità dichiarate dal vendor a settembre con le informazioni sulle versioni riportate nel bollettino degli attacchi di ottobre non ha chiarito la situazione. Anzi, tutt'altro: l'analisi incrociata tra le 14 vulnerabilità Zyxel scoperte tra il 2023 e il 2024 – le più plausibili per essere sfruttate nella catena di attacco di HellDown – ha evidenziato l'incompatibilità tra queste falle (note) e l'abuso effettivo da parte dei criminali. In altre parole, la falla sfruttata non sembra essere tra quelle note.

Allora, cosa può essere successo? È difficile dirlo con certezza. Tuttavia, è evidente che il vendor ha tenuto – e continua a tenere – nascosti parecchi dettagli. Probabilmente, la vulnerabilità non è stata censita in modo appropriato, forse per errore o per leggerezza dello staff di sicurezza di Zyxel. Oppure, potrebbe essere stata una scelta deliberata. La cura con cui Zyxel ha evitato di associare un identificativo preciso del bug agli attacchi è quantomeno "sospetta", così come l'apparizione della "v5.39patch-1" in seguito alla "v5.39patch-0".

Ciò che è certo è che questo livello di opacità non ha minimamente aiutato i clienti della casa taiwanese a proteggersi dalle campagne di attacco in corso.

HellDown - Perchè conta?

Torniamo ora su HellDown. HellDown è un gruppo cyber criminale che ha lanciato diverse ondate di attacchi ransomware contro aziende di varie dimensioni in tutta Europa e che, nell'agosto 2024, è stato persino autore di un'intrusione diretta nella rete Zyxel, avvenuta poco prima dell'ondata di attacchi di settembre.

Il bottino di questa intrusione? Sui propri blog, HellDown dichiarava di essere entrato in possesso di oltre 253 GB di dati dai server interni di Zyxel, tra cui codici sorgenti e documenti riservati del produttore di dispositivi di sicurezza.

A questo punto, il giallo si infittisce, diventando sempre più complesso. Per quale motivo questa reticenza da parte di Zyxel? Ancora una volta, non ci sono risposte definitive, ma qualche ipotesi può essere formulata. Ad esempio, il rilascio della patch-0 e poi della patch-1 potrebbe indicare che gli aggiornamenti rilasciati a settembre non erano in grado di mitigare lo sfruttamento della falla specifica, suggerendo una risoluzione inefficace che ha permesso agli attaccanti di continuare a compromettere i clienti Zyxel.

Ma c'è di più: la reticenza nel menzionare esplicitamente la falla rende il mistero ancora più profondo. È possibile che la vulnerabilità sia stata scoperta a seguito del furto di dati avvenuto nell'agosto 2024. Oppure, lo scenario potrebbe essere ancora più preoccupante: non si tratterebbe di una vera "falla", ma di una "funzionalità" nascosta, una backdoor del vendor o un accesso manutentivo che, a un certo punto, è diventato noto anche agli attaccanti.

Ovviamente, queste sono solo ipotesi. Tuttavia, è facile immaginare le problematiche a cui potrebbe andare incontro un vendor di questo tipo, se venisse dimostrato un collegamento tra una compromissione subita e gli attacchi estorsivi ai suoi clienti. Questo aprirebbe la strada a potenziali profili di responsabilità tutt'altro che banali.

Conclusioni: Supply Chain e Trasparenza (che ancora manca)

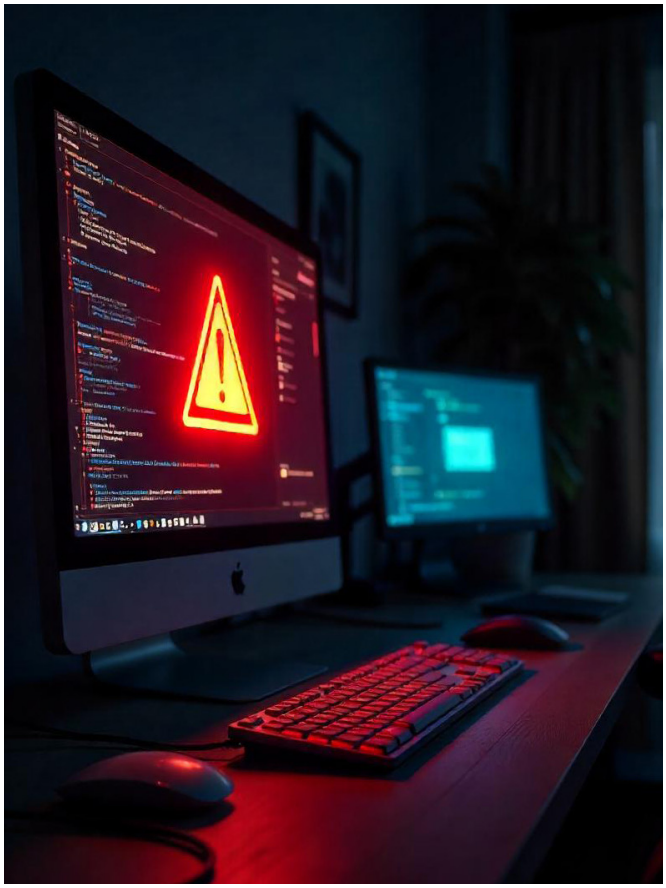
Il "caso Zyxel" ha evidenziato la delicata interdipendenza tra fornitori di tecnologia e aziende. La carenza di trasparenza nella gestione degli aggiornamenti e nella comunicazione delle vulnerabilità crea un vuoto di informazioni che può rapidamente trasformarsi in un problema sistemico di sicurezza. Quando i produttori scelgono di rimanere vaghi o omettono riferimenti chiari (ad esempio, CVE, advisory mirati o dettagli sulle patch), le organizzazioni restano nella totale incertezza su come e quando proteggersi in modo efficace.

D'altro canto, i criminali informatici sono ben consapevoli di queste lacune e le sfruttano con tattiche sempre più mirate. Non si tratta solo di una minaccia "high-end" tipica degli APT o degli attacchi nation-state, ma di veri e propri attori criminali che, potendo contare su informazioni sottratte al vendor stesso o su intelligence sui prodotti, riescono a sfruttare vulnerabilità – non di rado anche 0-day – per orchestrare campagne estorsive devastanti, con ricadute particolarmente gravi per le PMI.

"Ogni connessione rappresenta un'opportunità, ma anche un potenziale rischio: gestirle con attenzione è la chiave per un ambiente digitale sicuro".

In questo scenario sempre più complesso, la filiera produttiva e la catena di fornitura di soluzioni di sicurezza diventano elementi critici. Affidarsi a un vendor che non offre trasparenza e comunicazioni tempestive può vanificare gli sforzi difensivi.

Alla luce delle nuove normative NIS2 e DORA, e con attaccanti sempre più abili nell'identificare e sfruttare falle nei dispositivi tecnologici, diventa indispensabile una rinnovata cultura della sicurezza nella catena del valore. Questa deve promuovere la condivisione aperta delle informazioni sulle criticità e rafforzare i rapporti di fiducia tra fornitori e aziende. Solo così sarà possibile ridurre la superficie di attacco e garantire difese adeguate alle sfide poste dal cyber-crimine moderno.



Conoscere i rischi Cyber della propria azienda

A cura di Enzo Veiluva

La NIS 2 enfatizza un approccio proattivo alla gestione dei rischi, richiedendo alle aziende di anticipare le minacce e di prepararsi adeguatamente. Questo significa che le valutazioni dei rischi devono essere effettuate regolarmente e non solo in risposta a incidenti di sicurezza. Riservatezza, integrità e disponibilità dei servizi sono i principi da garantire, ma per farlo bisogna conoscere a fondo lo stato dei pilastri su cui si basa l'intera cybersicurezza di una azienda: ovvero i rischi dell'infrastruttura IT, i dati, le competenze e le policy.

La Direttiva NIS 2 rappresenta un passo importante verso il miglioramento della sicurezza delle reti e dei sistemi informatici nell'Unione Europea, ed il suo perimetro coinvolgerà, direttamente o indirettamente, molte imprese di tutte le dimensioni

Per proteggere i propri dati e i sistemi informatici, le PMI devono adottare una solida strategia di sicurezza, riconoscendo che le minacce informatiche possono variare in base al settore, alle dimensioni e alle attività aziendali.

Investimenti, acquisizioni tecnologie, formazione etc. sono indispensabili, ma poco efficaci se non c'e' la piena consapevolezza del proprio livello di rischio. Il tutto converge quindi nella necessità di un Cyber-security Risk Assessment. È fondamentale individuare le proprie vulnerabilità non solo in termini di sicurezza informatica ma affrontando anche gli impatti che esse possano avere sui processi produttivi aziendali.

Gli elementi chiave da valutare sono quattro: l'infrastruttura IT utilizzata, i dati gestiti, le competenze del personale e le policy adottate.

Ogni PMI dovrebbe prendere piena conoscenza del livello di aggiornamento (o di obsolescenza) presente nei propri sistemi; valutare le misure adottate per l'accesso al sistema (VPN e MFA, tecnologie oggigiorno imprescindibili, sono state implementate per tutti gli accessi?), conoscere il tempo massimo di fermo dei propri sistemi che può essere tollerato per il proprio business, (ci sono dei meccanismi di business continuity? i valori di RTO e RPO sono stati stabiliti? In caso di fermo di tutti i sistemi, è definito un piano di ripartenza con le priorità?).

È ovvio che utilizzare un cloud provider certificato sicuramente abbatte molti dei rischi rispetto ad una infrastruttura IT gestita in sede, ma non esime l'azienda dal fare una serie di valutazioni di rischio. Ad esempio legata alla propria catena di fornitura o alle attività IT di manutenzione assegnate all'esterno.

Secondo punto critico i dati. È previsto l'uso di tecniche crittografiche o di pseudonimizzazione?; Quanto sono replicati e distribuiti i dati importanti dell'azienda?: la maggior parte dei data breach avviene non per violazio-

ne dei database, ma perché è sufficiente collezionare l'enorme quantità di repliche di informazioni spesso copiate all'interno dei pc, delle caselle di mail o degli share di rete (Sono definite delle regole per evitarlo?). Infine, banali incidenti divengono catastrofici perché la progettazione del backup è stata carente o superficiale.

È stato attuato un programma di formazione Cyber per i dipendenti? (quante ore di formazione Cyber sono state effettuate? Quante simulazioni di incidente? Ci sono esercitazioni anti-phishing?). L'errore umano è una delle principali cause sfruttate dai cyber criminali. La formazione in sé non elimina il problema, purtroppo gli errori umani continueranno ad accadere, ma sicuramente si può incidere sulla loro frequenza.

Ultimo punto, ma non meno importante, sono le policy aziendali: quanti audit o simulazioni sono state fatte per verificarne l'efficacia? Le persone sanno riconoscere un tentativo di phishing o identificare una mail sospetta? Quanto le policy riportano a processi, ruoli e responsabilità ben definite, o quanto rimandano solo a norme generali?

Se queste domande non sono state ancora poste, forse allora è urgente iniziare a farlo!

"La formazione Cyber per i dipendenti è fondamentale per ridurre gli errori umani".

