Cybersecurity Trends

Edizione italiana, N. 3 / 2025

INTERVISTE VIP:

- GIAN MARIA FARA
- ANDREA GRANELLI e NICOLA SPAGNUOLO
- MARCO DI LUZIO
- ROBERTO MASIERO

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Folder centrale: Operational Technology

Cybersecurity Trends

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

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

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

www.cybertrends.it

Indice

Proteggere il cuore dell'industria connessa.

Autore: Nicola Sotira

La trasformazione digitale ha profondamente cambiato il mondo industriale. Oggi, macchine, sensori e sistemi di controllo che un tempo operavano in modo isolato comunicano in tempo reale con piattaforme cloud, software gestionali e algoritmi di intelligenza artificiale. Questo ha reso i processi più efficienti, ma anche più vulnerabili.

La sicurezza OT (Operational Technology) è il punto d'incontro tra la tecnologia operativa e la cybersecurity.

BIO

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

Quando parliamo di OT, ci riferiamo all'insieme dei sistemi che controllano i processi fisici di un'azienda: linee di produzione, centrali elettriche, reti idriche, impianti di trasporto, infrastrutture energetiche. Si tratta di **PLC, SCADA, DCS, sensori, HMI,** dispositivi che gestiscono operazioni in tempo reale.

A differenza dell'IT, che lavora con dati e informazioni, l'OT interagisce con il mondo reale: un comando errato può bloccare un macchinario, interrompere la produzione o persino causare danni fisici.

Per questo le priorità cambiano:

- **Disponibilità** – le macchine non devono fermarsi;
- **Integrità dei comandi e dei dati** – ogni segnale deve essere affidabile;
- **Riservatezza** – importante, ma secondaria rispetto alla continuità operativa.

Per decenni, gli impianti industriali sono stati protetti da un isolamento naturale; non erano collegati a Internet. Oggi questo non vale più. L'adozione di Industria 4.0, dell'IoT industriale e della manutenzione predittiva ha connesso la fabbrica digitale al mondo IT. Un enorme vantaggio in termini di efficienza, ma anche un punto debole. L'integrazione IT/OT ha aperto nuove porte d'ingresso agli attaccanti. Basta un accesso remoto mal configurato, un aggiornamento software compromesso o un vecchio PLC non aggiornato per esporre l'intero impianto. Secondo i dati di ENISA, oltre il 60% delle infrastrutture critiche europee ha subito tentativi di compromissione dei sistemi di controllo industriale negli ultimi anni. In questo contesto proteggere un ambiente OT richiede un equilibrio delicato: aumentare la sicurezza senza interrompere la produzione. Occorre poi, tenere in considerazione anche il tema della supply chain, oggi nessun impianto è un'isola. Ogni sistema OT si collega a fornitori, software, manutentori e integratori esterni. E proprio da lì possono arrivare gli attacchi più subdoli. Non trascurabile, anche in questo dominio, è il tema del fattore umano. La tecnologia non basta. Molti incidenti nascono da errori umani, da configurazioni sbagliate o da una scarsa consapevolezza e quindi formare il personale OT alla sicurezza è un investimento strategico. Su tutto questo, in arrivo le nuove normative europee, come la **Direttiva NIS2** e il **Cyber Resilience Act**, che renderanno obbligatorie misure minime di sicurezza anche per gli operatori industriali e i produttori di dispositivi OT.

La sicurezza OT diventa, quindi, il nuovo pilastro della trasformazione digitale industriale. Non si tratta più solo di proteggere i dati, ma di garantire che **le macchine continuino a funzionare**, che **i processi restino sicuri** e che **le persone non corrano rischi**. In un ecosistema in cui IT e OT si fondono, la sicurezza diventa una responsabilità condivisa tra tecnologi, ingegneri, manager e fornitori. Solo unendo competenze e cultura della prevenzione possiamo costruire **fabbriche connesse ma resilienti,** capaci di affrontare il futuro digitale senza compromettere l'affidabilità e la sicurezza del mondo fisico. ■

Vulnerabilità della supply chain nell'OT: rischi di terze parti che non puoi ignorare.

Autore: Lisa Ventura

Il panorama della tecnologia operativa (OT) ha subito una trasformazione profonda nell'ultimo decennio. Se un tempo i sistemi industriali operavano in totale isolamento, oggi le infrastrutture critiche si basano fortemente su reti interconnesse, fornitori di terzi parti e catene di approvvigionamento complesse che si estendono a livello globale. Questa evoluzione ha portato enormi vantaggi in termini di efficienza, capacità di monitoraggio e visibilità operativa. Tuttavia, ha anche introdotto un complesso di vulnerabilità informatiche che molte organizzazioni stanno appena iniziando a riconoscere.

La convergenza tra tecnologia informatica (IT) e tecnologia operativa ha creato nuovi vettori di attacco che gli attori malevoli sfruttano sempre di più. A differenza degli ambienti IT tradizionali, dove una violazione può comportare il furto di dati o l'interruzione dei sistemi, i sistemi OT compromessi possono causare danni fisici, disastri ambientali e minacce alla sicurezza delle persone. La posta in gioco non potrebbe essere più alta, eppure molte organizzazioni continuano ad affrontare la sicurezza informatica OT con una mentalità centrata sull'IT, che non riesce a considerare le sfide uniche degli ambienti industriali.

I rischi legati a terze parti negli ambienti OT rappresentano una delle minacce più significative e sottovalutate che oggi incombono sulle infrastrutture critiche. Dal software integrato nei controllori logici programmabili (PLC), alle soluzioni di accesso remoto fornite dai fornitori di apparecchiature. L'impianto industriale moderno dipende da un vasto ecosistema di fornitori esterni, ciascuno dei quali può introdurre vulnerabilità sfruttabili da attori di minaccia sofisticati.

L'evoluzione delle superfici di attacco OT

La tradizionale rete industriale isolata (air-gapped) sta rapidamente diventando un reperto del passato. Gli impianti industriali moderni richiedono connettività per l'efficienza operativa, la conformità normativa e il vantaggio competitivo. Questa connettività, tuttavia, ha modificato radicalmente il panorama delle minacce. Se un tempo un attaccante doveva avere accesso fisico per compromettere i sistemi industriali, oggi gli attori malevoli possono, potenzialmente, raggiungere le infrastrutture critiche da qualsiasi parte del mondo, attraverso componenti compromessi della supply chain.

La superficie di attacco negli ambienti OT moderni si estende ben oltre i sistemi di controllo industriale stessi. Comprende ogni componente hardware, software e servizio che interagisce con l'ambiente operativo. Questo include interfacce uomo-macchina (HMI), workstation di ingegneria,

sistemi storici (historians), sistemi di gestione degli asset e i sempre più diffusi dispositivi IIoT (Industrial Internet of Things) che monitorano tutto, dai livelli di vibrazione alle variazioni di temperatura.

Ogni componente di questo ecosistema rappresenta un potenziale punto di ingresso per attori malevoli. Un laptop compromesso di un fornitore, che si connette alla rete per la manutenzione ordinaria, una libreria software vulnerabile incorporata in un sistema di sicurezza critico, oppure una backdoor nascosta nel firmware, potrebbero tutti costituire da punto di ingresso per attacchi distruttivi. La difficoltà per gli esperti di sicurezza è che questi rischi spesso passano inosservati fino a quando non è troppo tardi per evitarne le conseguenze.

La complessità dei sistemi industriali moderni rende straordinariamente difficile una valutazione completa dei rischi. Una singola linea di produzione potrebbe incorporare componenti di decine di fornitori, ciascuno con le proprie dipendenze software, meccanismi di aggiornamento e requisiti di supporto. Le interdipendenze tra questi sistemi creano rischi a cascata, in cui la compromissione di un componente apparentemente minore può provocare il malfunzionamento di sistemi di sicurezza critici.

Comprendere i vettori di rischio delle terze parti

I rischi legati a terze parti negli ambienti OT si manifestano attraverso molteplici vettori, ciascuno dei quali richiede strategie di mitigazione specifiche. Il vettore più evidente è l'accesso diretto dei fornitori alle reti operative. I produttori di apparecchiature, gli integratori di sistemi e i fornitori di servizi richiedono spesso accesso remoto ai sistemi industriali per attività di manutenzione, risoluzione dei problemi e aggiornamenti. Sebbene tale accesso sia fondamentale per garantire l'efficienza operativa, esso crea percorsi persistenti che possono essere sfruttati da attori malevoli.

Le soluzioni di accesso remoto sono diventate un obiettivo privilegiato per gli attori delle minacce. Molte organizzazioni industriali si affidano a reti private virtuali (VPN), protocolli di desktop remoto o strumenti di accesso remoto specifici del fornitore che potrebbero non disporre dei controlli di sicurezza robusti necessari per proteggersi da attacchi sofisticati. La praticità della risoluzione dei problemi e della manutenzione da remoto spesso prevale sulle considerazioni di sicurezza, generando vulnerabilità che possono persistere ben oltre l'installazione iniziale.

Le compromissioni della supply chain software rappresentano un ulteriore vettore critico. I sistemi di controllo industriale si basano su stack software complessi che includono sistemi operativi, applicazioni, driver e componenti firmware provenienti da più fornitori. Ogni livello di questo stack rappresenta un potenziale punto di compromissione. L'attacco SolarWinds ha evidenziato come un singolo aggiornamento software compromesso possa consentire agli attaccanti di accedere a migliaia di organizzazioni a livello globale. Tecniche analoghe vengono ormai adottate con crescente frequenza anche negli ambienti industriali.

I rischi legati alla supply chain hardware sono altrettanto critici, ma spesso risultano più difficili da individuare. Componenti malevoli possono essere inseriti in diverse fasi del ciclo di vita, dalla produzione alla spedizione, fino alle operazioni di manutenzione apparentemente legittime. Le minacce hardware possono manifestarsi sotto forma di chip non autorizzati che abilitano accessi nascosti, firmware alterato che modifica il comportamento del sistema o componenti contraffatti che non rispettano gli standard di sicurezza.

La natura globalizzata delle supply chain industriali amplifica i rischi di compromissione. I componenti possono attraversare molteplici Paesi e organizzazioni prima di raggiungere la destinazione finale, generando numerose opportunità per interventi malevoli. La complessità delle supply chain moderne rende estremamente difficile garantire visibilità sull'origine e l'integrità dei componenti critici.

I rischi associati ai fornitori di servizi nella supply chain si estendono ben oltre quelli tradizionali, includendo provider di servizi cloud, fornitori di servizi gestiti e aziende specializzate in cyber sicurezza industriale. Pur offrendo competenze e soluzioni tecnologiche di alto valore, questi attori rappresentano anche potenziali punti di vulnerabilità critici. In particolare, una compromissione presso un fornitore di servizi gestiti può consentire agli attaccanti di accedere simultaneamente a più reti di clienti.

Anatomia degli Attacchi alla Supply Chain in OT

Gli attacchi alla supply chain che prendono di mira gli ambienti OT (Operational Technology) seguono schemi ricorrenti che i professionisti della sicurezza devono saper riconoscere per sviluppare difese efficaci. Generalmente, l'attacco inizia con una fase di ricognizione, durante la quale gli attori delle minacce analizzano la supply chain per individuare potenziali punti di ingresso. Questa fase può includere l'analisi delle relazioni con i fornitori, l'identificazione di soluzioni di accesso remoto vulnerabili e la mappatura delle dipendenze software delle organizzazioni target.

La compromissione iniziale avviene spesso nel punto più vulnerabile della supply chain. Questo può riguardare un fornitore secondario con risorse limitate in ambito di cybersicurezza, un componente software affetto da vulnerabilità note o un provider di servizi con controlli di accesso insufficienti. Una volta ottenuto l'accesso, gli attaccanti possono consolidare la loro presenza e muoversi lateralmente all'interno dell'ecosistema digitale, cercando di raggiungere asset critici o obiettivi strategici.

La persistenza rappresenta una caratteristica distintiva degli attacchi alla supply chain. Diversamente dagli attacchi opportunistici, orientati a

ottenere risultati immediati, le compromissioni della supply chain sono spesso progettate per garantire un accesso prolungato agli ambienti target. Gli attaccanti possono infiltrarsi attraverso aggiornamenti software legittimi, celarsi nei componenti firmware o creare canali nascosti sfruttando i meccanismi di accesso dei fornitori.

La fase di weaponizzazione implica l'adattamento dell'attacco alle caratteristiche specifiche dell'ambiente target. I sistemi OT richiedono spesso conoscenze specialistiche per essere compromessi in modo efficace, e gli attori delle minacce più sofisticati investono risorse considerevoli per comprendere protocolli industriali, sistemi di sicurezza e procedure operative. Questa conoscenza consente loro di creare attacchi in grado di eludere il rilevamento e di ottenere il massimo impatto.

L'obiettivo finale degli attacchi alla supply chain OT può variare significativamente in base alla natura dell'attore della minaccia. Gli attori statali, ad esempio, possono puntare a stabilire accessi persistenti per attività di spionaggio o per prepararsi a futuri scenari di conflitto. Le organizzazioni criminali, invece, tendono a distribuire ransomware o a sottrarre proprietà intellettuale di valore. Qualunque sia la motivazione, il potenziale impatto fisico e le conseguenze sulla sicurezza operativa rendono questi attacchi particolarmente critici e pericolosi.

Casi di studio sulla compromissione della supply chain in ambienti OT

Uno degli esempi più noti di sfruttamento delle vulnerabilità nella supply chain si è verificato nel maggio 2021, quando la Colonial Pipeline – responsabile del trasporto di quasi la metà del carburante consumato sulla costa orientale degli Stati Uniti – è stata colpita da un grave attacco ransomware che ha bloccato le operazioni per sei giorni. Il gruppo criminale DarkSide ha ottenuto l'accesso attraverso una password VPN compromessa, associata a un account inattivo privo di autenticazione a più fattori. Sebbene l'attacco abbia interessato principalmente l'infrastruttura di fatturazione, e non direttamente i sistemi OT, l'azienda ha scelto di interrompere proattivamente l'intera rete di oleodotti per evitare la propagazione del ransomware verso i sistemi operativi critici. Colonial Pipeline ha pagato un riscatto di 75 bitcoin – circa 4,4 milioni di dollari – entro poche ore, ma lo strumento di decrittazione fornito si è rivelato talmente lento da rendere necessario l'intervento manuale per il ripristino. L'incidente ha provocato gravi carenze di carburante, fenomeni di acquisto compulsivo e ha spinto il Presidente Biden a dichiarare lo stato di emergenza, dimostrando come gli attacchi informatici alle infrastrutture critiche possano generare effetti a cascata sull'intera società.

BIO

Lisa Ventura MBE è una pluripremiata specialista di cybersicurezza, scrittrice/autrice pubblicata e relatrice di conferenze. È la fondatrice di Cybersicurezza Unity, un'organizzazione comunitaria globale che si dedica a riunire individui e organizzazioni che lavorano attivamente nel campo della cybersicurezza per contribuire a combattere la crescente minaccia informatica. Come consulente, Lisa lavora anche con i team di leadership della cybersicurezza per aiutarli a lavorare insieme in modo più efficace e fornisce formazione sulla consapevolezza e la cultura della cybersicurezza e sui vantaggi dell'assunzione di persone con disabilità neurologiche. Ha una conoscenza specialistica dei fattori umani della cybersicurezza, della cyberpsicologia, della neurodiversità e dell'IA nel cyber, ed è anche cofondatrice del International Imposter Syndrome Awareness Day.
Ulteriori informazioni su Lisa sono disponibili su www.lisaventura.co.uk.
Lisa sui Social Media : X/Twitter - @cybergeekgirl; LinkedIn - https://www.linkedin.com/in/lisasventura/; Facebook - https://www.facebook.com/lisasventurauk; Instagram - https://www.instagram.com/lsventurauk/; YouTube - https://www.youtube.com/@CyberSecurityLisa/

Gli attacchi del 2024 contro Schneider Electric illustrano il persistente targeting dei fornitori di infrastrutture critiche. Il colosso francese dell'automazione ha subito tre incidenti separati in 18 mesi, tra cui un attacco ransomware Cactus nel gennaio 2024 alla sua divisione Sustainability Business, che ha compromesso 1,5 terabyte di dati, inclusi passaporti dei clienti. Successivamente, nel novembre 2024, il gruppo ransomware HellCat ha violato il sistema Atlassian Jira di Schneider, rubando 40 GB di dati di progetto e dettagli degli utenti. Questi attacchi contro uno dei maggiori fornitori OT al mondo dimostrano

come gli attori delle minacce stiano prendendo di mira aziende la cui compromissione può avere impatti su più clienti downstream contemporaneamente.

I sistemi idrici e di trattamento delle acque reflue sono diventati obiettivi privilegiati nello sfruttamento della supply chain, con numerosi incidenti documentati nel corso del 2024. Il gruppo Sandworm, celato sotto la falsa identità hacktivista "CyberArmyofRussia_Reborn", ha manipolato con successo i sistemi di trattamento delle acque a Muleshoe, Texas, causando il traboccamento dei serbatoi. Gli attaccanti si sono vantati sui social media di quanto fosse facile violare le difese informatiche dell'impianto, sfruttando soluzioni di accesso remoto. Attacchi simili si sono verificati in strutture situate in Indiana, New Jersey e altri stati, evidenziando una campagna coordinata che prende di mira infrastrutture con accesso remoto vulnerabile nel settore idrico.

Il settore manifatturiero continua a fronteggiare rischi significativi legati alla supply chain, con diversi incidenti di alto profilo nel 2024, che evidenziano la vulnerabilità del comparto. Keytronic Corporation, produttore di circuiti stampati, ha interrotto le operazioni per due settimane dopo aver rilevato attività anomale sulla propria rete IT, con il gruppo affiliato BlackBasta che ha rivendicato la responsabilità. Welch Foods ha subito un blocco produttivo di tre settimane, a seguito di un attacco ransomware che ha criptato i sistemi degli impianti, dimostrando come gli attacchi focalizzati sull'OT possano influire direttamente sulle capacità produttive.

L'emergere di nuove minacce ha aggiunto ulteriori dimensioni al panorama dei rischi della supply chain. Il malware FrostyGoop, scoperto nel 2024, prende di mira specificamente i dispositivi Modbus TCP ed è stato impiegato con successo contro un'utility di riscaldamento distrettuale a Leopoli, in Ucraina, lasciando 600 abitazioni senza riscaldamento per due giorni. Questo incidente ha segnato il primo caso noto di malware progettato per manipolare sistemi di riscaldamento industriale, evidenziando come gli attori delle minacce stiano sviluppando strumenti sempre più specializzati per attaccare diversi tipi di tecnologia operativa.

Le attività degli stati nazionali hanno intensificato la pressione sulla sicurezza della supply chain, con la campagna Volt Typhoon della Cina, che mantiene un accesso persistente alle infrastrutture critiche statunitensi, sfruttando vulnerabilità zero-day in router per uffici domestici e soluzioni di accesso remoto. L'obiettivo della campagna, volto a mantenere un accesso a lungo termine piuttosto che causare interruzioni immediate, suggerisce un posizionamento strategico in vista di potenziali conflitti futuri, rendendo particolarmente complessa la rilevazione e la mitigazione per le organizzazioni colpite.

Questi incidenti dimostrano collettivamente come i confini tradizionali tra sicurezza IT e OT si siano dissolti nella pratica. Gli attacchi moderni sfruttano la natura interconnessa dei sistemi industriali, prendendo di mira i punti più deboli delle supply chain complesse per ottenere il massimo impatto. L'attacco alla Colonial Pipeline rimane il momento spartiacque che ha portato le vulnerabilità della supply chain alla coscienza pubblica, ma gli incidenti successivi hanno mostrato che la minaccia si è solo intensificata, con attaccanti che sviluppano tecniche sempre più sofisticate e individuano nuovi obiettivi nei settori delle infrastrutture critiche.

Sicurezza della Supply Chain del Software

La sicurezza della supply chain del software negli ambienti OT richiede un approccio fondamentalmente diverso rispetto agli ambienti IT tradizionali. Il software industriale presenta spesso cicli di vita estesi, requisiti di certificazione complessi e meccanismi di aggiornamento limitati che complicano i processi tradizionali di gestione delle vulnerabilità.

L'**analisi della composizione del software** diventa essenziale per comprendere i componenti che costituiscono le applicazioni industriali. Le applicazioni moderne incorporano tipicamente numerose librerie, framework e componenti di terze parti, ciascuno dei quali può contenere vulnerabilità. Le organizzazioni devono mantenere inventari di questi componenti e monitorarli per le vulnerabilità di recente scoperta.

I meccanismi di **firma e verifica del codice** aiutano a garantire che gli aggiornamenti software provengano da fonti legittime e non siano stati manomessi durante la distribuzione. Tuttavia, molte applicazioni industriali non dispongono di implementazioni robuste di code signing, e alcuni fornitori utilizzano tecniche crittografiche deboli che possono essere compromesse da attaccanti determinati.

Il processo di aggiornamento software stesso rappresenta un vettore di attacco critico. Gli attaccanti hanno compromesso con successo i meccanismi di aggiornamento software per distribuire malware a un gran numero di organizzazioni simultaneamente. Gli ambienti industriali devono implementare processi di aggiornamento sicuri che verifichino l'integrità e l'autenticità degli aggiornamenti prima della distribuzione.

La **gestione delle vulnerabilità** negli ambienti OT richiede coordinamento tra i team di sicurezza e il personale operativo. A differenza degli ambienti IT, dove le patch possono essere distribuite rapidamente, i sistemi industriali possono richiedere test approfonditi, coordinamento con i fornitori e downtime pianificati per gli aggiornamenti. Questo crea finestre di vulnerabilità che devono essere gestite attraverso altri controlli, come la segmentazione della rete e il monitoraggio avanzato.

Il **software open source** presenta sfide particolari negli ambienti industriali. Sebbene i componenti open source possano offrire risparmi sui costi e flessibilità, trasferiscono anche la responsabilità della sicurezza all'organizzazione che li utilizza. Molte organizzazioni industriali non dispongono delle competenze necessarie per valutare la sicurezza dei componenti open source o per rispondere efficacemente quando vengono scoperte vulnerabilità.

Le **Software Bill of Materials (SBOM)** stanno diventando sempre più importanti per la gestione dei rischi della supply chain del software. Questi inventari dettagliati dei componenti software consentono alle organizzazioni di identificare rapidamente i sistemi che potrebbero essere interessati da vulnerabilità recentemente scoperte e di dare priorità agli interventi di remediation in modo appropriato.

Valutazione e gestione del rischio di terze parti

Una gestione efficace del rischio di terze parti richiede un programma completo che affronti i rischi lungo tutto il ciclo di vita del fornitore. Questo inizia con i processi di selezione dei fornitori, che devono valutare le capacità di sicurezza insieme alle considerazioni funzionali e di costo. Troppo spesso, le decisioni di procurement si concentrano esclusivamente su funzionalità e prezzo, ignorando implicazioni di sicurezza che possono persistere per decenni.

Le **valutazioni di sicurezza dei fornitori** devono essere adattate ai rischi specifici associati agli ambienti OT. Questionari generici di sicurezza IT sono insufficienti per valutare fornitori che avranno accesso a infrastrutture critiche. Le valutazioni devono affrontare competenze in cyber sicurezza industriale, comprensione dei sistemi di sicurezza, capacità di risposta agli incidenti e conformità agli standard di settore pertinenti.

I **requisiti contrattuali di sicurezza** forniscono la base per le relazioni continuative con i fornitori. I contratti devono specificare obblighi di sicurezza, requisiti di notifica degli incidenti, diritti di audit e allocazione delle responsabilità per le violazioni di sicurezza. Questi requisiti devono essere sufficientemente specifici da essere applicabili, pur rimanendo flessibili per adattarsi alle realtà operative degli ambienti industriali.

Il **monitoraggio continuo della postura di sicurezza dei fornitori** è essenziale ma complesso. Gli approcci tradizionali basati su valutazioni annuali sono insufficienti, dato il carattere dinamico delle minacce informatiche. I programmi moderni dovrebbero incorporare intelligence sulle minacce in tempo reale, scansioni automatiche delle vulnerabilità e revisioni regolari degli incidenti di sicurezza dei fornitori.

