Cyber Security Threat Radar 2023/2024

Rafforzare la cyberresilienza

swisscom

Indice

Cyber Security Threat Radar

Rafforzare la cyberresilienza

Soprattutto in periodi turbolenti e impegnativi come questo è fondamentale per le aziende e le organizzazioni essere resilienti. Ciò significa non solo salute fisica e sistemi IT stabili e ridondanti, ma anche direttive chiare che fungono da linee guida per un maggiore orientamento.

Questo Cyber Security Threat Radar evidenzia come la protezione dalle minacce informatiche e la riduzione dei rischi non costituiscono un processo unilaterale e non sono nemmeno di esclusiva responsabilità dell'IT. La cybersicurezza compete ai vertici aziendali e richiede la partecipazione dell'intera direzione aziendale.

Nel Cyber Security Threat Radar di quest'anno rinunciamo a trattare il quarto settore delle minacce informatiche: l'osservazione. Questo tema è già parte integrante del DNA di Swisscom in materia di Security e viene preso in considerazione ogni giorno nel nostro lavoro.

Il radar individua nella «disinformazione e destabilizzazione» una delle principali sfide del nostro tempo. La diffusione di informazioni false, contenuti manipolati e azioni di propaganda mirate può influenzare intere società, disturbare i processi politici e minare la fiducia nelle istituzioni. Anche le personalità esperte del Global Risks Report 2024 del World Economic Forum (WEF) considerano questa minaccia il rischio maggiore a breve termine. I temi trattati nel radar non sono certo esaustivi.

Con la revisione della legge sulla protezione dei dati in Svizzera nel settembre dello scorso anno e la nuova legge sulla sicurezza delle informazioni (LSIn), gli aspetti di governance tornano in primo piano. Gli sviluppi futuri promettono di essere entusiasmanti. Mi auguro che questo Cyber Security Threat Radar possa fornire preziosi spunti e contribuire a promuovere ulteriormente la cybersicurezza all'interno di aziende e organizzazioni.

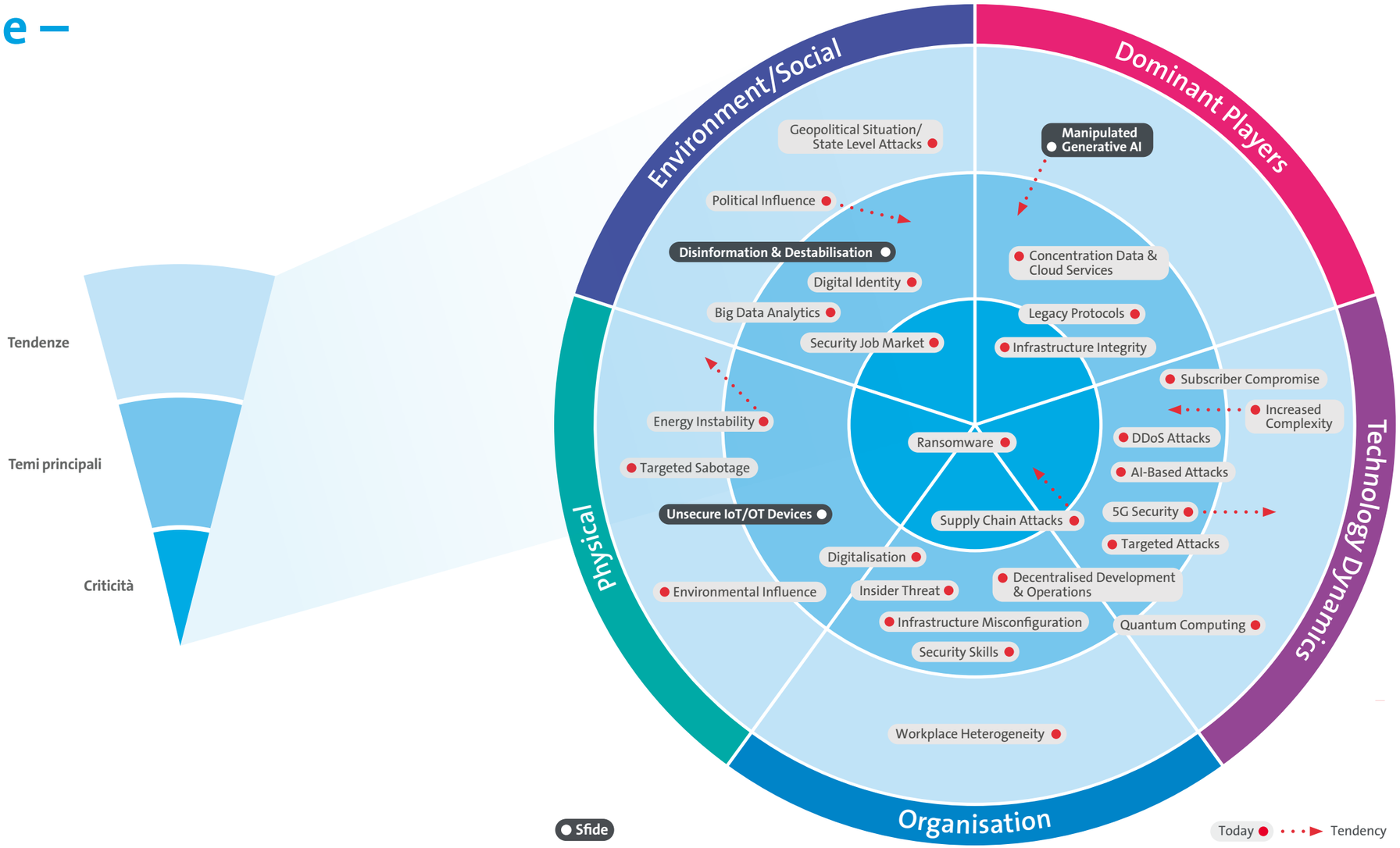
Marco Wyrsch
Head of Group Security
Swisscom (Schweiz) AG