SIEM: Pronti, via! Suggerimenti per un'implementazione rapida ed efficiente

A cura di Clara Caucci

In un contesto aziendale sempre più digitalizzato, la sicurezza informatica è diventata una priorità assoluta. I firewall proteggono la rete da minacce esterne, ma non sono sufficienti da soli. È quindi fondamentale implementare un sistema di monitoraggio interno della rete, con la finalità di rilevare e rispondere tempestivamente alle minacce. Qui entra in gioco il SIEM (Security Information and Event Management).

Per iniziare, è essenziale valutare le esigenze specifiche dell'azienda. Questo include determinare il volume di log da gestire e stabilire gli obiettivi di sicurezza. Una volta chiariti questi punti, si può procedere alla selezione del SIEM più adatto. La scelta deve tenere conto della scalabilità e dell'adattabilità del sistema, oltre che della facilità d'uso e dell'integrazione con l'infrastruttura esistente. È importante confrontare le soluzioni open-source con quelle commerciali per trovare quella che meglio risponde alle necessità aziendali.

La pianificazione dell'implementazione è un passaggio cruciale.

È necessario definire un piano di progetto dettagliato, stabilendo gli obiettivi, un budget e una timeline.

Processes	Work Package	Deliverable
Project implementation	Installation and initial configuration	Installation and configuration of SIEM on devl server using Hypervisor
		Installing SIEM agent on a test VM
		Adding log file of Firewall via "syslog" and selection of events to monitor
		Settings to eliminate false positives due to default (mistaken) configuration)
		Settings filters to display on dashboard only relevant data
		Activation of Vulnerabilities Detection
		Setting rules for alerting if a priviledge escalation event is detected out of working hours
		Setting filters to display on dashboard only high or critical vulnerabilities
		Setting e-mail notifications of alarms
	ACL and whitelisting	Access Control List (ACL) settings into the virtual FWs of VMs which hosts SIEM
		Whitelisting of servers and workstations authorized to connect to SIEM
	Adding events monitoring	Adding all other Firewalls logs to SIEM
		Adding AD Servers logs
		Adding Backup Servers
		Adding Vulnerable Servers
		Adding workforce management server
	Testing	White-Box Penetration test for testing SIEM performance
	Prj implementation closure	Handover to IT & InfSec Operations

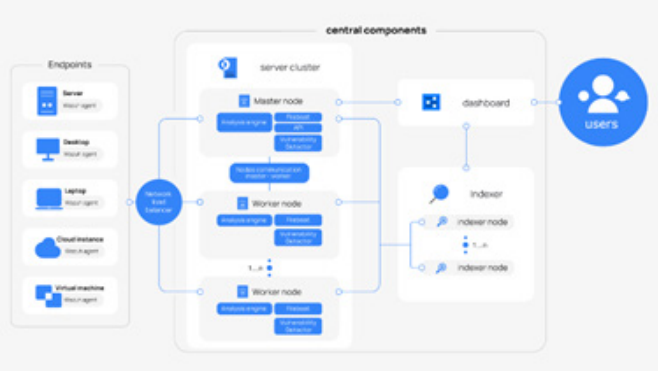
La configurazione iniziale del SIEM prevede l'installazione del software e la configurazione delle fonti di log, come firewall, server ed endpoint, ma anche servizi virtualizzati. È fondamentale impostare le regole di correlazione degli eventi, per garantire un monitoraggio efficace ed identificare i pattern di attacco. Molte soluzioni vengono fornite con set di regole preconfigurate, che permettono di rilevare i pattern più comuni, e possono essere integrate con altre personalizzate.

Il monitoraggio delle vulnerabilità è un altro aspetto chiave. Implementare il monitoraggio delle vulnerabilità informatiche consente di mantenere aggiornati i sistemi e di mitigare le CVE note. Si possono configurare notifiche su diversi canali, in modo da tenere sotto controllo la situazione in tutti i momenti.

La centralizzazione dei log è importante per migliorare la gestione degli incidenti. Configurare la raccolta centralizzata dei log e creare dashboard personalizzate per la visualizzazione dei dati permette di analizzare e correlare gli eventi di sicurezza in modo più efficace. Questo approccio non solo migliora la gestione degli incidenti, ma consente anche un'analisi approfondita dell'infrastruttura informatica, migliorando così la postura di sicurezza complessiva.

Un altro aspetto fondamentale è l'adattabilità e la scalabilità dei servizi SIEM.

Questi sistemi sono estremamente configurabili e possono essere adattati in base alla quantità di log da processare, mantenendo alte prestazioni. Ad esempio, per la gestione di grande quantità di dati possono essere configurati dei cluster in cui vengono implementati i nodi del sistema SIEM per aumentare le prestazioni di ogni componente.



Questo li rende ideali sia per piccole realtà aziendali che per grandi imprese con esigenze complesse.

Infine, l'implementazione di un SIEM facilita la conformità alle normative di sicurezza. La capacità di generare report dettagliati e di rispondere rapidamente agli incidenti di sicurezza è un vantaggio significativo.

Un SIEM ben implementato può integrarsi con altre soluzioni di sicurezza, come i sistemi di prevenzione ed intercettamento delle intrusioni (IPS/IDS), sistemi di Endpoint Detection and Responce (EDR) e i firewall di nuova generazione, creando un ecosistema di sicurezza robusto e integrato.

In conclusione, l'implementazione di un SIEM è un passo fondamentale per qualsiasi azienda che voglia proteggere i propri dati e garantire la continuità operativa. Non si tratta solo di rispondere agli incidenti, ma di prevenirli, creando un ambiente di lavoro più sicuro e resiliente.

"L'implementazione di un SIEM è un passo fondamentale per qualsiasi azienda che voglia proteggere i propri dati e garantire la continuità operativa".

Decadimento mentale
La tecnologia sta rovinando le nostre menti?

A cura di Massimiliano Brolli

Recentemente, questa espressione è diventata la parola dell'anno secondo la Oxford University Press. Questo termine si riferisce a "un sospetto deterioramento della condizione mentale o intellettuale associato al consumo eccessivo di materiali considerati minori o non stimolanti il pensiero".

Se la frase "decadimento mentale" veniva originariamente utilizzata per criticare il disinteresse verso idee complesse, oggi viene rievocata per esprimere un fenomeno che si manifesta quotidianamente nel consumo di contenuti digitali.

Ma di cosa si tratta?

L'uso del termine "decadimento mentale" è aumentato del 230% dal 2023 al 2024. Il primo uso documentato della frase risale al 1854, quando Henry David Thoreau, nel suo libro Walden, criticò la tendenza della società a svalutare idee complesse.

Benvenuti nell'era del Decadimento mentale

Nell'era dell'Intelligenza Artificiale generativa, dei social media e delle piattaforme di streaming, siamo circondati da contenuti facili e veloci. Questo ambiente favorisce la velocità e la semplicità, a discapito della riflessione profonda. Ciò che un tempo era visto come un rischio, oggi è diventato un problema concreto. Il dibattito sulla qualità del pensiero umano e sulla salute mentale è più vivo che mai.

Il termine "decadimento mentale" non si limita a descrivere la qualità del contenuto che consumiamo, ma allude anche alla nostra capacità di impegnarci con esso. La psicologia suggerisce che il nostro cervello è naturalmente incline a cercare gratificazione immediata, una tendenza che trova terreno fertile nelle forme brevi di contenuti digitali, come i video di TikTok o i post di Instagram. Questo tipo di stimolazione immediata può ridurre la nostra capacità di concentrarci per periodi prolungati, contribuendo a una "decadimento" della nostra attenzione e della nostra capacità di analizzare in profondità le informazioni.

Inoltre, il consumo di contenuti facilmente fruibili può ridurre l'inclinazione a sviluppare competenze cognitive complesse, come il pensiero critico e la riflessione profonda. In una società sempre più connessa, dominata dall'Intelligenza Artificiale, dove le informazioni si accumulano a ritmi vertiginosi, l'abilità di selezionare, filtrare e riflettere sulle informazioni diventa sempre più rara.

L'impatto della cultura digitale sulle generazioni Z e Alpha

Le generazioni più giovani sono particolarmente vulnerabili agli effetti del "decadimento mentale". Essendo cresciute in un ambiente dove la tecnologia permea ogni

aspetto della vita quotidiana, i ragazzi della Generazione Z e Alpha hanno un rapporto ambivalente con i media digitali. Da un lato, sono consapevoli dei pericoli legati al consumo passivo di contenuti, ma dall'altro, sono anche i maggiori consumatori di questi contenuti. Questo paradosso crea una frattura tra il desiderio di esplorare idee complesse e l'influenza delle piattaforme digitali che spesso promuovono una cultura del "clic veloce" e del "divertimento immediato".

Le discussioni sul "decadimento mentale" potrebbero rappresentare un campanello d'allarme per queste generazioni, portandole a riflettere sulle loro abitudini digitali e sull'impatto che queste hanno sul loro sviluppo cognitivo e sociale.

Ritorno alla qualità: Come contrastare il "decadimento mentale"

Per contrastare gli effetti negativi del "decadimento mentale", è fondamentale riscoprire l'importanza di contenuti che stimolino un pensiero più profondo e complesso. La promozione di letture più lunghe, la valorizzazione di contenuti educativi e la creazione di esperienze digitali che incoraggino l'interazione autentica, piuttosto che il consumo passivo, sono passi cruciali per invertire questa tendenza.

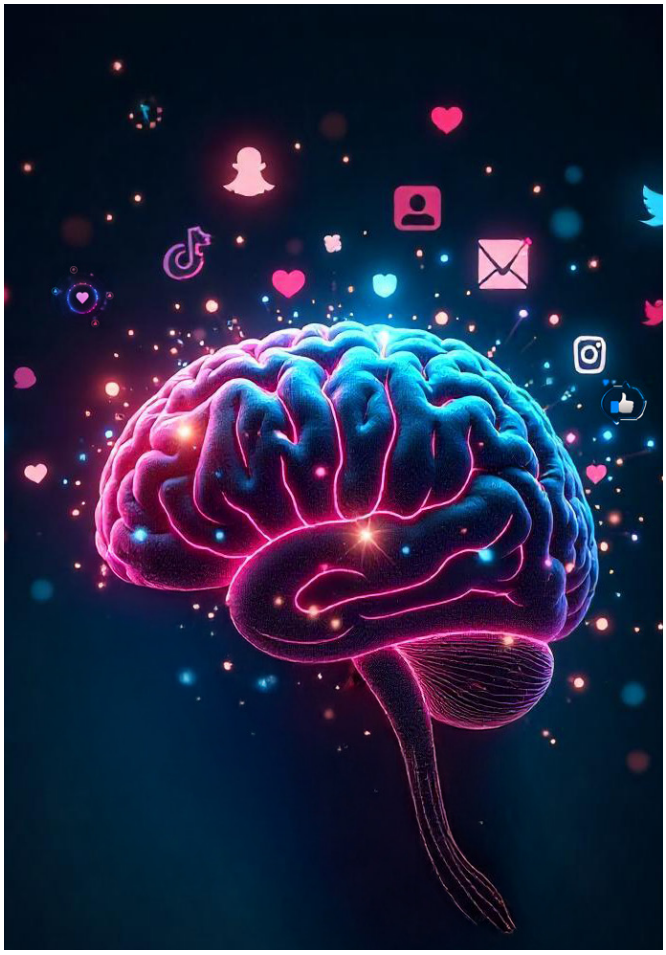
Inoltre, è essenziale educare le nuove generazioni alla consapevolezza digitale, insegnando loro a riconoscere e a districarsi tra contenuti di qualità e materiale superficiale. Solo così potremo mantenere un equilibrio tra il mondo virtuale e quello reale, favorendo la crescita intellettuale e il benessere mentale.