La sfida del **consolidamento dei fornitori rispetto alla diversificazione** crea compromessi complessi nella gestione del rischio. Collaborare con un numero ridotto di fornitori può semplificare la gestione e potenzialmente migliorare la supervisione della sicurezza, ma crea anche rischi di concentrazione, dove la compromissione di un singolo fornitore potrebbe avere un impatto diffuso. Al contrario, diversificare le relazioni con i fornitori può ridurre i rischi di concentrazione, ma aumenta la complessità della gestione della sicurezza.

Le **procedure di risoluzione del contratto con il fornitori** devono affrontare le sfide uniche degli ambienti OT. A differenza dei sistemi IT, dove le relazioni con i fornitori possono spesso essere terminate rapidamente, i

sistemi industriali possono avere dipendenze complesse che richiedono periodi di transizione prolungati. I team di sicurezza devono garantire che l'accesso sia adeguatamente limitato durante queste transizioni, mantenendo al contempo la continuità operativa.

Considerazioni normative e di conformità

Il panorama normativo per la cyber sicurezza OT si sta evolvendo rapidamente, con nuovi requisiti che affrontano specificamente i rischi della supply chain.

La **Direttiva NIS dell'Unione Europea** richiede agli operatori di servizi essenziali di implementare misure di sicurezza appropriate che affrontino i rischi della supply chain. Analogamente, le **Regolamentazioni NIS del Regno Unito** impongono obblighi specifici agli operatori di infrastrutture critiche.

Le normative specifiche di settore aggiungono ulteriori livelli di complessità. L'industria nucleare opera sotto rigorosi framework normativi che affrontano la cyber sicurezza lungo tutta la supply chain.

Allo stesso modo, l'industria aeronautica ha sviluppato standard completi per la garanzia del software che si estendono a tutti i fornitori e subappaltatori.

La conformità a queste normative richiede alle organizzazioni di implementare programmi formali di gestione del rischio della supply chain che documentino i processi, mantengano registri e dimostrino la dovuta diligenza nella selezione e gestione dei fornitori. Questo onere di conformità può essere significativo, ma fornisce anche un quadro per una gestione sistematica del rischio.

La sfida delle normative internazionali influisce sulle organizzazioni con operazioni globali o supply chain complesse. Giurisdizioni diverse possono avere requisiti in conflitto o interpretazioni differenti di obblighi simili. Le organizzazioni devono affrontare queste complessità mantenendo standard di sicurezza coerenti in tutte le loro operazioni.

I processi di certificazione e accreditamento svolgono ruoli importanti nella sicurezza della supply chain, ma possono anche creare false sensazioni di sicurezza. Le certificazioni di settore come **IEC 62443** forniscono quadri di riferimento preziosi per la valutazione della sicurezza, ma non possono garantire che i prodotti certificati siano privi di vulnerabilità o che i fornitori certificati mantengano pratiche di sicurezza adeguate.

Costruire Supply Chain OT resilienti

La resilienza nelle supply chain OT richiede di andare oltre i controlli preventivi tradizionali per adottare approcci adattivi in grado di rispondere efficacemente alle minacce in evoluzione. Ciò include la progettazione di sistemi e processi che possano continuare a operare in sicurezza anche quando alcuni componenti sono compromessi.

La **ridondanza e la diversificazione** nelle supply chain possono ridurre l'impatto delle compromissioni dei fornitori. Piuttosto che affidarsi a fonti uniche per componenti critici, le organizzazioni dovrebbero mantenere relazioni con più fornitori e opzioni di approvvigionamento alternative. Questa diversificazione dovrebbe estendersi oltre la semplice ridondanza per includere diversità negli approcci tecnologici, nelle ubicazioni dei fornitori e nelle rotte della supply chain.

La **pianificazione della risposta agli incidenti** deve affrontare specificamente le compromissioni della supply chain. I piani di risposta tradizionali si concentrano spesso sugli attacchi diretti ai sistemi organizzativi, ma possono non affrontare adeguatamente scenari in cui l'attacco ha origine da un fornitore o partner della supply chain considerato affidabile. I piani di risposta dovrebbero includere procedure per isolare l'accesso compromesso del fornitore, coordinarsi con i fornitori coinvolti e comunicare con altri potenziali obiettivi.

La **condivisione delle informazioni** all'interno delle comunità di settore migliora la sicurezza collettiva, consentendo alle organizzazioni di apprendere dalle esperienze reciproche e di identificare minacce emergenti. Le organizzazioni di condivisione delle informazioni specifiche di settore forniscono forum per discutere i rischi della supply chain e coordinare misure difensive.

Lo **sviluppo di capacità interne** riduce la dipendenza dai fornitori esterni e offre opzioni per affrontare i rischi della supply chain. Sebbene l'indipendenza completa dai fornitori non sia né pratica né desiderabile, le organizzazioni dovrebbero sviluppare competenze interne sufficienti per valutare le dichiarazioni di sicurezza dei fornitori, rispondere agli incidenti legati ai fornitori e mantenere i sistemi critici quando il supporto del fornitore non è disponibile.

Gli **investimenti nella ricerca e sviluppo sulla sicurezza** aiutano le organizzazioni a rimanere avanti rispetto alle minacce emergenti e a sviluppare soluzioni innovative alle sfide della supply chain. Ciò può includere partnership con istituzioni accademiche, partecipazione a programmi di ricerca di settore o iniziative interne di ricerca e sviluppo focalizzate sulla sicurezza della supply chain.

Considerazioni future e minacce emergenti

Il panorama delle minacce per le supply chain OT continua a evolversi man mano che vengono adottate nuove tecnologie e le tecniche di attacco diventano più sofisticate. L'adozione crescente del **cloud computing** negli

ambienti industriali crea nuove categorie di rischi per la supply chain che le organizzazioni stanno appena iniziando a comprendere.

Le tecnologie di **intelligenza artificiale e machine learning** vengono integrate nei sistemi industriali a un ritmo accelerato. Sebbene queste tecnologie offrano vantaggi significativi, introducono anche nuove vulnerabilità e vettori di attacco. Gli attacchi di **machine learning adversarial** potrebbero compromettere i processi decisionali dei sistemi automatizzati, mentre la complessità dei sistemi AI rende estremamente difficile la validazione della sicurezza.

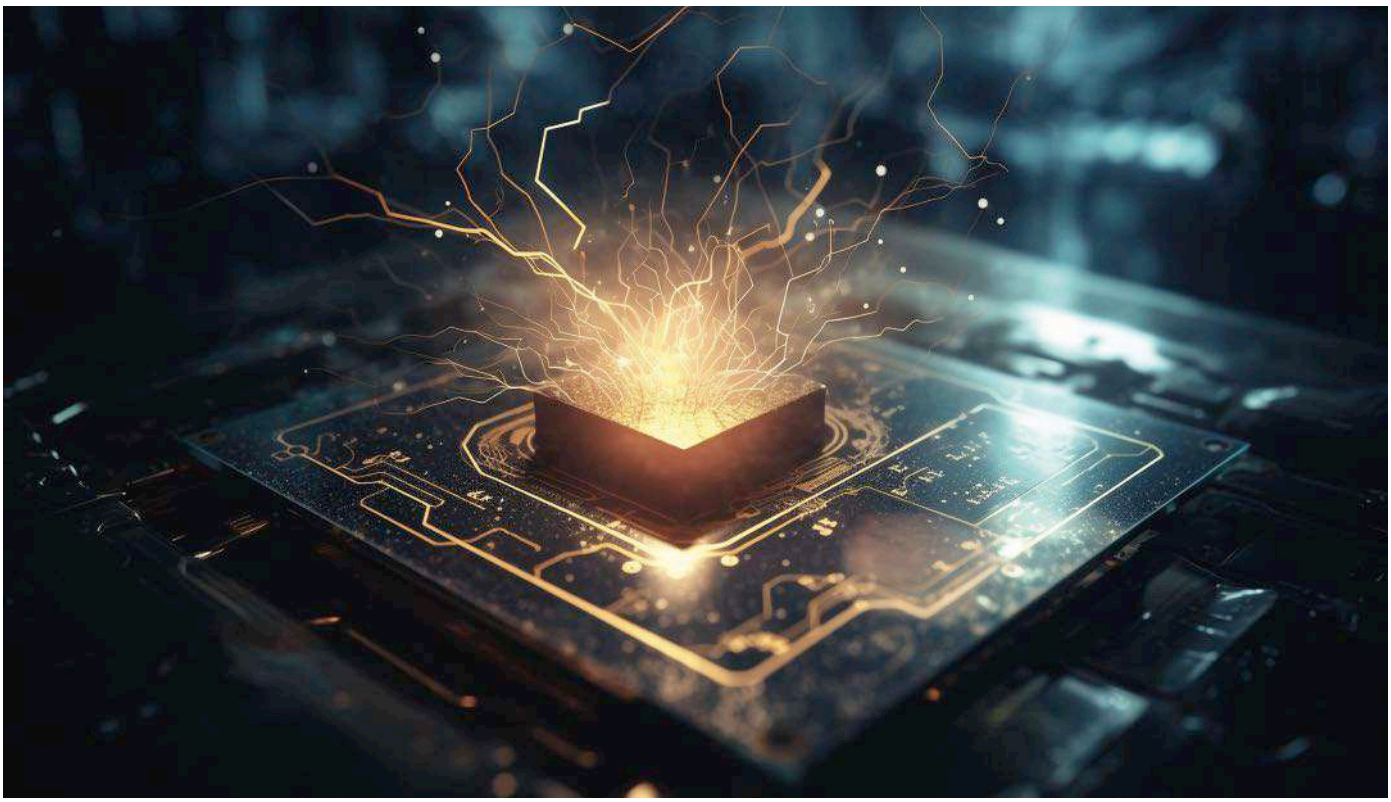
L'**Internet of Things (IoT)** continua ad ampliare la superficie di attacco degli ambienti industriali attraverso la proliferazione di sensori, attuatori e dispositivi di monitoraggio connessi. Molti di questi dispositivi sono prodotti da fornitori con competenze limitate in cyber sicurezza e vengono distribuiti con configurazioni di sicurezza minime. La portata delle implementazioni IIoT rende la gestione complessiva della sicurezza estremamente sfidante.

Gli **attacchi alla supply chain** stanno diventando più sofisticati e mirati. I gruppi di minacce persistenti avanzate (APT) stanno investendo pesantemente nelle capacità di compromissione della supply chain, e le tecniche pionieristiche utilizzate negli attacchi di alto profilo vengono adottate da attori meno sofisticati. La democratizzazione di queste tecniche di attacco aumenta la probabilità che le organizzazioni affrontino compromissioni della supply chain.

Il **calcolo quantistico** rappresenta una minaccia a lungo termine per le fondamenta crittografiche delle tecnologie di sicurezza attuali. Sebbene i computer quantistici sufficientemente avanzati, in grado di violare gli algoritmi crittografici attuali, possano essere ancora lontani anni, le organizzazioni devono iniziare a prepararsi a questa transizione valutando tecnologie crittografiche resistenti al quantum e pianificando strategie di migrazione.

Raccomandazioni per l'azione

Le organizzazioni responsabili delle infrastrutture critiche devono intraprendere azioni immediate per affrontare le vulnerabilità della supply chain nei loro ambienti OT. Questo inizia con la conduzione di valutazioni complete dei rischi attuali della supply chain, inclusi inventari dettagliati delle relazioni con i fornitori, dei meccanismi di accesso remoto e delle dipendenze software.



Lo sviluppo di **programmi formali di gestione del rischio della supply chain** dovrebbe essere una priorità per tutti gli operatori di infrastrutture critiche. Questi programmi devono affrontare i criteri di selezione dei fornitori, i requisiti di monitoraggio continuo, le procedure di risposta agli incidenti e i processi di rivalutazione periodica del rischio. I programmi devono essere adattati ai rischi specifici e ai requisiti operativi dell'organizzazione, incorporando al contempo le best practice di settore e i requisiti normativi.

Gli **investimenti in tecnologie di sicurezza** che affrontano specificamente i rischi della supply chain devono essere prioritari. Questo include soluzioni di monitoraggio della rete in grado di rilevare comportamenti anomali dei fornitori, piattaforme di accesso remoto sicure che implementano principi di zero trust, e strumenti di analisi della composizione del software che forniscono visibilità sui componenti che costituiscono le applicazioni critiche.

I **programmi di formazione e sensibilizzazione del personale** devono affrontare gli aspetti unici della sicurezza della supply chain negli ambienti OT. La formazione tradizionale sulla cyber sicurezza, focalizzata su phishing via email e sicurezza delle password, è insufficiente per il personale che gestisce le relazioni con i fornitori e supervisiona le operazioni delle infrastrutture critiche.

La **collaborazione con i pari del settore, le agenzie governative e i ricercatori di sicurezza** migliora le capacità organizzative e fornisce accesso a intelligence sulle minacce e best practice. La partecipazione attiva ai forum di settore e alle organizzazioni di condivisione delle informazioni dovrebbe essere una pratica standard per tutti gli operatori di infrastrutture critiche.

Il percorso da seguire richiede **impegno e investimenti costanti da parte della leadership organizzativa**. La sicurezza della supply chain non è un problema che può essere risolto solo attraverso la tecnologia; richiede programmi completi che affrontino persone, processi e tecnologia in modo coordinato. Le conseguenze dell'inazione sono semplicemente troppo gravi per essere ignorate, e il tempo delle mezze misure è finito.

La rivoluzione industriale ha trasformato il modo in cui le società creano valore e organizzano l'attività economica. La trasformazione digitale dei sistemi industriali di oggi rappresenta un cambiamento altrettanto profondo, che porta enormi opportunità insieme a rischi significativi. Gestire efficacemente questi rischi richiede comprendere che la sicurezza non è una funzionalità opzionale da aggiungere in seguito, ma un requisito fondamentale che deve essere integrato in ogni aspetto delle operazioni industriali.

Le vulnerabilità della supply chain presenti negli ambienti OT odierni rappresentano una delle sfide più significative per gli operatori di infrastrutture critiche. Queste sfide non possono essere risolte da una singola organizzazione che agisce da sola; richiedono azioni coordinate in interi settori e supply chain. Tuttavia, ogni organizzazione deve iniziare affrontando i rischi all'interno del proprio ambiente e costruendo le capacità necessarie per gestire efficacemente la sicurezza della supply chain.

La posta in gioco non potrebbe essere più alta. I sistemi che alimentano le reti elettriche, gestiscono gli impianti di trattamento delle acque, controllano i processi produttivi e supportano le reti di trasporto dipendono sempre più da supply chain complesse che si estendono a livello globale. La sicurezza di questi sistemi riguarda non solo le organizzazioni che li gestiscono, ma intere società che ne dipendono. Una sicurezza efficace della supply chain non è solo un imperativo aziendale; è una responsabilità sociale che non può essere ignorata.

La sfida è significativa, ma non insormontabile. Le organizzazioni che affrontano la sicurezza della supply chain con la dovuta serietà, investono nelle capacità necessarie e si impegnano in un miglioramento continuo possono ridurre significativamente la loro esposizione al rischio. La chiave è iniziare ora, prima che il prossimo grande attacco alla supply chain dimostri il vero costo dell'inazione. La sicurezza futura delle infrastrutture critiche dipende dalle azioni intraprese oggi per affrontare le vulnerabilità della supply chain che non possono più essere ignorate. ■

Nuove frontiere per la sicurezza dei sistemi cyber-fisici.

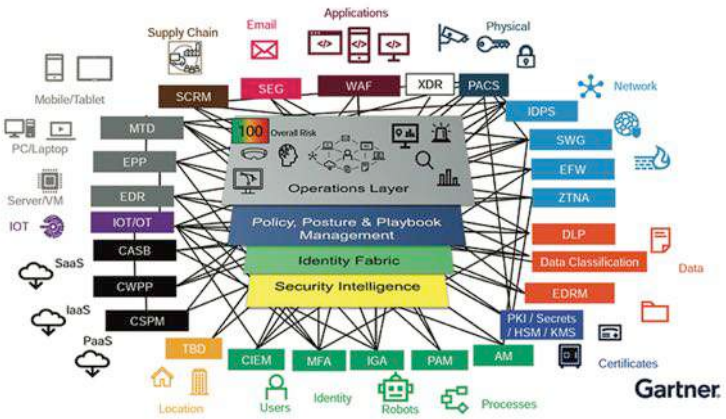
Autore: Francesco Corona

Generalita'

L'Operational Technology (OT), ovvero l'hardware e il software che controllano le operazioni industriali, sta notevolmente evolvendo in quelli che vengono definiti Cyber Physical Sistems (CPS): un termine reso popolare da Gartner, che riflette la crescente connettività e intelligenza negli ambienti industriali, senza tralasciare gli aspetti di cyber-sicurezza.

Man mano che l'OT diventa CPS, la superficie di attacco cyber si espande. Una volta che sistemi isolati come reti elettriche, linee di produzione, pipelines, vengono interconnessi, apportano vantaggi come il monitoraggio in tempo reale, ma li espongono a nuove minacce informatiche. Le conseguenze sono tangibili: interruzione della produzione, interruzioni di energia con potenziali incidenti fisici che possono propagarsi a tutte le reti di utilities interconnesse.

Questa evoluzione sta determinando la necessità di normative di sicurezza OT più stringenti. A differenza dell'IT, che tipicamente gestisce i dati, l'OT gestisce i processi fisici. La crescente convergenza tra i due ambiti comporta sfide uniche. Le normative stanno ora affrontando questo aspetto, obbligando le organizzazioni ad adattarsi a rivedersi in un nuovo approccio, orientandosi alla protezione delle infrastrutture critiche industriali.



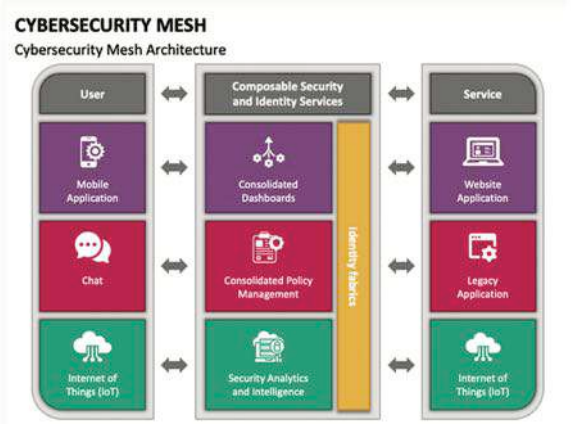


Fig.1A e 1B – Architetture MESH - Fonte Gartner 2025

BIO

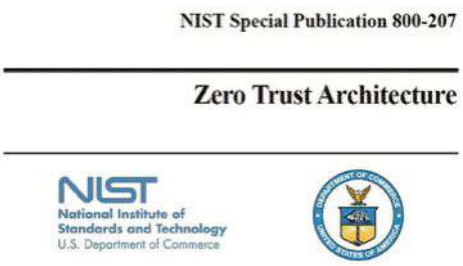
Francesco Corona è ricercatore e docente di Cyber Intelligence, già direttore del master di Hacking e Ingegneria della Sicurezza presso Link Campus University; è stato docente a contratto per 11 anni presso la Facoltà di Ingegneria Gestionale di Roma2 Tor Vergata, Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca nel campo dell'Intelligenza Artificiale e delle Reti Neurali per conto del CNR-IASI di Roma. Svolge attività di ricerca e sviluppo in svariati settori e in particolare in quello della Cybersecurity per conto di primari players nazionali e internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'Innovazione e il premio ICT Confindustria. f.corona@unilink.it

Nell'evoluzione della sicurezza informatica, due concetti fondamentali meritano la giusta attenzione:

A) la "Cyber Security Mesh Architecture"[B005] creata da Gartner.

B) lo Zero-Trust Framework di NIST-CISA e Forrester.

Entrambi si distinguono come elementi rivoluzionari nel settore OT/CPS e come vedremo sono tra loro correlabili. Questi due approcci, nel loro insieme, consentono alle organizzazioni di rafforzare i propri ambienti contro le minacce in modo più efficiente ed efficace, rispetto ai tradizionali modelli di sicurezza perimetrale. Quest'anno più che mai le normative sulla sicurezza OT hanno ridefinito la sicurezza informatica per le reti energetiche, la produzione e le infrastrutture critiche. Le organizzazioni dovranno districarsi tra le complessità degli standard di sicurezza informatica, sia statunitensi sia europei: dal modello Zero Trust del NIST al Cyber Resilience Act europeo. Questo studio fornisce spunti di riflessione e best practice per la sicurezza informatica industriale per aiutare le organizzazioni a proteggere i propri asset e a raggiungere le conformità.


NIST Special Publication 800-207

Zero Trust Architecture

NIST National Institute of Standards and Technology U.S. Department of Commerce

Le **Specifiche Zero Trust secondo il NIST** sono descritte principalmente nella pubblicazione NIST SP 800-207[B004], che definisce l'architettura Zero Trust come un insieme di principi guida piuttosto che tecnologie specifiche. Ecco i punti chiave:

1 Il modello si basa sul principio che nessuna entità (utente, dispositivo, rete) debba essere implicitamente attendibile, sia all'interno che all'esterno del perimetro aziendale.

2 Si richiede un'autenticazione e autorizzazione continua, basata sul rischio, per ogni accesso a risorse aziendali.

3 Il framework promuove il concetto di "privilegio minimo", ovvero concedere agli utenti solo i permessi strettamente necessari.

4 Includere la microsegmentazione della rete e un monitoraggio continuo dello stato degli utenti, dispositivi e attività per prevenire movimenti laterali delle minacce.

5 È raccomandato un approccio multidimensionale di sicurezza con più livelli e controlli.

6 Deve applicarsi ad ambienti multicloud, ibridi e con forza lavoro distribuita.

Altre pubblicazioni come NIST SP 1800-35B offrono indicazioni pratiche per l'implementazione del modello. In sintesi, il modello Zero Trust del NIST sposta la difesa dal perimetro statico a un controllo continuo e granulare, basato sulle identità e sul contesto di tutte le richieste di accesso alle risorse aziendali per migliorare la sicurezza complessiva.

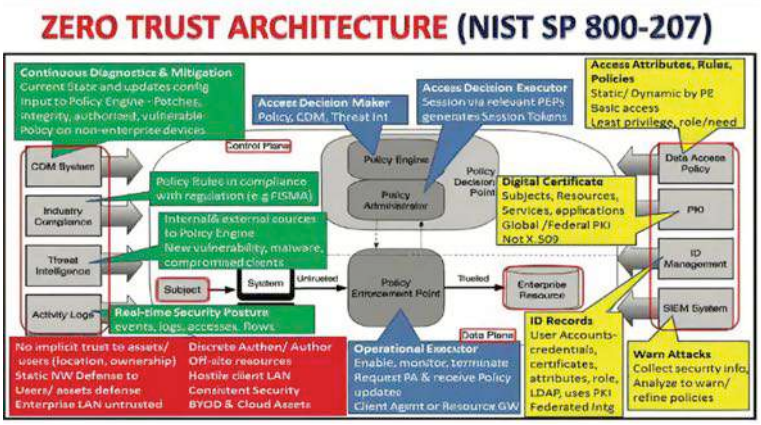
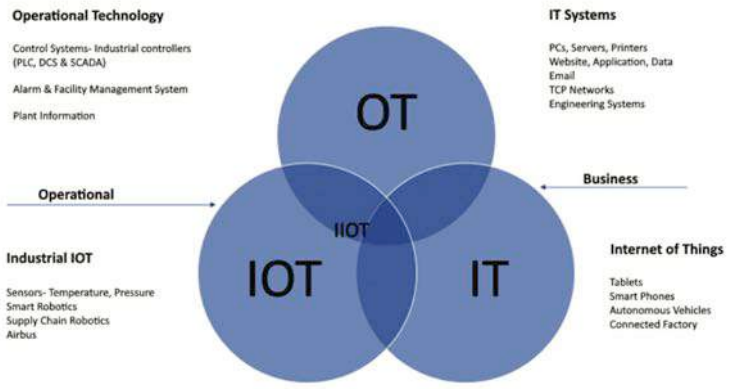


Fig. 2 – Architettura ZERO TRUST NIST 800-207 [B004] [B007] [B008]

Cyber Resilience Act (CRA) [B006] è un regolamento dell'Unione Europea entrato in vigore il 10 dicembre 2024, con l'obiettivo di migliorare la sicurezza informatica e la resilienza cibernetica in Europa. Il CRA introduce requisiti obbligatori di cybersecurity per i prodotti hardware e software con componenti digitali immessi sul mercato europeo, dal design alla manutenzione, garantendo così un livello più alto e coerente di sicurezza per consumatori e imprese. Il CRA nasce per affrontare due problemi chiave: la bassa sicurezza dei prodotti digitali e la carenza di aggiornamenti tempestivi per correggere vulnerabilità note. Mira inoltre a fornire agli utenti informazioni chiare e affidabili, utili per scegliere prodotti con adeguate caratteristiche di cyber-sicurezza e per utilizzarli in modo sicuro. Con questo regolamento si vuole spostare la responsabilità verso i produttori, che devono assicurare la sicurezza durante l'intero ciclo di vita del prodotto. Il regolamento si applica a tutti i prodotti con componenti digitali collegabili direttamente o indirettamente ad un dispositivo di rete, con alcune esclusioni come software open source e prodotti già regolati da altre normative (ad esempio dispositivi medici, aeronautica, automotive). Il CRA



si inserisce nel quadro più ampio delle strategie europee per la sicurezza informatica, come la Direttiva NIS2. Inoltre garantisce la convergenza tra IT, OT e IOT (Internet Of Things) anche in configurazione Industry (IIOT).

