swisscom

Cybersecurity Threat Radar 2026

Geopolitica e tecnologie dirompenti come fattori di minaccia

Indice

«La fiducia non è una promessa che si fa una volta sola, ma una responsabilità che dobbiamo assumerci ogni giorno. In qualità di Innovators of Trust proteggiamo non solo i dati, ma anche l'affidabilità digitale e la sovranità della Svizzera.

Cybersecurity Threat Radar

Geopolitica e tecnologie dirompenti come fattori di minaccia

Ogni giorno noi di Swisscom non ci limitiamo a proteggere i sistemi, ma promuoviamo anche la digitalizzazione della Svizzera. Milioni di persone si affidano a reti stabili, comunicazioni sicure e resilienza digitale. In qualità di CSO, noto quotidianamente come le tensioni geopolitiche e i balzi in avanti tecnologici si ripercuotano direttamente sulla sicurezza. Oggi le minacce nascono a livello globale, ma i loro effetti possono colpirci in qualsiasi momento anche localmente.

Il Cybersecurity Threat Radar è il nostro strumento di allerta preventiva, che ci mostra in quale direzione si muovono le minacce, quali nuovi schemi emergono e dove è necessario intervenire. Quest'anno mi ha particolarmente preoccupato il fatto che per la prima volta abbiamo dovuto incorporare come nuovo vettore di minaccia l'hybrid warfare, ovvero una combinazione di mezzi militari classici con attacchi informatici, disinformazione e influenza digitale e politica. Questo sviluppo dimostra quanto la sicurezza fisica e quella digitale siano ormai strettamente collegate.

Le incertezze geopolitiche e i conflitti di interesse economici stanno portando a un aumento degli attacchi informatici di matrice statale, attacchi che mettono a repentaglio non solo le aziende, ma la stabilità digitale di tutta la Svizzera. In qualità di operatore di telecomunicazioni avvertiamo quanto la capacità di adattamento e la resilienza rivestano un ruolo sempre più centrale.

Anche le tecnologie dirompenti cambiano il campo di gioco. L'intelligenza artificiale, l'informatica quantistica e i dispositivi connessi in rete aprono enormi opportunità di innovazione e, allo stesso tempo, nuove possibilità di attacco. La protezione della Svizzera digitale e delle persone che ogni giorno contano su di noi rimane la massima priorità per Swisscom.

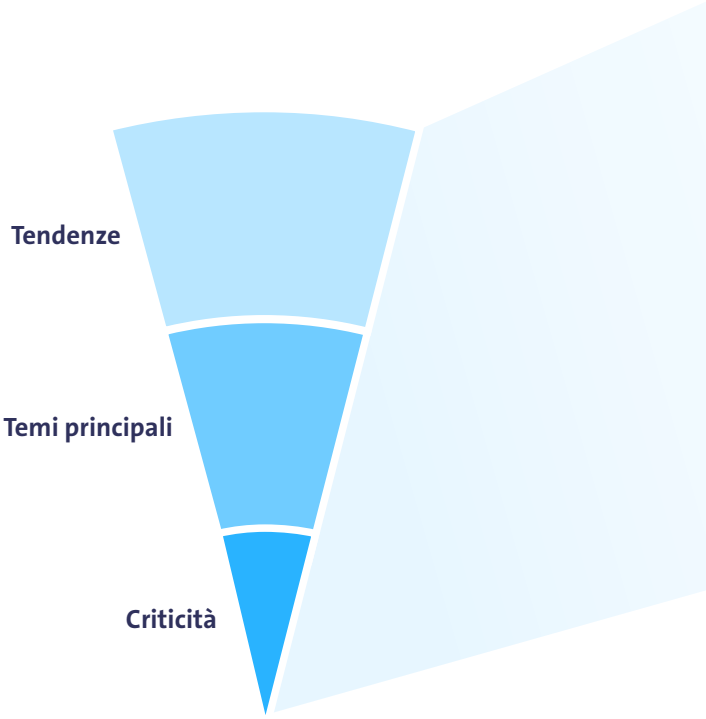
Tutto questo dimostra che la sicurezza non è qualcosa da dare per scontato, ma un processo continuo che richiede un'azione lungimirante, l'analisi costante delle nuove minacce e una cultura della sicurezza vissuta concretamente in tutta l'azienda. Solo sviluppando costantemente e attuando con coerenza le nostre misure di protezione potremo affrontare in modo efficace i complessi rischi del nostro tempo e rafforzare in modo affidabile la Svizzera digitale.

Marco Wyrsch
Head of Group Security
& Chief Security Officer

Quadro della situazione – radar delle minacce

Poter attingere, al momento opportuno, a strategie e procedure di sicurezza consolidate e testate ci aiuta a meglio affrontare gli imprevisti – i cosiddetti «cigni neri». Abbinandovi una cultura della sicurezza coerente, trasparenza degli errori e personale ben addestrato, gettiamo le basi per la resilienza organizzativa.

A tal fine bisogna riconoscere le minacce potenziali in una fase precoce e rilevarle sistematicamente. Per mappare lo stato attuale delle minacce e la sua evoluzione, ci avvaliamo dell'ormai noto Cybersecurity Threat Radar.




Environment/Social
Dominant Players
Technology Dynamics
Organisation
Physical
Security Job Market
Geopolitical Situation / State Level Attacks
Data-Centric Risks
Identity Theft & Impersonation
Disinformation & Destabilisation
Political Influence
Hybrid Warfare
Environmental Influence
Targeted Sabotage
Unsecure IoT/OT
Digital Transformation Risks
UAS Threats
Energy Instability
Manipulated Generative AI
Cloud Ecosystem Dependencies
Legacy Protocols
Infrastructure Integrity
Subscriber Compromise
Agentic AI
Increased Complexity
DDoS Attacks
Ransomware
AI-Based Attacks
Supply Chain Attacks
Targeted Attacks
Unsecure AI
Residential Proxies
Fraud
Security Skills
Insider Threat
Quantum Computing
Infrastructure Misconfiguration
Fragile Workforce
Decentralised Development & Operations
Workplace Heterogeneity
Sfide
Today
Tendency

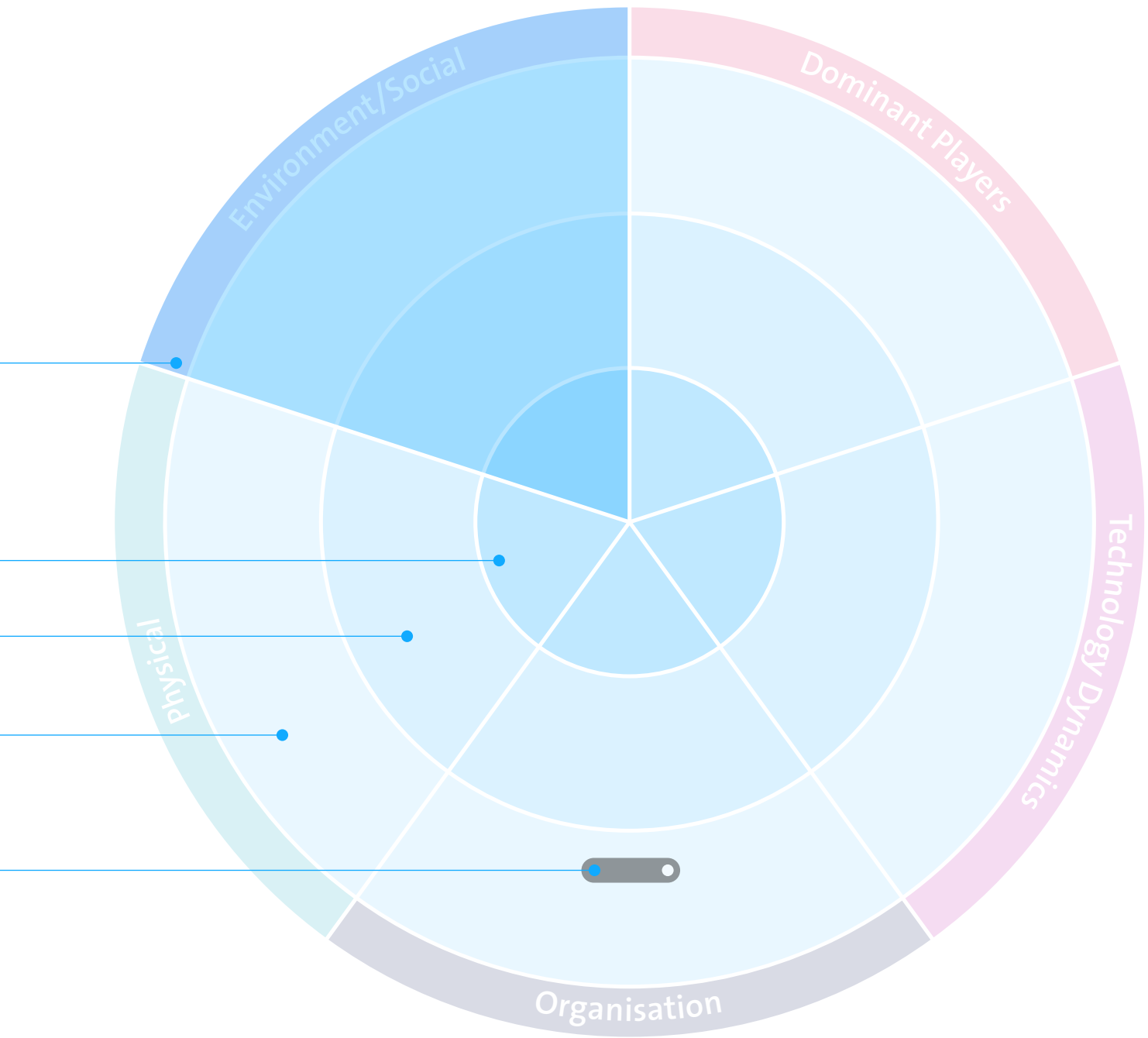
Metodica

Il radar delle minacce si suddivide in cinque **segmenti** assegnati ognuno a un diverso ambito di rischio. Le minacce appartenenti a un **segmento** possono essere assegnate a uno dei tre cerchi concentrici, che indicano il grado di attualità della minaccia e, quindi, anche il grado di severità con cui si valuta la minaccia. Quanto più la minaccia è vicina al centro, più è concreta e più è importante adottare contromisure appropriate.