« Monitoraggio e osservazione della nostra rete: in questo modo rendiamo la Svizzera sempre più sicura. I rischi informatici rimangono infatti una delle principali minacce dei prossimi anni per le organizzazioni, le imprese e la società in generale. »

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 Cyber Security Threat Radar.



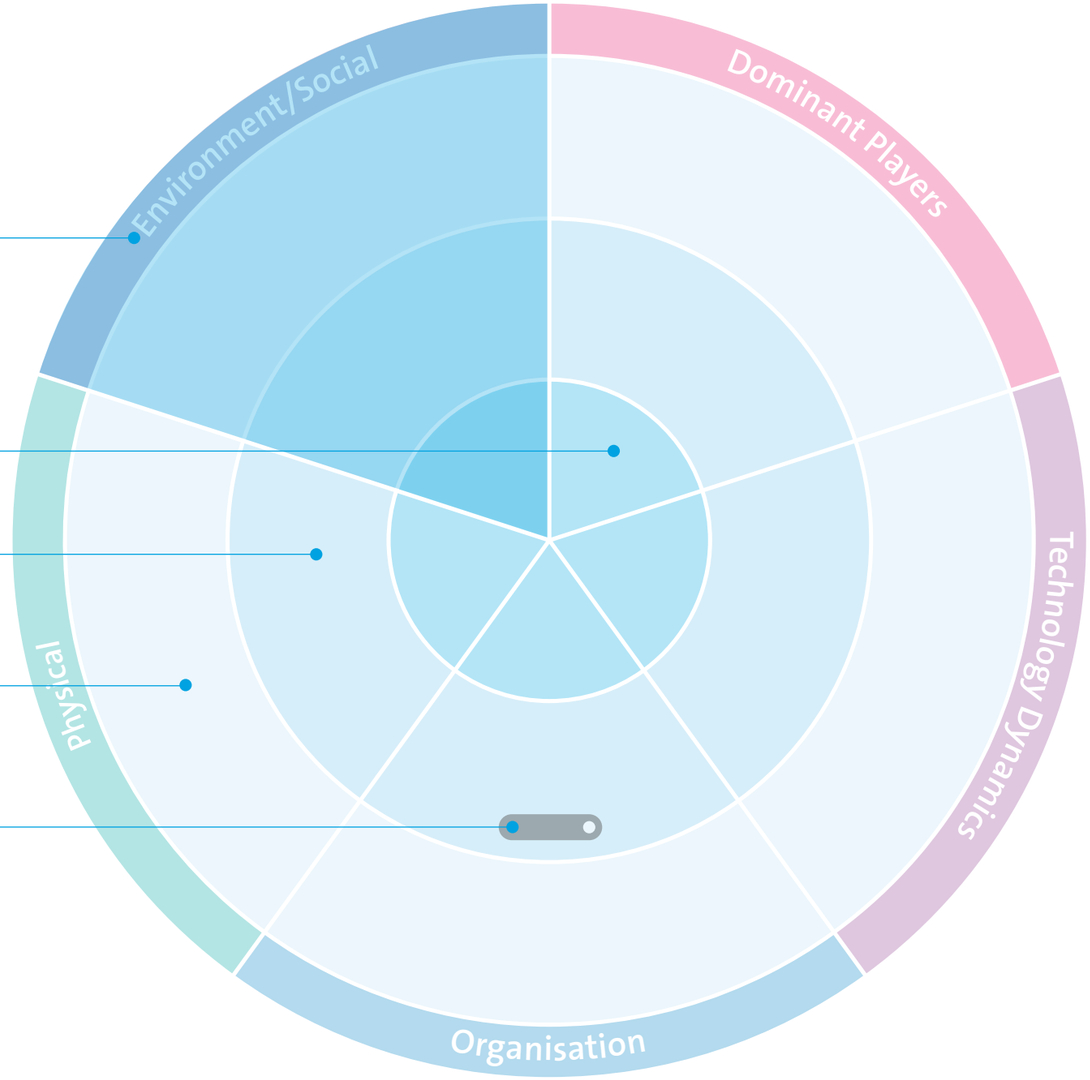
Metodica

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.