Convergenza IT/OT

La convergenza di IT con OT rappresenta l'integrazione dei sistemi informatici con i sistemi tecnologici operativi, consentendo ai sistemi fisici di comunicare con le reti digitali. Ciò si verifica quando i dispositivi IT e OT si interconnettono e interagiscono tra loro all'interno di uno stesso ambiente. Storicamente, le reti OT erano "air-gapped", ovvero isolate fisicamente dalle reti esterne di tipo IP. Queste reti si basavano per lo più su sistemi cosiddetti SCADA, ancora oggi operativi. La interconnettività con le reti IT (IP-based o tramite altri protocolli) consente una migliore gestione degli asset in fase manutentiva.

Gartner definisce questi approcci all'integrazione come "lo stato finale ricercato dalle organizzazioni in cui, invece di separare IT e OT come aree tecnologiche con diverse competenze e responsabilità, si instaura un flusso integrato di processi e informazioni".

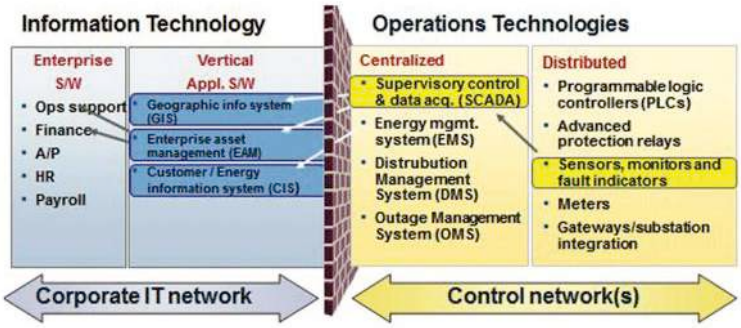


Fig.3 - Fonte SAP [B003]

La nuova frontiera della cybersecurity OT, convergente verso il mondo IT, si basa su un approccio integrato e proattivo che include l'adozione di tecnologie avanzate come l'intelligenza artificiale AI (Artificial Intelligence) e il cloud computing, una maggiore visibilità e gestione degli asset OT, nonché modelli di difesa capaci di affrontare le vulnerabilità specifiche degli ambienti OT, inclusa la forza lavoro ibrida. La sicurezza OT sta dunque evolvendo per affrontare minacce crescenti, come attacchi mirati, ransomware ed esposizione di asset OT a domini malevoli, con un focus sulle capacità di rilevamento avanzato tramite sistemi **Endpoint Detection and Response (EDR)**, adattati agli ambienti OT. Gli esperti sottolineano inoltre che per il futuro è fondamentale un modello graduale e strutturato di implementazione della cybersecurity OT, che consenta di migliorare la sicurezza senza compromettere l'operatività industriale. Una sorta di strategia incrementale sintetizzata nei seguenti tre punti, cui il management dovrà adeguarsi:

1. Analisi tecnica e organizzativa, per l'attribuzione corretta di ruoli e implementazione di policy di sicurezza.
2. Monitoraggio continuo, con azione proattiva per anticipare rischi e mitigare le vulnerabilità.
3. Collaborazione e integrazione tra team IT e team OT, per un approccio sinergico alla sicurezza industriale.

Come dicevamo, avremo un uso crescente di AI per la predizione delle minacce e automazione della risposta agli attacchi, con maggiore integrazione cloud e cybersecurity per la gestione continua e resiliente. Avremo inoltre un rilevamento avanzato e risposta automatica con EDR specifici per ambienti OT specifici, includendo capacità di isolamento di dispositivi compromessi. Infine, assisteremo a una crescente orchestrazione della sicurezza e dell'Edge Computing, per proteggere in tempo reale i nodi periferici critici. La trasformazione digitale rende fondamentale il raggiungimento di un equilibrio tra efficienza operativa e sicurezza avanzata degli ambienti OT, puntando verso sistemi sempre più resilienti e adattativi di fronte alle minacce cyber in continua evoluzione.

Aggiornamenti normativi USA/EU

L'adeguamento alle nuove normative USA/EU sulla sicurezza OT è particolarmente stringente. Con il continuo aumento delle minacce informatiche contro infrastrutture critiche e sistemi industriali, il 2025 segna una svolta nelle normative sulla sicurezza. I governi e organismi di regolamentazione hanno imposto obblighi di sicurezza più severi, volti a proteggere le reti energetiche, gli impianti di produzione e i servizi essenziali dagli attacchi informatici.

Eventi di alto profilo hanno evidenziato gravi lacune nella sicurezza OT, spingendo Stati Uniti e Unione Europea a ripensare profondamente la legislazione in materia. L'estensione di NIST 800-82 di NIS2 e del Cyber Resilience Act garantisce che gli ambienti OT non siano più esenti dagli standard di conformità applicati da tempo alle reti IT. Si segnala inoltre che:

- I sistemi di controllo industriale (ICS) sono obiettivi primari: gli attacchi ransomware e quelli da parte di Stati nazionali contro l'OT sono aumentati.
- L'interconnessione tra IT e OT aumenta il rischio di attacchi informatici laterali sulle reti.
- I governi stanno imponendo misure di reporting e sicurezza più severe: le organizzazioni devono ora implementare il monitoraggio in tempo reale, modelli Zero Trust e una maggiore sicurezza dei fornitori.
- Le aziende dovranno adattarsi rapidamente per evitare sanzioni e proteggere la propria infrastruttura OT.

Aggiornamenti normativi statunitensi alla sicurezza OT

Il panorama normativo, a partire dal 2025, sta introducendo cambiamenti significativi nel modo in cui le organizzazioni industriali e quelle operanti nelle infrastrutture critiche devono proteggere i propri

ambienti OT. Diversi framework chiave definiscono i requisiti di conformità, in particolare nei settori energetico, manifatturiero e in altri settori che fanno affidamento sui sistemi di controllo industriale (ICS):

1 **Cyber Performance Goals (CPG) di CISA 2025 – Rafforzamento delle difese OT**

I più recenti Cyber Performance Goals (CPG) di CISA si concentrano sul miglioramento della segmentazione della rete OT, sull'applicazione dei principi Zero Trust e sul rafforzamento della sicurezza della supply chain. Le organizzazioni devono adottare strategie di sicurezza informatica basate sul rischio per conformarsi a queste linee guida.

2 **Aggiornamenti NIST 800-82 – Best Practice per la Sicurezza Industriale**

Con l'evoluzione delle minacce informatiche, NIST 800-82 [B009] ora include:

- Zero Trust per reti OT, che sposta la sicurezza oltre i modelli basati sul perimetro
- Framework di valutazione del rischio su misura per ambienti ICS
- Linee guida per l'integrazione della sicurezza IT-OT, per ridurre le vulnerabilità

3 **FERC e NERC-CIP – Conformità alla sicurezza informatica nel settore energetico**

Per i fornitori di energia e servizi di pubblica utilità, gli aggiornamenti a NERC-CIP (Critical Infrastructure Protection), richiesti dalla FERC (Federal Energy Regulatory Commission), aumentano i requisiti per:

- Monitoraggio continuo migliorato
- Misure di risposta agli incidenti più rigorose
- Controlli di sicurezza estesi per terze parti.

Aggiornamenti normativi europei alla sicurezza OT

L'UE ha introdotto normative più severe sulla sicurezza OT. Framework chiave come NIS2, il Cyber Resilience Act (CRA) e la normativa ISO/IEC 62443 stanno definendo nuovi standard di conformità per la sicurezza informatica industriale in tutta Europa.

1 **Conformità NIS2 per la sicurezza OT- Ampliamento dell'ambito normativo**

La Direttiva NIS2, che sostituisce la NIS1, amplia significativamente gli obblighi di sicurezza informatica per i settori che dipendono dall'OT. Le principali modifiche includono:

- Copertura settoriale più ampia, che ora include energia, trasporti, produzione e servizi digitali.
- Requisiti di segnalazione degli incidenti più sostanziali, con notifiche di violazione 24 ore su 24.
- Valutazioni obbligatorie del rischio per le reti OT, per prevenire gli attacchi alla Supply Chain.

2 **Cyber Resilience Act (CRA) – Nuove responsabilità dei fornitori per la sicurezza OT**

Il Cyber Resilience Act stabilisce requisiti di sicurezza più rigorosi per i produttori di hardware e software OT. I principali obblighi di conformità includono:

- Sicurezza informatica integrata fin dalla progettazione, per garantire che i dispositivi OT soddisfino gli standard di sicurezza prima dell'implementazione.
- Aggiornamenti software continui e patch di sicurezza, per l'intero ciclo di vita dei prodotti industriali.
- Responsabilità per la sicurezza della supply chain, che richiede ai fornitori di valutare i rischi di terze parti.

3 **Allineamento a ISO/IEC 62443 – Rafforzamento dei framework di sicurezza OT**

Molte normative UE sono allineate allo standard ISO/IEC 62443, riconosciuto a livello globale per la sicurezza informatica industriale. La conformità a questo framework aiuta le aziende a:

- Implementare controlli di sicurezza basati sul rischio per reti ICS e OT
- Soluzioni di accesso remoto sicure in ambienti industriali
- Migliorare le strategie di rilevamento e risposta agli incidenti.

Con le normative USA e UE sempre più stringenti, che impongono una rigorosa sicurezza OT, le aziende devono necessariamente adattare le proprie reti industriali ai requisiti di conformità. Tuttavia, il raggiungimento di questo obiettivo è ulteriormente ostacolato dalla crescente convergenza tra sistemi IT e OT, che introduce nuovi rischi e sfide da affrontare attraverso nuovi modelli avanzati di sicurezza.

Panorama sulle nuove minacce

Le nuove minacce ai sistemi cyber-fisici si stanno evolvendo rapidamente, spingendo i difensori a sviluppare contromisure specifiche per proteggere queste infrastrutture critiche. In particolare avremo:

1 **Attacchi basati su intelligenza artificiale (AI):** Gli aggressori utilizzano l'AI per automatizzare e migliorare la sofisticazione degli attacchi, aumentando la velocità e l'efficacia nel bypassare le difese. L'AI viene usata anche per sfruttare vulnerabilità nei dispositivi IoT e OT, inclusi i rischi di compromissione di sensori e controllori utilizzati nelle infrastrutture critiche, come quelle dell'energia, della sanità e dei trasporti.

2 **Ransomware mirati e attacchi alle supply chain digitali:** I ransomware si focalizzano su settori critici, colpendo software

vulnerabili usati per gestire infrastrutture fisiche e digitali, causando interruzioni e danni estesi.

3 **Interconnessione IoT/IIoT come vettore di attacco:** La crescente diffusione di dispositivi IoT e Industrial IoT nei sistemi cyber-fisici (CPS) amplia la superficie di attacco, poiché questi dispositivi spesso presentano vulnerabilità che possono essere sfruttate per compromettere l'intero sistema.

4 **Cyber-warfare e attacchi infrastrutturali governativi:** I conflitti in scenari geopolitici e nelle zone di influenza economica inducono Stati antagonisti a condurre campagne sempre più sofisticate contro reti energetiche e di telecomunicazioni, mirando a ecosistemi cyber-fisici critici. Inoltre, non si può escludere che possibili fenomeni di escalation in scenari di guerra reale potranno trasformarsi in attacchi cinetici alle infrastrutture cyber-fisiche, in particolare quelle energetiche.

5 **Minacce fisiche collegate a vulnerabilità digitali:** Sistemi di videosorveglianza, controllo accessi e altre tecnologie fisiche integrate possono diventare bersagli attraverso le loro componenti digitali.

Contromisure

Le contromisure per i sistemi cyber-fisici possono essere sintetizzate nei seguenti sette punti:

1 **Architettura integrata di sicurezza cyber-fisica:** implementazione congiunta di misure di sicurezza informatiche (firewall, crittografia, autenticazione avanzata) e fisiche (telecamere, controllo accessi), per proteggere l'intero ecosistema CPS.

2 **Segmentazione e Zero Trust:** segmentazione rigorosa delle reti OT e IT con un modello Zero Trust che limita l'accesso ai soli dispositivi e utenti strettamente autorizzati, riducendo la propagazione di attacchi.

3 **Monitoraggio continuo e risposta in tempo reale:** sistemi di rilevamento e risposta attivi 24/7 basati su AI e machine learning per identificare anomalie e rispondere tempestivamente alle minacce.

4 **Controllo accessi avanzato:** uso di autenticazione multi-fattore (MFA), controllo accessi basato sui ruoli (RBAC) e biometria per garantire

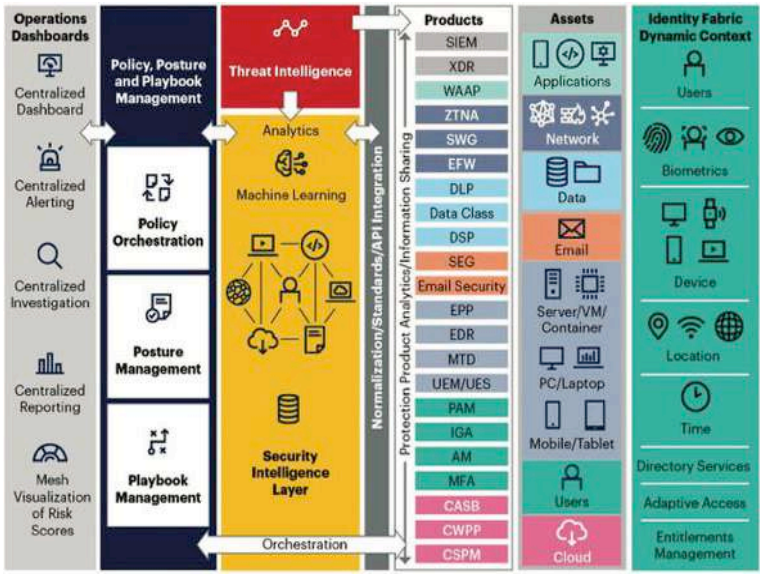


Fig.5 Convergenza MESH e Zero Trust, Fonte Check Point [B001]

l'integrità e la sicurezza sia degli ambienti digitali che fisici.

5 **Piani di resilienza e incident response:** sviluppo di strategie complete per assicurare la continuità operativa e il rapido recupero in caso di attacco o compromissione, con test regolari di piani di emergenza.

6 **Aggiornamenti tempestivi e cyber threat intelligence:** applicazione rapida di patch di sicurezza e uso di intelligence - sia umana che artificiale - sulle minacce, per anticipare e mitigare gli attacchi emergenti.

7 **Collaborazione pubblico-privato:** condivisione di informazioni sulle minacce e coordinamento delle risposte, per migliorare la sicurezza delle infrastrutture critiche a livello nazionale e internazionale.

Queste contromisure mirano a proteggere le risorse, sia digitali sia fisiche, dei sistemi cyber-fisici, rendendo più robuste le infrastrutture critiche contro un panorama di minacce sempre più sofisticato e dinamico. L'architettura integrata Mesh e Zero Trust - cui si rimanda alla bibliografia di riferimento - potrebbe rappresentare una valida soluzione alla sicurezza dei Cyber Physical Systems.

Bibliografia utile

[B001] Cyber Security Mesh Architecture (CSMA) Assessment and Consulting - Check Point Software

[B002] https://channels.theinnovationgroup.it/cybersecurity/convergenza-it-ot-security/

[B003] https://community.sap.com/t5/sap-for-utilities-blogs/the-why-how-and-what-of-it-ot-integration-for-energy-distribution-companies/ba-p/13044558

[B004] https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[B005] Conference-PPTs/Cyber Security Mesh Architecture_Abbas.pdf at master · akudrati/Conference-PPTs · GitHub

[B006] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[B007] https://www.youtube.com/watch?v=o3Or6zgYZx8

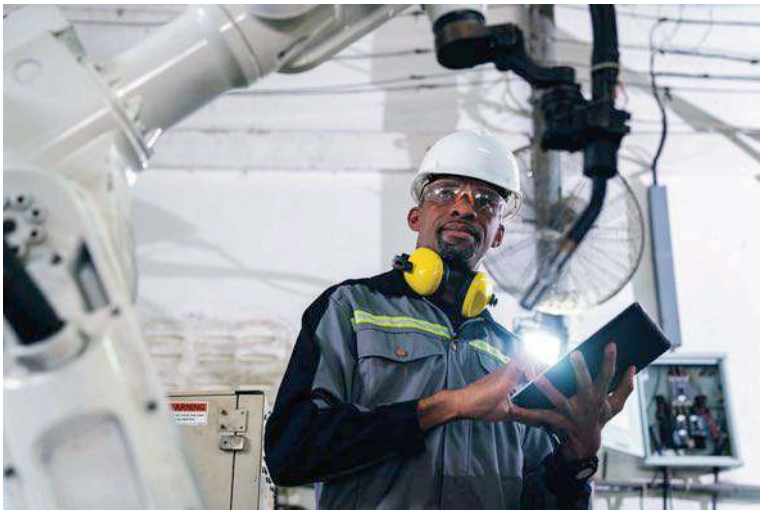
[B008] https://www.researchgate.net/figure/SecHard-Zero-Trust-Orchestrator-Analysis-IX-FUTURE-DIRECTIONS-AND-CONCLUSION_fig4_386070534

[B009] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

[B010] https://blog.tosibox.com/hubfs/Thought%20Leadership%20Articles/Thought%20Leadership%20Article%202%20-%20April%202025.pdf ■

Quando la trasformazione digitale incontra l'industria, la sicurezza non è più un optional.

Autore: Mimmo Salvatore Nisi



Nel pieno della digitalizzazione del tessuto imprenditoriale italiano, c'è un fronte che resta troppo spesso in ombra: quello della sicurezza operativa. Mentre parliamo di cloud, intelligenza artificiale e smart working, le aziende – soprattutto quelle piccole e medie, spesso radicate nel Sud Italia – stanno automatizzando impianti, interconnettendo macchinari, raccogliendo dati in tempo reale. Lo fanno con entusiasmo, talvolta con ingenuità, quasi sempre senza una reale protezione.

L'articolo che segue è un invito a guardare con occhi nuovi il cuore tecnologico delle nostre imprese. A riconoscere che la sicurezza OT non è un lusso da multinazionali, ma una necessità concreta per chiunque voglia innovare senza esporsi a rischi che possono compromettere produzione, reputazione e continuità operativa.

Un racconto autentico, che nasce dall'esperienza sul campo, tra aziende familiari che crescono, territori in fermento e tecnologie che avanzano più in fretta della consapevolezza. Perché oggi, più che mai, non esiste innovazione solida senza sicurezza industriale.

OT Security e cultura della protezione: la sfida silenziosa delle imprese del Sud.

C'è qualcosa di straordinario nelle aziende del Sud Italia. Una forza silenziosa, una tenacia ereditata, un'identità che affonda le radici nella terra, nella tradizione e nell'ingegno. Sono imprese che non nascono nei grattacieli, ma in officine riadattate, nei garage dei padri, nei magazzini trasformati con sudore e visione. Realtà spesso familiari, tramandate di generazione in generazione, che oggi – quasi senza accorgersene – si trovano dentro una rivoluzione: quella digitale.

Macchine che dialogano con il cloud, impianti che producono in modo automatico, software che ottimizzano tempi, scarti, costi. Una trasformazione potente, irreversibile. Eppure, in questo viaggio verso il futuro, manca ancora un compagno fondamentale: la sicurezza. Non solo quella «cyber» – che pure resta centrale – ma soprattutto la sicurezza operativa, quella che protegge le fondamenta industriali, le linee di produzione, i macchinari, i sensori, i sistemi che muovono la manifattura del Sud.

L'automazione avanza, la protezione no

Nel Sud, la sicurezza viene spesso confusa con l'informatica da ufficio. PEC, e-mail, backup, antivirus. Tutto importante, certo. Ma il vero rischio si annida anche altrove: nei capannoni, nei silos, nelle celle frigo, nelle etichettatrici automatiche, nei PLC collegati a internet e dimenticati da chi li ha installati anni fa.

È lì che si decide la continuità di un'azienda. È lì che la qualità del prodotto prende forma. È lì che si vince – o si perde – la competitività. Ma paradossalmente, è proprio lì che la parola "sicurezza" sembra assente. Nessun controllo, nessuna policy, nessuna segmentazione di rete, nessun aggiornamento, nessun allarme.

La verità è semplice quanto preoccupante: la OT Security – ovvero la protezione dei sistemi industriali connessi – è oggi la nuova frontiera delle minacce. E mentre le multinazionali si dotano di SOC e strumenti avanzati, il vero campo di battaglia è tra le PMI del Sud, che si sono digitalizzate con entusiasmo, ma spesso senza difese, senza guide, senza consapevolezza.

Eccellenze produttive, fondamenta fragili

Pensiamo a una cooperativa vinicola che controlla la fermentazione con sistemi SCADA. O a un'industria alimentare che confeziona biscotti con linee robotizzate. Sono eccellenze, vere. Ma basta un ransomware che blocca un PLC, un attacco DoS che manda offline un gateway industriale, per spegnere tutto.

La produzione si ferma. I dati si corrompono. I clienti aspettano. I fornitori premono. E il danno – che parte da una vulnerabilità banale – si propaga come una crepa in una diga.

Non si tratta di disinteresse. Non c'è superficialità. C'è piuttosto una assenza di cultura strategica. La sicurezza viene vista come un fastidio, un tema "da esperti", qualcosa che si risolve con un firewall o un backup. Ma chi lavora ogni giorno accanto ai macchinari sa che un attacco OT non è un rischio virtuale: è una minaccia concreta, devastante, sistemica.

L'illusione della lentezza

In molte conversazioni con imprenditori locali si sente ripetere una convinzione diffusa: "Qui la vita è lenta, qui non succedono certe cose". Ma oggi la lentezza non è più un vantaggio. In un mondo iperconnesso, la lentezza è un'illusione che espone al rischio.

Non servono 500 dipendenti per essere nel mirino di un attacco. Basta una rete non segmentata, un dispositivo connesso a Internet, un protocollo industriale non cifrato. E i criminali digitali non aspettano altro. Cercano le vulnerabilità più comuni, le falle invisibili, i bersagli deboli. E spesso li trovano proprio dove c'è meno rumore: nelle province, nei distretti agroalimentari, nei laboratori artigiani che hanno investito tutto nell'innovazione tecnologica, ma niente nella protezione.

BIO

Mimmo Salvatore Nisi è un Cyber Security Manager con oltre 10 anni di esperienza in ambito IT e sicurezza informatica, con un percorso trasversale tra settore militare, media e pubblica amministrazione. Ha iniziato presso la Marina Militare Italiana (Defense & Space), per poi passare al mondo corporate IT con Intarget Group, dove ha gestito progetti di infrastrutture e sicurezza per brand come (Autogrill, Zegna, Moncler, Brunello Cucinelli, BTicino e Invitalia...). Attualmente guida i progetti di cybersecurity di Studio Amica s.r.l.u., operando secondo i framework ISO/IEC 27001, NIS2 e DORA, con focus su VA/PT, SIEM, EDR, e governance. È certificato CISO (conformità UNI 11506 e UNI 11621-4, schema Accredia), DPO e IT Security EIPASS, Fortinet NSE, Red Hat, Google, Chronicle SIEM e ICTTF. È membro attivo di ASSOCISO, promuove la cultura della resilienza cyber nel Sud Italia, coniugando competenze tecniche e visione strategica con una forte attitudine al problem solving.