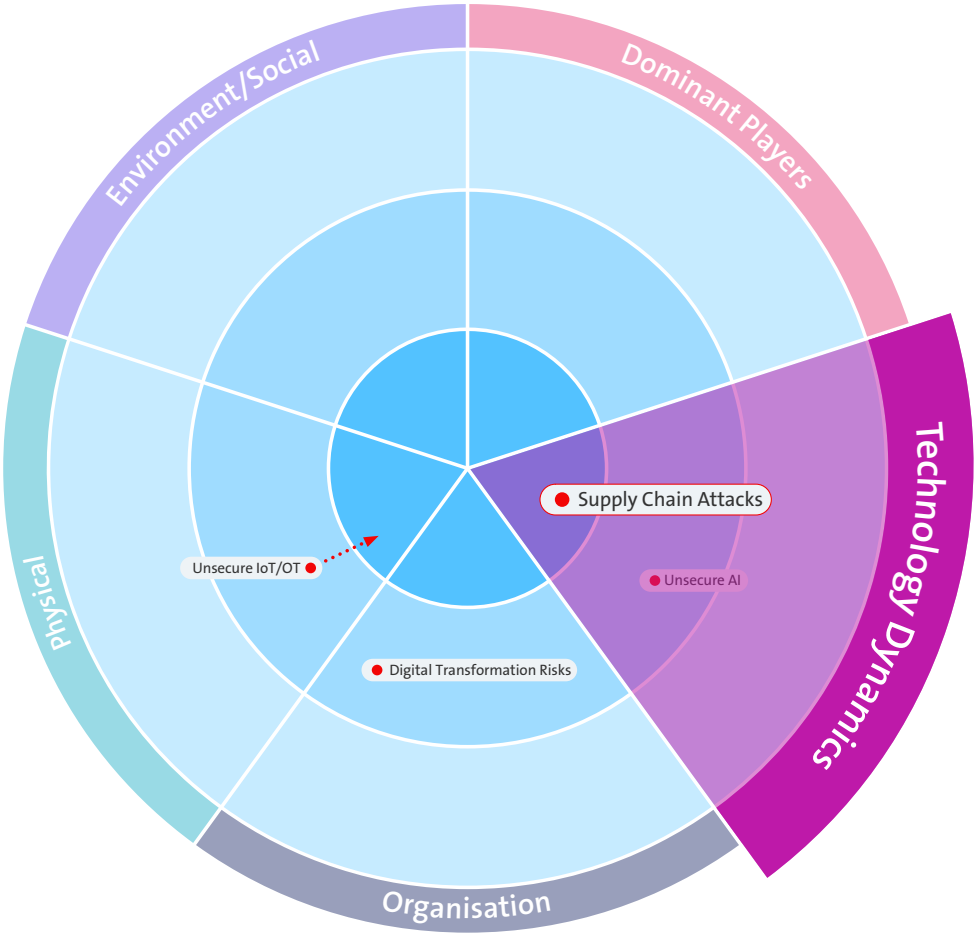
Descriviamo i cerchi come

- **criticità** per le minacce reali affrontabili con un dispendio di risorse relativamente importante;
- **temi principali** per le minacce già insorte sporadicamente e affrontabili con un impiego di risorse normale. Spesso esistono processi regolamentati per contrastare efficacemente tali minacce;
- **tendenze:** allerta precoce di minacce ancora mai concretizzate o attualmente piuttosto remote. Sono stati avviati progetti per contrastare in una fase precoce l'importanza crescente di queste minacce.

Inoltre, le singole **minacce** assegnate a questi ambiti delineano una **tendenza** la cui criticità può essere stabile, in aumento o in calo. La lunghezza del fascio di tendenza indica la probabile velocità con cui varierà la criticità della minaccia.


Environment/Social
Dominant Players
Technology Dynamics
Organisation
Physical

La catena di fornitura del software nella supply chain: un castello di carte fatto di codice straniero



In un mondo del business sempre più digitalizzato, le aziende dipendono da un'ampia gamma di soluzioni e servizi software. L'integrazione di componenti e moduli esterni è diventata da tempo uno standard, ed è proprio qui che risiede una delle maggiori sfide della sicurezza IT attuale: i supply chain attack, ovvero gli attacchi alla catena di fornitura di software. Un singolo punto debole è sufficiente per far crollare l'intero castello di carte.

Il software moderno è costituito da centinaia di componenti esterni e da build pipeline automatizzate. L'origine e la qualità di questo codice di terze parti spesso non sono tracciabili in maniera trasparente, il che rende molto più difficile individuare le vulnerabilità. Proprio questa mancanza di trasparenza rende la catena di fornitura del software un obiettivo privilegiato per gli attacchi. Bastano una libreria compromessa o un sistema CI/CD manipolato per avere un impatto su migliaia di aziende.

Particolarmente delicato è il fatto che molte aziende si affidano a componenti di cui non sono in grado di verificare autonomamente il livello di sicurezza.

Lo stato attuale delle minacce: esempi e tendenze

Nel 2025, eventi come «Shai-Hulud» nell'ecosistema npm (il più grande registro per i pacchetti JavaScript) hanno evidenziato l'avvento di una nuova realtà, nella quale gli hacker prendono di mira il codice open source e abusano della catena di fiducia dei pacchetti più diffusi per diffondere malware tramite update apparentemente legittimi. Poiché questi update vengono spesso adottati senza controlli di sicurezza aggiuntivi o verifiche manuali e poi distribuiti come dipendenze, questi attacchi possono diffondersi in modo particolarmente rapido lungo l'intera catena di fornitura del software.

Inoltre, esistono i cosiddetti single point of failure, servizi centralizzati o fornitori che in caso di guasti o compromissioni, come recentemente accaduto con CrowdStrike, Microsoft o Cloudflare, possono comportare conseguenze significative per molte aziende.

Perdita di dati, interruzione dell'attività e danni alla reputazione

Le conseguenze di attacchi riusciti alla catena di fornitura del software sono gravi. Oltre alla perdita di dati sensibili, vi è il rischio di interruzioni dell'attività che, nel peggiore dei casi, possono portare all'arresto di processi critici dal punto di vista commerciale. Non vanno inoltre sottovalutati i danni alla reputazione causati da incidenti di sicurezza resi pubblici e che possono minare durevolmente la fiducia di clienti, partner e investitori.

Rafforzare la verificabilità e la resilienza
Per far fronte alle sfide poste dalla moderna catena di fornitura del software sono necessarie misure tecniche e organizzative come le seguenti:

- La documentazione coerente e il tracciamento di tutti i moduli utilizzati e il loro aggiornamento
- Controlli di sicurezza regolari (audit) e penetration test lungo l'intera catena di fornitura
- Definizione di processi chiari per la selezione, la valutazione e l'approvazione di componenti software esterni
- Impiego di soluzioni di monitoraggio che riconoscono e segnalano tempestivamente attività sospette
- Sviluppo e attuazione di strategie di update per risolvere tempestivamente le vulnerabilità note

Dal punto di vista normativo, il **Cyber Resilience Act (CRA)** e la **Network and Information Security Directive 2 (NIS2)** dell'Unione europea segnano una svolta, perché costringono i produttori a dimostrare come è stato creato il loro software e gli operatori a verificare le prove fornite. SBOM (Software Bill of Materials), build riproducibili, firme e gestione documentata delle vulnerabilità diventano quindi obbligatori. L'integrità e l'origine non sono più presupposte, ma comprovate tecnicamente.

Da questo punto di vista, due concetti sono fondamentali:

- **Integrità:** un update è autentico e non modificato?
- **Provenance:** come, dove e con cosa è stato creato?

Standard come SLSA (Supply-Chain Levels for Software Artifacts) o SBOM firmate forniscono per la prima volta prove resistenti alla falsificazione.

> Solo quando ogni artefatto software viene firmato in modo crittografato e la sua origine può essere documentata in maniera inequivocabile si creano le basi per una vera fiducia.

Florian Lukavsky
Chief Innovation Officer, SignPath

Poiché tali verifiche sono difficilmente realizzabili manualmente, piattaforme specializzate per la sicurezza della supply chain del software adottano attestazioni automatizzate e crittografate direttamente nel processo di build. In questo modo la sicurezza può essere verificata e non è più basata solo sulla fiducia.

È necessario un cambiamento di mentalità anche a livello organizzativo. Le aziende devono monitorare costantemente la propria catena di fornitura, gestire attivamente le vulnerabilità e obbligare i propri partner a rispettare standard minimi per preservare la resilienza contro gli attacchi di tipo supply chain. Anche la sensibilizzazione del personale sui rischi e la creazione di una cultura della sicurezza sono elementi fondamentali.