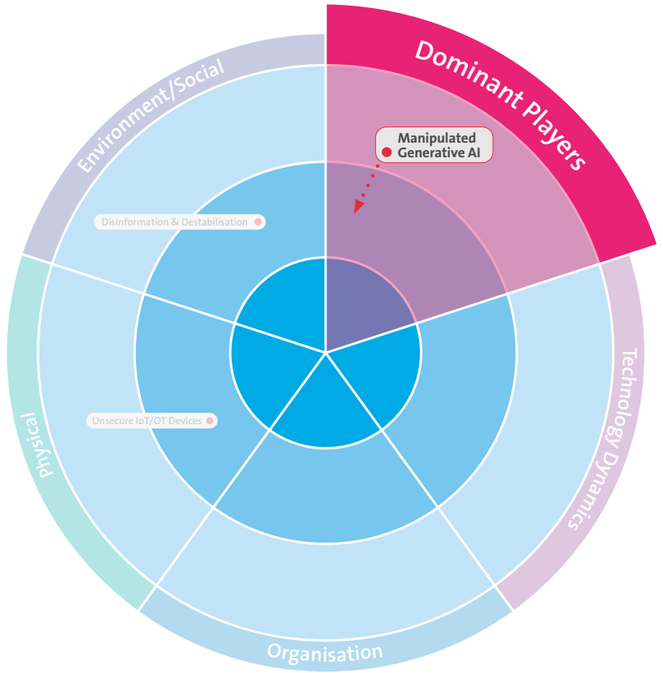
Descriviamo i cerchi come

- **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.



Manipulated Generative AI o: quanto è manipolabile l'intelligenza artificiale?



Negli ultimi 15 anni la digitalizzazione, la virtualizzazione e il trend del cloud sono stati di grande importanza nel settore informatico e hanno contribuito alla rapida diffusione dell'intelligenza artificiale generativa (AI generativa). Il lancio di ChatGPT nel novembre 2022 è stato accompagnato da un'enorme eco mediatica. L'IA generativa si è rapidamente diffusa nella società. Molte aziende innovative si sono lasciate contagiare dall'entusiasmo e da allora lanciano sul mercato numerose nuove applicazioni.

L'interesse a livello mondiale per l'intelligenza artificiale ha portato l'argomento anche al centro dell'attenzione della Security. Le domande sui rischi per la sicurezza si sono rapidamente moltiplicate ed esigevano una risposta, perché, come sempre, le innovazioni presentano anche lati oscuri. Nonostante i notevoli progressi compiuti dall'intelligenza artificiale e dall'apprendimento automatico, queste tecnologie sono vulnerabili agli attacchi. In molti sottosettori i nuovi standard sono ancora in fase di sviluppo, come ad esempio l'AI Act in ambito legislativo. Bisogna quindi fare i conti con alcune incognite alle quali ci si può preparare solo in parte.

I sistemi IA emergono nel contesto della cybersicurezza per tre aspetti:

1. utilizzo di sistemi IA per gli attacchi: esempi noti sono il perfezionamento di attacchi noti come CEO Fraud e Business Email Compromise (BEC) tramite video generati dall'intelligenza artificiale anziché semplici e-mail; e-mail di phishing più realistiche → attacchi basati sull'IA;

2. ricorso all'IA per il riconoscimento e la difesa da attacchi (ad es. filtri spam e phishing), nel riconoscimento di anomalie nel traffico di rete, nel supporto workflow nella Cyber Defence (ad es. come copilota), nell'automazione di fasi di analisi, nella creazione di Incident Timeline o nella comunicazione con utenti. Complessivamente si possono prevedere ulteriori soluzioni di sicurezza intelligenti e automatizzate;

3. falle nella sicurezza nei sistemi IA utilizzati; stiamo parlando di intelligenza artificiale manipolabile, concretamente elencate nella:
   Top 10 OWASP LLM (owaspai.org) e/o nel
   MITRE ATLAS (atlas.mitre.org).
   Si tratta quindi di rischi per la sicurezza dell'IA e non di rischi derivanti dall'utilizzo di sistemi IA.

Per quanto riguarda il terzo ambito, oltre a numerose altre possibilità di attacco, riteniamo rilevanti in particolare i seguenti temi:

- **Manipolazione degli input (ad es. Prompt Injections)**
  Con questi attacchi si cerca di aggirare i meccanismi di sicurezza esistenti manipolando i dati immessi e quindi di produrre risultati indesiderati da parte del gestore del sistema IA. Può trattarsi, ad esempio, della divulgazione di informazioni riservate o della generazione di contenuti indesiderati o di un comportamento indesiderato.

- **Attacchi di poisoning**
  Già nella fase di addestramento dei sistemi IA, il sistema può essere manipolato introducendo dati malevoli, falsi o corrotti. Un esempio potrebbe essere l'inserimento di un linguaggio inappropriato nelle registrazioni audio, in modo che un chatbot interpreti tali casi come abbastanza generici e quindi utilizzabili nelle interazioni con clienti.

- **Attacchi alla supply chain**
  In questo caso si tratta di attacchi contro componenti esterni del sistema IA. Un esempio potrebbe essere l'introduzione di codici dannosi in librerie open source utilizzate in un modello di IA.

Continua inoltre a sussistere il rischio di DoS (Denial of Service). Ad esempio, l'utente potrebbe, intenzionalmente o meno, consumare tutte le risorse attraverso un input e paralizzare il sistema.

Da menzionare brevemente anche altri rischi legati all'intelligenza artificiale, come ad esempio la «Shadow AI», in cui persone facenti parte del personale utilizzano sistemi IA in modo incontrollato, mettendo così a rischio la segretezza di aziende, clienti o altri dati degni di protezione. Ciò mette a repentaglio la sicurezza dei dati. Bisogna assicurarsi che i dati aziendali da mantenere segreti siano protetti e che il sistema IA sia affidabile.