Serve un racconto nuovo. E azioni concrete

La sfida, oggi, non è solo tecnica. È narrativa. È culturale. Serve un nuovo modo di parlare di sicurezza: senza gerghi, senza terrorismo psicologico, senza slide incomprensibili. Servono partner locali, professionisti che sappiano entrare nelle imprese, ascoltare, costruire fiducia, accompagnare passo dopo passo verso la protezione del valore.

Perché proteggere un impianto non significa rivoluzionare tutto. Si può iniziare da una mappatura, da un controllo accessi, da una segmentazione della rete tra IT e OT. Piccoli interventi, mirati, proporzionati. Ma che fanno la differenza.

E soprattutto, serve portare la cultura della sicurezza dove non è mai arrivata: negli stabilimenti, tra i responsabili di produzione, tra gli operai specializzati, tra i giovani che tornano al Sud per guidare il cambiamento.

Un futuro che si costruisce partendo dalla protezione

Il Sud ha tutto. Ha talenti artigiani e ingegneri silenziosi, ha aziende familiari che innovano senza clamore, ha territori che producono eccellenza sotto ogni latitudine. Ha la forza di chi è abituato a fare tanto con poco. Ha la creatività di chi trasforma ogni limite in un'opportunità. Ha la visione di una nuova generazione che vuole crescere restando fedele alle proprie radici.

Ma ha anche un bisogno urgente: proteggere ciò che ha costruito. Perché ogni impianto connesso, ogni linea di produzione automatizzata, ogni flusso dati che viaggia nei capannoni agricoli o industriali è anche una superficie di attacco. E ignorarlo significa mettere a rischio non solo i profitti, ma il lavoro, la storia, le persone.

Non possiamo più pensare che la sicurezza sia un tema tecnico, da affidare "a qualcuno". La sicurezza è un bene collettivo, è una responsabilità che riguarda imprenditori, tecnici, consulenti, fornitori, operai. È la rete invisibile che tiene insieme l'efficienza, la fiducia, la continuità.

Il futuro non si difende con un firewall. Si difende con la conoscenza, con la formazione, con la collaborazione tra chi conosce il territorio e chi padroneggia la tecnologia. Si difende parlando di sicurezza in modo semplice, inclusivo, diretto, senza barriere culturali né soglie di accesso.

E allora ripartiamo da qui: dalla consapevolezza. Costruiamo insieme una cultura della sicurezza operativa che parli la lingua delle imprese locali. Che non resti nei convegni, ma entri nei magazzini, nei frantoi, nelle aziende metalmeccaniche, nelle serre, nelle linee di imbottigliamento. Una cultura che protegga non solo i dati, ma i destini.

Perché nel Sud ogni impresa è più di un business: è una storia familiare, una comunità, una speranza che cresce con fatica. E ogni speranza, se non la si protegge, può spegnersi nel silenzio.

Ma oggi, quella protezione è possibile. Ed è il primo passo verso un futuro forte, solido, consapevole. ■

OT Security: Rischi e Opportunità in Sud Africa.

Autore: Corradino Corradi

Nel contesto della trasformazione digitale, le Operational Technologies (OT) stanno assumendo un ruolo sempre più centrale nei processi industriali. L'integrazione tra OT e tecnologie dell'informazione (IT), in particolare attraverso l'Internet delle Cose (IoT), ha aperto nuove opportunità per l'efficienza, la sicurezza e la sostenibilità dei processi industriali.

Le soluzioni OT moderne permettono di automatizzare processi, monitorare in tempo reale lo stato delle apparecchiature e raccogliere dati utili per l'ottimizzazione delle operazioni; l'adozione di queste tecnologie è diventata una realtà anche nei Paesi del cosiddetto Sud del Mondo.

Nonostante i benefici, la digitalizzazione delle infrastrutture OT espone le aziende a nuove minacce. I sistemi OT, spesso basati su tecnologie legacy, non sono stati progettati con la sicurezza informatica come priorità. La loro connessione a reti IT e a Internet li rende vulnerabili ad attacchi ransomware, manipolazione dei controllori logici programmabili (PLC), accessi non autorizzati ai sistemi SCADA e compromissione dei dati sensibili.

Opportunità e rischi in diversi settori industriali nel Sud Africa

Il settore minerario sudafricano è da sempre un elemento fondante dell'economia nazionale - in particolare l'estrazione di carbone, oro, diamanti e platino - e offre diverse opportunità legate all'uso dell'OT.

L'industria mineraria si sta orientando verso soluzioni tecnologiche in grado di migliorare l'efficienza e la sostenibilità ambientale. Le opportunità chiave includono lo sfruttamento di tecnologie come i droni per la sicurezza e le ispezioni, l'automazione per incrementare l'efficienza degli impianti e il monitoraggio digitale tramite sistemi IOT, finalizzato alla riduzione dei costi e alla conformità ambientale.

Le vulnerabilità specifiche dell'OT nel settore minerario includono firmware obsoleto e non aggiornato sui sistemi SCADA, autenticazione debole o assente, mancanza di segmentazione di rete tra IT e OT, e insufficiente

BIO

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

monitoraggio degli eventi di sicurezza informatica. Queste debolezze possono essere sfruttate per interrompere le operazioni (DoS), manipolare dati ambientali o causare danni fisici alle infrastrutture.

Nel 2024, diverse aziende minerarie hanno subito attacchi informatici, partiti dai sistemi IT ma con impatto anche su apparati OT.

Utility ed Energia

La convergenza tra IT e OT ha aumentato le vulnerabilità delle infrastrutture critiche nazionali del Sud Africa come le reti elettriche, le raffinerie e i sistemi di trasporto energetici.

Un recente attacco DDoS ha causato un sovraccarico della rete di una delle principali centrali elettriche del Sud Africa, bloccandone in parte il funzionamento.

Alcune "utility" nazionali hanno subito il furto di credenziali. Gli hacker, tramite le credenziali rubate, hanno ottenuto un accesso non autorizzato a sistemi remoti non protetti, sfruttando software obsoleti e non aggiornati. Questo ha permesso loro di manipolare i controllori logici programmabili (PLC), limitando o bloccando l'erogazione del servizio.

Sanità Digitale

La sanità connessa (IoT sanitario) sta rivoluzionando l'accesso alle cure in Africa, permettendo il monitoraggio remoto dei pazienti - si pensi agli abitanti di zone remote nella foresta o nelle zone semi-desertiche - e la gestione intelligente delle risorse ospedaliere. Tuttavia, la mancanza di infrastrutture di sicurezza adeguate rende il settore sanitario sudafricano vulnerabile e vittima di attacchi informatici.

Svariate strutture ospedaliere sudafricane sono state colpite da attacchi ransomware – con scenari e tecniche di hacking molto simili a quelle utilizzate per attaccare il sistema sanitario nazionale italiano - che hanno bloccato l'accesso ai dati dei pazienti e hanno interrotto i servizi essenziali come il pronto soccorso e la radioterapia. Sono inoltre in crescita gli attacchi hacker che prendono di mira le strutture sanitarie del Sud Africa, sia pubbliche che private, con l'obiettivo di rubare dati sensibili, come le cartelle cliniche, che possono essere venduti nel dark web a prezzi elevati. Questi dati includono informazioni finanziarie, codici fiscali e dettagli intimi sulle patologie delle persone.

Strategie di Mitigazione

Per affrontare queste sfide, le aziende devono adottare un approccio olistico alla sicurezza OT (incluse le componenti IoT), che comprenda le seguenti attività:

- **Valutazioni di rischio specifiche per OT**

È fondamentale condurre analisi dettagliate che considerino le peculiarità dei sistemi OT, come la loro criticità operativa e la scarsa tolleranza ai "down-time". Queste valutazioni devono includere anche la mappatura dei dispositivi OT e IoT, nonché la classificazione dei dati generati, al fine di identificare le aree più vulnerabili.

- **Segmentazione delle reti e controllo degli accessi**

La separazione tra reti IT e OT riduce la possibilità che un attacco informatico si propaghi tra ambienti diversi. È essenziale implementare politiche di accesso basate su ruoli e privilegi minimi (principi del *"need to know", "least privilege" e "segregation of duties"*), utilizzando firewall industriali e rete dati dedicate.

- **Aggiornamento continuo dei firmware e delle patch di sicurezza**

I dispositivi OT e IoT devono essere monitorati per individuare vulnerabilità note e aggiornati regolarmente, anche se operano in ambienti "isolati". È utile adottare sistemi di gestione centralizzata degli aggiornamenti *(centralized software update, patch management)* per garantire coerenza e tempestività.

- **Formazione del personale su pratiche di cybersecurity**

Gli operatori OT devono essere sensibilizzati sui rischi informatici e formati per riconoscere comportamenti sospetti e phishing. La formazione deve essere continua e adattata ai ruoli specifici, includendo simulazioni di incidenti e scenari reali.

- **Implementazione di sistemi di rilevamento e risposta agli incidenti**

Le soluzioni SOAR/SIEM e IDS/IPS devono essere integrate anche nei contesti OT, con capacità di analisi "ad-hoc" dei log industriali (che utilizzano protocolli proprietari e non basati su TCP/IP). I piani di "security incident management" e "business continuity" devono includere la gestione di incidenti OT e il ripristino sicuro delle operazioni OT.

- **Collaborazione con enti pubblici e privati per la condivisione di intelligence sulle minacce**

La partecipazione a gruppi di lavoro settoriali e a tavoli tra esperti di sicurezza IT/OT security consente di condividere le "best practice" e mettere a fattor comune la "lesson learned" post incidente, aumentando la consapevolezza sulle minacce. In Sudafrica, iniziative come il CSIR (Information and Cybersecurity Research Centre) e il C3SA (Cybersecurity Capacity Centre for Southern Africa) promuovono la cooperazione tra industria, governo e mondo accademico.

In conclusione, la sicurezza dell'OT rappresenta una sfida cruciale per il futuro dell'industria sudafricana in numerosi settori. Solo attraverso un approccio proattivo e collaborativo sarà possibile garantire la protezione dei sistemi OT, componenti fondamentali per il funzionamento della gran parte delle infrastrutture critiche nazionali.

PS – In allegato, un interessante confronto sulle ripartizioni dei rischi tra Italia a e Sudafrica, basato sull'Allianz Risk Barometer 2025. La maggior parte degli incidenti relativi all'OT rientrano in tre categorie: cyber incident, business interruption e blackout delle infrastrutture critiche. ■

Top 10 risks in South Africa

Source: Allianz Commercial. Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 206. Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2024 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	44%	*2 (39%)*	↑
2	Business interruption *(incl. supply chain disruption)*	33%	*3 (35%)*	↑
3	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	26%	*4 (26%)*	↑
4	Critical infrastructure blackouts *(e.g., power disruption)* or failures *(e.g., aging dams, bridges, rail tracks)*	24%	*1 (40%)*	↓
5	Changes in legislation and regulation *(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)*	22%	*10 (10%)*	↑
6	Climate change *(e.g., physical, operational and financial risks as a result of global warming)*	21%	*7 (18%)*	↑
7	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)*	16%	*6 (20%)*	↓
8	Fire, explosion[1]	12%	*8 (14%)*	→
9	Shortage of skilled workforce	12%	NEW	↑
10	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	11%	NEW	↑

1 Fire, explosion ranks higher than shortage of skilled workforce based on the actual number of responses.

Top 10 risks in Italy

Source: Allianz Commercial. Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 128. Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2024 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	55%	*1 (40%)*	→
2	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	44%	*4 (26%)*	↑
3	Business interruption *(incl. supply chain disruption)*	34%	*1 (40%)*	↓
4	Climate change *(e.g., physical, operational and financial risks as a result of global warming)*	27%	*3 (33%)*	↓
5	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)*	20%	*5 (21%)*	→
6	Changes in legislation and regulation *(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)*	16%	NEW	↑
7	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*	15%	*7 (17%)*	→
8	Critical infrastructure blackouts *(e.g., power disruption)* or failures *(e.g., aging dams, bridges, rail tracks)*	13%	NEW	↑
9	New technologies *(e.g., risk impact of artificial intelligence, connected / autonomous machines)*	10%	NEW	↑
10	Fire, explosion	9%	NEW	↑

Allianz Risk Barometer 2025

https://www.itweb.co.za/article/cyber-crime-threatening-mining-safety-how-to-stay-protected
https://www.mining-technology.com/features/cyber-threats-in-mining-the-hidden-cost-of-digitalisation/
https://mg.co.za/thought-leader/2025-02-16-cybersecurity-is-crucial-in-modernising-south-african-mining/
https://www.investec.com/en_za/focus/economy/transnet-cyberattack-could-have-catastrophic-consequences.html
South African private hospital systems still down after cyberattack – MyBroadband
Critical infrastructure blackouts & cyber top threats in SA as energy & Nat Cat risks rise | EBnet
https://www.hsfkramer.com/notes/africa/2023-08/high-profile-cyberattacks-increase-emphasis-upon-cyber-resilience-in-south-africas-energy-sector
Cyberattacks on energy infrastructure in South Africa ramped up
https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
https://www.csir.co.za/
https://c3sa.uct.ac.za/

Nuova disciplina NIS. I principi di proporzionalità e gradualità.

Autore: Prefetto Milena Antonella Rizzi

I principi di proporzionalità e di gradualità, come declinati nella direttiva NIS e nel decreto di recepimento, costituiscono l'asse portante del disegno attuativo della nuova disciplina NIS elaborato dall'Agenzia; principi che – come è stato sottolineato in più occasioni – permettono di interpretare la normativa non come mera imposizione burocratica, ma piuttosto come una forma di accompagnamento verso la compliance.

Ciò in quanto, l'obiettivo del decreto NIS è garantire un livello elevato di sicurezza informatica in ambito nazionale contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea in modo da migliorare il funzionamento del mercato interno. Per raggiungere questo obiettivo, il decreto stabilisce, tra le varie disposizioni, una serie di obblighi per gli organi di amministrazione e direttivi dei soggetti NIS, relativi alla gestione dei rischi per la sicurezza informatica e alle notifiche di incidente.

I soggetti oggetto del decreto sono numerosissimi, ad oggi sono registrati sulla piattaforma oltre

20.000 organizzazioni, afferiscono a molteplici settori di attività e sono caratterizzati da una vasta eterogeneità, anche in termini di livello di maturità in termini di cybersecurity.

Imporre "tutto e subito" potrebbe mettere in seria difficoltà questi soggetti, soprattutto quelli che per la prima volta sono oggetto di normative in materia di cybersicurezza. Si correrebbe il rischio di emanare una serie di *grida di manzoniana memoria* che non sarebbero utili allo scopo prefissato dal decreto e che si tradurrebbero in una mera imposizione burocratica.

Alla luce di queste considerazioni, si è ravvisata l'esigenza di definire gli obblighi, e il relativo percorso di implementazione, in accordo a principi di proporzionalità (nel definire gli obblighi) e gradualità (nel definire il percorso di implementazione).

L'art. 31 del decreto ("Proporzionalità e gradualità degli obblighi") risponde proprio a questa esigenza prevedendo che l'ACN stabilisca:

- **obblighi proporzionati** tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico;
- **termini, modalità, specifiche e tempi graduali di implementazione degli obblighi** di cui al comma 1, secondo le modalità di cui all'art. 40, co. 5, anche differenziandoli in relazione: a) alle categorie di rilevanza di cui all'art. 30, co. 2, delle attività e dei servizi che i sistemi informativi e di rete supportano, svolgono o erogano; b) al settore, al sottosettore e alla tipologia di soggetto, tenendo conto del grado di maturità iniziale nell'ambito della sicurezza informatica; c) all'individuazione del soggetto quale essenziale o importante.

BIO

Prefetto Milena Antonella Rizzi - Capo Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale (ACN). Laureata in Giurisprudenza con lode, vanta una solida esperienza nella regolamentazione e nell'applicazione delle normative sulla sicurezza digitale. Guida l'attuazione della Direttiva NIS2, promuovendo la resilienza cyber del Paese attraverso regolamentazione, governance e collaborazione pubblico-privato. Ha partecipato come relatrice a importanti conferenze nazionali e internazionali su cybersicurezza e protezione dei dati, contribuendo alla definizione di linee guida strategiche per la sicurezza digitale.

Il *principio di gradualità* ha orientato la definizione del percorso di implementazione degli obblighi.

È stata infatti prevista una fase di **prima applicazione** (art. 42 del decreto NIS) in cui sono stabilite le cosiddette **specifiche di base** ossia le *misure di sicurezza* che i soggetti devono adottare e gli *incidenti significativi* di base che i soggetti devono notificare in questa prima fase.

La *determina 164179 del 14 aprile 2025* del DG dell'ACN stabilisce tali specifiche di base mediante quattro allegati tecnici *(Allegati 1 e 2; misure di sicurezza di base rispettivamente per i soggetti importanti ed essenziali, Allegati 3 e 4: incidenti significativi di base rispettivamente per i soggetti importanti ed essenziali)* prevedendo 18 mesi per l'adozione delle misure di sicurezza di base e di 9 mesi per l'adempimento dell'obbligo di notifica degli incidenti significativi.

L'obiettivo di questa fase è quello di creare un livello comune *di base* tra tutti i soggetti in termini di sicurezza informatica. Sono state pertanto definite quelle misure di sicurezza (come, ad esempio, l'inventario dell'hardware e del software o la realizzazione di backup) che permettono di assicurare un tale livello comune di base.

A partire dal prossimo anno si entrerà invece nella *fase a regime* in cui l'Agenzia (presumibilmente nel mese di aprile) stabilirà le **specifiche avanzate** (il nome potrebbe variare) con misure di sicurezza avanzate e che potranno riguardare anche obblighi a livello settoriale. Le *specifiche avanzate* potranno inoltre prevedere tempistiche differenti a seconda della **categoria di rilevanza** delle attività e dei servizi dei soggetti NIS. Sempre a partire dal prossimo anno, i soggetti NIS (ai sensi dell'articolo 30 del decreto NIS) dovranno infatti provvedere all'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi che i sistemi informativi e di rete supportano, svolgono o erogano.

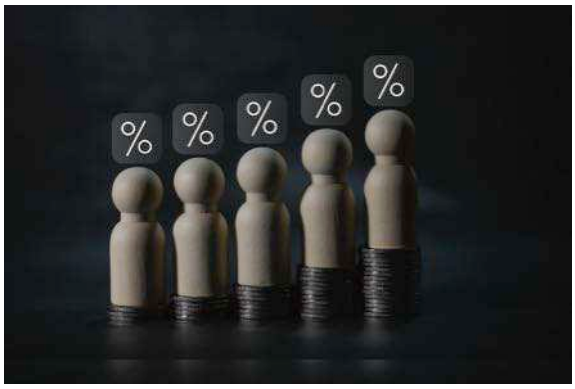
Il principio di gradualità è stato pertanto declinato introducendo un percorso realistico nell'implementazione degli obblighi che possa essere attuato da tutte le organizzazioni, anche quelle che si affacciano per la prima volta al tema della conformità alla normativa cyber.

Principio di proporzionalità

Il *principio di proporzionalità* ha orientato la definizione delle specifiche di base (misure di sicurezza e tipologie di incidenti) che sono state sviluppate tenendo conto del grado di esposizione dei soggetti ai rischi, delle loro dimensioni dei soggetti e della probabilità che si verifichino incidenti.

Nello specifico si è proceduto a differenziare le misure di sicurezza tra soggetti importanti ed essenziali e in particolare prevedendo per questi ultimi misure di sicurezza (6) e requisiti aggiuntivi (29).

Inoltre, i requisiti delle misure di sicurezza sono stati formulati in considerazione del differente grado di esposizione al rischio che caratterizza ogni sistema informativo e di rete. Nello specifico i requisiti di maggiore complessità delle misure di sicurezza sono stati formulati prevedendo le seguenti clausole: *per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete.*



Il principio di proporzionalità orienterà inoltre la definizione delle **specifiche avanzate** che potranno essere proporzionate alle categorie di rilevanza delle attività e dei servizi dei soggetti NIS. Se, ad esempio, saranno definite tre categorie di rilevanza per i servizi e le attività *(ordinari, critici, altamente critici)*, potranno essere definite misure di sicurezza di *livello base* per i sistemi informativi e di rete relativi ad attività e servizi *ordinari*, misure di sicurezza di *livello intermedio* per i sistemi informativi e di rete relativi ad attività e servizi *critici* e misure di sicurezza di *livello elevato* per i sistemi informativi e di rete relativi ad attività e servizi *altamente critici*.

I principi di proporzionalità e gradualità hanno orientato la strategia dell'ACN nell'attuazione della normativa NIS2 per disegnare un percorso per l'attuazione degli obblighi che ha come obiettivo un livello elevato di sicurezza informatica.

L'equilibrio tra la funzione di supporto ed i poteri di vigilanza ed esecuzione dell'Agenzia si fonda su una presenza costante di ACN a fianco delle organizzazioni.

L'ambizione di ACN è di rappresentare una sorta di *copilota* per le organizzazioni durante questo percorso:

- indicando la strada da percorrere (ad esempio tramite la pubblicazione di *linee guida*);
- verificando che sia quella corretta (l'art. 35 e l'art. 36 del decreto disciplinano rispettivamente le attività di monitoraggio e le verifiche e ispezioni);
- richiedendo le eventuali correzioni lungo la rotta che dovessero risultare necessarie (l'art. 37 prevede che l'ACN possa *intimare* ai soggetti una serie di misure di esecuzione quali, ad esempio, l'attuazione di istruzioni vincolanti).

In vista dell'implementazione di obblighi sostanziali come, ad esempio, quello di adozione delle misure di sicurezza, il principio di gradualità costituisce quindi la precondizione per porre in essere un percorso realistico di adeguamento progressivo, capace di portare tutti i soggetti – anche quelli meno strutturati o, al contrario, le organizzazioni con strutture complesse come le c.d. imprese collegate (holding) – a un livello di compliance effettiva. ■

Da informazione a trasformazione: Cyber Human Posture.