Resilienza e verifica continua come fattori chiave

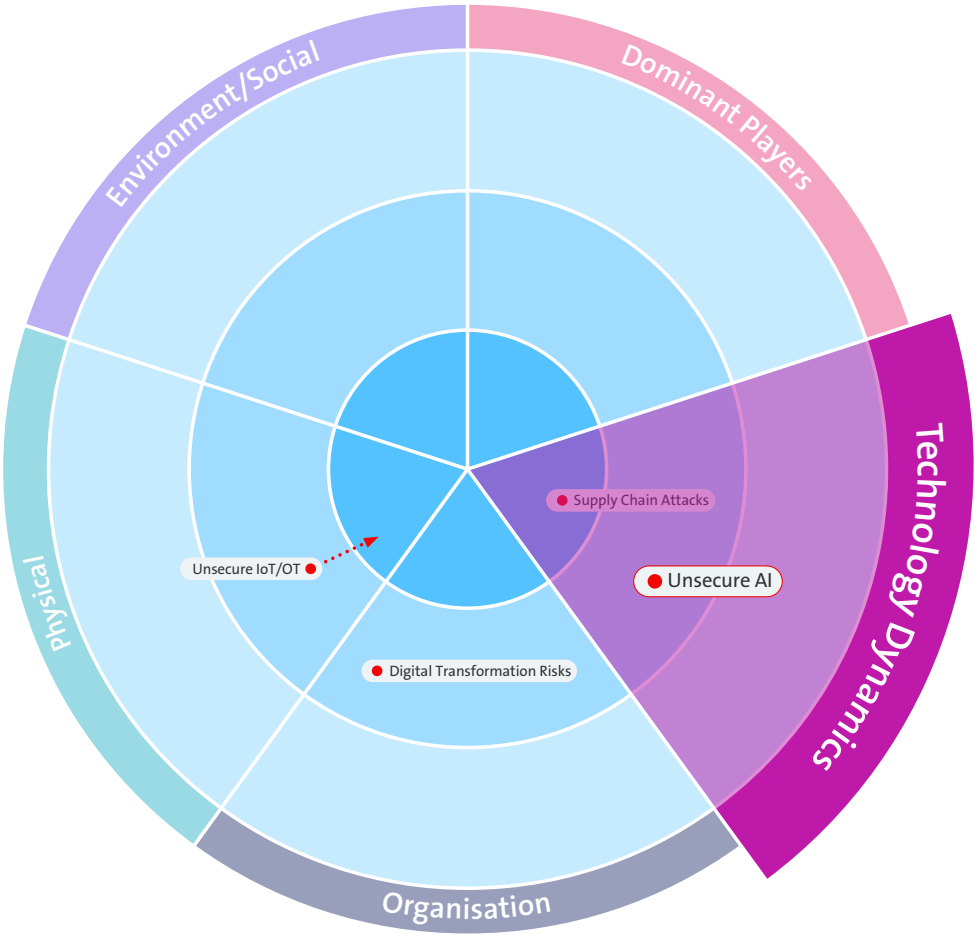
La minaccia rappresentata dagli attacchi supply chain continuerà ad accompagnare le aziende anche in futuro e a diventare sempre più rilevante. Chi punta sui vantaggi di un software moderno e modulare deve essere consapevole dei rischi e investire sistematicamente nella propria resilienza. Verifica continua, trasparenza e una gestione integrata del rischio sono i pilastri fondamentali per mantenere il proprio castello di carte IT stabile anche in tempi turbolenti ed evitare la «roulette russa» nella catena di fornitura del software.

> Oggi non si può ancora fare a meno della fiducia. Ma è assolutamente necessario confrontarsi con i possibili punti deboli nella catena di fornitura del software, ad esempio con una modellizzazione mirata delle minacce lungo l'intera supply chain.

Simon Röthlisberger
Security Architect

Sfide e tendenze

L’IA a tutto gas: il moltiplicatore del rischio



L'intelligenza artificiale si è diffusa a una velocità impressionante in molti settori della nostra società e dell'economia. Il clamore che circonda le tecnologie IA è talmente grande che le questioni critiche su sicurezza, trasparenza e sostenibilità possono passare in secondo piano. In particolare, il vettore di minaccia «unsecure AI» mostra con quale rapidità l'inesperienza possa trasformarsi in un'architettura di sistema pericolosa, con effetti che vanno ben oltre l'IT.

Questo articolo analizza perché ci troviamo a confrontarci con un'IA non sicura, come nascono questi rischi e cosa possono fare concretamente gli attori coinvolti per affrontare le sfide in modo positivo e responsabile.

Perché l'unsecure AI è un rischio

L'entusiasmo per l'IA induce spesso a introdurre innovazioni senza una comprensione approfondita o senza sufficienti considerazioni sulla sicurezza. I sistemi IA vengono utilizzati «a tutto gas», senza sapere dove e come influenzano le decisioni operative, con quali dati sono stati addestrati o chi è stato coinvolto nel processo di sviluppo. Non di rado vengono utilizzate soluzioni low-code e no-code la cui origine e architettura non sono tracciabili per gli utenti. Particolarmente critico è il fatto che anche le aziende partner integrano l'IA, il che crea supply chain risk (v. pagina 10) difficili da controllare. A ciò si aggiunge il fatto che sempre più spesso i software dannosi vengono introdotti nei sistemi direttamente durante la programmazione, ad esempio attraverso l'IA generativa.

Ma il pericolo non è solo la tecnologia, perché anche la mancanza di know-how da parte degli utenti e degli esperti informatici aggrava il problema. L'errata conclusione secondo la quale il personale meno esperto potrebbe essere sostituito dall'IA porta a una lacuna di competenze che a medio termine può indebolire l'intera struttura di sicurezza, inclusi settori come data quality management, supply chain management.

Come nascono i punti deboli?

Un'IA non sufficientemente sicura ha luogo quando i processi di sicurezza vengono trascurati, i requisiti di trasparenza ignorati e le regole di governance non sono rispettate. I modelli basati sull'IA vengono utilizzati nei sistemi produttivi senza che il loro funzionamento, la base di dati o la logica decisionale siano stati verificati e documentati.

I tool e le piattaforme low-code consentono anche alle persone meno esperte di creare applicazioni di intelligenza artificiale: un vantaggio in termini di innovazione, ma che aumenta anche l'area di attacco se ci si affida ciecamente al 100% agli output dell'IA. Nella catena di fornitura, i modelli e i dati vengono spesso acquisiti da terzi senza essere consapevoli dei rischi per la sicurezza e senza implementare preventivamente standard di sicurezza uniformi.

L'impiego dell'IA nel bug bounty management, dove le segnalazioni sono automatizzate e quindi più numerose ma di qualità inferiore, dimostra chiaramente quanto sia difficile distinguere tra vere vulnerabilità e false segnalazioni. Il risultato è un mosaico di sistemi in cui nessuno ha più il controllo di come, dove e con quale integrità viene impiegata l'IA.

Strategie positive per più sicurezza

I rischi sono grandi, ma esistono numerosi approcci con cui aziende e privati possono affrontare queste sfide in modo costruttivo:

- **Creare trasparenza:** ogni applicazione IA deve essere documentata, includendo l'origine dei dati, gli algoritmi utilizzati e la logica decisionale. Solo in questo modo è possibile individuare e controllare i rischi.
- **Formazione e sensibilizzazione:** la formazione continua è essenziale per tutte le persone coinvolte. La competenza in materia di IA non deve essere riservata solo agli esperti, ma radicata in tutta l'organizzazione.
- **Team multidisciplinari:** nello sviluppo e nell'introduzione dell'IA dovrebbero essere coinvolti anche team di IT, diritto, etica e altri settori specialistici. In questo modo si sfruttano diverse prospettive e competenze per individuare tempestivamente i rischi.
- **Responsabilità e governance:** definire responsabilità chiare per i sistemi di IA e regole per la sua gestione. Questo include anche l'esecuzione di audit e revisioni da parte di organismi indipendenti.
- **Cultura dell'errore e scambio di opinioni:** errori e lacune nella sicurezza dovrebbero essere comunicati apertamente per trarne insegnamenti e migliorare continuamente i processi. Una gestione trasparente dei punti deboli rafforza l'intera organizzazione.

> « In un mondo di low-code chaos e automazione IA, un programma bug bounty diventa un sismografo per i rischi reali.

Antoine Neuenschwander
Head Bug Bounty

- **Etica e sostenibilità:** oltre a criteri tecnici ed economici, ogni applicazione IA deve essere valutata anche dal punto di vista etico e sociale.
- **Promozione delle nuove leve:** la promozione delle nuove leve nel settore della sicurezza rimane fondamentale. Junior e senior devono lavorare insieme a soluzioni, perché l'IA può integrare le competenze, ma non sostituirle.

Coinvolgere il personale

È importante affrontare apertamente gli aspetti etici, morali e legati alla sostenibilità dell'IA. Affinché il personale possa tenere il passo con la rapidissima evoluzione dell'IA, è necessario creare l'ambiente adatto. In questo modo, le competenze dei dipendenti possono essere rafforzate attraverso training mirati, ad esempio tramite format di sensibilizzazione come i promptathon.

Questo corrisponde a un change management attivo e consapevole.

« Se vogliamo ‹l'IA a tutto gas› nelle aziende, abbiamo bisogno soprattutto di una leadership che metta l'umanità davanti alla velocità nella digitalizzazione. La cultura non nasce dai tool, ma dai modelli. E prima di diffondere l'IA su larga scala, dobbiamo fornire alle persone le competenze necessarie per servirsene.

Marcus Beyer
Security Awareness Officer

Sfide e tendenze

Sovranità digitale: a chi l'ultimo salvagente nel vortice della trasformazione?