Conclusione

In definitiva, il "decadimento mentale" non è solo una riflessione sulla superficialità dei contenuti che consumiamo, ma una sfida culturale che invita ciascuno di noi a riflettere su come la tecnologia influisce sulla nostra vita quotidiana.

Se da un lato la tecnologia offre innumerevoli opportunità di apprendimento e connessione e facilità il lavoro quotidiano (vediamo ad esempio le AI Generative), dall'altro, richiede anche una maggiore consapevolezza e responsabilità nel suo utilizzo.

Le nuove generazioni, in particolare, devono trovare il giusto equilibrio che consenta loro di utilizzare il digitale in modo sano, con una mente attenta e critica, pronta ad affrontare le sfide del futuro, perché nel bene o nel male, ce ne saranno tante da affrontare.



Riflessioni sulla Figura del CISO: standardizzazione prima di tutto?

A cura di Paolo Cannistraro

Negli ultimi anni, il Chief Information Security Officer (CISO) è stato al centro di un acceso dibattito. Articoli e conferenze si susseguono per analizzare come questo ruolo si stia evolvendo, passando da una funzione prevalentemente tecnica a un partner strategico del business. Tuttavia, dietro l'apparente consenso sul futuro brillante del CISO, si nasconde una domanda fondamentale: come può evolversi un ruolo che, di fatto, non è nemmeno standardizzato?

L'assenza di una chiara collocazione aziendale del ruolo del CISO crea una serie di problemi strutturali. Da un lato, questa ambiguità può essere vista come una forza, permettendo al CISO di adattarsi alle necessità specifiche di ciascuna organizzazione e settore. Un CISO in un'azienda tecnologica avrà probabilmente responsabilità e obiettivi molto diversi rispetto a un CISO in una banca o in una struttura sanitaria. Questa flessibilità, però, rischia di trasformarsi in un punto debole quando si tratta di allineare una figura all'interno dell'organigramma aziendale.

Per esempio, non esiste un consenso universale su dove il CISO debba collocarsi all'interno dell'organigramma. Dovrebbe rispondere al Chief Information Officer (CIO), al CTO o, direttamente al consiglio di amministrazione (CEO)? Ogni opzione comporta implicazioni diverse in termini di priorità, indipendenza e accesso alle risorse. La mancanza di uno standard crea, inevitabilmente, differenze di approccio che possono rendere difficoltoso confrontare le performance e, soprattutto, promuovere una visione strategica unitaria.

Un altro elemento che mette in discussione l'evoluzione del ruolo del CISO è la varietà di competenze richieste. Oggi, al CISO si chiede di essere un esperto tecnico, un abile comunicatore, un negoziatore capace e, soprattutto, un leader strategico. Tuttavia, è difficile trovare tutte queste competenze in un unico individuo, soprattutto considerando che non esiste un percorso formativo standard per chi aspira a ricoprire questa posizione. Molti CISO provengono dal mondo IT, altri dal settore della sicurezza fisica o delle compliance, altri ancora da percorsi meno convenzionali. Questa eterogeneità di background può essere un arricchimento, ma, allo stesso tempo, alimenta la confusione su quali siano le reali priorità del ruolo.

Un punto cruciale da non trascurare è il ruolo della cultura aziendale. Anche con una definizione standardizzata del CISO, è la cultura di un'organizzazione che determina quanto questo ruolo sia veramente efficace. Se l'azienda non riconosce l'importanza della sicurezza come parte integrante del business, il CISO, indipendentemente dalle sue competenze o dalla sua posizione nell'organigramma, rischia di essere relegato a un ruolo marginale. La standardizzazione, quindi, dovrebbe andare di pari passo con uno sforzo educativo e culturale che promuova una maggiore consapevolezza dell'importanza della sicurezza informatica a tutti i livelli aziendali.

L'evoluzione del ruolo del CISO è inevitabilmente legata al panorama delle minacce informatiche. Con l'emergere di nuove tecnologie come l' Intelligenza Artificiale e l'aumento delle normative in materia di sicurezza e privacy, vedi la DORA e la NIS2, il CISO dovrà continuare a evolversi per stare al passo. La vera sfida sarà trovare un equilibrio tra standardizzazione e adattabilità, tra leadership strategica e competenza tecnica. Solo affrontando questi dilemmi, il CISO potrà realmente consolidarsi come una figura chiave per il futuro delle organizzazioni con responsabilità e competenze crescenti.

Il CISO: una figura multiforme

Come precedentemente accennato una delle principali problematiche che affligge il ruolo del CISO è la sua collocazione aziendale, che varia significativamente da un'organizzazione all'altra. In alcune aziende, il CISO risponde direttamente al Chief Information Officer (CIO), configurandosi come una figura subordinata alle strategie IT. In altre realtà, viene collocato sotto il Chief Technology Officer (CTO), con un focus più orientato agli aspetti tecnologici che non a quelli strategici o di governance. E ancora, esistono situazioni in cui il CISO dipende dal Chief Financial Officer (CFO), una scelta che riflette la crescente importanza della gestione dei rischi finanziari legati alla cybersecurity, oppure persino dal dipartimento delle Risorse Umane (HR), quando il tema della formazione e consapevolezza del personale viene considerato cruciale.

Questa frammentazione riflette la mancanza di un consenso condiviso sulla natura e sull'importanza del ruolo, creando di fatto un contesto disomogeneo. Mentre altre figure aziendali, come il CFO o il COO, hanno ottenuto nel tempo una collocazione chiara e universalmente riconosciuta, il CISO rimane una figura sfuggente, con responsabilità e aspettative che cambiano a seconda dell'organizzazione.

Questa mancanza di standardizzazione non è solo una questione accademica o formale, ma ha ripercussioni tangibili sulla capacità delle aziende di affrontare le sfide della sicurezza informatica. Un ruolo poco definito rende difficile costruire strategie efficaci, allocare risorse adeguate e, soprattutto, garantire che il CISO abbia il peso necessario per influenzare le decisioni strategiche dell'azienda.

L'importanza della standardizzazione

Prima di parlare di un'evoluzione del ruolo del CISO, è fondamentale affrontare la questione della standardizzazione. Come si può promuovere una trasformazione strategica se non esistono linee guida comuni sulla sua collocazione e sulle sue responsabilità? In un panorama in cui le minacce informatiche diventano sempre più sofisticate e pervasive, il rischio di lasciare questa figura in una posizione ambigua è troppo alto.

Uno degli strumenti che potrebbero favorire una standardizzazione è rappresentato dalle normative. In Europa, ad esempio, la direttiva NIS2 (Network and Information Security Directive) introduce obblighi precisi per le organizzazioni critiche, chiedendo loro di designare un responsabile per la sicurezza delle informazioni. Tuttavia, è lecito chiedersi se questa misura sia sufficiente. Sebbene la NIS2 rappresenti un passo avanti, il suo impatto dipenderà dalla capacità di tradurre i requisiti normativi in pratiche operative, che includano anche una collocazione chiara e strategica del CISO nell'organigramma aziendale.

La standardizzazione non è solo un tema normativo, ma una necessità per garantire chiarezza e coerenza all'interno delle aziende. Una collocazione uniforme del CISO consentirebbe di definire con precisione le sue responsabilità, di stabilire metriche comuni per valutare le performance e, soprattutto, di garantire che questa figura abbia un accesso diretto al top management. Solo così sarà possibile affrontare in modo sistematico le sfide sempre più complesse della sicurezza informatica.

"La standardizzazione non è solo un tema normativo, ma una necessità per garantire chiarezza e coerenza all'interno delle aziende".

I benefici di una posizione univoca

Garantire al CISO una collocazione uniforme e riconosciuta all'interno delle aziende è fondamentale per diverse ragioni:

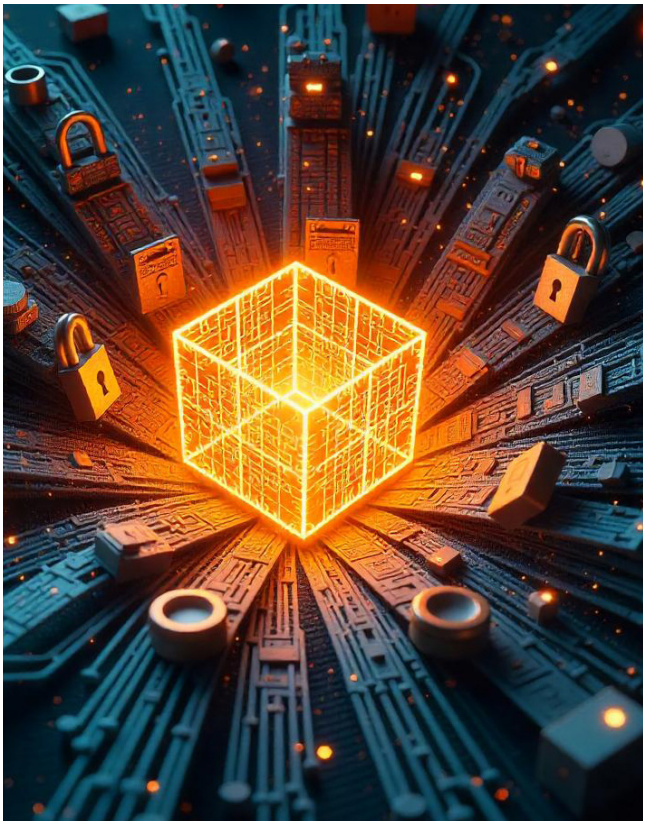
1. **Chiarezza nei processi decisionali:** una posizione chiara nell'organigramma evita conflitti di competenza e garantisce che il CISO abbia accesso diretto al top management con una posizione univoca nelle aziende. Questo è essenziale per integrare la cybersecurity nelle strategie aziendali, piuttosto che relegarla, a volte, in un ruolo puramente operativo.
2. **Responsabilità definite:** la standardizzazione permette di delineare responsabilità specifiche e misurabili, facilitando la valutazione delle performance e creando aspettative realistiche sul contributo del CISO al successo aziendale.
3. **Allineamento con il business:** un ruolo strategico consente al CISO di lavorare a stretto contatto con le altre funzioni aziendali, come il marketing, le vendite e le operation, per integrare la sicurezza nelle decisioni di business e contribuire all'innovazione.
4. **Miglioramento della consapevolezza:** una chiara collocazione del CISO favorisce anche una maggiore sensibilizzazione dell'intera azienda sul tema della sicurezza informatica, promuovendo una cultura aziendale in cui la cybersecurity è percepita come una responsabilità condivisa.