Autore: Veronica Patron

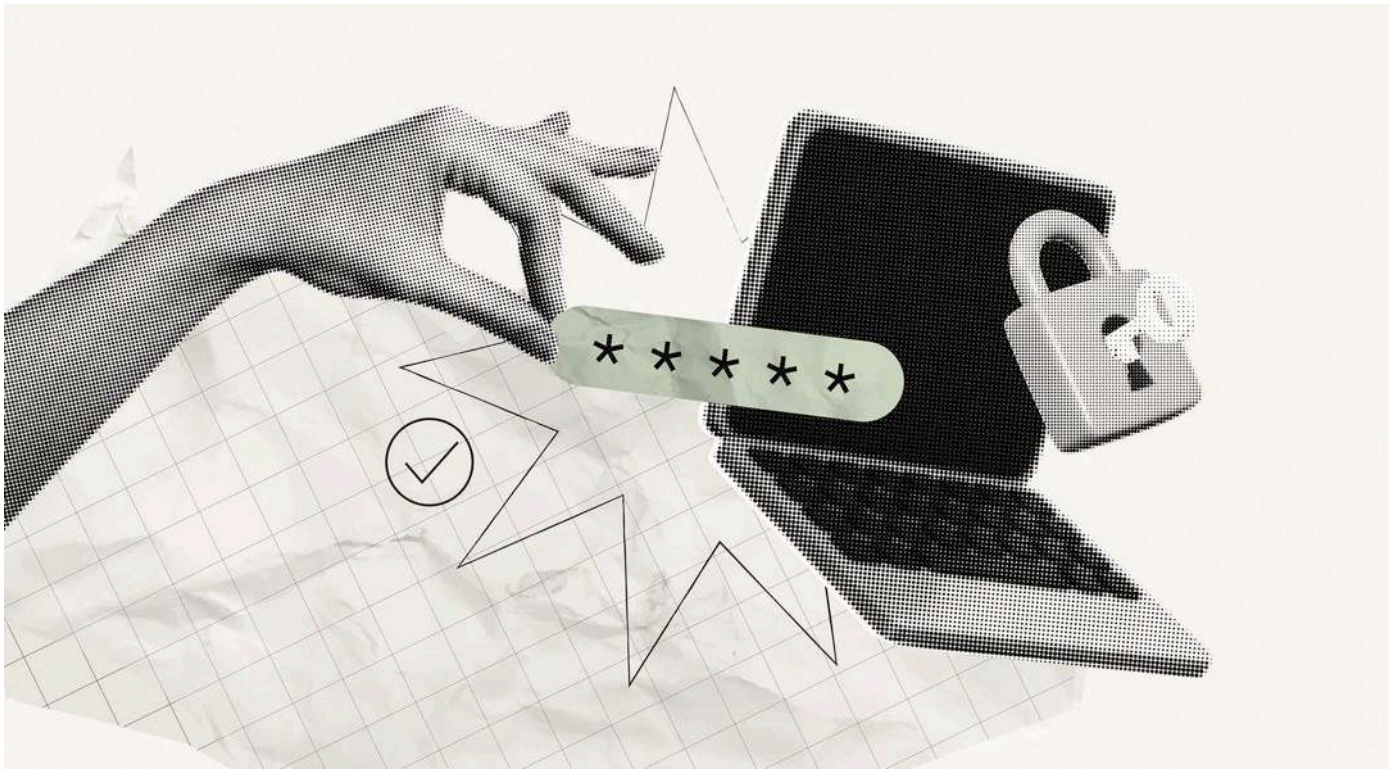
Un nuovo paradigma per la sicurezza digitale

La cybersecurity evolve di giorno in giorno. Le tecnologie diventano sempre più sofisticate, i sistemi di difesa più intelligenti, le soluzioni capaci di intercettare minacce complesse in tempi ridottissimi. Eppure, i dati raccontano una verità che non possiamo ignorare: la maggior parte degli incidenti informatici non nasce da vulnerabilità dei sistemi, ma da comportamenti umani.

Secondo i principali report di settore, oltre l'80% delle violazioni ha origine da errori, disattenzioni o scelte inconsapevoli degli utenti. Basta un clic su un link malevolo, una password troppo semplice o la mancata segnalazione di un'anomalia per aprire la strada ad attacchi critici.

Oggi la sicurezza informatica rappresenta una sfida con una forte componente culturale oltre che tecnologica. Il rischio più grande non riguarda più la possibilità di un attacco, ma la capacità delle persone di reagire in modo consapevole quando accadrà.

Ed è proprio qui che la Cyber Human Posture fa la differenza: un approccio innovativo che supera la logica dell'awareness per accompagnare le persone in un autentico percorso di trasformazione digitale e comportamentale.



Perché la Cyber Human Posture è il passo successivo all'awareness

La Cyber Human Posture analizza e misura la cosiddetta "postura digitale" delle persone, ovvero il modo in cui percepiscono, reagiscono e agiscono di fronte ai rischi informatici. Non si limita quindi a valutare le competenze tecniche, ma prende in considerazione fattori emotivi, cognitivi e sociali che influenzano le decisioni quotidiane.

Gli elementi che modellano la postura digitale sono molteplici:

- **Fattori emotivi:** stress, urgenza e pressione lavorativa aumentano il rischio di errore, riducendo la capacità di valutazione.
- **Percezione soggettiva del rischio:** chi non ha mai vissuto un attacco tende a sottovalutarlo, mentre chi lo ha sperimentato sviluppa maggiore attenzione.
- **Influenza sociale:** i comportamenti di colleghi e superiori diventano modelli da imitare. Se in un team si condivide la password o non si segnalano incidenti, i nuovi arrivati tenderanno a fare lo stesso.
- **Pregiudizi cognitivi:** bias come l'ottimismo irrealistico ("a me non succederà") o l'euristica della disponibilità (basarsi solo su ricordi immediati) portano a sottovalutare i pericoli reali.

Studiare la postura digitale significa, dunque, andare oltre la tecnica e comprendere come emozioni, contesti e dinamiche sociali influenzino le scelte degli utenti.

Analisi, misurazione e trasformazione

Il percorso parte da tre azioni chiave: analisi, misurazione e mitigazione. Attraverso simulazioni di phishing, smishing, vishing, test pratici e questionari comportamentali viene calcolato l'**Human Risk Index**, un indicatore che misura il livello di rischio umano a livello individuale e collettivo.

Questo approccio permette di analizzare la popolazione aziendale, identificare i gruppi più esposti al rischio e concentrare su di essi gli interventi formativi più efficaci. Gli obiettivi sono due:

- Agire in modo concreto sui comportamenti a rischio, come il clic su link malevoli, l'inserimento improprio di credenziali o la mancata segnalazione di attività sospette.
- Creare un cambiamento culturale, trasformando il fattore umano da vulnerabilità a risorsa attiva, attraverso strategie di mitigazione personalizzate basate su contenuti formativi e leve psicologiche.

BIO

Veronica Patron è psicologa specializzata in psicologia cognitiva e comportamentale, con una formazione accademica presso l'Università degli Studi di Padova, dove ha conseguito la laurea in Psicologia. Ha successivamente approfondito le tematiche di behavioral design, scienze decisionalie psicologia applicata alla cybersecurity, partecipando a corsi di alta formazione e programmi internazionali. Nel 2022 ha co-fondato Security Mind, piattaforma focalizzata sull'Human Risk Management in ambito cyber, dove ricopre il ruolo di Responsabile della Strategia Comportamentale. All'interno del team multidisciplinare, Veronica guida la progettazione di percorsi formativi basati su modelli scientifici, con l'obiettivo di trasformare i comportamenti a rischio in abitudini sicure e sostenibili. Partecipa regolarmente a conferenze e seminari sul tema del fattore umano nella sicurezza informatica, ed è autrice di articoli e contenuti divulgativi sul ruolo della psicologia nella prevenzione delle minacce digitali.

La Cyber Human Posture è dinamica e in continua evoluzione: cambia nel tempo, modellata dalle esperienze e dal contesto. Un reparto che partecipa a simulazioni e percorsi formativi mirati sviluppa gradualmente una postura più matura, elevando il livello di attenzione collettivo.

Gli obiettivi principali del programma possono essere sintetizzati in cinque punti:

1. **Mappare la postura digitale delle persone:** Il primo passo consiste nel fotografare la situazione attuale, individuando come i dipendenti percepiscono e affrontano i rischi informatici. Oltre a verificare le competenze tecniche, vengono anche analizzati gli atteggiamenti, le abitudini e i livelli di consapevolezza.
2. **Segmentare la popolazione in base a ruolo, funzione e livello di esposizione:** All'interno di ogni organizzazione, i livelli di esposizione al rischio variano in base a ruolo, funzione e responsabilità. Segmentare la popolazione aziendale consente di creare cluster omogenei e di progettare percorsi formativi calibrati sulle specifiche esigenze di ciascun gruppo.
3. **Definire strategie di mitigazione personalizzate:** Una volta individuate le aree di criticità, sarà possibile sviluppare interventi mirati. Le strategie di mitigazione vanno oltre la formazione classica: includono micro-contenuti mirati, rinforzi comportamentali, reminder

periodici. L'obiettivo è fornire a ciascun gruppo le leve più efficaci per ridurre i comportamenti a rischio, evitando approcci generici che risultano poco incisivi.

4 **Favorire un cambiamento culturale verso responsabilità e consapevolezza:** La vera sfida è trasformare la percezione della sicurezza da obbligo imposto a responsabilità condivisa. Per riuscirci è necessario agire sulla cultura aziendale, stimolando la collaborazione e premiando i comportamenti virtuosi. Un contesto in cui le persone si sentono coinvolte e parte attiva nella difesa digitale favorisce il consolidarsi di nuove abitudini: segnalare un'anomalia diventerà un gesto naturale invece di un compito aggiuntivo.

5 **Costruire percorsi formativi dinamici, capaci di adattarsi all'evoluzione dei comportamenti:** le campagne formative verranno adattate sulla base dei risultati ottenuti. In questo modo la formazione diventerà un processo continuo e dinamico, capace di sostenere nel tempo il cambiamento culturale.

Le componenti del programma

1. Cyber Awareness

Elemento cardine di questo approccio è la piattaforma Security Mind Awareness, concepita per andare oltre la logica della formazione tradizionale, un ecosistema integrato che supporta l'organizzazione in un processo strutturato, graduale e misurabile di trasformazione culturale.

I moduli sono brevi, progressivi e pensati per essere accessibili a tutti, anche a chi non possiede competenze tecniche. L'obiettivo è rendere la sicurezza parte della quotidianità, trasformandola da semplice obbligo formativo a vera e propria abitudine condivisa. La piattaforma mette a disposizione una reportistica avanzata che consente di monitorare i progressi e ottimizzare le strategie formative in tempo reale.

2. Cyber Phishing Simulation

Allenamenti pratici attraverso campagne di phishing e scenari realistici. L'obiettivo è trasformare un errore in un'occasione educativa immediata. KPI come tasso di clic, credenziali inserite o tempi di segnalazione permettono di misurare i progressi.

3. Cyber Vishing Simulation

Nel panorama delle minacce digitali, le tecniche di vishing (voice phishing) rappresentano una delle forme più insidiose di ingegneria sociale. Attraverso telefonate apparentemente legittime, i criminali informatici sfruttano la voce – lo strumento di comunicazione più umano e persuasivo – per ottenere informazioni riservate, indurre azioni indebite o compromettere interi processi aziendali.

La Cyber Vishing Simulation nasce per mettere alla prova e potenziare la capacità delle persone di riconoscere, gestire e segnalare questo tipo di attacco. Si tratta di un'esperienza immersiva che unisce psicologia comportamentale e tecnologia, con l'obiettivo di trasformare ogni chiamata simulata in un momento di apprendimento reale e misurabile.

Attraverso scenari realistici e metriche precise, l'organizzazione può valutare la propria maturità comportamentale, identificare i punti di vulnerabilità e orientare gli interventi formativi dove servono davvero.

4. Cyber Experience

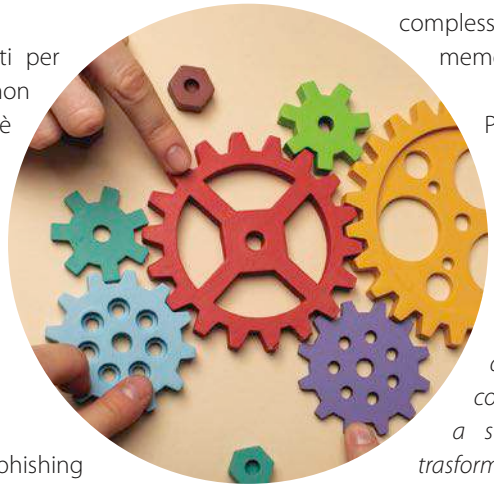
Sessioni live con un Cyber Coach, rivolte ai gruppi con rischio medio-alto, che affrontano i temi psicologici legati alla sicurezza: bias, urgenza, pressione emotiva. Questi momenti diventano spazi di confronto e coaching motivazionale.

Un approccio multidisciplinare che fa la differenza.

Ciò che distingue Security Mind è l'integrazione sinergica di tre ambiti fondamentali – cybersecurity, psicologia comportamentale e comunicazione.

Un'unione unica che trasforma la sicurezza da semplice competenza tecnica a valore culturale condiviso, capace di modellare le abitudini e i comportamenti quotidiani delle persone.

- **Cybersecurity:** la conoscenza tecnica degli attacchi e delle contromisure.
- **Psicologia comportamentale:** l'analisi dei meccanismi decisionali, dei bias cognitivi e delle leve emotive.
- **Comunicazione:** la capacità di tradurre concetti complessi in messaggi semplici, coinvolgenti e memorabili.



Come affermano i fondatori Veronica Patron e Loreno Patron, insieme a Federico Incoronato del Board of Advisors:

"Nel contesto attuale, il principale fattore di rischio per la sicurezza è rappresentato dai comportamenti umani più che dagli aspetti tecnologici. Grazie all'applicazione delle neuroscienze e della psicologia comportamentale, aiutiamo le persone a sviluppare riflessi di autodifesa digitale, trasformando il fattore umano da vulnerabilità a risorsa di protezione attiva". ■

L'orizzonte delle cose intelligenti.

Autore: **Alessandro Curioni**

La casa moderna sta scomparendo. Non nel senso letterale, ovviamente: gli oggetti sono ancora lì, ma arretrano nel nostro campo visivo fino a dissolversi dietro un'icona. La caldaia non è più una scatola rumorosa nel locale tecnico, ma è un riquadro sulla schermata del telefono. Il citofono, il campanello, il termostato, il contatore, l'allarme: tutti presenti, tutti remoti. I nostri figli, in un domani nemmeno tanto lontano, potrebbero passare accanto alla caldaia senza riconoscerla come tale. Sapranno regolare l'acqua calda, ma non sapranno indicare "dov'è" il calore. È un paradosso dell'era smart: più un oggetto è connesso, meno è "presente".

Questa invisibilità ha un prezzo. La relazione fisica, che un tempo imponeva una manutenzione minima - ascoltare un rumore, leggere una spia, girare una valvola - viene sostituita da una relazione testuale e tattile, fatta di scroll, tap, conferme. L'oggetto diventa un servizio; il servizio diventa un'app; l'app diventa la realtà. Nel passaggio, perdiamo non solo manualità ma anche geografia: non sappiamo più "dove" finisca quella funzione. È nel telefono, certo. È nel router, nel cloud del produttore, nel gateway del fornitore di energia, nel firmware di un componente OEM. In questa catena di astrazioni accumuliamo comodità e, insieme, punti ciechi.

La sicurezza di questi sistemi IoT e OT nasce dove nascono tutte le sicurezze: nella comprensibilità del perimetro. Ma il perimetro, oggi, non è la porta del locale caldaia; è la somma di API, credenziali, certificati, reti domestiche, reti industriali, aggiornamenti programmati, ma neppure tanto. Per l'utente, la caldaia è il pulsante "Eco". Per l'attaccante, è una superficie:

BIO

Dopo 15 anni di attività giornalistica, alla fine degli anni Novanta, Alessandro Curioni inizia a occuparsi di nuove tecnologie e nel 2001 si dedica a tempo pieno alle tematiche della sicurezza informatica. Nel 2003, dopo due anni di studio, pubblica per Jackson Libri il volume "Hacker@tack - Guida alla sicurezza informatica". Da questa esperienza nasce, in collaborazione con il Gruppi I.Net (in seguito British Telecom) un programma di corsi di formazione dedicati a quelle tematiche. All'attività di formatore affianca quella di consulente per i clienti del gruppo I.Net, attività che si protrae fino al 2008, anno in cui fonda DI.GI. Academy, azienda specializzata nella formazione e nella consulenza nell'ambito della sicurezza informatica, della quale è azionista e presidente. Negli ultimi quindici anni è stato consulente per primarie aziende nazionali e multinazionali tra le quali Edison S.p.A., Cardif Assicurazioni del Gruppo BNP Paribas, Vittoria Assicurazioni, Pepsico Italia, attività che alterna con quella di formatore (ENI, Poste Italiane, A2A, etc.) e conferenziere. Nel 2015 riprende la sua attività pubblicistica per diverse testate cartacee - tra cui "Il Sole 24 ore" (compresi gli allegati sul tema) - e on line e nel 2016 pubblica, con la casa editrice universitaria Mimesis, il libro "Come pesci nella rete – Guida per non essere le sardine di Internet" dedicato a problemi della sicurezza informatica personale, a cui seguono diversi altri pamphlet di successo ("La privacy vi salverà la vita", "Questa casa non è un hashtag", "CyberWar" etc) mentre con Chiarelettere ha pubblicato nel 2021 il suo primo giallo intitolato "Il giorno del Bianconiglio". Dal 2018 Curioni è anche docente a contratto nel corso di sicurezza dell'informazione per la Cattolica di Milano.

l'app di controllo con permessi larghi; il router lasciato alle impostazioni di fabbrica; l'account condiviso con altri servizi; la connessione del produttore che monitora "per migliorare l'esperienza".

L'oggetto scompare e al suo posto si apre a noi il suo ecosistema, che però non vediamo. E ciò che non vediamo, poco lo controlliamo.

Il risultato è quasi ludico: crediamo di governare perché muoviamo il dito su un'interfaccia che risponde. In realtà governa chi controlla gli strati sotto: firmware, chiavi, logiche di aggiornamento, accessi remoti. A volte basta un certificato scaduto per spegnere, a distanza, il concetto stesso di "casa confortevole". Più spesso basta l'umano medio: riuso delle password, Wi-Fi con nome parlante, app installate "tanto per provare". Ma questa non è una colpa morale: è un fatto biologico.

La mia tesi è semplice: **siamo biologicamente inadeguati** a valutare i rischi del digitale **oltre lo schermo.** Ci siamo evoluti per reagire al visibile, all'udibile, al tangibile: fumo dalla caldaia, odore di gas, vibrazione anomala. Sullo schermo, il pericolo non grida; si presenta come un'icona grigia, una voce di menu, un consenso frettoloso. Il nostro cervello fatica a registrare l'urgenza di una notifica di sicurezza; reagisce invece a ciò che occupa spazio e fa rumore. Non "sentiamo" un token compromesso; "sentiamo" l'acqua che non esce più calda. La cognizione arriva dopo la sensazione.

Nel mondo industriale la storia è nota: l'OT è nato per resistere, non per comunicare; l'IoT è nato per comunicare, non per resistere. L'incontro ha prodotto ambienti ibridi, dove la logica di disponibilità del campo (la caldaia deve scaldare) convive con la logica di esposizione del cloud (il servizio deve "parlare"). Quando la caldaia è un'app, il ciclo di vita dell'oggetto non è il ciclo di vita dei suoi componenti fisici: è il ciclo di vita delle sue dipendenze digitali. Se un fornitore "depreca" un servizio, non si rompe un pezzo: si rompe un legame. Ma noi vediamo solo il pulsante, e lo premiamo più forte.

Questa scomparsa dell'oggetto produce un altro effetto: la perdita del diritto alla verifica. Un tempo, di fronte a un malfunzionamento, si poteva intervenire: staccare l'alimentazione, aprire un pannello, chiamare un tecnico con competenze ben definite. Oggi l'oggetto risponde "errore 503". Da dove? Da chi? L'app consiglia di riprovare più tardi. La consapevolezza si contrae a un universo di schermate; il domicilio tecnico dell'oggetto slitta altrove, in una filiera che non abitiamo e che spesso nemmeno conosciamo.

Si potrebbe obiettare che tutto questo sia un prezzo accettabile per il comfort, l'efficienza, il risparmio energetico. Lo è, se adottiamo un nuovo galateo della presenza: riportare in casa almeno un frammento di realtà

fisica. Un'etichetta chiara, un manuale vero, un punto di disconnessione leggibile, un segnale locale non mediato dal cloud. E sul lato digitale, la traduzione pratica dell'alfabetizzazione: forse un password manager al posto dei promemoria, aggiornamenti automatici senza "magari domani", doppia autenticazione dove conta, reti separate tra oggetti e computer, permessi che scadono come i cibi in frigo. Non è eroismo: è igiene. Ma la pulizia funziona solo se prima riconosciamo il "cosa pulire" e nel caso di specie, non è la caldaia, ma siamo noi. Se non vediamo l'oggetto, dobbiamo vedere di più **noi stessi** mentre lo usiamo: riconoscere che stiamo delegando, che stiamo spostando fiducia fuori da casa, che stiamo scambiando il tatto con il tocco. Ogni volta che la nostra vita materiale diventa una collezione di app, stiamo costruendo una casa con molte porte invisibili. Non possiamo presidiare ciò che non ammettiamo di avere.

Non torneremo indietro: va benissimo così. Ma possiamo procedere in avanti con misura. Rimettiamo qualche vite al suo posto: una valvola vera che chiude davvero, un pannello che racconti lo stato anche senza rete, un registro di ciò che abbiamo autorizzato e che possiamo revocare con un gesto altrettanto semplice. Se riportiamo una minima materialità del controllo, l'oggetto ricompare, e con lui ricompare un pezzo della nostra responsabilità.

Perché l'epoca smart non ci chiede di essere più intelligenti; ci chiede di essere più **presenti.** Se l'oggetto scompare dall'occhio, non deve scomparire dalla portata della mano, perché troppa distanza potrebbe uccidere. ■

L'uomo, anello debole nell'ecosistema della sicurezza.

Autori: Lucio G. Insinga e Alessio Bandini

Il 30 giugno 2025, la software house brasiliana C&M è finita al centro di una clamorosa violazione informatica. La società sviluppa la piattaforma che collega gli istituti finanziari alla Banca Centrale del Brasile, permettendo le transazioni tramite PIX, il sistema di pagamento istantaneo più utilizzato nel Paese.

Secondo le prime ricostruzioni, gli hacker sono riusciti a sottrarre 800 milioni di Reais (circa 140 milioni di dollari) da sei istituti finanziari. L'attacco non è stato frutto di una sofisticata intrusione tecnica, ma di un tradimento interno: un dipendente di C&M avrebbe venduto le proprie credenziali di accesso a un gruppo criminale per appena 2.700 dollari.

Le indagini hanno rivelato che i fondi sono stati trasferiti in poche ore attraverso exchange in Brasile, Argentina e Paraguay, con una parte riciclata in criptovalute tramite broker locali. Il dipendente infedele, João Roque, è stato arrestato, mentre le autorità brasiliane sono alla ricerca dei complici.

Oltre al danno economico, l'episodio accende i riflettori su un tema cruciale: la cybersecurity lungo la supply chain. Non è sufficiente proteggere il proprio perimetro aziendale: occorre considerare anche fornitori, partner e clienti.

La direttiva europea NIS2 (Dlgs 184/2024, Direttiva UE 2022/2055) insiste proprio su questo punto: una catena è solida solo quanto il suo anello più debole. Per questo richiede che ogni attore della filiera adotti misure di sicurezza proporzionate al proprio settore e alle normative di riferimento.

Fra le misure da adottare, l'incidente C&M pone l'accento sul monitoraggio delle attività interne. Tecnologie come User Behaviour Analytics e Data Loss Prevention possono aiutare a individuare comportamenti anomali e a prevenire la fuga di dati sensibili, riducendo il rischio di incidenti come quello che ha colpito C&M.

L'importanza di uno sguardo retrospettivo

La ricostruzione di quanto accaduto dimostra che l'anello debole della catena rimane l'uomo e ciò non solo in un contesto illegale ma anche in quello che riguarda il quotidiano agire.

Ci riferiamo in particolare a tutte quelle leggerezze che compiamo giornalmente e che da un lato, vanificano gli sforzi che gli istituti compiono per rendere più sicuri tutti i passaggi necessari per garantire la sicurezza delle nostre transazioni, dall'altro a causa dell'impostazione giornalistica non contestualizzata, appare perfino che un dato Istituto Bancario sia meno sicuro di un altro. A ben guardare il numero di atti o l'ammontare degli

importi sottratti ad una banca deriva dal fatto che i malviventi in certi periodi prediligono i clienti di quell'Istituto anziché di un altro. Precisiamo infatti che i sistemi informativi dei nostri Istituti oltre a rispettare le più stringenti norme europee in materia di sicurezza come la Direttiva DORA (Digital Operational Resilience Act) che impone requisiti stringenti alle istituzioni finanziarie, sono soggetti a una supervisione ancora più rigorosa da parte della Banca d'Italia e della BCE, che ne testano regolarmente la resilienza attraverso "stress test cyber".

Interessante appare anche l'excursus storico, utile a verificare come il passaggio dai sistemi di sicurezza basati unicamente su sistemi fisici (cassaforte, caveau) - nel tempo resi sicuri da sistemi anti-intrusione comandati a distanza, ecc. - alla ridotta, e in alcuni casi totale, indisponibilità di contanti presso le varie filiali, non abbia coinciso con una riduzione dei reati.

Ciò è dovuto, almeno per l'Italia a precise cause storiche, politiche e culturali.