Nella vita di tutti i giorni o al lavoro, la trasformazione digitale è ormai ovunque e porta con sé regole del tutto nuove per le aziende svizzere. I dati stanno diventando sempre più importanti, l'IT sta migrando nel cloud e molti processi vengono ormai eseguiti esternamente. Ed è proprio per questo che il tema della sovranità digitale è così in voga al momento. Inoltre, i cambiamenti geopolitici ne aumentano l'urgenza. Oggi più che mai, le aziende devono mantenere una visione d'insieme dei loro dati e delle loro operazioni digitali; un compito non facile in un mondo interconnesso.

Ma cosa significa esattamente sovranità digitale e perché è così importante per le aziende svizzere proprio ora? Mentre la digitalizzazione avanza costantemente e sempre più processi vengono trasferiti dalle mani delle aziende al cloud o a fornitori di servizi esterni, si pone la questione di come le organizzazioni possano assicurarsi capacità di agire e controllo. È quindi necessario comprendere chiaramente il significato della sovranità digitale e le sfide e opportunità concrete che comporta.

In linea di principio, le aziende e le organizzazioni devono essere sempre in grado di controllare, gestire e proteggere le proprie risorse digitali in modo autonomo e indipendente, in particolare i dati e le infrastrutture IT. La dipendenza da fornitori di servizi esterni stranieri, in particolare per quanto riguarda cloud e outsourcing, non deve superare un livello commensurato.

Per le imprese svizzere la sovranità digitale è rilevante per diversi motivi:

- Le leggi sulla protezione dei dati, come la nuova legge svizzera sulla protezione dei dati (nLPD) e il GDPR europeo, richiedono che le aziende sappiano dove vengono archiviati i loro dati e chi vi ha accesso.
- Il controllo di dati e sistemi è un fattore di importanza centrale per la sicurezza delle informazioni. Con l'aumentare della dipendenza da terzi, incrementa anche l'area di attacco.
- Nel peggiore dei casi, chi non controlla i propri dati può compromettere l'accesso al proprio capitale più importante e rischia di perdere forza innovativa e posizione sul mercato.

Outsourcing e cloud – la perdita di controllo come rischio: la sovranità dei dati è un'illusione?

L'esternalizzazione dei servizi IT e l'utilizzo di piattaforme cloud offrono enormi vantaggi in termini di scalabilità, costi e flessibilità. Soprattutto per le aziende svizzere, l'outsourcing a fornitori specializzati è spesso conveniente dal punto di vista economico. Allo stesso tempo, con ogni atto di outsourcing si perde una parte del controllo su dati e processi.

Molte aziende sottovalutano i rischi associati alla cessione di dati a fornitori terzi:

- **Dipendenza dal fornitore:** i costi di cambio e gli ostacoli tecnici rendono difficile cambiare operatore o tornare al precedente («vendor lock-in»).
- **Perdita di trasparenza:** spesso non è chiaro dove e come i dati vengano effettivamente elaborati, in particolare per i fornitori di servizi cloud internazionali.
- **Incertezza giuridica:** spazi giuridici diversi (ad es. conservazione dei dati nell'UE o negli USA) rendono più difficile l'applicazione dei propri requisiti in materia di protezione dei dati e sicurezza.
- **Rischi di cybersicurezza:** la concentrazione di dati sensibili su grandi piattaforme cloud le rende bersagli allettanti per i criminali informatici.

La tanto decantata sovranità dei dati rimane spesso un'illusione nella pratica, soprattutto quando le aziende non dispongono dei meccanismi di controllo e delle competenze necessari per gestire i flussi di dati e le dipendenze.

Con la nuova legge sulla protezione dei dati (nLPD), dal settembre 2023 la Svizzera dispone di una delle normative sulla protezione dei dati più moderne d'Europa. Le aziende svizzere devono attuare i principi «Privacy by Design» e «Privacy by Default», rispettare i diritti delle persone interessate e adempiere agli obblighi di notifica in caso di violazioni della protezione dei dati.

Particolarmente rilevante è la questione se e come i dati possano essere trasferiti all'estero. In questo caso si applicano disposizioni rigorose per la trasmissione a paesi terzi, in particolare se questi non offrono un livello adeguato di protezione dei dati. Per molte aziende si pone quindi la questione se i partner per cloud e outsourcing debbano avere sede in Svizzera o all'estero.

I grandi fornitori svizzeri come Swisscom si posizionano esplicitamente come partner affidabili per le infrastrutture digitali e offrono soluzioni cloud con conservazione dei dati in Svizzera. In questo modo affrontano i requisiti specifici di protezione dei dati e sovranità che sono decisivi per molte aziende.

> «Oggi tutte le aziende hanno l'obbligo di essere consapevoli della propria sovranità digitale e di gestirla attivamente.

Lukas Hebeisen
Senior VP Cloud & Datacenter Solutions

Oltre alla conservazione dei dati in Svizzera, è rilevante anche la questione sul diritto nazionale al quale è soggetto il fornitore. Occorre tenere presente che i fornitori statunitensi sono soggetti al diritto americano, anche se i dati si trovano in centri di calcolo svizzeri.

«Plus AI o Minus AI?»: effetti sulla sovranità digitale

L'attuale dibattito sull'intelligenza artificiale è sempre più caratterizzato da una situazione conflittuale che si può suddividere a grandi linee in due schieramenti: Plus AI, una prospettiva ottimistica delle opportunità tecnologiche, e Minus AI, una visione da realistica a critica di rischi, dipendenze e perdita di controllo. Per le imprese svizzere questo ambito conflittuale è particolarmente rilevante, poiché influisce sulla questione della sovranità digitale in misura mai vista prima.

Da un lato, l'uso dell'IA promette enormi vantaggi, come l'automatizzazione delle attività ripetitive, l'aumento dell'efficienza, processi decisionali basati sui dati e nuovi modelli di innovazione. Le aziende che utilizzano l'IA in modo sistematico e responsabile ottengono un netto vantaggio competitivo e possono rafforzare la propria resilienza digitale. In questo contesto, l'IA può addirittura fungere da motore per la sovranità, a condizione che le aziende mantengano il controllo sui dati, i modelli e le catene del valore di loro proprietà.

> La sovranità digitale nasce quando si identificano dati e applicazioni di importanza critica e si scelgono soluzioni locali affidabili. Questo non esclude l'utilizzo di servizi globali innovativi per ambiti meno critici.

Thomas Stemmler
Head of Regulatory & Policy

Dall'altro lato, le tecnologie IA rafforzano i rischi già esistenti della trasformazione digitale. Con ogni nuova generazione di sistemi IA aumenta la dipendenza da grandi provider tecnologici, spesso internazionali. Modelli, dati sulla formazione, infrastrutture e manutenzione sono spesso al di fuori del controllo diretto delle aziende. Il pericolo rappresentato dalla «shadow AI», ossia l'utilizzo nel lavoro quotidiano di tool di IA non autorizzati o non controllati, è in aumento e mina le strutture di governance esistenti. A ciò si aggiunge la crescente complessità dei requisiti normativi, che rende ancora più difficile un utilizzo dell'IA conforme alla legge. In questo scenario «Minus AI», la sovranità digitale diventa rapidamente una sfida, se non addirittura un'illusione.

Non è la tecnologia a determinare se l'IA rafforzerà o indebolirà la sovranità digitale, quanto piuttosto il modo in cui le aziende la affrontano. Scelta consapevole dei partner, flussi di dati trasparenti, governance chiara, competenze interne e meccanismi tecnici di protezione sono decisivi per determinare se l'IA porterà a un guadagno in termini di sovranità o a una perdita di controllo. Le aziende che investono in queste competenze possono utilizzare l'IA come leva strategica, non solo per l'efficienza e l'innovazione, ma anche per proteggere la propria indipendenza digitale.

Qualche consiglio: cosa possono fare attivamente le aziende per mantenere la sovranità digitale?

Per evitare che la sovranità digitale diventi un'illusione, le aziende svizzere dovrebbero adottare le seguenti misure:

- **Gestione strategica:** definire una chiara strategia di digitalizzazione e dati, che disciplini anche il rapporto con fornitori di servizi esterni e cloud service.
- **Valutazione e gestione del rischio:** analizzare regolarmente i rischi legati all'outsourcing e all'utilizzo del cloud e sviluppare piani di emergenza in caso di perdita o uso improprio dei dati. Valutare anche gli effetti della perdita improvvisa dell'accesso ai sistemi IT o della modifica inattesa delle condizioni quadro da parte di un produttore.
- **Misure tecniche e organizzative:** utilizzare la crittografia, la gestione degli accessi e il monitoraggio per rendere i flussi di dati e gli accessi trasparenti e controllabili.
- **Copertura contrattuale:** adottare chiare regole contrattuali in materia di protezione, accesso e portabilità dei dati, oltre a strategie di uscita in caso di cambio di fornitori di servizi.
- **Scelta oculata dei partner:** affidarsi a fornitori che garantiscano la conservazione e l'elaborazione dei dati in Svizzera. Verificare regolarmente il rispetto degli standard concordati.