Il futuro del CISO: evoluzione e standardizzazione

Il dibattito sull'evoluzione del CISO è certamente importante, ma rischia di perdere di vista la vera priorità: la standardizzazione del ruolo. Senza una base comune su cui costruire, l'idea di un CISO strategico e partner del business rimane un obiettivo lontano. Prima di poter parlare di evoluzione, dobbiamo garantire che il CISO trovi finalmente una collocazione chiara e riconosciuta all'interno delle aziende.

Le normative, come NIS2 e DORA, possono rappresentare un punto di partenza, ma da sole non bastano. Sarà necessario un impegno collettivo da parte delle aziende, delle istituzioni e dei professionisti del settore per creare standard condivisi, che definiscano in modo univoco il ruolo del CISO. Solo allora potremo veramente parlare di evoluzione, trasformando il CISO in un leader strategico riconosciuto, capace di guidare le aziende verso un futuro più sicuro e resiliente.

CYBER
Think Tank
ASSINTEL



Assintel Cyber Hub

CYBER
Think Tank
ASSINTEL

Obiettivo:

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

Uniti per una sicurezza digitale senza confini!

Per info scrivi a:
segreteria@assintel.it

Cybersecurity e sanità

A cura di Corrado Giustozzi

In appena dieci anni dai primi attacchi specifici contro le strutture sanitarie, avvenuti negli Stati Uniti nel 2015, il settore healthcare è diventato uno dei bersagli preferiti da parte delle organizzazioni specializzate nel cybercrime.

Anche in Italia sono oramai un fenomeno quotidiano i casi di strutture sanitarie violate, con sistemi bloccati, servizi interrotti e dati dei pazienti esfiltrati. È evidente che attacchi del genere non comportano solo un danno economico diretto alla struttura colpita, ma hanno conseguenze importanti sulla privacy dei pazienti e soprattutto espongono al rischio la loro salute. Essi rappresentano dunque un vero e proprio pericolo sociale in quanto colpiscono i cittadini più fragili privandoli proprio dei servizi di assistenza sanitaria di cui hanno più necessità.

Solitamente queste azioni hanno finalità estorsive, con gli attaccanti che chiedono alla struttura vittima il pagamento di un riscatto per ripristinare il funzionamento dei sistemi bloccati oppure per non divulgare i dati sottratti. Ma all'estorsione generalmente segue comunque la rivendita dei dati a terzi, tipicamente dei ricettatori specializzati, quindi il danno è comunque elevato e duraturo.

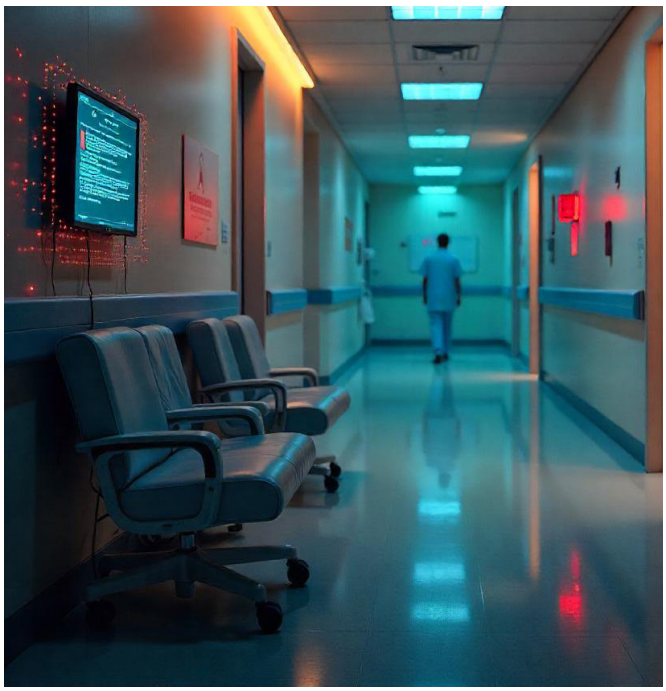
Tutti i settori di attività sono colpiti da attacchi del genere, ma la sanità purtroppo lo è in misura speciale: per la propria natura infatti le strutture sanitarie ne costituiscono la vittima perfetta, come i criminali sanno bene. Purtroppo si tratta di un crimine in forte crescita, perché è relativamente facile da compiere e garantisce un elevato livello di impunità a chi lo commette.

Sanità vulnerabile

Le cause per cui la sanità è diventata uno dei bersagli preferiti di questi attacchi particolarmente vili ed odiosi sono sostanzialmente tre.

La prima è l'impreparazione culturale del settore sanitario nei confronti del rischio specifico. A fronte di un fortissimo senso della safety, intesa come tutela della salute dei propri pazienti contro eventi di natura accidentale, vi è infatti assai meno sensibilità per gli aspetti di security, ossia della protezione contro azioni malevole condotte deliberatamente verso la struttura operante. Non di rado anzi, la security viene percepita come ostacolo all'operatività, e viene vissuta quindi con insofferenza o addirittura viene osteggiata. Questa scarsa sensibilità favorisce ovviamente gli attaccanti, i quali sanno di trovare le proprie vittime sostanzialmente indifese.

La seconda è la relativa arretratezza tecnologica che affligge il settore, non solo per l'endemica scarsità di risorse economiche ma anche per una storica scarsa sensibilità verso l'informatica. Questa infatti, salvo rare eccezioni, non viene considerata una funzione strategica ma un mero supporto tecnico all'operatività della struttura, e pertanto non riceve un adeguato livello di investimenti in tecnologie e in personale. Di conseguenza il parco dei sistemi informatici delle organizzazioni sanitarie è spesso tecnologicamente obsoleto, oltre che architetturalmente strutturato nel modo più semplice e basilare possibile per poter essere gestito da personale numericamente scarso e non particolarmente specializzato. Tutto ciò va ovviamente a scapito della sicurezza informatica, perché nelle infrastrutture gestite al minimo livello di presidio è inevitabile che si annidino vulnerabilità tecniche ed architetturali che costituiscono punti privilegiati di attacco per i criminali.



La terza riguarda i valori in gioco. Contrariamente infatti a quanto accade negli altri settori produttivi, dove ciò che viene messo a repentaglio da un attacco è il profitto o il business aziendale, nel caso della sanità ciò che è a rischio è la salute dei pazienti ricoverati o assistiti, la quale ovviamente ha un valore incommensurabile. I criminali lo sanno bene, ed è infatti questo il principale fattore di pressione su cui fanno leva: le loro vittime hanno tantissimo da perdere, e saranno quindi più disposte a cedere all'odioso ricatto.

"Le strutture sanitarie sono tra i soggetti più a rischio, proprio a causa delle loro peculiarità che le rende particolarmente vulnerabili".

Cosa fare

Per contrastare il fenomeno è soprattutto necessario operare un cambio di passo culturale nel settore. Va innanzitutto compreso che la cybersecurity non è un tema che riguarda solo le aziende di tecnologie: oggigiorno ogni organizzazione che faccia uso di reti e computer nella sua operatività quotidiana è a rischio, soprattutto se non ne padroneggia completamente gli aspetti tecnici. Tutti sono attaccati, e chi è meno preparato subirà i danni maggiori.

In secondo luogo bisogna rendersi conto che un attacco informatico non è, come purtroppo molti pensano, un'azione dilettantesca condotta da qualche ragazzino asociale e un po' autistico ma in fondo non cattivo, come invece l'immaginario collettivo delle serie TV e dei film americani dipinge i fantomatici "hacker". I reali autori sono criminali professionisti, freddi e spietati, che operano tramite strutture transnazionali ben organizzate e dotate di ingenti mezzi e risorse. Tuttavia non bisogna neppure mitizzare o sopravvalutare le loro capacità, che non sono straordinarie: la maggiore abilità degli attaccanti è quella di saper scegliere bene le proprie vittime, individuandole fra i soggetti più deboli e indifesi in modo da massimizzare le proprie probabilità di successo. Così se un attacco va a buon fine la colpa è di solito della sciatteria dell'attaccato, il quale non si è difeso abbastanza o addirittura non si è difeso affatto.

Al giorno d'oggi le strutture sanitarie sono tra i soggetti più a rischio, proprio a causa delle loro peculiarità che le rende particolarmente vulnerabili. Prevenire e respingere gli attacchi cui vanno soggette è un'esigenza sociale, ma la risposta non può giungere esclusivamente dall'esterno del settore: ogni organizzazione in ambito deve fare la sua parte per innalzare la propria resilienza, anche se in un'ottica di collaborazione sistemica fra tutti i portatori di interessi.

Ciò significa in primo luogo che tutto il personale operante nella sanità deve sviluppare una corretta sensibilità al problema; ma significa anche che le alte direzioni delle strutture devono convincersi della necessità irrinunciabile di dedicare maggiori fondi e risorse al rafforzamento delle tecnologie, alla formazione del personale e all'istituzione di adeguati processi di resilienza. Il percorso è certamente lungo, complesso ed oneroso: le normative internazionali, non ultima la Direttiva NIS2 in corso di attuazione, stanno però illuminando la via. Ai singoli operatori sta seguirlo al più presto e con attenzione.

L’intelligenza artificiale e il futuro dell’umanità: tra manipolazione, controllo e la sfida per preservare il pensiero critico

A cura di Ettore Guarnaccia

Al World Economic Forum 2025 gli esperti hanno lanciato un allarme: disuguaglianza sociale, polarizzazione del pensiero, mancanza di opportunità economiche ed erosione di diritti fondamentali e libertà sono tra le minacce più gravi per il futuro dell’umanità. Un fattore determinante lega questi aspetti: la manipolazione dell’informazione. Il WEF ha evidenziato come la diffusione di “misinformazione” (informazioni errate ma non intenzionali) e “disinformazione” (notizie false diffuse deliberatamente) stia alimentando instabilità e divisione sociale, censura e sorveglianza di massa, operazioni di propaganda ideologica, spionaggio e guerra sul piano cibernetico. Questi fenomeni sono accomunati dall’intelligenza artificiale, sempre più integrata in ogni aspetto della società moderna.

L’IA generativa sta trasformando il mondo a una velocità impressionante, cambiando come lavoriamo, apprendiamo e ci informiamo. Moltissimi compiti quotidiani e lavorativi vengono già svolti dall’IA, che si sta rivelando decisiva nel migliorare molti settori, dalla medicina ai processi industriali. Anche il modo di accedere alle informazioni è mutato radicalmente: sempre più persone preferiscono chiedere all’IA anziché utilizzare motori di ricerca tradizionali. Questo crea una crescente dipendenza da risposte univoche e preconfezionate, e il progressivo azzeramento della capacità di analisi e confronto.

L’IA sta anche minando il pensiero critico. L’accesso all’informazione è filtrato e controllato, con poche realtà editoriali a dominare i media. Quelle italiane sono in mano a pochi gruppi con forti legami economici, finanziari e politici, a scapito di pluralità e obiettività dell’informazione. Non è un caso se l’Italia è scesa al 46° posto nella classifica globale della libertà di stampa dopo Fiji e Tonga, mentre la principale fonte di influenza mediatica, gli Stati Uniti, è al 55°. Meta e Google hanno annunciato la chiusura dei programmi di fact-checking per Facebook, Instagram e YouTube, seguendo l’esempio di X e ammettendo di aver impedito la libera informazione su temi economici, sanitari e politici a causa dell’eccessiva censura.