Nel secolo scorso, i reati contro le Banche avevano finalità specifiche, prevalentemente legate alla lotta armata. Tali reati sono passati dal furto alla rapina, fino ad arrivare perfino al sequestro di persona. Le nuove tecnologie, la videosorveglianza diffusa e un ceto politico consapevole che l'integralismo politico professato dei gruppi armati avrebbe condotto, se tradotto in linea di Governo, a un isolazionismo internazionale, hanno comportato un graduale abbandono di quelle forme di lotta che, in qualche caso, avendo comportato peraltro anche vittime civili, l'opinione pubblica non poteva tollerare.

Per contro sono progressivamente aumentati e non rallentano i reati informatici.

Un nuovo paradigma professionale

Da questa visuale appare dirompente anche il cambio radicale del paradigma professionale.

In passato, mai un'istituzione avrebbe avuto una relazione professionale con un ladro per ricevere consigli o simulare intrusioni e testare la sicurezza dei propri luoghi. Oggi, invece, appare giustificato rivolgersi a una persona "tecnicamente capace", anche se moralmente discussa, per verificare la presenza di punti deboli, bug o punti di intrusione non presidiati nei sistemi.

Anche l'opinione pubblica ha un atteggiamento diverso. In passato, la gravità delle azioni, la pericolosità e il coinvolgimento di dipendenti e comuni cittadini in fatti criminali non potevano che suscitare una condanna senza appello. Oggi, se apprendiamo che un sistema viene violato da un ragazzo, non lo deploriamo: anzi, ne tessiamo le lodi.

L'unico elemento storicamente immutato resta la prudenza, la riservatezza e quel pizzico di diffidenza verso l'altro, lo sconosciuto, che consente di mantenere una certa distanza di sicurezza.

BIO

Lucio G. Insinga, coniuga l'attività di Dottore Commercialista e Revisore Contabile con quella di Business Angel e Advisor. La vocazione aziendalista gli consente di essere uno dei primi cinque Innovation Manager certificati da Cepas. È il primo in Italia ad effettuare un'operazione di aumento di capitale in Bitcoin. È autore di: La Responsabilità sociale. Le PMI alla prova del modello 231, per Plenum Editore (2017), Come finanziare l'impresa. Attori Strumenti e metodi per potenziare la crescita, pubblicato Salvatore Primiceri Editore (2019) . La compliance integrata Plenum Editore (2022). Di imminente pubblicazione il suo quarto testo "Dizionario Finanziario commentato".

BIO

Alessio Bandini è Cybersecurity Specialist, si occupa di Cybersecurity Assessment, con specializzazione in ambito CTI. Fa parte di Incident Response Team e L2 SOC. Proviene dal mondo dello sviluppo software per banche e assicurazioni e dalla progettazione di piattaforme web, con attenzione agli aspetti security-by-design. Si occupa anche di formazione in ambito cybersecurity awareness.

Per saperne approfondire l'argomento, vi invitiamo a consultare le fonti riportate di seguito:

https://cointelegraph.com/news/brazil-central-bank-service-provider-hacked-140-million

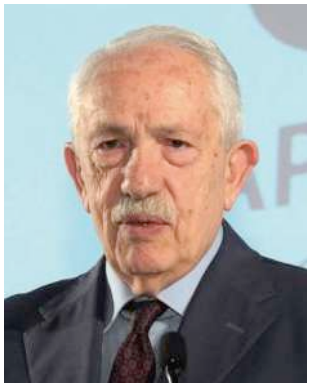
https://en.spaziocrypto.com/hack/140m-heist-at-brazilian-reserve-via-c-m/?utm_source=chatgpt.com

https://www.reuters.com/world/americas/brazilian-tech-services-company-cm-resumes-operations-after-cyberattack-2025-07-03/?utm_source=chatgpt.com

https://apnews.com/article/brazil-hack-cyberattack-bank-5e39633b2ce3a662b90978dcf4647510 ■

La simbiosi uomo - macchina va governata esercitando il pensiero critico.

Intervista VIP a Gian Maria Fara.



Autore: Massimiliano Cannata

La sfida di oggi è trasformare l'accesso al digitale in una strategia di crescita. Il sistema Italia dovrà investire prima di tutto in educazione e in competenze per poter reggere i ritmi del cambiamento. Il salto quantico, di cui parla il Presidente Fara nell'intervista, non riguarda solo i traguardi pur eccezionali della tecno-scienza, perché si è aperta una sfida cognitiva, simbolica, relazionale che dobbiamo prepararci ad affrontare per abitare con consapevolezza la complessità e tornare ad esercitare una cittadinanza attiva e responsabile.

BIO

Gian Maria Fara ha fondato e presiede, dal 1982, l'Eurispes. Nel corso degli anni ha insegnato presso Università di Roma "Sapienza", l'Università di Salerno, l'Università di Teramo, la Scuola Ufficiali Carabinieri di Roma, la LUISS e la LUMSA di Roma. Dal 1999 al 2004 è stato Presidente dell'IPSEMA (Istituto di Previdenza per il Settore Marittimo). Dal 1990 al 2011 è stato membro del Pontificio Consiglio per le Comunicazioni Sociali. È membro del Comitato scientifico della Fondazione Italia-USA, del Comitato scientifico dell'Istituto per l'Europa dell'Accademia delle scienze di Russia, del Comitato scientifico della rivista GNOSIS.

"Il Rapporto delle persone con il digitale" *curato dall'Eurispes analizza un tratto distintivo della contemporaneità. Presidente Fara, che cosa emerge nella vostra indagine?*

L'individuo di oggi vive il digitale in una dimensione omeopatica. Non riusciamo a farne a meno, fa parte di noi. *Il virtuale*, come ha scritto in un celebre saggio che ha anticipato i tempi, il filosofo francese Pierre Levy è una categoria dell'essere. C'è un fattore cruciale che va considerato per capire come si è evoluto il nostro rapporto con gli strumenti *hi-tech*. Mi riferisco allo spartiacque che separa le generazioni prima del Duemila che hanno vissuto in spazi fisici, geometricamente delimitati e definibili e i nati nel terzo millennio, che fin dai primi vagiti si sono mossi in ambienti interconnessi, "ibridi", in cui non è possibile distinguere tra reale e virtuale. Lo scarto che esiste tra questi universi non è solo tecnologico, ma cognitivo, simbolico, relazionale. È cambiata la natura stessa del rapporto uomo - macchina, la simbiosi che stiamo sperimentando nell'uso di strumenti come lo smartphone ha modificato la percezione della nostra identità rispetto alla fluidità dell'ecosistema in cui si matura la nostra personalità e ruolo sociale.

Le conseguenze di quella che appare come una profonda mutazione antropologica hanno spinto molti pensatori a parlare di "fine dell'umano". Stiamo correndo realmente questo rischio?

L'approccio all'analisi del cambiamento deve seguire un metodo razionale, senza cedere a tentazioni di tipo assolutistico. Nel divenire che investe tutti, il valore dell'educazione deve rimanere un punto centrale, se vogliamo attuare una digitalizzazione rispettosa dell'uomo e dei principi di solidarietà ed equità. Il prepotente sviluppo della tecnoscienza, negli ultimi venti anni, non è stato accompagnato da una crescita culturale, educativa, etica e istituzionale all'altezza della complessità del tempo presente. Le tecnologie hanno mutato il nostro rapporto con il tempo, con la costruzione dell'identità, stanno alterando le dinamiche interpersonali e i processi sociali, dobbiamo imparare ad affrontare con consapevolezza queste trasformazioni per non subirle. Le generazioni analogiche vedevano il tempo in modo sequenziale, narrativo, riflessivo; le "generazioni del pollice" vivono una dimensione esistenziale frammentata, veloce, orientata in modo estremo alla performante. Non potrebbe essere altrimenti se, come ci dicono i dati dell'*Atlante dell'infanzia a rischio*, l'età di accesso allo smartphone continua ad abbassarsi: già i bambini tra sei e dieci anni che ne fanno uso sono più del 30%. Sarà dunque necessario lavorare fin dai primi anni di scuola sui linguaggi del digitale, che hanno una precisa sintassi che bisogna conoscere a fondo per poterli padroneggiare, per ridurre le paure diffuse e, nel contempo, aumentare la fiducia e il senso di sicurezza oggi messo sotto scacco dal potere crescente da usi distorti delle tecnologie come fa il cyber crimine.

Nel delicato ambito delle relazioni sociali si registrano criticità che meritano attenzione. Possiamo cercare di tratteggiarle in sintesi?

Vi sono vulnerabilità cognitive, psicologiche, che oltre ad avere dei riflessi sulla sfera dell'io, hanno delle ricadute sulla coesione sociale e persino, come si sta vedendo molto bene sul terreno della geopolitica, sulla stabilità dei sistemi democratici. L'informazione *on line* continua, che genera una sorta di esaurimento che si manifesta con ansia, sensazione di sopraffazione e una diminuzione della sensazione di benessere è un caso emblematico. Gli esperti parlano di burnout cognitivo, dettato da una saturazione che non innalza il nostro livello di conoscenza dei fatti e degli eventi; al contrario, porta a una distrazione sistematica, fino all'incapacità di sviluppare quel pensiero critico, che è necessario alimento della vita democratica. Il nostro cervello si sta appiattendo sui tempi di reazione di un tweet o su un reel di *Instagram*, che smorza l'ampiezza del ragionamento e la capacità di progetto del singolo. FOMO (acronimo che sta per *Fear of Missing Out* n.d.r.) è un altro fenomeno emergente, nasce dalla percezione amplificata dai social network, attraversati dagli innumerevoli eventi e opportunità cui tutti partecipiamo. Stories, post in scadenza, notifiche creano un bisogno costante di presenza, di vigilanza. In Italia l'impatto di questa fenomenologia è particolarmente forte se consideriamo che oltre il 70% dei giovani tra i 14 e i 19 anni prova forme di ansia legate alla necessità di rimanere esposti in una sorta di "vetrina digitale", che genera dipendenza, espone al rischio, imprigiona in "camere dell'eco" autoreferenziali, dove ascoltiamo e leggiamo solo chi la pensa come noi, con il risultato di un restringimento dell'orizzonte conoscitivo che soffoca il livello di consapevolezza individuale.

La rivoluzione dell'IA

L'irruzione dell'IA nella complessa dinamica di rapporti tra uomo-macchina che sta descrivendo, che cosa ha comportato?

Un "salto quantico" e una potente accelerazione dei fattori di trasformazione delle reti sociali e del sistema produttivo. Il termine "opacità algoritmica" è quello che fotografa meglio l'incapacità da parte degli utenti di comprendere appieno i meccanismi di funzionamento che portano l'IA ad assumere decisioni e comportamenti. In molti casi, specialmente con l'uso di *machine learning* (apprendimento automatico n.d.r) e del deep learning (reti neurali complesse che studiano i meccanismi cerebrali), le logiche interne rimangono incomprensibili persino agli stessi sviluppatori. L'ultima rilevazione

dell'Eurispes, pubblicata nel *Rapporto Italia 2025*, mette in evidenza un atteggiamento verso l'IA che potremmo definire prudente: solo il 20% degli italiani la considera un'opportunità, appena il 7% la vede come una soluzione a moltissimi problemi. Luci e ombre prevalgono, infatti, tra le persone sollecitate dall'indagine: emerge una richiesta di controllo del prepotente sviluppo dell'IA, che si innesta in una visione in generale critica. La frattura generazionale, cui facevo prima riferimento, appare qui in maniera netta: tra i 18-24enni, il 44% considera l'IA una opportunità, il 16% una soluzione, mentre tra gli over 64 solo il 10% è favorevole, prevale la paura e l'incertezza. Due universi che non comunicano, che invece sarebbe importante far dialogare perché potrebbero insieme costituire un antidoto importante a quella che molti studiosi definiscono "alienazione tecnologica". Per arginare la deriva si sta sperimentando il *digital detox*, come pratica di limitazione e di spazi di disconnessione che sta prendendo piede in Europa: è la nuova frontiera della salute pubblica e del benessere che guadagnerà molta attenzione in futuro.

Le fragilità e le paure con cui milioni di utenti hanno a che fare investono sempre più i modelli di convivenza e la vita collettiva delle città. Quali scenari si stanno aprendo?

La trasformazione digitale sta modificando tutte le strutture che governano la vita collettiva. Basti considerare quello che sta avvenendo riguardo alla qualità del dibattito pubblico, alla coesione sociale, alla difficoltà del sistema educativo di adattarsi ai cambiamenti. Quest'ultimo aspetto ha dei riflessi importanti sulla possibilità di attuazione del Programma per il Decennio Digitale dell'UE. Va ricordato che solo il 46% degli italiani tra i 16 e i 74 anni possiede competenze digitali, un dato molto inferiore alla media europea (54%) ben lontano dall'obiettivo fissato dalla Commissione UE (80%). La percentuale scende sotto il 30% tra la popolazione over 60 con picchi di marginalità nelle aree rurali e del Mezzogiorno. Bisogna inoltre tenere conto che entro il 2030 avremo bisogno di almeno 20 milioni di specialisti nel settore ICT per sostenere lo sviluppo nei settori più innovativi. Siamo ancora fermi a circa 9 milioni: l'offerta formativa non riesce a stare al passo con l'evoluzione delle tecnologie. A questo si aggiunge la rappresentanza di genere nelle professioni digitali: oggi, in Europa, meno di 2 degli specialisti ICT su 10 sono donne. La rimozione di ogni barriera culturale, il rafforzamento delle competenze nelle aree STEM sarà decisivo perché segnerà un reale crescita della cittadinanza digitale, scandendo un miglioramento delle performance delle nostre imprese.

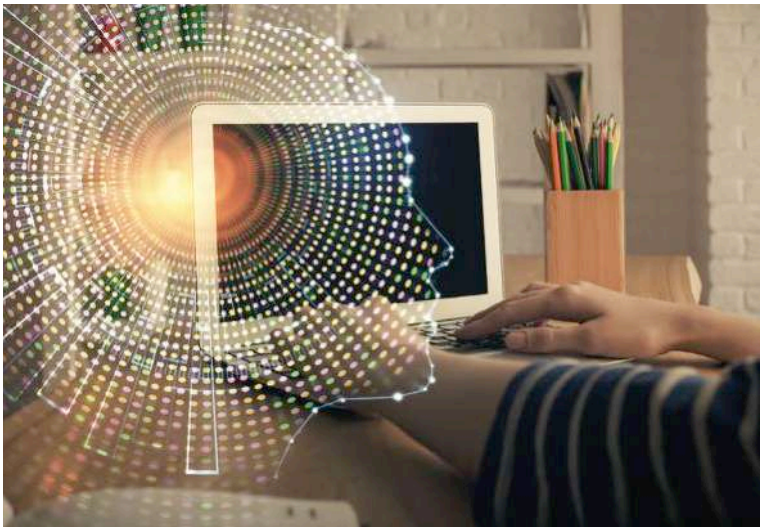
Il ruolo delle PMI

Quello che ha toccato è un nodo strategico. Le PMI nella rivoluzione in atto che posto occuperanno?

Sono destinate a rimanere il perno del nostro sistema produttivo. Non mancano anche su questo fronte delle debolezze strutturali da colmare. Secondo Eurobarometro 2025, solo il 58% delle PMI italiane ha raggiunto un livello base di intensità digitale, rispetto al 69% della media Ue. Il divario non riguarda solo il numero di imprese digitalizzate, ma anche la qualità e la maturità delle tecnologie adottate. Solo il 6% delle aziende italiane utilizza l'intelligenza artificiale, rispetto al 10% della media Ue, mentre il cloud computing è adottato dal 22% delle imprese italiane, contro una media Ue del 34%.

Quali sono i maggiori ostacoli che non consentono di compiere il salto necessario?

La mancanza di competenze digitali interne; la scarsa disponibilità di consulenza; la difficoltà di accesso al credito e agli incentivi pubblici in forma semplificata; modelli gestionali poco innovativi. Il divario territoriale continua a essere significativo: nelle regioni del Nord, le imprese mostrano un livello medio di digitalizzazione superiore rispetto a quelle del Centro-Sud. Guardando ai vari settori, le imprese manifatturiere risultano mediamente più digitalizzate rispetto a quelle dei servizi tradizionali, mentre le filiere agroalimentari, turistiche e artigianali, in generale,



sono meno digitalizzate. Vi sono, e non vanno sottaciuti, alcuni segnali positivi che vengono dal nostro contesto: nel triennio 2020–2023, grazie agli incentivi del Piano Transizione 4.0, si è registrato un aumento del 12% negli investimenti digitali nel manifatturiero. Da questo dato credo si debba ripartire, per avviare il percorso di una crescita effettiva di sistema. ■

Per "abitare" il tempo complesso, bisogna andare "oltre"…

Intervista VIP a Andrea Granelli e Nicola Spagnuolo.

Autore: Massimiliano Cannata

Nell'interessante saggio ***Oltre la formazione*** *(ed. Harvard Business Review e CFMT,) vengono tracciate le coordinate dei nuovi orizzonti del sapere nella società digitale.*

Complessità e tecnologia sono due termini chiave nel nuovo paradigma che domina la società e i cicli produttivi. Quale spazio deve occupare la formazione nella dinamica dei cambiamenti in atto?

Più il mondo cambia, più risulta fondamentale che la formazione aiuti le persone, soprattutto i manager, i leader, che hanno la responsabilità di guidare "la macchina" a capire il contesto e a muoversi di conseguenza. Quando il cambiamento si intreccia, in particolare, con livelli di complessità crescenti in un universo sempre più connotato dalla tecnologia, il know-how diventa un asset cruciale.

Traducibile, memorabile, transdisciplinare, il sottotitolo del libro apre un universo di concetti. Possiamo soffermarci su questi aggettivi circoscrivendone il senso?

Comincerei dal primo termine: "traducibile". La formazione è sempre universale, è sempre *erga omnes*; si rivolge a una collettività, a un gruppo di persone. Poi ciascuna delle persone che partecipa deve tradurre il tema generale nel contesto particolare e operativo entro cui si muove. Questa attività di traduzione è molto importante, molto delicata; non possiamo lasciarla solo al discente, che faccia da solo. Il ruolo, per esempio, della mentorship che viene fatta a valle di un percorso formativo è proprio questo: aiutare la persona a *tradurre*, adattare i contenuti generali universali al suo contesto particolare. Ricordiamoci - come ci dice l'etimologia della parola - che "tradurre", che è molto vicino a tradire. Non a caso gli editori dicono: *traduttore* e *traditore*. Ogni volta che traduciamo, rischiamo sempre di tradire il contenuto che stiamo traducendo. Per questa ragione bisogna che ci sia un'adeguata assistenza per svolgere questa delicata attività.

Memoria e futuro

Con il termine "memorabile", entra in gioco il tempo, la memoria: una sfida anche questa non facile da affrontare. Cosa pensate al riguardo?

La memorabilità si realizza se quello che impariamo rimane tale, se ce lo ricordiamo. Sapere è ricordare, come sosteneva Platone. Ricordare vuol dire, in particolare, accedere a dei contenuti che abbiamo acquisito, adattandoli al nuovo contesto, La parola "memorabile" in italiano è molto potente: richiama una dimensione epica e implica un giudizio di qualità su fatti ed eventi degni di essere richiamati alla mente. L'espressione spagnola "memorioso", spesso usata da Papa Francesco, fa riflettere: significa che qualcosa deve essere ricordato, rendendo molto bene l'idea che vogliamo rappresentare.

E sulla parola "transdisciplinare", cosa possiamo dire?

Che non basta più avere competenze singole: servono competenze articolate, costruite attraverso molte discipline. La complessità richiede interdisciplinarità. Pensiamo ai gesuiti, che hanno fanno scuola in termini di metodo, sperimentando una *ratio studiorum*, elaborata alla fine del Cinquecento e costantemente aggiornata, adattandola alle sollecitazioni dell'era digitale in cui tutti viviamo immersi.

BIO

Andrea Granelli è appassionato di innovazione, si occupa dei rapporti fra nuove tecnologie e scienze umane e combatte i lati oscuri del digitale. Dopo la maturità classica, si laurea con lode in informatica e completa gli studi con un diploma post-universitario in psichiatria e un Executive MBA in McKinsey. Ha fondato Kanso, società di consulenza che si occupa di innovazione e change management. Prima ha lavorato per Enel, Montedison, McKinsey ed è stato CEO di tin.it e della R&D del gruppo Telecom.

BIO

Nicola Spagnuolo è direttore di CFMT Centro di Formazione e Management del Terziario, con 25.000 dirigenti e 8.600 aziende associate. Esperto di processi formativi ha ricoperto, per circa tre anni, la direzione del settore sviluppo associativo di Confcommercio nazionale, organo italiano di rappresentanza delle imprese impegnate nel commercio, nel turismo e nei servizi. Dal 2006 al 2016 è stato direttore generale Iscom Emilia Romagna, l'ente di formazione di Confcommercio - Imprese per l'Italia dell'Emilia Romagna, ed è stato Presidente per la Fondazione I.T.S. "Turismo e Benessere".

Viviamo, per usare un termine caro a Edgar Morin, nel tempo delle "policrisi". La più grave di tutte è la "crisi cognitiva", che concerne - scrive Mauro Ceruti - "proprio la difficoltà di pensare la complessità". La formazione può aiutare il sistema a superare i tanti gap conoscitivi che frenano la competitività delle nostre imprese?

Potenziare il pensiero è un compito della formazione. La capacità di ragionare, la retorica, l'arte di argomentare, di negoziare, il pensiero critico: è questo il volto più grave delle "policrisi" cui si riferiscono i pensatori citati prima. Il rischio è alto, soprattutto se consideriamo la potente diffusione dell'IA, che potrebbe determinare un depotenziamento cognitivo. Spesso ci fidiamo di quello che dice un sistema che consideriamo esperto, non preoccupandoci nemmeno di verificare le fonti. Bisogna cambiare passo, tornando ad esercitare la lettura, rispolverando i classici e i grandi autori, che tanto hanno da insegnarci.

La tavola pitagorica dei processi cognitivi

L'evoluzione digitale sta modificando la "tavola pitagorica" dei processi cognitivi, mentre è in atto una rivoluzione epistemologica profonda. Nel saggio si avverte la spinta ad andare "oltre". Cosa vuol dire, in concreto?

Andare oltre l'apprendimento vuol dire capire che c'è qualcosa da osservare con un ragionamento di ampio respiro, rispetto al quale l'apprendimento è solo un tassello di un processo che va potenziato per scandire lo sviluppo della personalità e la maturazione del singolo. Bisogna superare - andare oltre - il modo in cui oggi vengono definiti i contenuti e i perimetri dei saperi. Dobbiamo avere il senso dell'irriducibile legame tra le competenze, perché non ci può essere un progresso delle conoscenze nella parcellizzazione e nella frammentazione. Abitare la complessità vuol dire riconoscere i limiti del vecchio paradigma, che tendeva a separare, creando steccati tra professioni e competenze. Oggi abbiamo bisogno di una "nuova paideia", che ci permetta di guardare la realtà in tutte le sue articolazioni.

In conclusione, vi chiedo: finito il tempo della "sacralità dell'aula" che l'età industriale ha vissuto e anche la nostra generazione che credeva il "proprio banco" quale baricentro di un mondo anche relazionale. Nell'età delle intelligenze generative, quali sono i luoghi della formazione?

Il tema dei luoghi rimane fondamentale, innanzitutto bisogna parlare di luoghi fisici e luoghi virtuali. Ormai il concetto di luogo si è dilatato. L'aula è certamente un luogo ma lo è anche il territorio. Ma pensiamo anche al Genius Loci, al Grand Tour che è stato anch'esso un grande luogo formativo, l'aula in quel caso si poteva identificare nei territori che attraevano turisti d'eccezione. Anche questi "visitatori" eccellenti "andavano oltre" quello che vedevano, perché loro interesse era conoscere, i percorsi erano generatori di creatività. Il caso di Goethe è emblematico: venuto in Italia non voleva più tornare nella sua Germania, nel nostro paese produceva e scriveva meglio. Ecco che l'aula diventa il territorio, la cui storia si articola nel rapporto natura-cultura. In questa dinamica non possiamo non considerare "il Virtuale", che ha ragione Pierre Levy a considerare una nuova categoria dell'essere. La capacità immaginifica, amplificata dal digitale non è solo uno spazio virtuale, è anche un luogo dove si possono generare opzioni possibili, si possono creare mondi "oltre" il visibile. Quella che va sviluppata è una nuova competenza, che potremmo definire *space awareness*, che vuol dire reinterpretare continuamente i luoghi che "significano", tenendo insieme il sensibile e il soprasensibile, l'architettura e la memoria che li fanno essere, sollecitando continui interrogativi al fruitore. Questa è formazione, che segue canoni pedagogici e comunicativi non convenzionali, che dovremo imparare a padroneggiare e ad esercitare per comprendere il cambiamento d'epoca entro cui siamo immersi. ■

Come cambia il ruolo del CISO: da custode del "perimetro" a vero abilitatore della resilienza aziendale.