« A causa delle caratteristiche probabilistiche di GenAI e LLM, ci troviamo di fronte a nuove sfide e rischi per la sicurezza. Una comprensione approfondita di come funzionano gli LLM è il presupposto per definire e implementare misure di sicurezza adeguate. »

Beni Eugster
Swisscom Outpost

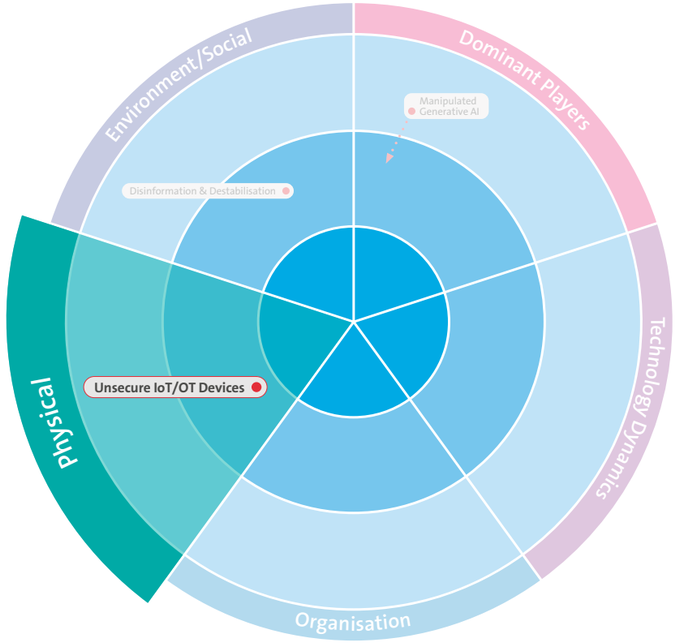
Di seguito gli aspetti su cui le aziende e le organizzazioni dovrebbero concentrarsi nella gestione dei rischi dell'intelligenza artificiale:

- monitoraggio degli sviluppi attuali e reazione rapida ai cambiamenti;
- formazione del personale;
- analisi accurata dei rischi prima di ricorrere a sistemi di intelligenza artificiale (anche di terze parti), per evidenziare possibili ripercussioni;
- esame e attuazione di misure di sicurezza a tutti i livelli del ciclo di vita dell'IA. Considerare i controlli di sicurezza di NIST AI RMF, MITRE ATLAS e OWASP per la sicurezza IA;
- assicurare buone relazioni tra l'IA e i team di sicurezza. Adeguare periodicamente i regolamenti e le direttive in base ai nuovi sviluppi;
- elaborazione di istruzioni operative per la gestione dell'IA nella propria organizzazione;
- condizioni quadro giuridiche: l'AI Act prevede già speciali misure di sicurezza per sistemi IA rischiosi o che ne limitano l'utilizzo. Il regolamento UE sull'IA ha effetto extraterritoriale e, a determinate condizioni, si applica quindi anche alle imprese svizzere. Ma anche il diritto d'autore e la responsabilità in caso di utilizzo di sistemi IA di terze parti come soluzioni SaaS rappresentano rischi da non sottovalutare.

« A causa del rapidissimo sviluppo nel settore dell'IA aumenteranno le sfide nella gestione dei rischi per la sicurezza, il tutto a un ritmo incalzante. Bisognerebbe quindi monitorare continuamente gli attuali sviluppi per poter reagire rapidamente ai cambiamenti. »

Raiko Zwilling
Security Officer Group Companies

Rischi per la sicurezza dovuti alla crescente digitalizzazione anche in officina e sala operatoria



Nell'odierno mondo complesso e interconnesso, i dispositivi IoT (Internet of Things) e OT (Operational Technology) assumono un ruolo centrale nell'attività quotidiana in diversi settori. Questa tecnologia svolge un'ampia gamma di funzioni, sia semplici che complesse, dall'home entertainment e dalle applicazioni smart home al controllo dei sistemi di produzione in stabilimenti industriali fino al monitoraggio delle infrastrutture critiche.

Tuttavia, la crescente interconnessione di questi dispositivi comporta anche notevoli rischi per la sicurezza. I dispositivi IoT/OT non sicuri oppure scarsamente protetti possono essere compromessi e sabotati e diventare così la porta d'accesso per gli attacchi informatici. In questo modo possono non solo limitarne il funzionamento, ad esempio la disponibilità o l'integrità dei dati, ma anche minacciare la sicurezza fisica e il benessere delle persone. La sicurezza dei sistemi IoT/OT è quindi fondamentale, poiché gli attacchi a tali sistemi possono causare danni considerevoli.

I rischi dei dispositivi IoT/OT non sicuri sono molteplici e possono variare a seconda del campo di applicazione. Tra i pericoli principali rientrano:

- **Interruzioni dell'attività**
  Una violazione della sicurezza può mettere fuori servizio, temporaneamente o permanentemente, i sistemi critici con conseguenti interruzioni rilevanti della produzione e perdite finanziarie.

- **Furto della proprietà intellettuale oppure perdita o furto di dati**
  Gli accessi non autorizzati a dispositivi IoT/OT possono provocare il furto di dati sensibili, come la proprietà intellettuale e i segreti aziendali, indebolire il vantaggio competitivo di un'azienda e causare violazioni della protezione dei dati e perdite finanziarie.