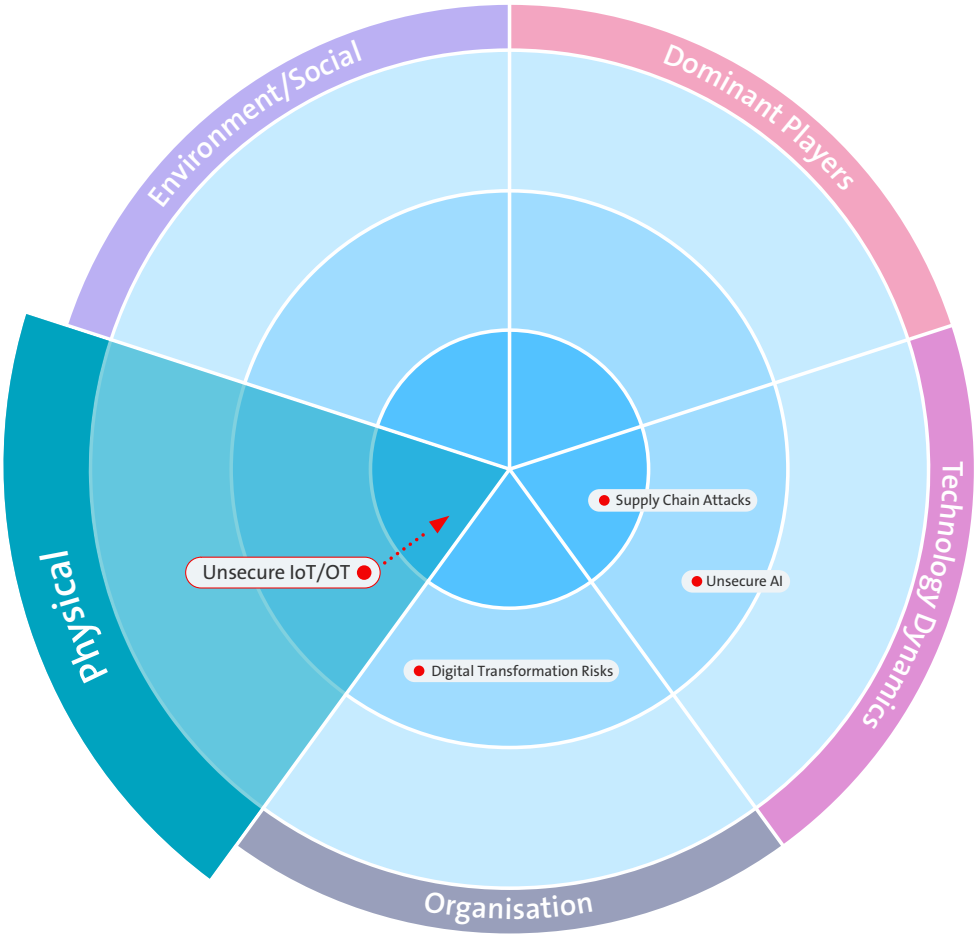
- **Formazione e sensibilizzazione:** istruire regolarmente il personale sulla gestione dei dati sensibili e sui rischi della trasformazione digitale.
- **Monitoraggio normativo:** seguire gli sviluppi nella protezione dei dati e adeguare costantemente i propri processi ai nuovi requisiti di legge.

La sovranità come obiettivo

In un'economia globalizzata e digitalizzata, il controllo completo su tutti i processi e i dati digitali è difficilmente realizzabile. La sovranità digitale rimane un obiettivo impegnativo, al quale le aziende possono avvicinarsi solo attraverso una combinazione di gestione strategica, competenza tecnica e scelta accurata dei partner. L'outsourcing e l'utilizzo del cloud non comportano di per sé una perdita di controllo, a condizione che le aziende adottino le misure giuste e gestiscano attivamente i propri rischi. Ma si tratta di un compito complesso che richiede conoscenze molto specializzate. È fondamentale stabilire consapevolmente quali competenze vengono sviluppate internamente e quali acquisite esternamente.

Chi è consapevole dei rischi, agisce in modo proattivo e punta su partner affidabili può gestire la trasformazione digitale con successo e in sicurezza e quindi non soccombere nel vortice della trasformazione, ma uscirne addirittura rafforzato.

OT security: l'elefante nella stanza che lentamente diventa visibile



Cosa hanno in comune gli impianti di produzione, le infrastrutture di approvvigionamento, i sistemi di trasporto, i dispositivi medici e l'automazione degli edifici? Negli ultimi anni molti di questi sistemi, importanti per l'operatività delle aziende, sono stati fortemente trascurati dal punto di vista della cybersicurezza e ora sono sempre più esposti alle minacce. La progressiva digitalizzazione nella produzione, il crescente interesse dei cybercriminali per le «prede facili» e la mutata situazione della sicurezza globale hanno determinato un aumento degli attacchi alle infrastrutture critiche.

I rischi che ne derivano per le imprese sono molteplici: da costi elevati dovuti a macchine guaste, produzione inutilizzabile, danni alla reputazione e all'ambiente fino a pericoli immediati per l'incolumità fisica e la vita del personale. Per molto tempo questi rischi sono stati il proverbiale elefante nella stanza, di cui nessuno voleva parlare. Ora però tutto questo è finito, l'elefante diventa sempre più visibile e non può più essere ignorato.

L'operational technology (OT) comprende tutti i sistemi che controllano, monitorano e automatizzano i processi fisici e interagiscono con il mondo reale: dall'impiantistica degli edifici alle linee di produzione e alle reti di approvvigionamento energetico, fino ai dispositivi medici negli ospedali. Con la crescente interconnessione (Industria 4.0 e IoT), i confini tra IT e OT diventano sempre più confusi. L'interfaccia tra IT e OT è il punto più critico delle moderne architetture degli impianti. Mentre nell'IT domina il paradigma della riservatezza, nell'OT sono disponibilità e tempi di reazione immediati ad avere la massima priorità. Un riavvio del sistema dopo un aggiornamento di sicurezza nella routine dell'IT può comportare un arresto della produzione nell'OT, che può influire direttamente sul bilancio.

Le sfide maggiori sono:

- **Varietà di protocolli:** i sistemi OT utilizzano spesso protocolli proprietari o obsoleti che in origine non erano stati progettati per il collegamento a internet.
- **Diversi cicli di vita:** mentre l'hardware IT viene rinnovato ogni 3-5 anni, gli impianti OT rimangono spesso in uso per decenni, compresi i sistemi operativi obsoleti per i quali non esistono più patch di sicurezza.
- **Penetrazione di malware:** le interfacce non sicure consentono ai ransomware di passare direttamente dalla rete dell'ufficio al livello di controllo (SPS/PLC) e di manipolare fisicamente la produzione.
- **L'«air gap» non offre una protezione assoluta:** un laptop hackerato è sufficiente per far penetrare un codice dannoso direttamente nel cuore della produzione. Grazie a questo accesso diretto, gli hacker aggirano i classici meccanismi di difesa IT e possono sfruttare immediatamente le vulnerabilità dei componenti industriali.

I sistemi OT che si sono estesi con il tempo risalgono a un'epoca precedente a quella della connettività. Spesso si basano su software obsoleti senza autenticazione moderna, mentre rigidi processi di certificazione bloccano le patch di sicurezza necessarie. La conseguenza è che i meccanismi di sicurezza IT standard spesso non sono tecnicamente utilizzabili in questi ambienti o possono causare interruzioni imprevedibili.

Qual è la posta in gioco per le aziende?
I rischi vanno dalle interruzioni della produzione dovute a sabotaggi o manipolazioni fino alla perdita di reputazione. Nel caso di infrastrutture di importanza critica come l'energia, l'acqua o il sistema sanitario possono esprimersi addirittura in termini di vite umane. Vanno considerate anche le conseguenze legali e normative, poiché il mancato rispetto delle disposizioni di sicurezza può comportare pesanti multe o rischi di responsabilità personale.

Molte aziende sottovalutano questo rischio perché finora «non è mai successo nulla». Ma proprio attacchi spettacolari come Stuxnet, BlackEnergy, Colonial Pipeline o quelli scatenati contro le centrali idroelettriche in Polonia e Norvegia dimostrano che i sistemi OT sono nel mirino degli hacker e che la minaccia è molto reale.

Pressione normativa
Legislatori e regolatori prendono sempre più sul serio i rischi per le infrastrutture critiche. Ne è un esempio l'aggiornamento dell'ordinanza svizzera sull'approvvigionamento elettrico, che prescrive alle imprese energetiche di adeguarsi allo standard minimo TIC, oppure il regolamento UE NIS2, valido anche per molte aziende svizzere con clienti nell'UE.

Cosa possono fare le aziende?
Qui c'è una buona notizia: esistono approcci collaudati per migliorare la sicurezza OT. Il framework NIST prevede le funzioni Identify, Protect, Detect, Respond e Recover, che aiutano e danno una struttura al tutto anche in ambito di OT security.

Identify: il primo passo è, come quasi sempre, la trasparenza. Le aziende dovrebbero farsi un'idea chiara dei sistemi OT disponibili, di come comunicano tra loro, con l'IT o con internet e di quali presentano punti deboli critici. Un tale inventario costantemente aggiornato costituisce la base per qualsiasi struttura di gestione del rischio.

Protect: la migliore separazione possibile dell'OT dall'IT, una segmentazione finissima nella rete OT e, laddove possibile, la protezione degli endpoint e la gestione delle vulnerabilità sono importanti misure preparatorie

« I lunghi cicli di vita e i sistemi proprietari non sono più una scusa. Con l'aumentare dell'interconnessione aumenta anche la responsabilità di proteggere i sistemi OT con la stessa sistematicità con cui proteggiamo l'IT tradizionale.

Thomas Dummermuth
Head of Physical Security

per ridurre al minimo i rischi. Questo include anche la limitazione dell'accesso ai sistemi OT attraverso un rigoroso access management.