Intervista VIP a Marco di Luzio.

Autore: Massimiliano Cannata

"Siamo dei maratoneti, dobbiamo camminare con continuità e ritmo nell'orizzonte delle organizzazioni complesse", mi approprio di un pensiero di Yuri Rassega, CISO di Enel che abbiamo ospitato in questa rubrica per iniziare la nostra conversazione.

Dott. Di Luzio come si può definire oggi il ruolo di Chief Information Security Officer?

Il ruolo del CISO è quello di guidare l'organizzazione verso una gestione matura del rischio informatico. Non si tratta solo di proteggere i sistemi, ma di garantire la continuità operativa, la reputazione e la fiducia degli stakeholder. Serve, in particolare, saper unire competenze tecnologiche con capacità di gestione del rischio, comunicazione e leadership, diventando un ponte tra il mondo tecnico e quello del business. In sintesi, è un ruolo che evolve da "custode del perimetro" a vero abilitatore della resilienza aziendale.»

La tradizionale concezione che vede nel manager della security essenzialmente un tecnologo non regge più, dunque, alla luce dei profondi processi di mutazione che le aziende stanno sperimentando?

Certamente no. L'efficacia nel mitigare il rischio cyber dipende dall'essere in grado di operare su almeno tre dimensioni, che sono intrecciate: la dimensione tecnologica è quella più immediata che si concretizza nella definizione di strumenti di difesa, nel monitoraggio delle minacce, nella threat intelligence, nella crittografia, nell'automazione della risposta. Tutte cose importanti, ma che però non bastano.

Cosa intende dire?

Che senza governance e consapevolezza, la tecnologia resta un "guscio vuoto". La sicurezza deve essere incorporata nei processi aziendali, non è una semplice aggiunta, uno strato esterno. Introdurre policy, framework di gestione del rischio, modelli di governance chiari, sono tutti aspetti della governance del rischio imprescindibili. Ugualmente importante risulta il lavoro di compliance, audit, risk management che concorrono a creare resilienza organizzativa. Un processo si può definire maturo quando riduce il rischio di errori umani e garantisce continuità anche in caso di incidente.

Qualità delle persone e la centralità del capitale umano. Si insiste molto su questi aspetti. Qual è la sua idea in merito?

Le persone sono al tempo stesso il punto più fragile e il primo strumento di difesa. Occorre sviluppare percorsi di awareness diffusi, programmi di

formazione e una cultura che riconosca la sicurezza come responsabilità condivisa. Non scordiamoci che il CISO deve essere anche un comunicatore e motivatore, capace di tradurre concetti complessi in linguaggio accessibile. Creare engagement significa trasformare i dipendenti da potenziali vulnerabilità a veri "cyber ambassador". Ecco perché insisto sul carattere "ibrido" e "multidisciplinare" di questa figura che si muove tra tecnologia, processi e persone. Solo facendo leva congiuntamente su queste tre dimensioni organizzativa è possibile passare da una logica della semplice protezione a quella della resilienza complessiva di tutta l'organizzazione.

Dalla protezione del perimetro al governo del rischio informativo.

Con quali attori della catena del valore deve interloquire il CISO per raggiungere i risultati attesi?

Con una molteplicità di attori: Verso l'interno è fondamentale un continuo allineamento e un'azione di "fine tuning" con tutte le funzioni aziendali e quindi con il top management al fine di migliorare la postura cyber di tutta l'azienda. Una delle criticità principali è rappresentata dal fatto che il perimetro aziendale esposto al rischio cyber e quindi la sicurezza non ha un'unica ownership e rischia di disperdersi tra le varie funzioni. É compito CISO ricondurre ad unità questa complessità organizzativa attraverso una govenance efficace del rischio cyber che insiste sull'intero perimetro.

Un'altra sfida più rivolta verso l'esterno è la gestione del rischio cyber della intera supply chain: oggi la sicurezza e la continuità operativa dei processi di erogazione dei servizi critici prevede il coinvolgimento dei partner e fornitori che contribuiscono all'intera catena del valore. Compito del CISO è dunque anche quello di garantire la supply chain security attraverso processi di monitoraggio audit e capacità di intervento che devono prendere in considerazione complessivamente il rischio a cui è esposta questa catena del valore "estesa". Per ultimo, anche se molto rilevante in termini di effort organizzativo, va preso in considerazione il rapporto verso l'esterno che il CISO è chiamato a gestire con i clienti. Proprio in questa ottica di "catena del valore estesa" i clienti ci considerano a loro volta parte della loro stessa continuità operativa,

come richiesto dalle recenti normative DORA, NIS2 che definiscono un ventaglio di attività molto articolate di audit e remediation, rispetto a cui il CISO è chiamato a rispondere.

Nella "Quarta rivoluzione", come ci insegnano gli scritti di Luciano Floridi, la sicurezza non ha nulla a che vedere con la visione tradizionale della tutela del "recinto" e dello "spazio fisico", perché è la terza dimensione dell'"infosfera" di cui dobbiamo prenderci cura. Siamo preparati per farlo?

Nell'era dell'infosfera non bastano le competenze tecniche. Oggi servono team multidisciplinari che integrino hard skills e soft skills. Non mi riferisco solo alle esigenze della cybersecurity engineer, ma anche di esperti di risk management, legali, comunicatori e formatori. Il CISO deve saper mappare e aggiornare continuamente queste competenze, perché la velocità con cui si evolvono le minacce rende obsolete le conoscenze in pochi mesi. L'elemento distintivo è, e lo sarà anche in futuro, la capacità di leggere la sicurezza come un fenomeno socio-tecnologico che riguarda persone, processi e cultura, non solo macchine. Questo comporta di combinare hard skills (tecniche) e soft skills (comunicazione, negoziazione, leadership), in un aggiornamento continuo delle competenze, che vanno distribuite in team diversificati.

Spazio e tempo sono le categorie della conoscenza da sempre indagate dai grandi filosofi. Nel vocabolario della sicurezza che ogni CISO deve padroneggiare come vanno declinate?

La categoria del tempo, nella sicurezza digitale, si traduce nella capacità di reazione e nella velocità di risposta. Più riduciamo il tempo di detection e di remediation, più aumentiamo la resilienza. Lo spazio, invece, rappresenta l'ecosistema digitale distribuito: cloud, edge, IoT, ambienti ibridi che rendono i confini sempre più sfumati. "Space awareness" significa avere consapevolezza costante di dove risiedono i nostri dati, quali sono gli accessi e come circolano le informazioni. In sintesi, tempo e spazio diventano le coordinate entro cui il CISO deve esercitare la propria consapevolezza situazionale.

Siamo immersi in una "non-guerra" "non-pace" come ha scritto sul Corsera il politologo Angelo Panebianco in cui stati, aziende, e comunità combattono un conflitto di reciproche interferenze. La cybersecurity è ormai logistica militare, l'informazione è il terreno della contesa cognitiva. Per i manager della sicurezza crescono le responsabilità in maniera esponenziale. Una sfida nella sfida.

La guerra ibrida, cui lei fa riferimento porta la sicurezza a un livello che va oltre il perimetro tecnico: parliamo di disinformazione, manipolazione delle identità, attacchi reputazionali. In questo contesto, la valutazione del rischio deve basarsi su un approccio dinamico, che unisce threat intelligence, scenari predittivi e collaborazione tra pubblico-privato. Sicurezza, equilibri geopolitici, presidi tecnologici sono fattori interdipendenti, che vanno bilanciati su scala globale. È evidente che l'investimento in competenze e aggiornamento del know-how deve crescere per reggere i ritmi della trasformazione in atto.

Le sfide si affrontano insieme, "nessuno si salva da solo"

Proviamo a gettare lo sguardo nel contesto produttivo entro cui Lei opera. Qual è il posizionamento della Cyber security?

In Tinexta Cyber la sicurezza non è un servizio accessorio, ma un pilastro strategico della mission aziendale. Il nostro obiettivo è accompagnare clienti e partner nel proteggere gli asset digitali più critici e garantire la continuità operativa del loro business, coniugando innovazione tecnologica, compliance normativa e capacità di risposta alle minacce. Ci posizioniamo come partner di fiducia, puntando su una visione integrata della sicurezza: dalla protezione dei dati alla gestione del rischio reputazionale, fino alla resilienza della supply chain. La cyber security per noi non è solo difesa, ma un obiettivo strategico che impone l'introduzione di logiche di miglioramento continuo e innovazione su processi persone e tecnologie divenendo di fatto un fattore abilitante di competitività.

TINEXTA CYBER

L'organizzazione nel suo complesso è impegnata a rafforzare la capacità di mitigazione del rischio cyber, che stiamo attuando con un presidio puntuale del nostro perimetro cyber (spazio) attraverso una pianificazione stingente di tutte le innumerevoli azioni preventive e capacità di detection e remediation efficaci dei tentativi di azioni malevoli (timing). Per ottenere questo risultato stiamo lavorando molto sull'innovazione e adeguamento delle nostre tecnologie, procedure e persone messe a presidio del rischio cyber. Questo è il nostro core business; a cui è legato il nostro rischio reputazionale. Per questo ci siamo dati l'obiettivo di portare verso gli standard più elevati la sicurezza di processi, tecnologi e persone all'interno della nostra organizzazione. Recentemente abbiamo completato il processo di certificazione ISO 22301:2019 – Sicurezza e resilienza – Sistemi di gestione per la continuità operativa La ISO 22301 è lo standard internazionale per la gestione della continuità operativa (Business Continuity Management System, BCMS). Definisce i requisiti per pianificare, implementare, mantenere e migliorare un sistema che garantisca la capacità dell'organizzazione di continuare le proprie attività essenziali anche in caso di incidenti, crisi o eventi imprevisti. Sono ancora poche le aziende possono vantare questo tipo di certificazione. Noi ci siamo dati questo obiettivo e lo abbiamo conseguito perché vogliamo portare la resilienza dei nostri processi, tecnologie e persone, come asset strategico e valore per i nostri clienti.

Nel DNA di Tinexacyber è insita l'idea di polarità, di collaborazione tra soggetti. A dimostrazione di quanto Lei crede nella prospettiva del confronto e del dialogo, ha scelto di entrare a far parte di Associso. Cosa vuol dire questo impegno per chi fa un mestiere come il suo?

Le reti di collaborazione rappresentano un elemento chiave per chi fa sicurezza. Nessuno può affrontare da solo sfide così complesse. ASSOCISO è un luogo di confronto, di scambio di pratiche e di crescita comune, ma è anche uno strumento di advocacy per far emergere la voce dei responsabili della sicurezza nelle istituzioni e nel mercato. La polarità, intesa come collaborazione tra soggetti diversi, è in questa ottica parte integrante della nostra forza: competizione e collaborazione possono convivere, anzi devono convivere, se vogliamo alzare il livello di resilienza del sistema complessivo delle imprese. ■

BIO

Marco Di Luzio ha iniziato la sua carriera occupandosi di sviluppo organizzativo in primarie società di consulenza di direzione, tra cui Butera e Partners e Accenture, dove ha seguito progetti di innovazione e reingegnerizzazione dei processi per grandi aziende e pubbliche amministrazioni.
Successivamente ha lavorato in InfoCert, contribuendo allo sviluppo del mercato delle soluzioni digitali e ricoprendo il ruolo di Direttore Marketing, con responsabilità sul posizionamento strategico, l'espansione internazionale e progetti di M&A.
È stato inoltre Membro del Board di Camerfirma(Spagna).
Dal 2021 è in Tinexta Cyber, dove ha guidato le attività di integrazione e sviluppo della funzione Marketing, definendo la strategia di posizionamento del gruppo.
Da settembre 2024 ricopre il ruolo di CIO – CISO in Tinextacyber, con l'obiettivo di integrare sistemi IT, organizzazione e processi post M&A delle tre aziendeacquisite, promuovendo innovazione, efficienza e governance tecnologica. In questo ruolo si occupa di portare ai livelli più elevati gli standard di sicurezza cyber del nuovo perimetro aziendale sia rispetto alle nuove normative di settore DORA NIS 2 che rispetto agli standard di certificazione in ambito cybersecurity.
Marco ha conseguito la laurea in Sociologia dell'economia dell'organizzazione e del lavoro presso l'Università La Sapienza di Roma e un Executive MBA presso l'Università di Tor Vergata. Ha inoltre frequentato programmi di sviluppo manageriale presso SDA Bocconi e MIT Sloan School of Management di Boston.

Il gemello digitale svela il profilo di una rivoluzione che cambia il nostro modo di essere nel mondo.

Intervista VIP a Roberto Masiero.

Autore: Massimiliano Cannata

"Possiamo immaginare il gemello digitale come un simbionte, un quasi organismo, dotato di memoria, capacità di apprendere e valutare, che ci aiuta a decidere al meglio. Tutto con il digitale, prende la forma dei dati che possono essere tra loro confrontati e addirittura essere resi interoperabili… In questo contesto il tema della sicurezza informatica è indubbiamente cruciale, ma non va affrontato, come accade fin troppo spesso, demonizzando il digitale e alimentando la paura di ciò che è nuovo…" Roberto Masiero Ordinario di Storia dell'Architettura dell'IUAV di Venezia sta per dare alle stampe "Pensare digitale" per Meltemi. Nei suoi studi ha affrontato i molteplici fattori di trasformazione che lo sviluppo della tecnoscienza sta comportando in ogni ambito del sapere. Cybersecurity Trends in questa intervista ha cercato di approfondire le implicazioni della rivoluzione in atto, per chi opera nel delicato ambito della sicurezza informatica.

Professore, quando parliamo di gemello digitale cosa dobbiamo intendere?

Possiamo immaginare il gemello digitale come un simbionte, un quasi organismo, dotato di memoria, capacità di apprendere e valutare, che ci aiuta a decidere al meglio. Uso il termine simbionte per indicare il passaggio in atto con il digitale dal predominio della meccanica a quello della biotica. Immaginiamo la mappa di una città e tutto ciò che una città è: la vegetazione, le strade, i servizi, le abitazioni, i monumenti e i luoghi pubblici, gli abitanti, ognuno con le proprie caratteristiche (età, stato della salute e quant'altro), e perchè no, anche i turisti. E per non farci mancare nulla anche tutto il denaro che muove questa città, quello nelle banche come quello che rende vivo il mercato, o i saperi che in questa città si diffondono in vario modo ovunque, scolarità, mostre, iniziative culturali, musei. Ora tutto questo può, con il digitale, prendere la forma dei dati che possono essere tra loro confrontati e addirittura essere resi interoperabili.

Siamo a un'ulteriore tappa della "mutazione" digitale che investe ogni ambito della società?

Certamente sì, soprattutto se consideriamo gli scenari di innovazione che si stanno aprendo. Il gemello digitale è l'insieme (pressoché infinito) dei dati su fenomeni materiali quanto immateriali raccolti come un processo continuo che possono riguardare tutto ciò che può accadere in un determinato contesto. Posso fare il gemello digitale di tutto ciò che accade in una scuola, in un territorio, in una fabbrica e l'elenco potrebbe continuare. L'insieme di questi dati e la loro elaborazione può permetterci di comprendere, controllare e governare i processi ed elaborare sistemi decisionali, verificandone nel tempo l'efficacia. Oggi siamo in grado di analizzare e valutare possibili decisioni in merito al rapporto tra dati ambientali e malattie distribuite variamente tra gli abitanti, o valutare i dati sulla scolarità e il rapporto tra le conoscenze acquisiate nel sistema scolastico rispetto all'organizzazione produttiva espressa dal territorio.

La* governance *dei territori si sta modificando. Il presente e il futuro delle città (di cui lei si è ampiamente occupato da architetto) stanno mutando il loro profilo. Nel saggio Il* gemello digitale territoriale *- cfr. spazio recensioni di questo numero (n.d.r) si parla di "spazio intermedio" e di una platmorfizzazione della società. Siamo oltre le categorie kantiane, a che cosa stiamo andando incontro?

La rivoluzione in atto è soprattutto di natura epistemica cioè riguarda il modo nel quale possiamo fare e decidere del nostro rapporto con il mondo. Dobbiamo cambiare modo di pensare. Dal punto di vista filosofico si dovrebbe ri-partire da questa semplice ma radicale affermazione: gli enti, materiali e immateriali, sono stati di relazione, quindi dovremmo ripensare proprio i "trascendentali kantiani" accettando la generale relativizzazione che ci viene oramai da più di un secolo proposta dalla fisica quantistica. Si tenga presente che non esiste una civiltà se non si dia una cosmogonia (vera o falsa che sia) e la civiltà del digitale ha come propria cosmogonia la quantistica. Se tutto è stato di relazione è assolutamente evidente che i rapporti sociali non possono che essere pensati, gestiti governati attraverso piattaforme digitali che rendono il tutto connesso e interoperabile.

I dati sono il "nuovo petrolio"

I dati sono il nuovo petrolio. Michele Mezza in una recente pubblicazione "Connessi a morte" ne parla diffusamente per esemplificare le conseguenze sul piano esistenziale e non solo produttivo che l'IA e gli algoritmi stanno generando. Malgrado questo, il salto di qualità nella PA tarda a venire. Come si spiega questo ritardo? Dati, persone e territori: trovare una sintesi sarebbe compito della politica?

E' vero che i dati sono il nuovo petrolio, ma come il petrolio è l'esito di processi di raffinazione, così i dati hanno bisogno di elaborazione e interpretazione. Da anni molte regioni in Italia hanno provveduto a raccogliere in modo sistematico ad esempio i dati riguardanti la salute dei cittadini, ma il tutto si è risolto con un ulteriore processo di burocratizzazione e non certo con la trasformazione possibile, con il digitale, da una medicina universale a una medicina singolare, cioè un cambiamento sia nella diagnostica che nella terapeutica. Da anni nelle scuole dell'obbligo del nostro paese tutto, ripeto tutto, è digitalizzato ma la didattica è sempre la stessa di molti anni fa. Da anni tutte le fatturazioni e le transazioni finanziarie sono digitalizzate, eppure non riusciamo ad avere in questo settore cruciale trasparenza e controllo.

Esiste un ritardo generalizzato del sistema paese che è di natura epistemologica e quindi anche culturale. Di tale ritardo la politica si alimenta, spesso perché è essa stessa parte di quel ritardo, ma sovente anche per semplice esercizio di cinismo.

Smart city, smart land, digital twin, ***sono tutti "orizzonti" del digitale. Quali sono le implicazioni sul piano della sicurezza informatica di questi "nuovi piani di realtà" con cui ci misuriamo ogni giorno?***

Il tema della sicurezza informatica è indubbiamente cruciale, ma non va affrontato, come accade fin troppo spesso, demonizzando il digitale e alimentando la paura di ciò che è nuovo. Una paura che nasce perché ci costringe a cambiare in maniera profonda il nostro stesso modo di pensare e questo è indubbiamente profondamente inquietante sino ad apparire demoniaco. Mi permetto di fare sulla questione della sicurezza una considerazione: il digitale nel suo insieme è predisposto e predisponibile per auto correggersi; può produrre i propri anticorpi visto che nelle sue configurazioni attuali procede anche in costante feedback ed è animato sistemi di *machine learning*.

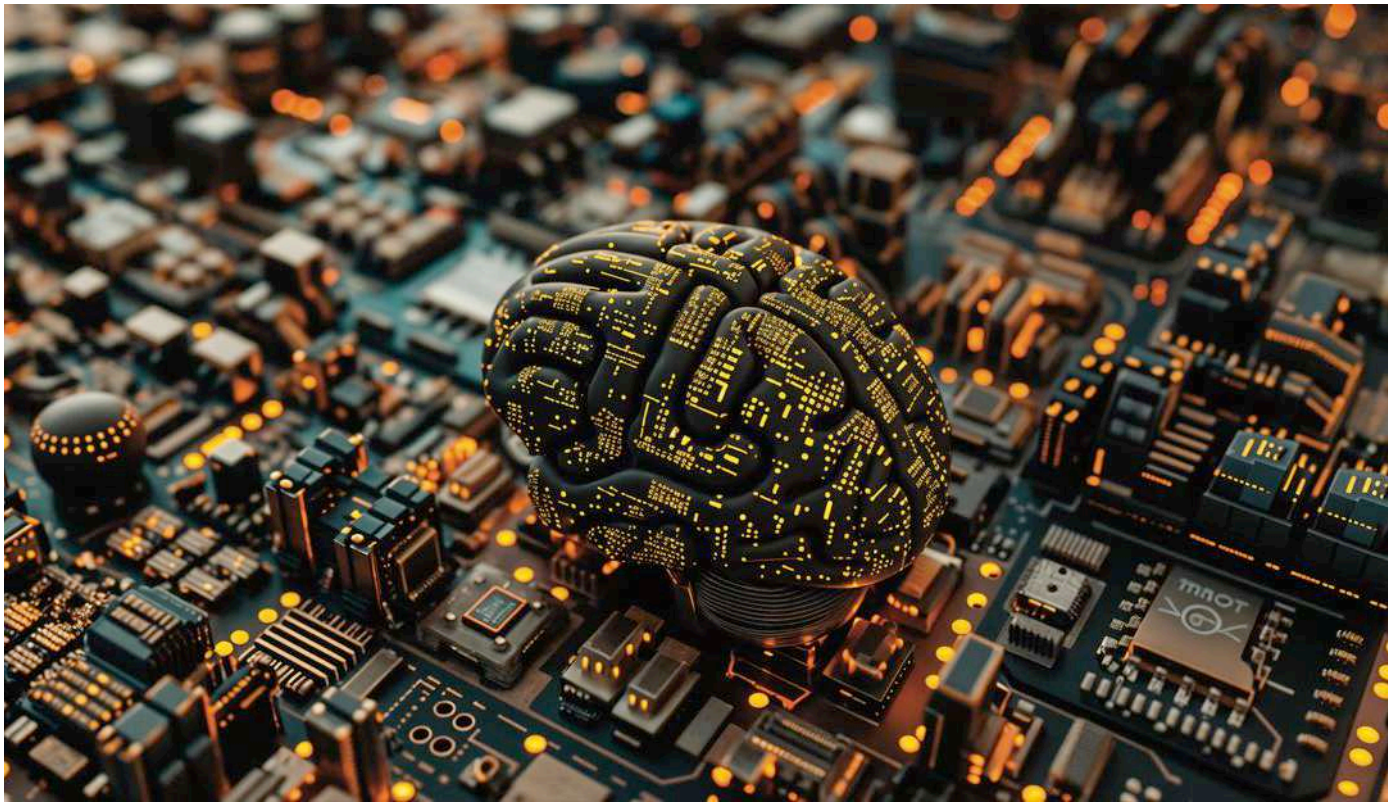
Tutto è cyber security

Tutto sembra esser* cyber security*, la connettività è divenuta logistica militare, come la guerra che ha un codice ibrido, per nulla convenzionale. Algoritmi e automazione dei processi hanno dato forma a un potere computazionale. Finita l'era dei contenuti tayloristici, si assiste a una riorganizzazione antropologica. Le imprese in questo stravolgimento non solo organizzativo ma culturale, di quali strumenti devono dotarsi per reggere la sfida della competitività?