- **Manipolazione dei dati dei dispositivi e sabotaggio**
  Hacker possono manipolare i dati dei dispositivi IoT/OT per generare informazioni false che a loro volta sfociano in decisioni o prodotti errati. Negli ambienti industriali, hacker possono paralizzare o manipolare infrastrutture critiche, provocando così guasti e mettendo persino a rischio la sicurezza delle persone.

- **Infiltrazione nella rete**
  Una volta compromessi, i dispositivi IoT/OT possono fungere da trampolino di lancio per penetrare più a fondo nelle reti e arrecare ulteriori danni. I dispositivi IoT/OT possono essere infettati da ransomware, che blocca funzioni importanti o crittografa i dati fino al pagamento di un riscatto. Possono anche essere integrati nelle reti bot, rappresentando un pericolo per altri sistemi.

- **Violazioni della compliance**
  Le falle nella sicurezza nei sistemi IoT/OT potrebbero portare le imprese operanti in settori regolamentati a violare la normativa sulla protezione dei dati o gli standard industriali, con conseguenti multe e sanzioni. In futuro, il Cyber Resilience Act (la legge europea sulla resilienza informatica) svolgerà un ruolo importante soprattutto nell'ambito della responsabilità per danno da prodotti difettosi. I potenziali danni e le conseguenze finanziarie dei dispositivi IoT/OT non sicuri sono considerevoli e possono comprendere perdite economiche, danni alla sicurezza pubblica, interruzione dei servizi critici e perdita di fiducia del pubblico. In casi estremi, gli attacchi a sistemi OT nell'infrastruttura critica possono addirittura causare disastri ambientali o pericoli per la vita umana.

Oltre ai costi diretti per eliminare le violazioni della sicurezza e per ripristinare i sistemi interessati, le imprese devono sostenere anche costi indiretti, ad esempio le perdite di fatturato dovute a interruzioni dell'attività, i pagamenti di indennizzi a clienti o partner commerciali interessati e l'aumento dei premi assicurativi.

Di seguito sono elencate le sfide relative ai sistemi OT:

- dispongono in parte di accessi per l'assistenza da remoto, raggiungibili tramite internet;
- dispongono di tecnologie molto datate, come pure di tecnologie nuove e complesse; inoltre esistono anche protocolli e dispositivi legacy, mancano i meccanismi di sicurezza (crittografia, autenticazione ecc.) e con la crescente digitalizzazione vengono interconnesse reti un tempo separate;
- il know-how e la tecnologia per il supporto praticamente non sono più disponibili (vecchie versioni di Windows, laptop con collegamento RS232 ecc.);
- sussiste ancora una discrepanza tra Security e Safety e ne deriva una diversa finalità, ad esempio per la protezione dell'accesso tramite password rispetto alla possibilità di intervenire rapidamente in caso di pericolo;
- la generazione dei baby boomer, che conosce i sistemi, sta andando in pensione;
- si constata una crescente pressione normativa per gli operatori (NIS2, DORA ecc.) e i produttori (RED2, CRA ecc.);
- le organizzazioni ignorano l'importanza della Security oppure non sono chiare le competenze in termini di Security all'interno delle organizzazioni.

Di fronte a queste sfide, le aziende devono adottare proattivamente misure per proteggere i loro dispositivi IoT e OT, tra cui:

- **Valutazione del rischio**
  Valutazioni periodiche della sicurezza e audit per identificare ed eliminare le potenziali lacune.

- **Direttive sulla sicurezza**
  È importante elaborare e implementare direttive sulla sicurezza basate su standard collaudati come la serie IEC 62443. Queste direttive consentono di configurare e gestire in modo sicuro i dispositivi IoT/OT. Inoltre, Security by Design può contribuire a una maggiore sicurezza già nella fase di sviluppo dei dispositivi.

- **Mantenere aggiornata la tecnologia**
  Aggiornare i sistemi obsoleti e aggiungervi patch, tenere sotto controllo la gestione delle vulnerabilità ed eventualmente segmentare la rete.

- **Formazione del personale generale e tecnico di servizio**
  Sensibilizzare e formare il personale all'uso dei dispositivi IoT/OT per ridurre al minimo gli errori umani.

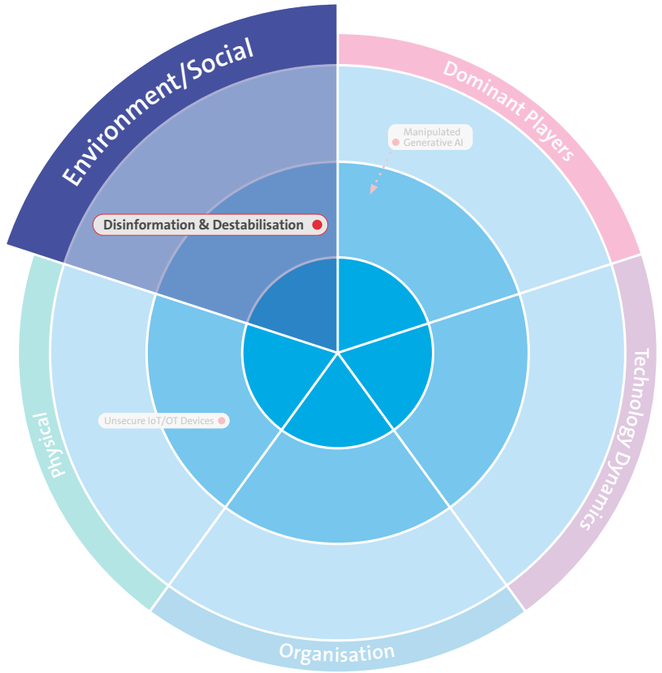
- **Monitoraggio e controlli attivi**
  Effettuare controlli di sicurezza regolari e sorvegliare costantemente i sistemi.