Un motore di ricerca induce a visitare diverse fonti e analizzarne i contenuti, scartando elementi falsi o sospetti, e correlando ciò che appare fondato, per formulare un pensiero, un’idea o una teoria. L’IA non presenta alternative di pensiero, ma un’unica risposta, impedendo valutazione e analisi critica, e incoraggiando una pericolosa uniformità ideologica che riflette inevitabilmente filosofie, dogmi e pregiudizi derivanti dalle sue fonti e dall’addestramento. Le ripercussioni sono evidenti: le nuove generazioni non sviluppano capacità linguistiche e logico-matematiche, e cresce il tasso di analfabetismo funzionale. Le prove INVALSI nelle scuole sono impietose: solo un diplomato su due raggiunge il livello minimo in italiano e matematica. Il dilagare di deepfake rende indistinguibili realtà e finzione: immagini, video e audio manipolati vengono diffusi per finalità ludiche o per inganno, con il risultato di distorcere la percezione pubblica e generare un sentimento comune di sfiducia.

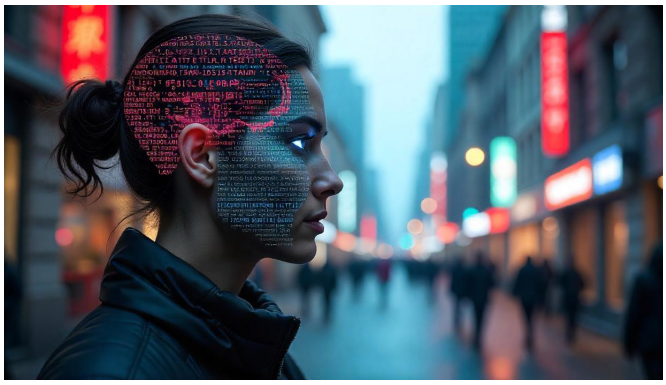
Inoltre, l'IA attinge da fonti sempre più contaminate da testi e immagini prodotti da forme di intelligenza artificiale, quindi non più espressione di creatività e conoscenza umane, diventando autoreferenziale. Un circolo vizioso che rischia di eliminare ogni forma genuina di pensiero, cultura e arte.

Un altro problema fondamentale è la fallibilità dell'IA. I suoi modelli si basano su algoritmi matematici che non garantiscono certezze: a differenza di un umano, l'IA non conosce la risposta esatta, ma calcola quella probabilmente più vicina a quella esatta sulla base delle logiche interne, delle fonti e dell'addestramento ricevuto. Questo la rende vulnerabile a errori, allucinazioni e manipolazioni. Gli utenti esperti possono riconoscere queste distorsioni, ma la maggior parte delle persone assume le risposte come verità assolute. Inoltre, essendo sempre basati su hardware e software, i sistemi IA sono esposti a cyberattacchi e violazioni. Se non adeguatamente protetto, il prompt di un'IA può essere manipolato per indurre comportamenti indesiderati, e, a causa della struttura complessa delle reti neurali, il risultato delle elaborazioni è quasi sempre imprevedibile.

Non è possibile addestrare un'IA per tutte le possibili casistiche o situazioni che dovrà gestire, quindi, non è possibile prevedere quale comportamento adotterà in situazioni complesse e sconosciute. Cosa potrebbe succedere con dispositivi sanitari chirurgici, macchinari industriali o mezzi di trasporto autonomi in situazioni impreviste in cui è in gioco la vita umana? Sistemi di sorveglianza e armamenti autonomi si stanno rivelando inaffidabili, con algoritmi che identificano erroneamente individui innocenti come minacce. Negli Stati Uniti le auto a guida autonoma stanno dimostrando i loro limiti: causano ingorghi, prendono direzioni errate, si bloccano tenendo in ostaggio i passeggeri, non riescono a gestire situazioni complesse e non riconoscono ostacoli, causando incidenti anche gravi. Ma gli utenti appaiono così inconsapevoli dei rischi che corrono da affidare la loro vita all'IA, guardando un film, interagendo con il cellulare, indossando un visore VR o addirittura dormendo mentre il pilota automatico conduce l'auto su strade molto trafficate. E in caso di errori o incidenti di chi è la responsabilità? Mancano basi giuridiche in materia.

Tuttavia, la minaccia più grave dal punto di vista sociale è l'accumulazione di un potere smisurato da parte delle Big Tech, mentre i governi faticano a comprendere e regolamentare la tecnologia. Queste aziende possiedono e controllano i dati di miliardi di persone, gestiscono infrastrutture tecnologiche che consumano e producono emissioni al pari di intere nazioni, indirizzano le strategie politiche e stanno ridefinendo il concetto stesso di potere. Come è già successo per social media, dispositivi digitali e videogiochi, sono i pentiti di Silicon Valley a metterci in guardia: i premi Nobel per la fisica John J. Hopfield e Geoffrey Hinton, pionieri delle reti neurali, Mustafa Suleyman, creatore di Deepmind ed ex Google, o Federico Faggin, inventore di microprocessore e touchscreen, che ha lavorato per 38 anni sulle reti neurali. La transizione è iniziata, Amazon sta sostituendo i lavoratori con robot basati su IA, nascono biglietterie con IA, Hollywood sta esplorando la creazione di film e sceneggiature generate interamente da intelligenza artificiale sfruttando il volto degli attori, e gli influencer vengono rimpiazzati da versioni digitali ottimizzate per massimizzare l'engagement e complete di profilo Onlyfans.

L'AI Act europeo, che entrerà in vigore il 2 febbraio, non è sufficiente a contrastare l'espansione incontrollata dell'IA e le sue conseguenze sul tessuto sociale. Se non si agirà subito, la tecnologia potrebbe pervadere ogni aspetto della nostra vita, influenzando non solo



il lavoro e l'economia, ma anche il modo in cui pensiamo, comunichiamo e percepiamo il mondo e la realtà che ci circonda. Il rischio più grande è che l'intelligenza artificiale, anziché essere uno strumento al servizio dell'uomo, diventi il mezzo attraverso il quale pochi soggetti potranno esercitare un controllo assoluto sulle masse.

Non sottovalutiamo il problema, l'IA generativa è solo una prima forma di intelligenza artificiale, ben altre molto più potenti sono in arrivo e apriranno la strada ad altre tecnologie invasive, dalla robotica alle interfacce cervello-macchina, dal quantum computing al metaverso. Quello che stiamo vivendo non è un semplice progresso tecnologico, ma un cambiamento epocale che minaccia di ridefinire l'essenza stessa dell'essere umano. Dobbiamo decidere se permettere alla tecnologia di governare la nostra vita o se riprendere il controllo prima che sia troppo tardi. È fondamentale favorire, soprattutto nei giovani, lo sviluppo del pensiero critico e delle competenze funzionali necessarie a difendersi dalla falsa informazione e dalla manipolazione della realtà. Non è un problema di natura tecnica, ma di coscienza.

"La manipolazione dell'informazione è il fattore determinante che alimenta instabilità, censura e guerra cibernetica".

L’Intelligenza Artificiale e la Geopolitica: un nuovo paradigma di potere

A cura di Pierluigi Paganini

L’intelligenza artificiale (IA) sta rapidamente trasformando il panorama geopolitico globale, influenzando inevitabilmente le relazioni tra stati. Ci si confronta con una tecnologia emergente, distruttiva, uno strumento di potere che ha il potenziale di alterare gli equilibri esistenti. È cruciale comprendere come gli stati si stiano adattando a questa nuova realtà, in bilico tra opportunità e minacce emergenti.

L’IA è di fatto terreno di confronto geopolitico, con paesi come Stati Uniti e Cina in prima linea nella corsa alla supremazia tecnologica. Assistiamo ad una corsa senza precedenti ed investimenti economici senza pari, la competizione non è una mera questione tecnologica, bensì una delicata questione di sicurezza nazionale e influenza globale.

Si aprono quindi accesi dibattiti sulla sostenibilità energetica di questi sistemi, sulla disponibilità di terre rare per l’estrazione di materiali fondamentali dell’innovazione tecnologica, sul controllo delle filiere per la produzione dei semiconduttori, e soprattutto sull’accesso ai dati.

Questa rivoluzione sta avvenendo sotto gli occhi degli ignari cittadini, che poco comprendono di quanto stia realmente accadendo e che non sono in grado di esprimere un giudizio oggettivo su tematiche complesse che inevitabilmente influenzeranno l’evoluzione dell’uomo sulla terra e nello spazio nei prossimi anni.

Stati Uniti e Cina in primis, stanno cercando di ottenere un vantaggio strategico attraverso l’innovazione tecnologica e il controllo delle risorse critiche necessarie per alimentare l’intelligenza artificiale.

Il governo cinese ha annunciato l’obiettivo di diventare leader mondiale nell’intelligenza artificiale (IA) entro il 2030. Nel 2017, la Cina ha pubblicato un piano strategico chiamato “New Generation Artificial Intelligence Development Plan”, che stabilisce obiettivi specifici per lo sviluppo dell’IA in vari settori, tra cui la sicurezza, l’industria, la sanità e l’automazione.

Si tratta di un piano ambizioso che vuole qualificare la Cina come eccellenza in ambito IA, nel panorama globale entro il 2030, con una forte caratterizzazione sulla ricerca, l’innovazione e lo sviluppo tecnologico.

Gli Stati Uniti d’altro canto dispongono di un ecosistema tecnologico avanzato, con aziende private come Microsoft, OpenAI, Google, e Meta che sostengono l’innovazione del sistema paese.

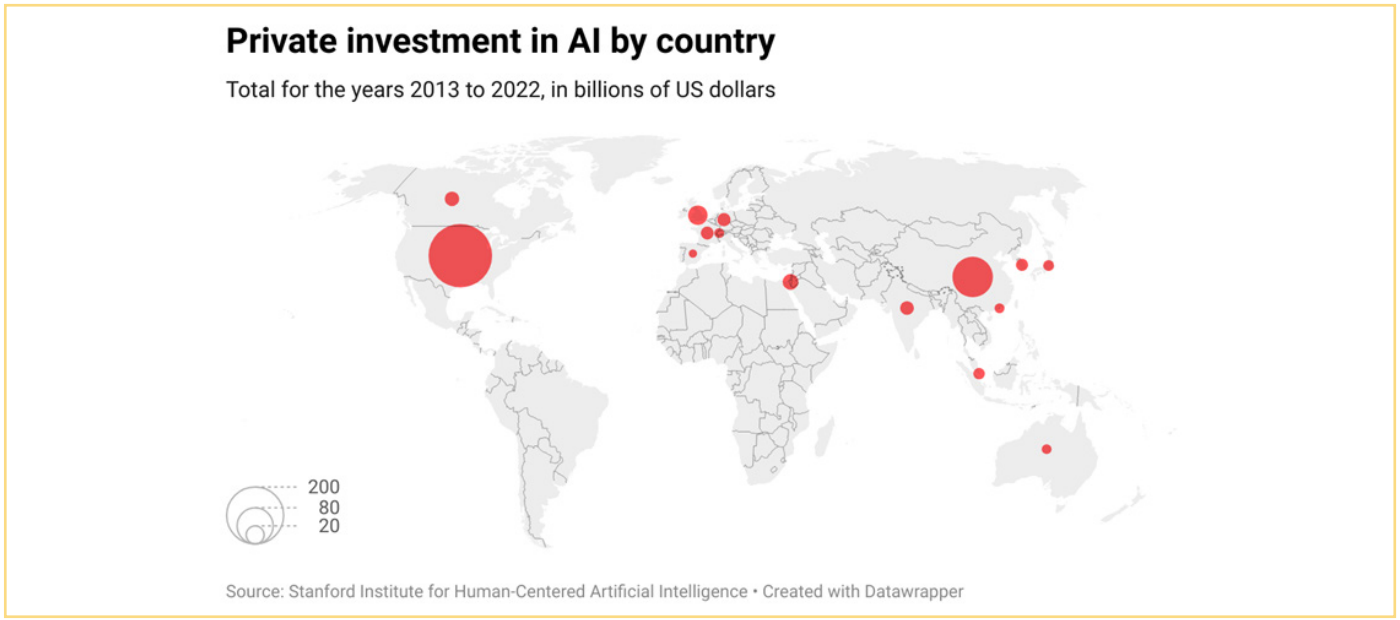


Figura 3 - Source: World Economic Forum

Gli approcci dei due paesi sono profondamente diversi in quanto la Cina ha adottato un approccio centralizzato, demandando lo sviluppo del settore direttamente al governo.