Un fattore decisivo è la sensibilizzazione del personale. Chi conosce i rischi specifici e le best practice può contribuire attivamente alla sicurezza nella vita di tutti i giorni.

Detect: parallelamente è utile anche un monitoraggio continuo. Le reti OT dovrebbero essere costantemente monitorate per rilevare irregolarità e indicatori di attacco e poter così reagire rapidamente in caso di emergenza. A tale scopo sono disponibili sistemi di rilevamento delle intrusioni (IDS) specializzati in OT che attivano un allarme in caso di comportamento anomalo. La definizione di ciò che è considerato «anormale» è strettamente specifica del settore e richiede competenze adeguate da parte del security partner.

Respond e Recover: in caso di emergenza è necessario essere in grado di reagire, anche al di fuori degli orari d'ufficio. Un SOC IT/OT convergente è un approccio utile, che tuttavia di norma richiede anche adeguamenti procedurali all'interno dell'azienda, ad esempio l'accertamento delle responsabilità o delle catene di allertamento, che devono essere concordate con i principali fornitori per garantire un ripristino tempestivo in caso di emergenza.

Per poter affrontare queste fasi, OT, IT e management devono essere strettamente integrati nella strategia di sicurezza. La gestione dei rischi per la sicurezza dell'OT rientra nell'agenda della direzione o del consiglio di amministrazione.

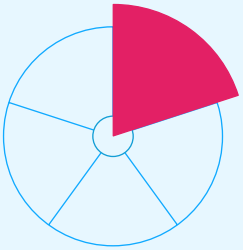
Il momento di agire è ora

Trascurare la sicurezza dell'OT non è più un'opzione. Chi gestisce la produzione della propria azienda con i livelli di sicurezza del passato non solo rischia interruzioni della produzione e danni economici, ma mette anche a repentaglio la propria reputazione e, nel peggiore dei casi, vite umane. La sfida è grande, ma alla portata. È fondamentale che le aziende affrontino la questione in modo proattivo e comprendano che la sicurezza dell'OT è parte integrante della trasformazione digitale. L'elefante si trova al centro della stanza, è giunto il momento di parlargli e di adottare le misure giuste.

« Sicurezza dell'OT significa sfruttare i vantaggi dell'IT senza compromettere la stabilità della produzione. L'interfaccia tra IT e OT è decisiva.

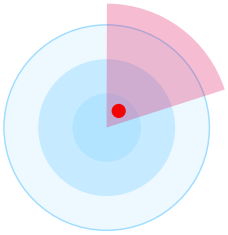
Tobias Balcon
Strategic Program Manager

Dettagli comprensivi di tendenze e confronto con l’anno precedente



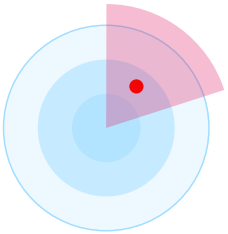
Dominant Players

Questo segmento comprende le minacce provenienti dalle dipendenze da fornitori, servizi o protocolli dominanti.



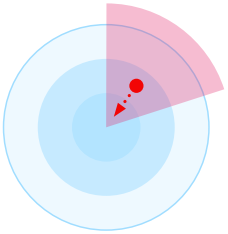
Infrastructure Integrity
In componenti essenziali delle infrastrutture critiche possono essere state inserite, per negligenza o in modo deliberato, vulnerabilità che mettono a repentaglio la sicurezza dei sistemi.

- Stabile



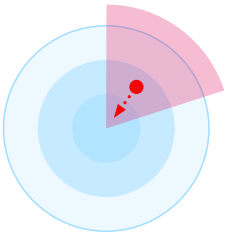
Legacy Protocols
Le dipendenze tra software fanno sì che si utilizzino ancora protocolli completamente obsoleti e vulnerabili (ad es. NTLMv1, SMBv1, RC4), per cui singole applicazioni mettono a repentaglio la sicurezza di intere infrastrutture.

► Stabile



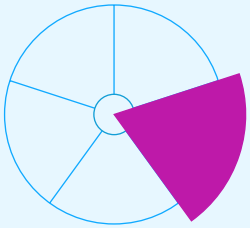
Cloud Ecosystem Dependencies
Gli ecosistemi cloud centralizzati generano rischi di accumulazione e dipendenze che, in caso di interruzioni o pressioni politiche, possono compromettere gravemente la sovranità digitale e la disponibilità.

▲ In aumento



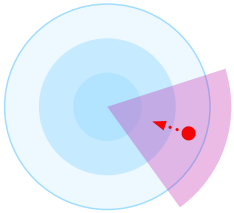
Manipulated Generative AI
Attraverso manipolazioni mirate è possibile modificare l'output di un sistema IA. In questo caso si tratta dell'immissione di dati malevoli, errati o corrotti già nella fase di addestramento, del furto di modelli LL ma anche della prompt manipulation, che può portare a conseguenze indesiderate e legalmente vincolanti. Stiamo parlando di AI security risks e non di rischi derivanti dall'utilizzo dell'IA (vedi AI-Based Attacks).

▲ In aumento



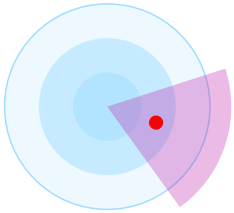
Technology Dynamics

Questo termine si riferisce alle minacce che provengono dalla rapida innovazione tecnologica e beneficiano della disponibilità sempre più immediata ed economica dei dispositivi e del know-how informatico. Ciò moltiplica le aree vulnerabili, aumenta la disponibilità di strumenti di attacco, e offre ad hacker ulteriori opportunità di creare nuove minacce attraverso il proprio sviluppo.



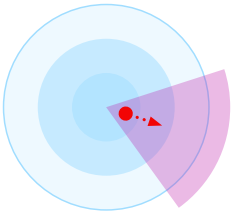
Quantum Computing
I computer quantistici possono rendere inutilizzabili le procedure crittografiche esistenti poiché riescono ad aggirarle in tempi molto brevi.

▲ In aumento



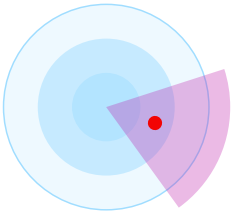
Unsecure AI
I sistemi IA non sicuri mettono a rischio le catene di fornitura e la protezione dei dati, poiché i modelli generativi possono divulgare dati sensibili in modo incontrollato. Questo non solo mette a rischio la continuità operativa, ma può anche compromettere seriamente la reputazione di un'azienda. Inoltre, l'inosservanza delle normative sull'IA, in particolare in relazione alla nuova legislazione, può comportare gravi conseguenze legali e sanzioni.

► Stabile



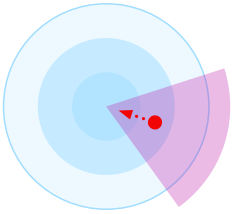
Ransomware
Dati critici vengono crittografati su larga scala e (forse) decrittati nuovamente contro il pagamento di un riscatto.

▼ In calo



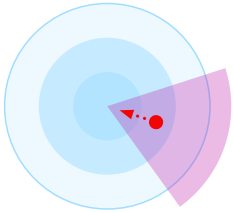
Increased Complexity
La complessità dei sistemi, in particolare quelli operanti al di là di confini tecnologici e aziendali, è in costante crescita. Soprattutto in ambito ibrido/multi-cloud con molti provider cloud, gli ambienti IT stanno diventando sempre più complessi, il che aumenta l'esposizione al rischio e rende più difficile individuare le falle, spalancando le porte agli zero-day exploit.

► Stabile



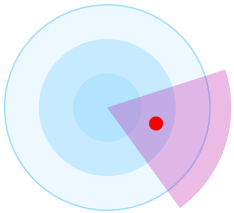
AI-Based Attacks
Gli attacchi che utilizzano l'intelligenza artificiale (AI) sono più mirati e quindi più difficili da riconoscere. L'intelligenza artificiale può essere utilizzata per sferrare attacchi più efficienti attraverso vettori classici quali ransomware, phishing, spear phishing e, occasionalmente, anche in nuovi scenari come deepfake, disinformazione.

▲ In aumento



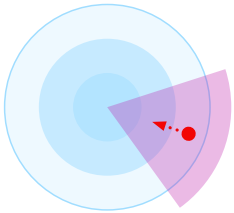
Agentic AI
L'agentic AI è proattiva e in grado di prendere decisioni autonomamente, adattando le proprie strategie. Tuttavia, ciò aumenta la superficie di attacco, poiché i sistemi di autoapprendimento e adattivi possono sviluppare comportamenti imprevedibili e interagire autonomamente con i sistemi periferici. Se compromessi, questi agenti potrebbero consentire accessi non autorizzati a dati sensibili e componenti di sistema, aumentando drasticamente il rischio di escalation e frodi. Anche un assistente IA apparentemente innocuo può causare danni considerevoli a causa di istruzioni errate o manipolazioni da parte degli autori degli attacchi.

▲ In aumento



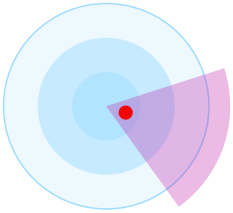
Targeted Attacks
Si tratta di attacchi mirati e complessi per raggiungere un obiettivo specifico. Le persone chiave sono identificate e prese di mira direttamente o indirettamente (ad es. lateral movement, social engineering) per ottenere informazioni rilevanti o causare il massimo danno. Un aspetto essenziale è la persistenza, ovvero gli hacker agiscono inosservati il più a lungo possibile variando altresì i canali di attacco (dall'e-mail all'SMS o anche tramite posta fisica).