- **Collaborazione con fornitori affidabili**
  Scelta di dispositivi e software di fornitori che comprovatamente danno importanza alla sicurezza e mettono a disposizione aggiornamenti regolari.

« La sicurezza delle infrastrutture IoT e OT è un compito da non sottovalutare per le aziende, fondamentale per mantenere la sicurezza dell'esercizio e il successo commerciale a lungo termine. La sicurezza dei sistemi OT non è un optional e al giorno d'oggi deve avere la stessa rilevanza della sicurezza dei sistemi IT. »

Thomas Dummermuth
Head Physical Security & Safety, BCM

Disinformazione e destabilizzazione: i fatti



Al giorno d'oggi la disinformazione è un tema estremamente importante per le aziende. Data la crescita esponenziale delle piattaforme digitali e la rapidità con cui le informazioni possono essere diffuse, le imprese devono proteggere l'integrità delle loro informazioni, contrastando allo stesso tempo le informazioni false che potrebbero compromettere il loro marchio, la loro attività e le loro disposizioni di sicurezza.

Il Global Risks Report 2024 del World Economic Forum (WEF) sottolinea che la disinformazione rappresenta una sfida per la società e quindi anche una minaccia per aziende e organizzazioni. Le fake news generate dall'intelligenza artificiale e gli attacchi informatici rappresentano il rischio più immediato in tutto il mondo, soprattutto in vista delle imminenti elezioni in diversi grandi Paesi come gli USA, la Gran Bretagna e l'India.

Anche le imprese sono sempre più spesso oggetto di campagne di disinformazione che mirano a danneggiare la loro immagine, a ingannare i consumatori o addirittura a influenzare il valore di borsa. In un'epoca in cui le informazioni possono essere diffuse a livello globale in pochi secondi, la capacità di un'azienda di reagire in modo efficace alla disinformazione è fondamentale per mantenere l'integrità aziendale e la fiducia degli stakeholder.

I rischi derivanti dalla disinformazione non comprendono solo minacce esterne, come una percezione negativa da parte dell'opinione pubblica, ma anche minacce interne, per esempio la diffusione di informazioni false all'interno dell'azienda, che possono portare a decisioni errate e a falle nella sicurezza. Gli esperti di sicurezza sottolineano che la sicurezza dei dati e delle infrastrutture aziendali è strettamente legata alla capacità di riconoscere e combattere la disinformazione. Soprattutto con il rapido sviluppo dell'intelligenza artificiale e la conseguente evoluzione di IA che generano immagini e video sono possibili attacchi deepfake e campagne di disinformazione difficilmente identificabili con i mezzi convenzionali.

Nell'ambito della cibersicurezza, le campagne di disinformazione non solo possono influenzare l'opinione pubblica, ma anche danneggiare i protocolli di sicurezza interni di aziende e organizzazioni. Hacker possono utilizzare la disinformazione per orchestrare attacchi di phishing mirati,

diffondere l'incertezza e indurre il personale a divulgare informazioni riservate o compiere azioni dannose. Il tema della «disinformazione e destabilizzazione» si ritrova anche nei vettori di attacco «AI-Based Attacks» e «Big Data Analytics». Per questo motivo, l'individuazione della disinformazione e la relativa difesa devono costituire una parte rilevante delle direttive aziendali in materia di sicurezza.

Strategie aziendali per gestire la disinformazione

1. **Rafforzare i canali di comunicazione interni:** una strategia di comunicazione interna chiara e trasparente è essenziale per garantire che il personale riceva e diffonda informazioni corrette.

2. **Formazione e sensibilizzazione:** il personale deve essere regolarmente informato in modo da riconoscere la disinformazione, reagire correttamente e comprendere inoltre i rischi associati alla diffusione di informazioni false.

3. **Utilizzo delle tecnologie:** l'intelligenza artificiale e l'apprendimento automatico possono aiutare le imprese a smascherare precocemente le campagne di disinformazione. L'IA può aiutare ad analizzare la diffusione di informazioni false, a identificarne le fonti e ad adottare contromisure adeguate.

4. **Pubbliche relazioni proattive e gestione delle crisi:** in caso di attacco di disinformazione è necessaria una risposta rapida e decisa. Le aziende dovrebbero sviluppare piani preparatori per reagire alla disinformazione, anche collaborando con i media e utilizzando i propri canali per diffondere informazioni corrette.

5. **Partenariati e collaborazioni:** la collaborazione con esperti esterni, altre aziende e organizzazioni può essere utile per conoscere le buone pratiche in materia di disinformazione e promuovere lo sviluppo di standard e risposte comuni.