Si stima che l'investimento nell'IA da parte della Cina abbia raggiunto i 14,75 miliardi di dollari nel 2023. Il governo cinese ha istituito fondi statali per sostenere aziende ad alto potenziale e promuovere l'innovazione in tutto il paese. Pechino ha risposto alle restrizioni all'esportazione di semiconduttori verso la Cina con investimenti massicci nella raccolta di dati attraverso piattaforme digitali e nell'espansione della sua capacità produttiva di chip.

Negli Stati Uniti, gli investimenti nell'IA provengono principalmente dal settore privato. Sebbene le aziende tecnologiche stiano investendo miliardi nello sviluppo dell'IA, la mancanza di una strategia coordinata a livello nazionale può portare a disuguaglianze nella distribuzione delle risorse e nella formazione dei talenti.

"La governance dell'IA sarà cruciale per un uso sicuro e responsabile, e la cooperazione internazionale tra stati e settori sarà essenziale per affrontare le sfide".

Nel 2024, le startup americane di IA hanno raccolto circa 131,5 miliardi di dollari a livello globale, di cui 97 miliardi (circa il 74%) sono stati investiti negli Stati Uniti. Si stima un incremento del 52% rispetto all'anno precedente, evidenziando il crescente interesse degli investitori per le tecnologie emergenti legate all'IA. Queste cifre rappresentano un monito per l'Europa, che ha raccolto appena 14 miliardi di euro nello stesso periodo.

Altro elemento caratterizzante dell'ecosistema americano è la capacità di attrarre talenti da tutto il mondo grazie alle principali aziende tecnologiche e alle prestigiose università del paese.

In questo contesto così sfidante l'Unione Europea sta assumendo un ruolo cruciale candidandosi come leader globale nella regolamentazione e nello sviluppo di tecnologie IA affidabili e sicure. Tuttavia, la principale sfida per paesi europei è colmare il divario tecnologico rispetto ad altre potenze, come gli Stati Uniti e la Cina.

La Commissione Europea ha avviato diverse iniziative strategiche con l'obiettivo è di creare un ecosistema di IA di eccellenza.

Nel suo discorso sullo stato dell'Unione del 2023, la presidente della Commissione Europea, Ursula von der Leyen, ha sottolineato l'importanza di garantire che l'IA sia al servizio dell'umanità. Per questo motivo, è stato istituito un Ufficio per l'IA per consentire lo "sviluppo, la diffusione e l'uso futuri dell'IA in modo da promuovere i benefici sociali ed economici e l'innovazione, attenuando nel contempo i rischi." L'Ufficio si occupa dell'attuazione della legge sull'IA, in particolare in relazione ai modelli di IA di uso generale. Compito dell'ufficio è la promozione della ricerca e l'innovazione in un'IA affidabile e il posizionamento dell'UE come leader nelle discussioni internazionali.

Le azioni intraprese a livello europeo per colmare il gap con le altre super potenze sono:

- **Investimenti:** L'UE punta a investire 20 miliardi di euro l'anno in IA e a potenziare il calcolo ad alte prestazioni per favorire lo sviluppo di applicazioni avanzate.
- **Regolamentazione:** Il Regolamento IA dell'UE, in vigore dal 1° agosto 2024, stabilisce un quadro normativo basato sul rischio per garantire sicurezza e rispetto dei diritti fondamentali.
- **Formazione e Sviluppo delle Competenze:** L'UE investe nella formazione in IA, colmando lacune di talento e infrastrutture con programmi educativi per preparare i cittadini alle nuove opportunità.
- **Cooperazione Internazionale:** L'UE punta ad alleanze internazionali per affrontare le sfide dell'IA, collaborando su ricerca, sviluppo e governance a livello globale.

Rispetto agli Stati Uniti, dove il settore privato è trainato da investimenti massicci da parte di aziende come Google, Microsoft, Meta e Amazon, la mancanza di una strategia centralizzata in Europa ha portato a un approccio più frammentato. Ad oggi mancano ancora fondi idonei allo sviluppo dell'ecosistema AI europeo e sebbene siano molte le iniziative, i paesi europei non riescono ad

attirare investimenti che possano sostenere una crescita comparabile a quella di Stati Uniti e Cina.

L'analisi del contesto geopolitico non può prescindere dal constatare la concentrazione del potere economico nelle mani delle principali aziende tecnologiche mondiali che ad oggi dominano lo sviluppo dell'IA. La concentrazione del potere economico solleva non poche preoccupazioni su disuguaglianze crescenti sia all'interno dei paesi sia tra diverse regioni del mondo.

Aziende come Microsoft, Google e Facebook hanno accumulato enormi quantità di dati sugli utenti, linfa vitale per lo sviluppo di modelli di IA che possono influenzare comportamenti e decisioni a livello globale.

In un contesto internazionale, i paesi in via di sviluppo corrono il rischio di rimanere esclusi dai benefici dell'intelligenza artificiale a causa della carenza di infrastrutture tecnologiche adeguate e di competenze specializzate. Questa disuguaglianza sta inevitabilmente acutizzando il divario economico tra il Nord e il Sud del mondo, con le nazioni più povere incapaci di sfruttare le potenzialità dell'IA per la crescita economica e il miglioramento sociale. Inoltre, le potenze tecnologiche avanzate potrebbero approfittare dei dati raccolti da questi paesi senza che ne derivino benefici tangibili per le loro comunità.

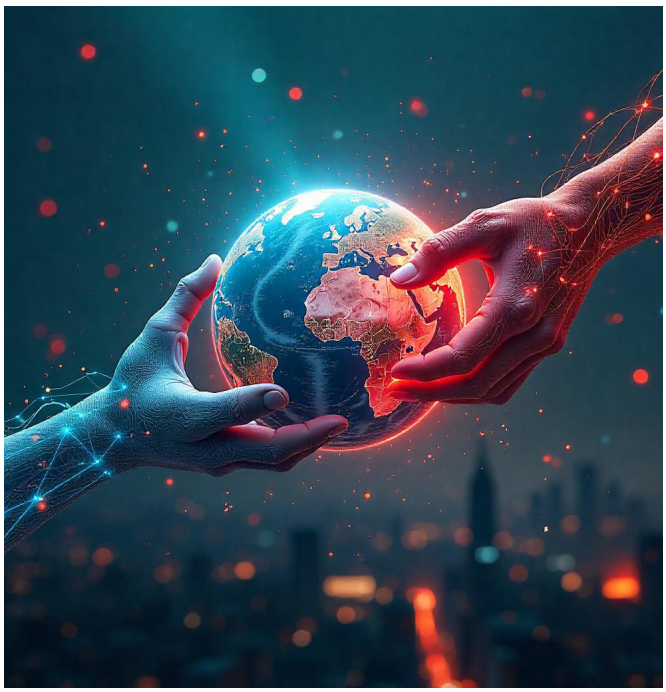
Il rischio di fenomeni di "colonizzazione digitale" è reale, le nazioni meno sviluppate si troveranno inevitabilmente in una posizione di dipendenza.

L'adozione di sistemi basati sull' IA ha poi implicazioni etiche e sociali che possono essere affrontate solo attraverso l'adozione di schemi di collaborazione internazionale.

I paesi coinvolti nella corsa all'IA, come Cina e Stati Uniti, si trovano ad affrontare sfide complesse legate all'uso responsabile di questa tecnologia. Uno dei problemi principali è relativo al bias nei modelli di IA, che possono perpetuare o amplificare pregiudizi esistenti se addestrati su dati distorti.

Un'altra questione centrale è quella della privacy dei dati. L'enorme quantità di dati personali utilizzata dai sistemi di IA rappresenta una crescente minaccia alla privacy individuale. La principale sfida per ogni governo è trovare un equilibrio tra il progresso tecnologico e la protezione dei diritti fondamentali dei cittadini. Infine, l'autonomia decisionale delle macchine introduce interrogativi complessi sulla responsabilità morale e legale in caso di errori o incidenti causati da sistemi automatizzati, aprendo nuove riflessioni sul rapporto tra uomo e tecnologia.

Concludendo, l'intelligenza artificiale sta ridefinendo le dinamiche geopolitiche globali, richiedendo ai paesi di investire nelle proprie capacità tecnologiche e sviluppare strategie a lungo termine. La governance dell'IA sarà cruciale per un uso sicuro e responsabile, e la cooperazione internazionale tra stati e settori sarà essenziale per affrontare le sfide. È fondamentale garantire un accesso equo ai benefici dell'IA e affrontare le disuguaglianze globali. In un contesto di crescente competizione tra Stati Uniti e Cina, si potrebbe assistere ad una "guerra fredda tecnologica", con conseguente aumento di sanzioni e dazi e la nascita di nuove alleanze strategiche tra stati.



CYBER
Think Tank
ASSINTEL

Cybersecurity Trends da monitorare nel 2025

A cura di Sofia Scozzari

Il panorama della cybersecurity continua ad evolvere ad un ritmo senza precedenti, guidato dai progressi tecnologici e dall'aumento della sofisticazione delle minacce informatiche.

Nel 2024 sono stati rilevati 8.302 cyber attacchi di successo e di pubblico dominio a livello globale, con un aumento del 17% rispetto all'anno precedente.

La quasi totalità delle minacce (92%) è di origine cybercriminale, spesso facilitate da strumenti consolidati come il ransomware, mentre, tra i settori più colpiti, il Manufacturing si conferma al primo posto, sia a livello globale (15% degli attacchi totali) che nazionale (17% degli incidenti italiani).

Inoltre, dato ben peggiore, 9 attacchi su 10 hanno impatti gravi o gravissimi, delineando uno scenario sempre più preoccupante.