► Stabile



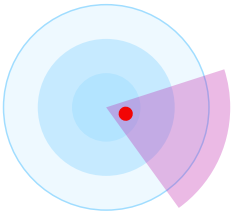
Subscriber Compromise
Il software dannoso ottiene l'accesso ai dati privati di utenti mobili o è utilizzato per attaccare l'infrastruttura di telecomunicazione o IT. Gli attacchi di phishing, smishing, vishing e MFA bypass prendono di mira le credenziali di utenti con abbonamento, mentre gli attacchi successivi hanno lo scopo di sottrarre e assumere illecitamente le loro identità digitali.

▲ In aumento



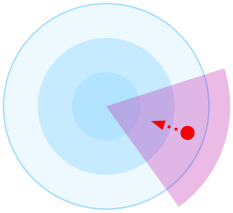
DDoS Attacks
Un attacco DDoS (Distributed Denial of Service) è un tentativo doloso di perturbare il normale traffico di dati di un server, di un servizio o di una rete target inondando di traffico internet l'obiettivo o l'infrastruttura circostante. Gli attacchi DDoS raggiungono la loro efficacia utilizzando più sistemi informatici compromessi come fonti di traffico di attacco. Le macchine sfruttate possono includere computer e altre risorse collegate in rete, come gli apparecchi IoT. La crescente diffusione a fronte di una scarsa protezione, ad esempio degli apparecchi IoT, accresce il numero di potenziali «candidati» per le botnet.

► Stabile



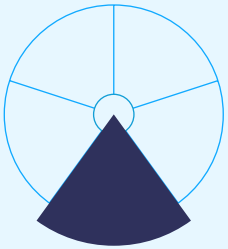
Supply Chain Attacks
Gli attacchi alla catena di fornitura mirano a sfruttare la relazione di fiducia e commerciale tra un'azienda e terze parti, come partenariati, rapporti di fornitura o l'utilizzo di software di terze parti. In questo contesto, gli attacchi agli ecosistemi software dei partner raggiungono una nuova dimensione.

► Stabile



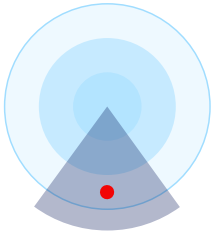
Residential Proxies
I residential proxy sono connessioni tramite indirizzi IP reali che vengono utilizzate per mascherare l'origine del traffico dati. Di conseguenza, i controlli di sicurezza basati sulla reputazione IP o sulla geolocalizzazione perdono efficacia, favorendo rischi come il furto di credenziali e di informazioni o l'aggiramento del geoblocking. Anche la mitigazione DDoS diventa più difficile.

▲ In aumento



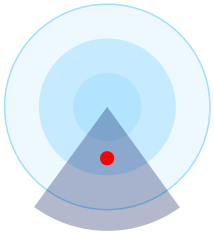
Organisation

In questo settore ricadono le minacce provenienti da cambiamenti nelle organizzazioni o che sfruttano lacune nelle organizzazioni.



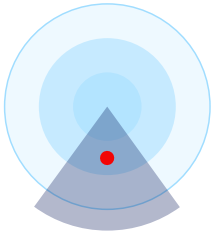
Workplace Heterogeneity
I nuovi modelli di lavoro offrono numerose opportunità, ma il loro uso incontrollato – ad esempio «Bring Your Own Device» (BYOD) o il crescente utilizzo di postazioni di lavoro remote – espone maggiormente ai rischi.

► Stabile



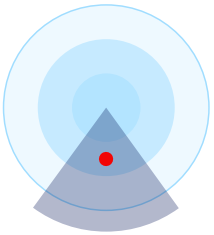
Decentralised Development & Operations
I reparti di sviluppo classici si stanno «estinguendo», mentre lo sviluppo applicativo è sempre più vicino alle unità aziendali e i cicli di release sono sempre più brevi. Ciò rende difficile controllare/gestire la sicurezza.

► Stabile



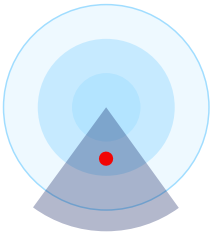
Insider Threat
Partner o personale manipolano, abusano o vendono informazioni in modo negligente o intenzionale.

► Stabile



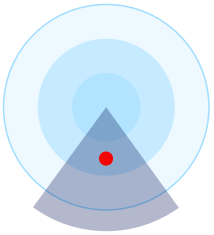
Digital Transformation Risks
La crescente interconnessione del mondo reale con il mondo virtuale nella vita privata e lavorativa moltiplica le vie di attacco. Anche il «new work» e lo spostamento del lavoro in ambienti di home office aumentano i rischi informatici e la vulnerabilità dell'infrastruttura IT causati da terminali non protetti.

► Stabile



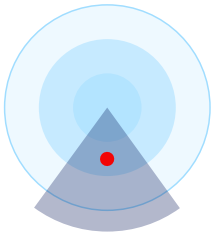
Security Skills
La complessità degli attacchi informatici e la crescente digitalizzazione rendono indispensabile disporre di competenze di sicurezza e impiegare personale informatico qualificato nell'organizzazione. Un imminente «downskilling» (ovvero il disapprendimento di conoscenze) attraverso l'automazione nell'IT può originare nuovi vettori di attacco se, ad esempio, i sistemi SCADA non possono più essere gestiti e sottoposti a manutenzione da personale qualificato.

► Stabile



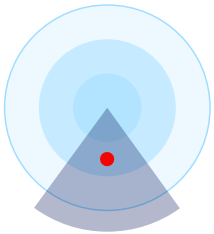
Fragile Workforce
Un'organizzazione del lavoro fragile mette in evidenza la vulnerabilità dei team di cybersicurezza e difesa informatica allo stress psicologico, nonché l'assenza di un'adeguata prevenzione dallo stress e dal burn-out. Se un individuo è mentalmente instabile e non è in grado di gestire adeguatamente la pressione, incrementa il rischio di errori umani. Questo, a sua volta, aumenta le falle nella sicurezza e i punti di attacco, che potrebbero compromettere la stabilità complessiva dell'azienda.

► Stabile



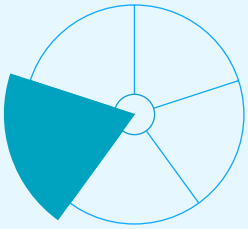
Infrastructure Misconfiguration
È lo sfruttamento di componenti delle infrastrutture configurati in modo errato e/o di lacune identificate e colmate in ritardo. Con l'aumento dell'automazione dei processi operativi tecnici, ciò avrà un impatto maggiore in caso di attacchi riusciti o configurazioni errate.

► Stabile



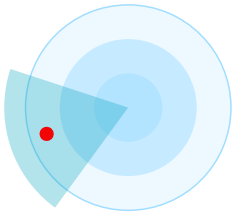
Fraud
Per frode si intendono azioni fraudolente basate sull'inganno e sull'arricchimento indebito che si manifestano attraverso transazioni falsificate, furto d'identità o manipolazione di documenti. La frode rappresenta un rischio serio per aziende e privati, poiché può comportare perdite finanziarie significative e danneggiare la reputazione.

► Stabile



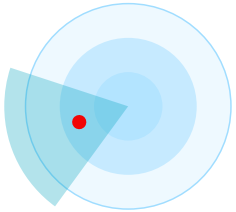
Physical

Questo termine comprende gli attacchi a infrastrutture nel cyberspazio, che causeranno danni sempre maggiori al mondo fisico. Racchiude però anche minacce provenienti dall'ambiente fisico e solitamente indirizzate contro obiettivi fisici.



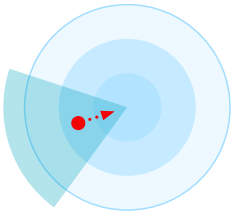
Energy Instability
Attacchi a infrastrutture critiche come gestori di reti elettriche. L'affidabilità è essenziale e la continuità dell'esercizio è sempre più oggetto di discussione anche nel dibattito sulla resilienza informatica. Fra i punti salienti rientrano la penuria di energia elettrica, i blackout (interruzioni di corrente su ampia scala) o anche i cosiddetti blueout (interruzioni dell'erogazione di acqua potabile su ampia scala). Stando ai media, la vulnerabilità delle infrastrutture critiche agli attacchi informatici è aumentata notevolmente.

► Stabile



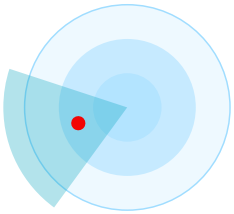
Targeted Sabotage
Si tratta di attacchi mirati a importanti infrastrutture critiche, impianti di distribuzione e linee che possono limitare notevolmente internet. Il sabotaggio mirato di linee nevralgiche in fibra ottica è in aumento, rappresenta un rischio e va monitorato. Le contromisure sono difficili da implementare ed è necessario fare affidamento su un rilevamento rapido e su soluzioni alternative.

► Stabile



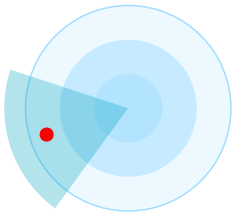
Unsecure IoT/OT
Che si tratti di tecnologia operativa (OT) per monitorare e manovrare processi fisici, dispositivi e infrastrutture o di dispositivi IoT, l'internet delle cose è onnipresente. I compiti svolti sono i più disparati, dai più semplici ai più complessi, e spaziano dalle applicazioni di home entertainment al controllo di robot in una fabbrica, al monitoraggio di infrastrutture critiche (CI). Qualsiasi apparecchio dotato di scarsa protezione può essere compromesso e sabotato, il che ne limiterà il funzionamento, ad esempio la disponibilità o l'integrità dei dati.