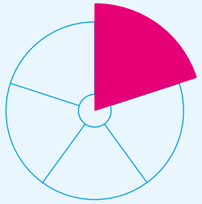
Le imprese devono comprendere che la disinformazione costituisce una grave minaccia per la loro attività e la loro reputazione. Già nel 2019, nel proprio studio sulla sicurezza e gli attacchi di disinformazione alle imprese, l'Allianz für Sicherheit in der Wirtschaft e.V. aveva giustamente inserito la protezione contro la disinformazione come quarto quadrante del proprio «focus sulla sicurezza».

Il WEF Global Risks Report 2024 evidenzia ancora una volta che la lotta alla disinformazione è una componente decisiva della sicurezza e della strategia aziendale. Implementando una strategia globale che comprenda informazione, tecnologia e impegno proattivo, le aziende possono proteggere efficacemente se stesse e i loro stakeholder. In un'epoca in cui i confini tra la verità e la falsa informazione sono sempre più labili, è fondamentale che le aziende siano in prima linea per preservare l'integrità e l'affidabilità delle loro informazioni.

« La diffusione consapevole di informazioni false, le cosiddette fake news, può portare alla destabilizzazione economica e sociale. A questo scopo si sfrutta in modo mirato anche il cyberspazio. Le imprese devono essere consapevoli di questo rischio per prepararsi e reagire adeguatamente a questo tipo di minaccia. »

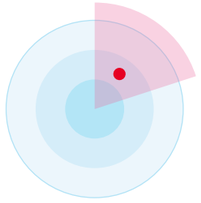
Marcus Beyer
Security Professional &
Security Awareness Officer

Dettagli comprensivi di tendenze e confronto con l’anno precedente



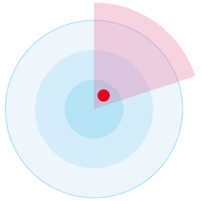
Dominant Players

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



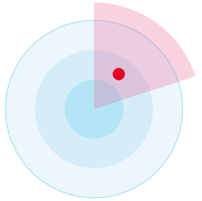
Concentration Data & Cloud Services
L’intensa centralizzazione dei dati nel cloud porta a rischi di accumulazione. Il guasto di un servizio o di un servizio centrale può avere ripercussioni in tutto il mondo.

► Stabile



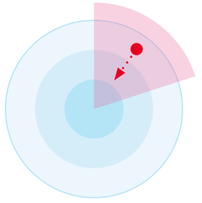
Infrastructure Integrity
In componenti essenziali delle infrastrutture critiche possono essere state inserite, per negligenza o in modo deliberato, vulnerabilità che mettono a repentaglio la sicurezza dei sistemi.

► Stabile



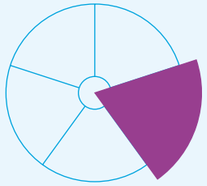
Legacy Protocols
Le dipendenze tra software fanno sì che si utilizzino ancora protocolli completamente obsoleti e vulnerabili (ad es. NTLMv1, SMBv1, RC4), per cui singole applicazioni mettono a repentaglio la sicurezza di intere infrastrutture.

► Stabile



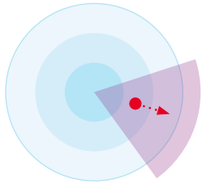
Manipulated Generative AI
Attraverso manipolazioni mirate è possibile modificare l’output di un sistema IA. In questo caso si tratta dell’immissione di dati malevoli, errati o corrotti già nella fase di addestramento, del furto di modelli LL ma anche della prompt manipulation, che può portare a conseguenze indesiderate e legalmente vincolanti.

▲ In aumento



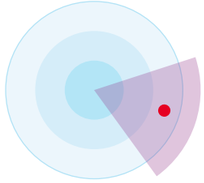
Technology Dynamics

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 di attacco, aumenta la disponibilità di strumenti di attacco e offre ad hacker nuove opportunità di creare nuove minacce attraverso il proprio sviluppo.



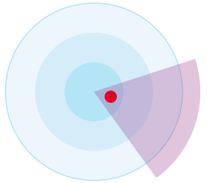
5G Security
Il 5G è una tecnologia di comunicazione mobile ancora recente. Oltre a molte opportunità, la sua introduzione comporterà anche nuove minacce.

▼ In calo



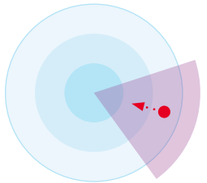
Quantum Computing
I computer quantistici possono rendere inutilizzabili le procedure crittografiche esistenti poiché riescono ad aggirarle in tempi molto brevi.

► Stabile



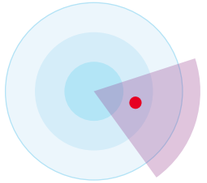
Ransomware
Dati critici vengono crittografati su larga scala e decrittati (forse) nuovamente contro il pagamento di un riscatto.