Per proteggere efficacemente il proprio business, in particolare nel caso di piccole e medie aziende, è quindi prioritario riconoscere ed indirizzare correttamente le più importanti tendenze della cybersecurity nel 2025.

Principali Cybersecurity Trends per il 2025

1. Attacchi Basati sull'Intelligenza Artificiale

L'intelligenza artificiale svolge ormai un duplice ruolo nella cybersecurity, sia come alleato dei difensori, che come arma degli attaccanti. I criminali informatici stanno infatti sfruttando ampiamente l'IA per creare attacchi complessi. Ad esempio, l'IA può generare e-mail di phishing altamente personalizzate e pressoché indistinguibili da comunicazioni legittime, aumentando significativamente il tasso di successo degli attacchi.

Il risultato dello sfruttamento malevolo di questi nuovi strumenti tecnologici è una democratizzazione del crimine informatico, che permette anche a soggetti con competenze tecniche limitate di condurre attacchi su larga scala, superando persino le barriere linguistiche.

Per contrastare questa minaccia, le aziende devono investire in soluzioni di sicurezza basate sull'IA, in grado di rilevare anomalie ed identificare minacce in tempo reale, senza però sottostimare l'importanza della formazione del personale, fondamentale per ridurre il rischio di attacchi mirati come il phishing.

2. Quantum Computing

Il quantum computing rappresenta un enorme potenziale per le aziende, soprattutto grazie alla possibilità di ottimizzare processi complessi e supportare tecnologie come Intelligenza Artificiale e Machine Learning.

Ma, al tempo stesso, uno dei principali svantaggi del quantum computing in ambito cybersecurity è il rischio che le attuali soluzioni crittografiche diventino obsolete, compromettendo la riservatezza dei dati, in particolare quella di dati sensibili.

È necessario essere consapevoli e preparati per questa problematica, valutando alternative per la protezione dei dati e pianificando la migrazione a tecnologie di crittografia quantum-resistant prima che il rischio diventi concreto.

3. Ransomware Multisfaccettati

Il ransomware continua a essere una minaccia significativa, grazie a strategie di estorsione consolidate e sempre più sofisticate. Gli attaccanti non si limitano più a cifrare i sistemi delle vittime rendendoli inoperativi, ma minacciano anche di esporre informazioni sensibili, dopo averle sottratte nel corso dell'attacco, per aumentare la pressione sulle vittime, con una tecnica chiamata double extortion.

Non a caso nel 2024 il ransomware è la tecnica più utilizzata dai cybercriminali, sfruttata nel 64% degli attacchi globali e nel 38% di quelli italiani.

La double extortion è così efficace che alcuni gruppi ransomware hanno iniziato a condurre attacchi senza più cifrare i sistemi, limitandosi a sottrarre i dati per chiedere il riscatto.

Per mitigare questo rischio, le aziende non possono più fare affidamento esclusivamente su soluzioni di backup, ma devono necessariamente implementare strategie preventive come l'identificazione e la mitigazione delle vulnerabilità dei sistemi informatici. Inoltre è utile sviluppare piani dettagliati di risposta agli incidenti per identificare, contenere e recuperare rapidamente in seguito ad un attacco informatico.

4. Insider Threat

L'insider threat è spesso trascurata nella cybersecurity, poiché l'attenzione tende a focalizzarsi sulle minacce esterne, sottovalutando i rischi derivanti da dipendenti o collaboratori.

La sicurezza di un'azienda può invece essere compromessa, non solo a causa di operazioni malevole da parte di cybercriminali, ma anche per negligenza, errore o intenzione dolosa.

Per prevenire questi rischi, le aziende dovrebbero sensibilizzare il personale con programmi di formazione ad hoc di cybersecurity awareness, oltre che implementare controlli di accesso rigorosi e monitorare le attività sospette anche all'interno della rete.

Creare una cultura della cybersecurity in cui i collaboratori siano consapevoli delle minacce, sia interne che esterne, può ridurre notevolmente il rischio di incidenti.

5. Attacchi alla Supply Chain

Le supply chain sono fondamentali per il corretto funzionamento del business, ma, d'altra parte, nella cybersecurity rappresentano anche una vulnerabilità significativa.

I criminali informatici possono, infatti, compromettere fornitori e terze parti per ottenere accesso a più vittime contemporaneamente, causando gravi problematiche e disservizi che possono essere difficili da prevenire.

Per proteggere le proprie infrastrutture, le aziende dovrebbero valutare attentamente la sicurezza dei loro fornitori e pretendere standard di protezione più elevati.

6. Cyber Resilience

Per quanto rigorose ed avanzate possano essere le strategie di difesa, non tutti gli attacchi possono essere evitati.

Per un'azienda, soprattutto una PMI, investire nel miglioramento della propria resilienza, ovvero la capacità di riprendersi rapidamente da un incidente e di adattarsi continuamente alle nuove minacce, è un elemento chiave per rafforzare la propria sicurezza informatica.

Per potenziare la cyber resilience, le aziende dovrebbero sviluppare piani di risposta agli incidenti ben strutturati e testarli regolarmente. Inoltre, è fondamentale informare dipendenti e collaboratori sulle minacce attuali e sulle policy aziendali, coinvolgendoli attivamente nelle tematiche di cybersecurity. Questo approccio consente al personale di comprendere il valore della protezione degli asset aziendali, migliorando la capacità di risposta dell'azienda e riducendo il rischio di attacchi.

Conclusione

I cybersecurity trends per il 2025 evidenziano l'importanza di adottare un approccio proattivo anziché reattivo, un aspetto particolarmente rilevante per piccole e medie imprese e professionisti.

Le realtà di dimensioni ridotte, infatti, spesso non dispongono delle risorse necessarie per riprendersi rapidamente da un attacco, esponendosi al rischio di danni irreversibili. Per questo motivo, è fondamentale concentrarsi sulla prevenzione e sulla corretta valutazione dei rischi cyber per poter implementare misure difensive adeguate.

Comprendere l'evoluzione del panorama delle minacce ed investire in soluzioni mirate, sia per ridurre l'esposizione ai rischi che per aumentare la resilienza, consente alle aziende non solo di proteggere i propri asset in modo più efficace, ma anche di distinguersi come realtà affidabili, rafforzando il proprio valore competitivo.

CYBER Think Tank ASSINTEL

Cyber Think Tank Assintel

Cyber per tutti

Istruzioni semplici per questioni complesse!

Video pillole

Podcast

Infografiche

Fumetti

Check list

Per info scrivi a:
segreteria@assintel.it

Botnet: la minaccia silenziosa che sta alimentando il crimine

A cura di Francesco Iezzi

Negli ultimi anni la quantità di attacchi informatici a cui siamo esposti ha avuto un netto incremento. Uno dei maggiori timori che affliggono esperti e aziende di tutto il mondo riguarda proprio la diffusione delle botnet nell'ambiente digitale. Ma cosa sono le botnet e perché rappresentano una minaccia? Per dare una risposta a queste domande, basta prendere spunto dall'attacco subito recentemente da DeepSeek, una start-up cinese specializzata in intelligenza artificiale e machine learning.

Cos'è una botnet?

Immaginate una rete composta dai vostri PC, smartphone e altri dispositivi elettronici che usate quotidianamente. Questi dispositivi, apparentemente innocui, possono essere infettati da malware che li trasforma in "zombie", dispositivi controllati a distanza tramite server di comando e controllo (C&C). In poche parole, le botnet consentono agli hacker di inviare comandi a questi dispositivi per eseguire attacchi informatici su larga scala, come i noti attacchi DDoS (Distributed Denial-of-Service). Questi attacchi consistono nell'inviare un'enorme quantità di richieste a un server, sovraccaricandolo e impedendogli di svolgere le normali operazioni, rendendo impossibile fornire servizi agli utenti.

L'evoluzione degli attacchi e il caso DeepSeek

DeepSeek, start-up nota per il suo ingresso nel settore e per il lancio di modelli avanzati di intelligenza artificiale e machine learning, è diventata un bersaglio privilegiato per i nuovi metodi di attacco adottati dai cybercriminali. Sin dal mese di gennaio, l'azienda è stata soggetta ad attacchi DDoS. Inizialmente, si trattava di attacchi informatici che sfruttavano meccanismi relativamente semplici, come l'amplificazione tramite SSDP (Simple Service Discovery Protocol) e NTP (Network Time Protocol). Tuttavia, ben presto è diventato chiaro che il pericolo avrebbe assunto toni fin troppo minacciosi per essere ignorato.

Nelle ultime ore di giovedì, DeepSeek ha subito attacchi devastanti: l'unità cinese per la cybersecurity, XLab, ha identificato due botnet, HailBot e RapperBot – entrambe varianti della ben nota famiglia Mirai – hanno lanciato attacchi sincronizzati contro DeepSeek, scagliando due ondate devastanti di comandi, utilizzando fino a 118 porte di comando attraverso ben 16 server C&C. Rispetto all'ultima ondata di attacchi, il numero di comandi inviati è cresciuto di oltre 100 volte, evidenziando come le botnet siano uno strumento sempre più efficace nelle mani dei cybercriminali.

Perché le botnet stanno diventando sempre più pericolose?

Ciò che rende così sconvolgente questo nuovo modello di attacchi è la facilità con cui è possibile noleggiare botnet sul dark web. In questa "mercatizzazione" del cybercrime, l'accesso a questi servizi è estremamente economico, richiedendo spesso solo pochi passaggi, come scaricare un'applicazione. In un mondo in rapida evoluzione digitale, tutto ciò rappresenta una minaccia formidabile per la sicurezza a livello industriale.

L'incidente di DeepSeek è in effetti un caso lampante dell'intensificarsi degli attacchi. Fino a un paio di anni fa, molte aziende riuscivano a fronteggiare, in misura variabile, gli attacchi DDoS basati sull'amplificazione grazie alle strutture di protezione ormai consolidate. Ma ora l'integrazione, ad esempio, di botnet come HailBot e RapperBot ha cambiato radicalmente lo scenario. Negli attacchi attuali, non si tratta più semplicemente di una tecnica isolata, ma di una combinazione di metodi che rende estremamente difficile identificare e bloccare i colpi.

Le conseguenze per le imprese

Per una società ambiziosa e in rapida crescita come DeepSeek, le ripercussioni di questi attacchi vanno ben oltre il semplice fastidio dell'interruzione del servizio. Quando, infatti, un attacco DDoS di tipo avanzato viene rivolto contro una piattaforma web, i danni che ne conseguono possono essere seri:

- Interruzione del servizio: Durante gli attacchi, gli utenti non riescono ad accedere al portale web, causando periodi di inoperatività, a volte molto gravi.
- Perdita di fiducia: Ogni interruzione indebolisce la fiducia degli utenti, soprattutto se si tratta di clienti business o investitori, con ripercussioni negative sul brand e sulla reputazione aziendale.
- Costi elevati: Difendersi da attacchi botnet e DDoS complessi richiede risorse ingenti, con investimenti significativi per proteggere l'infrastruttura, monitorare il traffico e adottare costantemente i più moderni standard e tecnologie.