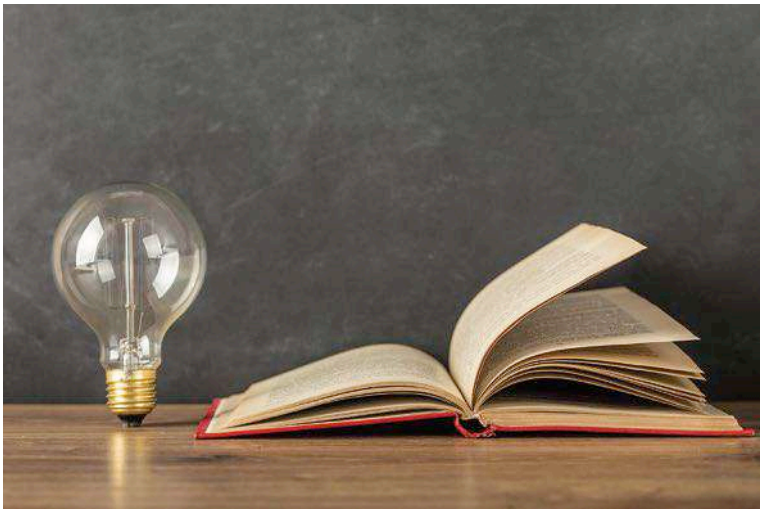
La risposta a questa domanda pretenderebbe una analisi attenta e molto articolata del sistema produttivo italiano non solo in chiave economica ma soprattutto culturale. Quello che per l'industria dovrebbe essere fondamentale è comprendere che il modo di produzione digitale (che integra quello industriale, avendo però logiche di produzione di valori sia economici che di sistema completamente diversi) è fondamentalmente *disruptive* e quindi è necessario cambiare completamente i modi e le forme della programmazione, dell'organizzazione e del *marketing*. Un grande cambiamento di visone delle cose del mondo che non viene assolutamente non dico alimentato ma nemmeno immaginato dai sistemi formativi tradizionali. Inoltre, il digitale tende (a differenza di quello industriale) a ridurre al minimo le distanze tra teoria e prassi, cioè tra pensiero e decisione e si sa quanto importante sia la decisione nell'azione produttiva.

Per i manager una sfida non da poco, non crede?

Per esemplificare la figura del manager dovrebbe essere scelta non in base alla sua capacità di prevedere il possibile, ma valutando la sua capacità di rispondere all'inaspettato. Inoltre, in questo contesto cambia l'idea tradizionale sia di innovazione che di sviluppo. La questione fondamentale per capire e agire nel digitale è che si alimenta costantemente non tanto di dati, quanto di saperi che rielaborano i dati. Per queste ragioni il mondo della imprenditoria dovrebbe chiedere alla politica una radicale trasformazione dell'intero sistema scolastico purtroppo ancora strutturato secondo logiche funzionali al modo di produzione industriale (separazione teoria/prassi, organizzazione gerarchica di saperi divisi, con una ragione sottesa: la divisone sociale del lavoro e dei suoi conflitti, etc, etc, etc.). Con il digitale è



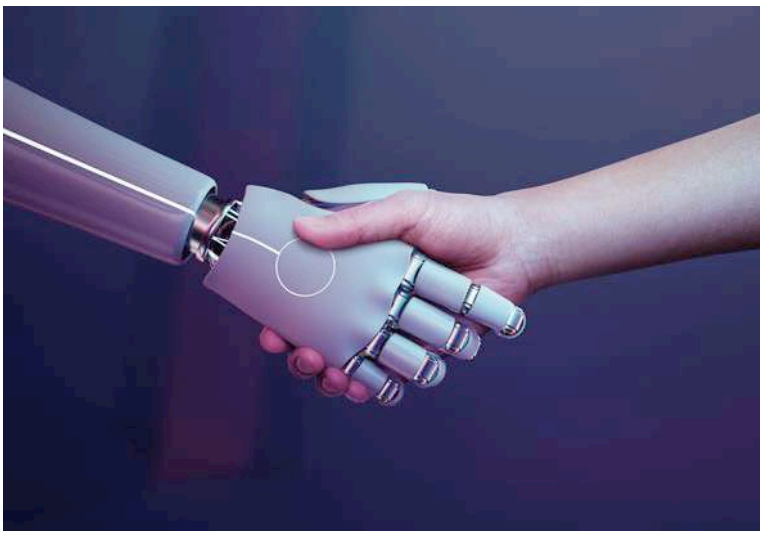
pensabile un continuo, aperto, diffuso, fluido trasferimento dei saperi verso una intelligenza e creatività collettiva. Questo serve ad un assetto industriale inteso come processo sociale di emancipazione collettiva



"Etica il nome nuovo da dare al pensiero", come sostiene Edgar Morin in numerosi scritti recenti. Di "Algoretica" parla con insistenza padre Benanti, c'è anche tutta una saggistica, penso agli scritti di Luciano Floridi che si stanno occupando di questo tema. Qual è la sua idea in merito?

Siamo già nella connessione tra intelligenza biologica e intelligenza digitale e sappiamo con certezza che quest'ultima è estremamente più potente di quella biologica che ci caratterizza in quanto specie. L'intelligenza artificiale non prova remore e timore per ciò che sta pensando; non si stanca mai di pensare, accumulare dati e mettere in relazione informazioni e concetti e ha una memoria pressoché illimitata, mentre la nostra è selettiva. Il conflitto tra le due intelligenze è indubbiamente il pericolo. Ma come dice il poeta *"… solo nel pericolo ci si salva"* (Holderlin).

La questione etica è quindi la seguente: l'intelligenza biologica deve adattarsi a quella digitale o viceversa? Se non vogliamo o non possiamo diventare più simili all'intelligenza artificiale dobbiamo trovare il modo per renderla più simile a noi. Questo è comunque il nostro compito etico: ripensare la nostra stessa umanità. ■



BIO

Già professore Ordinario di Storia dell'Architettura nell'Istituto Universitario di Architettura di Venezia, è studioso delle arti e delle scienze nel quadro di una generale storia delle idee e architetto. Ha insegnato anche nell'Università di Genova e di Trieste. Ha contribuito alla nascita della Facoltà di Architettura di Trieste e della facoltà Design e Arti dell'IUAV, della quale è stato anche Vicepreside. E' stato responsabile per l'UE di un Osservatorio sulle Accademie d'arte, Facoltà di Architettura e Ingegneria in Europa. E' stato nel Comitato direttivo della Fondazione Collodi ed è responsabile scientifico della Fondazione Francesco Fabbri per la quale, in particolare, segue il Laboratorio Politico con Quaderni come: Pensare l'Europa; Riflessioni sulla crisi; Gli spazi della politica. e con la pubblicazione di un Manifesto per lo smart land (con F. Della Puppa) e uno sulla Società circolare/ Economia digitale, con A. Bonomi e F. Della Puppa. Nel 2015 partecipa agli incontri di Italiadecide per la formazione del Rapporto 2016. Italiadecide: 8 Tesi per l'innovazione e la crescita intelligente, Dal trasferimento delle tecnologie al trasferimento dei saperi: il digitale, il Mulino, Roma 2016. Nel 2020 firma con Federico Della Puppa, la redazione del Piano strategico per il Dossier Pieve di Soligo, città della cultura italiana 2022. Tra le sue pubblicazioni più recenti: Qualcosa in più (forse) da sapere sul digitale, in AA.VV. Filosofia del digitale, Mimesis, Milano 2020; Cosa accade dell'economia (politica) là dove domina il digitale (con Paolo Zanenga), in AA.VV. Filosofia del digitale, Mimesis, Milano 2020; Per una epistemologia dell'architettura (con Vittorio Ugo), Librìa, Melfi, 2024; Gemello digitale territoriale, Zel ed, Treviso, 2024; Dall'industrial design, all'interaction design, Libria, Melfi,29024; Canto e Controcanto, opere e tempo lungo; Territorio, ambiente, paesaggi, metadomini, Librìa, Melfi (con Silvano Tagliagambe e Paolo Zanenga); Le architetture con volta a Tholos: origine e sviluppo nel Mediterraneo, Delfino editore, Sassari. In corso di pubblicazione un volume sul passaggio dal modo di produzione industriale al modo di produzione digitale dal titolo Pensare digitale, Meltemi, ed. Milano , un volume dal titolo Oltre-tutto, l'eta Kitsch, Zel ed. Treviso, sulla nascita e i significati dell'opera d'arte in età Contemporanea, Una serie di saggi sul digitale dal titolo E' il digitale, bellezza! Zel, ed.

Bibliografia - Cybersecurity Trends

La sfida della complessità (a cura di) Gianluca Bocchi Mauro Ceruti ed. Mimesis

Autore: Massimiliano Cannata

Un'impresa culturale che ha aperto nuovi orizzonti di pensiero

Il ponderoso saggio curato da Gianluca Bocchi e Mauro Ceruti, che ha avuto un successo planetario senza precedenti, rappresenta una stagione intensa e particolarmente feconda della storia del pensiero. L'espressione *"sfida della complessità"*, termine ormai entrato nell'uso comune, raccoglie un panorama multidisciplinare di specialisti che, in quasi mezzo secolo, hanno affrontato le grandi questioni del nostro tempo. Scienza, tecnologia, cibernetica, progettazione, neurologia, psicologia, biologia, geopolitica: l'analisi ampia e penetrante sollevata dagli studiosi — tra cui il Premio Nobel Ilya Prigogine, solo per ricordare una delle tante celebri firme contenute nel volume, editato per la prima volta nel 1985 — apre ancora oggi interrogativi di pressante attualità.

L'originalità del metodo

Sergio Manghi, nella prefazione, spiega molto bene il valore di quella che si può definire "un'impresa culturale", perché portatrice di una visione del mondo, di un metodo aperto di indagine, che mette al centro l'uomo nel rapporto con l'ecosistema. *"La cifra distintiva di quell'audace scommessa – scrive il sociologo - non era data dalla solo dalla quantità e varietà dei saperi coinvolti. Quel che faceva la differenza, rispetto a una mera operazione di confronto interdisciplinare, per quanto generosamente esteso, era il convergere del tutto inedito di quel vasto insieme di saperi eterogenei in un medesimo crocevia problematico unitario. Quell'effervescente crocevia, insieme epistemologico ed etico-politico, che si riconosceva, appunto, nella parola-sfida della complessità.*

A partire, in modo particolare, dalle riflessioni magistrali dedicate a questa parola-sfida da Edgar Morin nei primi due tomi del suo Metodo, La Nature de la nature e La Vie de la vie, e ancor prima nel "programmatico" Le Paradigme perdu; ma sviluppando per vie anche molto diverse l'esigenza unitaria condivisa riassunta nell'etimo stesso della parola complessità (da complexus, intrecciato insieme): coltivare un modo d'intendere e praticare i saperi attento in permanenza alle loro molteplici e inesauribili interconnessioni, e insieme, riflessivamente, alle loro premesse epistemologiche e al loro esser parte viva di più ampi processi antropologici, ecologici e sociali…. La parola complessità non fungeva, in questa chiave interattivo-riflessiva, da parola-risposta, nome di una possibile teoria unificatrice generale dello scibile, formulata da un qualche punto di osservazione "cartesianamente" incorporeo e asociale; ma da parola-problema, nome di un conoscere plurale e sempre incompiuto, praticato da osservatori concretamente mondani che sanno di andare costruendo, interattivamente, il mondo osservato, del quale sono anch'essi parte…

Un termine-problema

Intorno a questo termine problematico prendeva vita in quegli anni nel nostro paese un'intensa e feconda stagione culturale, imperniata sul tema delle premesse epistemologiche e delle implicazioni etico-politiche dei saperi. Una "stagione" estesa ben oltre i soli ambiti scientifico-filosofici, che avrebbe coinvolto diffusamente i mondi delle professioni tecnico-intellettuali – educazione, psicoterapia, organizzazione, medicina, cooperazione, servizio sociale… –, dell'attivismo ecologico-politico e più in generale del dibattito culturale, prolungando il suo raggio d'influenza fino ancora ai nostri giorni…".

Verso una "comunità di destino"

E se ha ragione Manghi a ribadire la forza di questa audace sfida, che ha creato un "collegio invisibile" di intellettuali e ricercatori in costante dialogo sui destini della Terra, va anche detto che questo prestigioso "collegio" ha il suo nume tutelare in Edgar Morin, riconosciuto "maestro di complessità", e il suo "motore" infaticabile in Mauro Ceruti, che ha saputo tenere ben salde le fila di un indirizzo di pensiero che vive dell'intreccio multidisciplinare e degli apporti di esperti che convergono da ogni angolo del globo. Abitare la complessità non è mestiere facile: impone di misurarsi con equilibri geopolitici in divenire e con un assetto dei "saperi" che non ha più nulla a che vedere con il paradigma novecentesco.

La comunità di destino è la condizione che connota l'individuo nella contemporaneità. La lettura del saggio ci mette di fronte a questo dato di realtà, cui non possiamo sfuggire, perché "nessuno è incolpevole". Il "metodo" della complessità, antidogmatico e aperto alla molteplicità degli apporti, è lo strumento di cui dobbiamo servirci, ispirandoci ai valori di un neoumanesimo planetario, che sappia riconoscere a tutti, nessuno escluso, la piena dignità della cittadinanza globale. ■

Oltre la tecnofobia Vittorio Gallese Stefano Moriggi Pier Cesare Rivoltella ed. Raffaello Cortina

Autore: Massimiliano Cannata

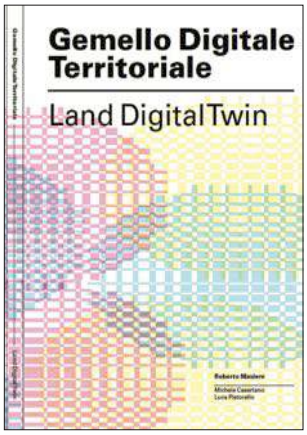
Il vecchio brontolone e Pollicina, perché dobbiamo fidarci della tecnologia

Il *vecchio brontolone* deve lasciare in pace *Pollicina* una volta per tutte, perché i bei tempi andati non erano l'età dell'oro, non è vero che si stava meglio quando si stava peggio. Il percorso che abbiamo fatto, dalla povertà e dalle guerre del Novecento, il superamento dello stato di ignoranza diffuso fino a tempi molto recenti, non può ammettere nostalgie. Alt, dunque, alla "Retrotopia" quello stato dello spirito ben descritto dall'ultimo Bauman, che ci porta a mitizzare il passato, in un

capovolgimento dell'utopia, che lavora sulla speranza per costruire mondi possibili. Il saggio di Gallese, Moriggi e Rivoltella dà, con una scrittura brillante che invoglia il lettore ad andare fino in fondo, una scossa forte alle vecchie categorie degli "apocalittici" e "integrati", non più praticabili in un mondo che è cambiato. Inutile, oltre che improduttivo, condannare lo sviluppo delle tecnologie: fanno parte di noi, *l'homo digitalis*, come spiegano gli autori, ha una sua visione della realtà, una postura, un modo nuovo di essere nel mondo. Lo scritto del grande Michel Serres, richiamato dagli studiosi, fotografa, nella forma del dialogo platonico, uno spaccato del confronto-scontro generazionale che da sempre connota il passare delle epoche. Vecchi e giovani, come scriveva Pirandello; boomer contro nativi digitali come si scrive oggi: il tema rimane sempre lo stesso: comprendere l'innovazione, invece di negarla; farla entrare nel quotidiano sfruttandone le potenzialità, invece di demonizzarla. Esercizio difficile da sempre e in qualunque contesto, ma che non possiamo rinunciare a fare se vogliamo stare nel mondo senza subirlo. "La ricetta non è il controllo, ma la fiducia": concetto particolarmente adatto a chi opera nella cyber security, e che si trova davanti continui cambi di attori e scenario. Il libro propone, nell'ultimo capitolo il "Manifesto dell'Oltretecnofobo", che dovremmo cercare tutti di consultare e praticare. Poche regole chiare e straordinariamente utili per percorrere la strada di una piena cittadinanza digitale, che vale la pena ripercorrere punto per punto.

La tecnologia è umana: non siamo spettatori ma agenti. Pensare con la tecnologia non contro di essa. Critica sì, rifiuto no. La tecnologia non è solo consumo; il digitale è un ambiente, non una minaccia. Non esiste un'unica alfabetizzazione. Il vero pericolo è il determinismo: tecnofobia e tecnolatria sono due facce della stessa medaglia. Il futuro è da scrivere, non da temere.

Il manifesto redatto dagli autori è stato redatto tramite l'interazione con GPT-40. La cooperazione uomo-macchina è dunque possibile. E se cominciassimo da lì, superando le paure che lo stesso Platone nutriva rispetto alla scrittura, tecnologia che - consegnando pensieri e parole alla pagina scritta - avrebbe, per il grande filosofo, portato tutti a perdere la memoria. Il "farmacon" che nella lingua greca è rimedio, ma anche veleno (come viene detto nel dialogo platonico del Fedro, che si può considerare il primo saggio di teoria della comunicazione dell'Occidente) è termine che si addice perfettamente all'ambiguità di fondo che avvolge la nostra visione degli strumenti digitali. Per tramutarsi in rimedio, gli autori suggeriscono di rifarsi a Tisseron, che in *"Diventare grandi all'epoca degli schermi digitali" (ed. Scholé Brescia n.d.r.)* enuncia tre indicazioni operative: *Alternanza, Autoregolazione, Accompagnamento*. Il suo pensiero è rivolto soprattutto ai nostri figli, ma vale per tutti. Come per la dieta mediterranea, non si può stare davanti a uno schermo dimenticando il mondo che ci circonda. E soprattutto, autoregolazione - che si sposa con l'accompagnamento - può emergere se ritorna la parola, il dialogo a interpolarsi tra noi e la macchina. È su questo terreno che l'insegnamento di Platone può tornare utile, a patto di utilizzare correttamente la preposizione, come fanno gli autori che intitolano un capitolo: *Educare nel digitale*, "nel", piuttosto che "al" o "sul", perché siamo dentro il virtuale, come in una dimensione omeopatica. Lo sosteneva Derrick De Kerckhove abituato a seguire le lezioni di un certo McLuhan, che in fatto di media e messaggio qualcosa di importante l'ha certo detta. ■



Gemello digitale territoriale
Land Digital twin
Roberto Masiero (a cura di)
ed. Osservatorio per il paesaggio delle colline di Conegliano Valdobbiadene
Fondazione Francesco Fabbri

Autore: Massimiliano Cannata

Gemello digitale e governance future

Pubblichiamo per gentile concessione dell'editore un estratto dell'introduzione di ***Roberto Masiero****, che figura nelle interviste Vip di questo numero e che ha curato questo approfondito dossier su un tema destinato ad avere impatti sempre più forti per chi si occupa di cyber security .*

"…Scopo dello studio è quello di riflettere, sulle implicazioni e le prospettive aperte dalla costruzione di gemelli digitali territoriali: per rendere efficienti ed efficaci le governance future; per permettere processi di simulazione e gestione della complessità dei fenomeni economici e sociali oltre che territoriali, ambientali e paesaggistici; per poter così organizzare, con e sui dati, piattaforme che permettano la diffusione dei saperi fondamentali per le dinamiche dell'attuale capitalismo cognitivo, in modo da alimentare positivamente l'intelligenza e la creatività collettive; per riaffermare che il paesaggio non è solo ciò che si vede, ma soprattutto ciò che si fa e quindi non va valutato solo dal punto di vista estetico, ma soprattutto da quello etico e politico.

L'idea di fondo è dunque quella di individuare, e mettere in rete, interessi comuni tra coloro che stanno elaborando sperimentazioni e ricerche attorno a queste potenzialità, le istituzioni e le molte professionalità che le animano, i tecnici e gli operatori dei vari momenti e forme del governo dei territori, la politica con la sua progettualità socio economica nella speranza di potere elaborare una roadmap condivisa verso la sperimentazione locale di aree animate e aiutate nella costruzione continua di una propria identità e nella realizzazione altrettanto continua delle proprie potenzialità, da un gemello digitale. Questo perché convinti che se siamo ciò che mangiamo è altrettanto vero che siamo il territorio, l'ambiente e soprattutto il paesaggio che abbiamo costruito e possiamo costruire. Il paesaggio non è ciò che vediamo, ma ciò che facciamo e questo fare può essere governato nel suo insieme dal digitale e in particolare dal gemello digitale e dal metaverso.

Il gemello digitale: una definizione

È la copia di qualcosa di reale, sia esso materiale che immateriale e, nel contempo è una proprietà emergente di quella realtà, maggiore della somma delle parti. Facciamo qualche esempio per intenderci: la riproduzione in modalità digitale della Divina commedia di Dante e la rielaborazione interoperabile di quante interpretazioni vogliamo

dell'opera stessa. L'una e le altre con la propria identità e con le infinte relazioni ed elaborazioni possibili. Non c'è solo l'oggettività delle opere ma anche lo spazio di libertà tra di loro. Uno spazio a nostra disposizione. Altro esempio: la riproduzione in 3D del signor Mario così come noi possiamo riconoscerlo, ma è anche la possibilità di rappresentare e analizzare il suo scheletro, i suoi organi, il suo DNA, ma anche le sue opere, la sua storia, i suoi pensieri, i suoi sogni… aiutando lui e noi a scoprire il di più della sua stessa vita, come dei suoi talenti e persino della sua salute. Altra esemplificazione: la riproduzione in digitale di una macchina reale o immaginaria per simulare tutti i suoi possibili comportamenti reali o potenziali per una valutazione sulla sua efficacia e di tutti i suoi aspetti sociali ed economici, interagendo sia con la simulazione digitale sia con l'integrazione con la cibernetica governandone processi e possibili sviluppi.

Il gemello digitale agisce per interoperabilità. L'interoperabilità è quella capacità di un prodotto o di un sistema informatico di interagire e funzionare con altri prodotti o sistemi esistenti o ancora in divenire senza alcuna restrizione per l'accesso o per le relative implementazioni. Grazie all'interoperabilità, sistemi informativi eterogenei possono quindi dialogare tra loro, attivando in modo automatico dei processi elaborativi con scambi di informazioni e con la possibilità di attivare autonomamente azioni, quindi applicazioni. Con il supporto dell'Intelligenza artificiale il gemello digitale può attivarsi in modalità decisionale e può interagire con un orizzonte pressoché infinito di informazioni (di saperi) e di relative rielaborazioni sia cognitive che decisionali. È la possibilità di valutare (anche in autovalutazione) e di governare tutte le relazioni che esistono tra i dati materiali e immateriali del territorio, degli ambienti, dei paesaggi e tutte le attività materiali e immateriali che caratterizzano quei determinati territori. Non essendo più il territorio mero oggetto di estrazione di valori materiali, ma deposito dell'intelligenza e della creatività collettiva, il gemello digitale territoriale è ciò che rende riconoscibile, attivo, propositivo e fattuale questo deposito, rendendo i singoli soggetti pubblici e privati consapevoli e responsabili delle loro stesse decisioni, nella trasparenza e condivisione che solo il digitale può permettere.

A cosa serve il gemello digitale

A comprendere e governare le relazioni esistenti tra i molteplici fattori che caratterizzano i territori in quanto produttori e accumulatori di intelligenza e creatività collettiva e quindi di innovazione. Il gemello digitale territoriale elabora le relazioni tra i dati permettendo di governare le dinamiche e i flussi secondo ragioni predeterminate, ma anche di cogliere aspetti che usualmente non vengono comparati. Per esempio, può mostrare in tempo reale, e in continuo, come processi, le relazioni tra mobilità territoriale, inquinamento, salute pubblica e privata. Oppure può permetterci di individuare le relazioni fattuali tra la formazione, il trasferimento dei saperi e le varie attività produttive. Il gemello digitale non permette solo l'accumulazione e la elaborazione dei dati, ma individua e analizza processi ed è infinitamente implementabile (tende quindi ad essere un sistema vivente) ed è la base di un fondamentale oggi processo di sensorizzazione dei territori sempre più necessario per attivare una qualche governance rivolta all'economia circolare e alla sostenibilità. Il gemello digitale può essere liberamente disponibile per qualsiasi soggetto che operi in un determinato territorio che potrà nel contempo risultare sia come utente dei dati e della loro elaborazione che produttore degli stessi in un rinnovato intreccio tra pubblico e privato, permettendo infine di valutare singolarmente e collettivamente (cioè politicamente) il bene comune e le sue dinamiche"... ■

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

www.swissacademy.eu

www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

DONA ORA

Il tuo contributo è prezioso 💎
https://www.cybertrends.it/supportaci/