▲ In aumento



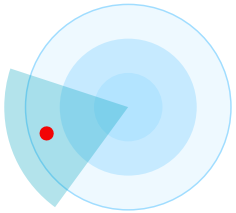
Environmental Influence
A causa degli effetti del cambiamento climatico e dell'urbanizzazione si verificano sempre più spesso fenomeni meteorologici imprevedibili o estremi, come forte caldo, piogge intense, tornado, grandine, fulmini e simili, che si ripercuotono sulla resilienza dell'infrastruttura e quindi hanno un elevato potenziale di danni all'ambiente esterno e interno di un sistema d'informazioni o di una rete.

► Stabile



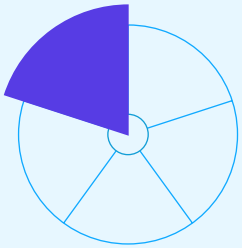
UAS Threats
Le UAS threat (Unmanned Aerial System Threat) sono i rischi derivanti dall'impiego di velivoli senza pilota, ovvero droni. Questi spaziano dallo spionaggio, dalla sorveglianza e dal furto di dati, passando per il contrabbando e il sabotaggio, fino agli attacchi fisici alle infrastrutture o al personale. Nel contesto aziendale, gli scenari rilevanti sono in particolare lo spionaggio industriale, la sorveglianza degli spazi aerei di aree industriali e il malfunzionamento di impianti sensibili. Con la crescente diffusione e autonomia delle tecnologie basate sui droni, l'importanza di queste minacce ai fini della sicurezza aumenta notevolmente.

► Stabile



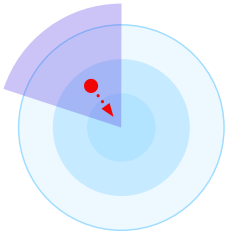
Hybrid Warfare
La combinazione di mezzi militari classici con tattiche non militari come attacchi informatici, disinformazione, pressione economica o influenza politica viene definita guerra ibrida. Poiché gli attacchi avvengono spesso in modo occulto e al di sotto della «soglia bellica», è difficile riconoscerli e respingerli. L'obiettivo è destabilizzare gli Stati, minare la fiducia e provocare divisioni sociali. La loro efficacia aumenta grazie alla digitalizzazione, ai social media e all'interconnessione globale.

► Stabile



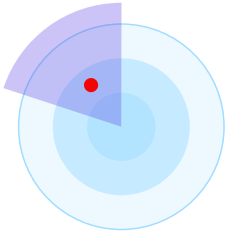
Environment/Social

Si riferisce alle minacce provenienti da cambiamenti sociopolitici o che, a causa di essi, si prestano maggiormente all'abuso e sono quindi più preziose per hacker.



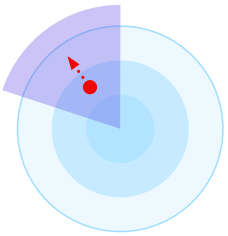
Identity Theft & Impersonation
Le identità digitali personali autenticate possono essere rubate o utilizzate impropriamente per impersonare un'altra persona o organizzazione. In questo modo gli hacker possono accedere senza autorizzazione a sistemi e informazioni o eseguire azioni per conto di terzi come stipulare contratti, effettuare pagamenti o condurre operazioni di comunicazione.

▲ In aumento



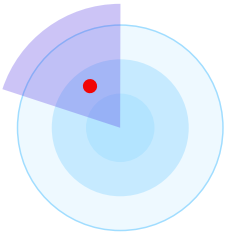
Geopolitical Situation / State Level Attacks
In tempi di guerre, terrorismo e instabilità politica di paesi e società, sono sempre più evidenti le conseguenze negative anche nel cyberspazio. Si tratta di attacchi su commissione di diversi paesi e gruppi politici di hacktivisti, attori statali e criminalità organizzata, che attraverso attività di questo tipo accrescono anche la pressione su imprese e organizzazioni. Anche i danni collaterali causati dalle strategie di hack-back di singoli paesi vengono considerati con maggiore attenzione.

► Stabile



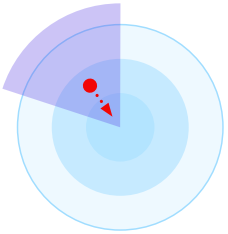
Security Job Market
La domanda di persone specializzate in sicurezza è enorme e molto difficile da soddisfare. Ciò comporta una diminuzione del know-how a fronte di attacchi sempre più complessi e intelligenti.

▼ In calo



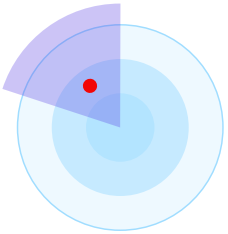
Disinformation & Destabilisation
La diffusione intenzionale di informazioni false può causare instabilità economica e sociale ed è sempre più utilizzata in scenari di crisi anche attraverso il cyberspazio.

► Stabile



Political Influence
Le correnti politiche, ma anche regolamenti e direttive possono influire sulle decisioni tecnologiche o economiche, ad esempio nella scelta dei fornitori di tecnologia. Da ciò possono nascere nuovi rischi.

▲ In aumento



Data-Centric Risks
Più dati e migliori modelli analitici possono essere utilizzati in modo improprio per influenzare il comportamento delle persone. Le decisioni sono sempre più lasciate a sistemi autonomi. Si ricorre sempre più spesso a dati provenienti da «Big Data Lake» per disinformare, diffondere notizie false, realizzare analisi sociali e psicosociali e creare modelli di movimento. In quest'ultimo caso sussiste una violazione della sfera privata.

► Stabile

Conclusioni

La trasformazione digitale comporta una dipendenza sempre maggiore da ecosistemi esterni.

Piattaforme cloud, catene di fornitura di software, modelli IA e sistemi di controllo industriale sono altamente interconnessi e spesso al di fuori del controllo diretto delle aziende, spostando i limiti di sicurezza classici. La fiducia da sola non basta più. La sicurezza deve essere comprensibile, verificabile e controllabile. Origine, integrità e dipendenze di software, dati e sistemi devono essere rese trasparenti e gestite attivamente.

Questo emerge con particolare evidenza negli attacchi alla supply chain e alla sovranità digitale. Chi non sa come nasce il software, dove vengono elaborati i dati o a quali condizioni legali sono soggetti i fornitori rischia una perdita di controllo con conseguenze potenzialmente gravi per l'intera azienda. Sviluppi normativi come NIS2, CRA o leggi sulla protezione dei dati rafforzano ulteriormente questa pressione e rendono la sicurezza verificabile uno standard.

L'intelligenza artificiale agisce da acceleratore: può aumentare la produttività, l'innovazione e la resilienza, ma in assenza di una governance rafforza i rischi esistenti lungo l'intera catena del valore. Modelli poco trasparenti, shadow AI, perdita di competenze e nuove aree di attacco dimostrano chiaramente che ciò che conta non è l'impiego dell'IA in sé, ma il modo in cui viene introdotta, controllata e gestita.

Un settore spesso sottovalutato ma di importanza critica rimane quello della sicurezza di OT e IoT. La crescente convergenza tra IT e OT rende gli impianti di produzione e le infrastrutture di rilevanza critica degli obiettivi allettanti. L'OT security non dovrebbe più essere trattata come una disciplina tecnica marginale, ma trovarsi all'ordine del giorno della direzione aziendale.

Il quadro delle minacce 2026 mostra che i rischi nascono sempre più dall'interazione tra tecnologia, organizzazione e geopolitica. La resilienza diventa così una competenza chiave dal punto di vista tecnico, organizzativo e culturale.

I pericoli maggiori nascono laddove la complessità incontra la mancanza di trasparenza, l'automazione la mancanza di responsabilità e la velocità la mancanza di competenze. La

risposta non è un singolo tool, ma un approccio integrato. Occorrono strategie chiare, una sicurezza verificabile, una scelta consapevole dei partner, una formazione continua e una cultura della sicurezza vissute attivamente e in modo credibile dai dirigenti.

Gli sviluppi individuati nell'edizione attuale del Cybersecurity Threat Radar dimostrano chiaramente che la cybersicurezza non è più solo una disciplina tecnica, ma un fattore di successo strategico e non rappresenta una situazione statica, ma un processo strategico continuo. Organizzandola attivamente si rafforza la resilienza, la fiducia e la sovranità digitale.

#EngageYourSecuritySkills

Colophon

Editore
Swisscom (Svizzera) SA, Group Security

Concetto/realizzazione
Agenzia Nordjungs, Zurigo

Redazione
Swisscom (Svizzera) SA
Marcus Beyer (Group Security)
Manuel Bühlmann (Group Communications)
Claudia Lehmann (B2B Communications)

Traduzione
Apostroph Bern AG

Stampa
OK DIGITALDRUCK AG, Zurigo

Tiratura
140 copie

Oggi la cybersicurezza riveste un'importanza decisiva per la fiducia e la capacità d'azione, perché la trasformazione digitale, l'IA e le dipendenze geopolitiche stanno abbattendo i confini di sicurezza e rendono una sicurezza trasparente e verificabile e una resilienza integrata degli obblighi strategici.

Per saperne di più sui nostri prodotti, servizi e sul nostro impegno a favore della sicurezza in Svizzera, visitate il portale della sicurezza Swisscom su swisscom.ch/sicurezza

Stai cercando un lavoro nel settore della sicurezza presso Swisscom? Allora candidati qui: swisscom.com/securityjobs

#EngageYourSecuritySkills