Questo quadro spinge le aziende a rivedere le proprie politiche di sicurezza e a dotarsi di strumenti più evoluti, come firewall di nuova generazione, WAF (Web Application Firewall), nonché strumenti per l'analisi in tempo reale del traffico, al fine di contrastare efficacemente una minaccia in continua evoluzione.

"Il caso di DeepSeek dimostra chiaramente che le botnet rappresentano una minaccia reale di cui devono tenere conto non solo le aziende più innovative, ma anche i partner e gli investitori".

Una sfida su cui collaborare

In un'epoca in cui la tecnologia dell'informazione e della comunicazione rimane il motore della crescita economica e del progresso, è necessario implementare misure di sicurezza informatica capaci di fronteggiare le nuove minacce. Il caso di DeepSeek dimostra chiaramente che le botnet rappresentano una minaccia reale di cui devono tenere conto non solo le aziende più innovative, ma anche i partner e gli investitori. Poiché gli attacchi orchestrati da queste reti di dispositivi controllati, in grado di variare i loro colpi e di aumentare le risorse a disposizione degli aggressori, rendono sempre più difficile la difesa, è necessario un impegno collettivo e una cooperazione costante per limitare il fenomeno.

AI – domande e risposte facili facili
L'AI per l'automazione

A cura di Gianpiero Cozzolino

Qual è il ruolo dell'AI nei sistemi informatici convenzionali?

I sistemi di intelligenza artificiale sono ovviamente sistemi informatici, di tipo particolare per le caratteristiche che abbiamo visto nei numeri precedenti, e che oramai tutti intravediamo; ma per loro natura, possono anche intervenire nei sistemi informatici tradizionali.

Per prima cosa, sono degli ottimi scrittori di codice (cioè, le istruzioni che definiscono il comportamento del sistema) e della relativa documentazione tecnica ed, in parte, di quella d'uso; questo perché il codice segue regole molto precise e, se il dataset di addestramento è sufficientemente ampio e contiene codice privo di errori, il risultato ha altissima probabilità di essere corretto, nel senso che fa ciò che è stato richiesto senza errori.

Il secondo utilizzo può essere quello di analisi continua dei dati, per esempio il "LOG" cioè dei registri di funzionamento dei sistemi, che contengono gigantesche quantità di informazioni molto tecniche; da questa mole di informazioni è possibile ricavare indicazioni sulle prestazioni del sistema, o sul comportamento degli utenti, o sulle possibilità di guasti, ma ciò è estremamente complicato per un essere umano, mentre diventa fattibile se automatizzato, e soprattutto ha maggior apprendimento in modo continuativo ed esponenziale.

Infine, in un mondo in cui le minacce informatiche sono in continuo aumento, l'IA sta diventando uno degli elementi nuovi nel campo della cybersecurity, permettendo di individuare situazioni pericolose (e di conseguenza intervenire tempestivamente) anche quando si tratta di attacchi non ancora noti e gestiti.

Quali sono le ultime attività che vengono supportate con l'IA

In ambito aziendale le applicazioni delle varie tecnologie di IA sono molteplici: gestione della produzione e della supply chain (suddivisione delle forniture, razionalizzazione delle scorte, ottimizzazione dei costi), della gestione dei trasporti (tragitti ottimali, razionalizzazione dei carichi e delle spedizioni), ricerca e sviluppo (nuovi materiali, tecnologie di produzione, robotica avanzata), e di tutta una serie di processi aziendali (es. turnazioni, selezione del personale, analisi finanziaria, controllo qualità, manutenzione predittiva, marketing).

Peraltro, in campo industriale ci sono problemi, anche apparentemente semplici ma la cui soluzione è invece estremamente complessa (qualcuno ha detto "il problema del commesso viaggiatore"?), che sono stati indagati per decenni e per cui esistono approcci che non costituiscono una reale soluzione ma solo una buona approssimazione di essa, e finora ci si è accontentati anche perché non si poteva fare di meglio. Indubbiamente ora l'IA rappresenta una nuova metodologia che può portare ad arrivare alle soluzioni tanto cercate.

Possiamo anche accennare ad altro interessante campo di applicazione, quello della meteorologia, cioè le previsioni del tempo: sono in corso sperimentazioni in cui, a fianco dei modelli previsionali tradizionali basati sull'applicazione (per quanto approssimata) delle leggi della fisica dell'atmosfera, si utilizzano sistemi IA che utilizzano i dati del passato per addestrarsi e quindi forniscano una previsione basata, per così dire, sull'esperienza (come d'altra parte hanno fatto i contadini per secoli...).

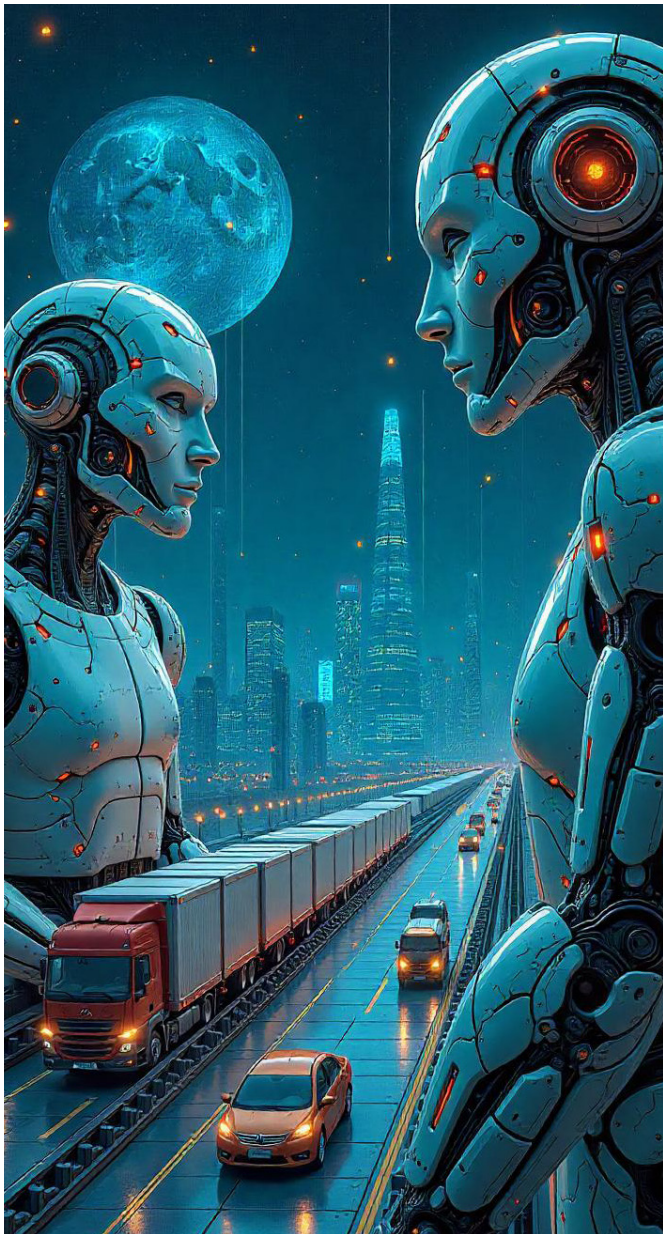
Cosa ne penso?

Tutte le automazioni di tipo "decisionale" comportano che le scelte su come operare un processo siano delegate ad una macchina. Un primo problema riguarda l'affidabilità, che corrisponde a dire che le decisioni prese siano coerenti con i requisiti o i desideri dell'utilizzatore (normalmente l'affidabilità aumento con il tempo, raffinando il sistema). Ma il grande problema, che non è solo tecnico ma anche giuridico, è su quale soggetto ricade la responsabilità delle conseguenze di queste scelte. Mentre nei sistemi automatici o informatici deterministici è possibile indagare come il sistema possa essere arrivato ad una certa scelta, e di conseguenza individuare tra il produttore del sistema, il titolare dell'utilizzo ed eventuali soggetti terzi (es. lavoratori infedeli, hackers) chi e quanto abbia influenzato il verificarsi di quella data scelta, nei sistemi non deterministici, tra cui le IA, spesso non è possibile ricostruire come la scelta sia stata determinata e quindi anche la ripartizione delle responsabilità diventa estremamente più complicata, con il concreto rischio che nessuno possa essere considerato responsabile di conseguenze inattese o dannose (nonostante ciò, c'è chi ritiene che le IA possano essere responsabili di per loro).

Purtroppo, come peraltro spesso accade con le nuove tecnologie, succede che le questioni regolatorie e giuridiche vengano affrontate ben dopo che una tecnologia sia stata largamente adottata, e nel frattempo tutta una serie di problematiche anche dovute alla sua non completa affidabilità non possano essere affrontate, causando spesso grave danno alla società.

Facile Facile, supponiamo che un utente esperto digitale dica (inserisca un set di dati errato falso nei log), che sulla Cristoforo Colombo ce traffico bloccato per incidente non risolvibile prima di 2 ore, dopo 5 min si ritroverebbe la strada per andare a lavoro completamente scorrevole inquanto la IA avrà deviato i percorsi di tutti gli altri guidatori e se il log errato lo scrive lo stato? La software house? Un'altra IA?

Se l'etica non viene presa come caposaldo di tutto il nostro agire ci ritroveremo ad avere una battaglia infinita su chi sia il più bravo a fare "trucchetti" di magia.



"Le questioni regolatorie e giuridiche vengono affrontate ben dopo che una tecnologia sia stata largamente adottata, e nel frattempo tutta una serie di problematiche anche dovute alla sua non completa affidabilità non possano essere affrontate, causando spesso grave danno alla società".

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

- S.Rodotà, “Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione”, Bari, Laterza, 2004, pag.57

- K.Schwab, “La quarta rivoluzione industriale”, Milano, Franco Angeli, 2016, pag.5

- Rappresenta un ramo delle scienze informatiche che si occupa di tutelare i sistemi di elaborazione, intesi sia come singoli computer che sistemi di reti complesse, dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti. Vocabolario Neologismi, 2008, Treccani

- Una solida struttura di sicurezza informatica è la difesa fondamentale per mitigare e ridurre i rischi relativi alle minacce informatiche. La maggior parte degli attacchi informatici sono automatizzati e indiscriminati, ossia una volta che identificano una vulnerabilità, la sfruttano per colpire qualsiasi organizzazione piuttosto che un’azienda specifica. Di conseguenza, è fondamentale disporre delle giuste misure di sicurezza informatica per proteggere la propria organizzazione

- Ciò che è stato appena espresso, viene anche comunemente definito con la definizione “CIA Triad” (Confidentiality, Integrity, Availability)

- Virtual Private Network, ossia “rete privata virtuale”, un servizio che protegge la connessione internet e la privacy online

- Autenticazione multifattore (MFA) è una tecnologia di sicurezza che utilizza diversi fattori di autenticazione per la verifica dell’identità

- Recovery Time Objective (RTO): è il tempo massimo che può trascorrere tra il fermo di un sistema e il recupero della sua operatività

- Recovery Point Objective (RPO): stabilisce la quantità massima di dati a cui la tua azienda è disposta a rinunciare a seguito di un problema.

- Hackmanac Global Cyber Attacks Report 2025

CYBER MAGAZINE

CYBER Think Tank ASSINTEL

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

Contattaci:

segreteria@assintel.it
www.assintel.it