► Stabile



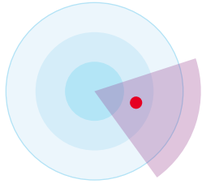
Increased Complexity
La complessità dei sistemi, in particolare quelli operanti al di là di confini tecnologici e aziendali, è in costante crescita. Soprattutto in ambito ibrido/multi-cloud con molti provider cloud, gli ambienti IT stanno diventando sempre più complessi, il che aumenta l'esposizione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

▲ In aumento



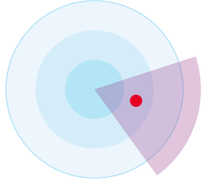
AI-Based Attacks
Gli attacchi che utilizzano l'intelligenza artificiale (AI) sono più mirati e quindi più difficili da riconoscere. L'intelligenza artificiale può essere utilizzata per sferrare attacchi più efficienti attraverso vettori classici quali ransomware, phishing, spear phishing e, occasionalmente,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

► Stabile



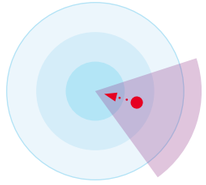
Targeted Attacks
Si tratta di attacchi mirati e complessi per raggiungere un obiettivo specifico. Le persone chiave sono identificate e prese di mira direttamente o indirettamente (ad es. Lateral Movement, Social Engineering) al fine di ottenere informazioni rilevanti o causare il massimo danno. Un aspetto essenziale è la persistenza, ovvero gli hacker agiscono inosservati il più a lungo possibile variando altresì il canale di attacco (tra e-mail e SMS o anche posta fisica).

► Stabile



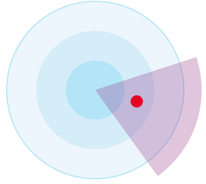
DDoS Attacks
Un attacco DDoS (Distributed Denial of Service) è un tentativo doloso di perturbare il normale traffico di dati di un server, di un servizio o di una rete target inondando di traffico internet l'obiettivo o l'infrastruttura circostante. Gli attacchi DDoS raggiungono la loro efficacia utilizzando 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



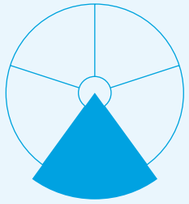
Supply Chain Attacks
Gli attacchi alla catena di fornitura mirano a sfruttare la relazione di fiducia e commerciale tra un'azienda e terze parti, come partenariati, rapporti di fornitura o l'utilizzo di software di terze parti.

▲ In aumento



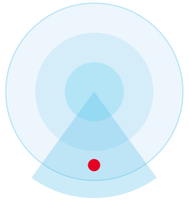
Subscriber Compromise
Il software dannoso ottiene l'accesso ai dati privati di utenti mobili o è utilizzato per attaccare l'infrastruttura di telecomunicazione o IT. Gli attacchi di phishing, smishing, vishing e MFA bypass prendono di mira le credenziali di utenti con abbonamento, mentre gli attacchi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

► Stabile



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.

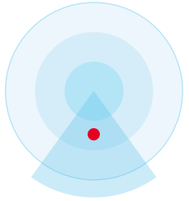
► Stabile

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



Digitalisation
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.

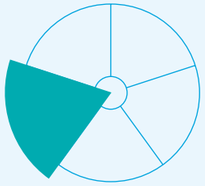
► Stabile

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

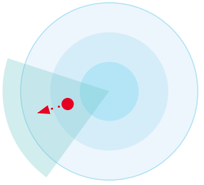
Infrastructure Misconfiguration
È lo sfruttamento di componenti delle infrastrutture configurati in modo errato e/o di lacune identificate e colmate in ritardo. Con l'aumento dell'automazione dei processi operativi tecnici, ciò avrà un impatto maggiore in caso di attacchi riusciti o configurazioni errate.

► Stabile



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.

▼ In calo

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.

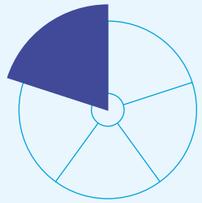
► Stabile

Unsecure IoT/OT Devices
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.

► Stabile

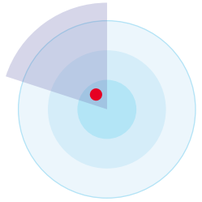
Environmental Influence
A causa della crisi climatica si verificano sempre più spesso fenomeni meteorologici imprevedibili o estremi, quali forte caldo, piogge intense, tornado, grandine, fulmini e simili, che possono provocare danni all'infrastruttura di organizzazioni e aziende e quindi avere un notevole impatto sull'ambiente esterno e interno di un sistema informativo o di una rete.

► Stabile



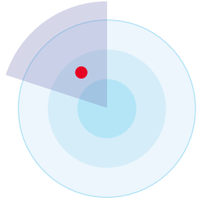
Environment/Social

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



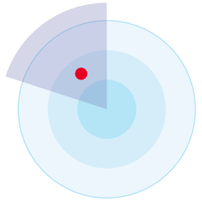
Security Job Market
La domanda di persone specializzate in sicurezza è enorme e molto difficile da soddisfare. Ciò comporta una diminuzione del know-how a fronte di attacchi sempre più complessi e intelligenti.

► Stabile



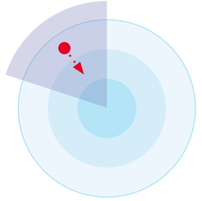
Digital Identity
Le identità digitali personali certificate possono essere utilizzate in modo improprio o rubate, ad esempio per concludere contratti a nome di altre persone.

► Stabile



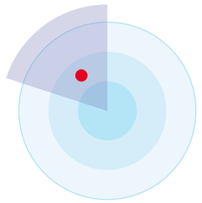
Disinformation & Destabilisation
La diffusione intenzionale di informazioni false può causare instabilità economica e sociale ed è sempre più utilizzata in scenari di crisi anche attraverso il cyberspazio.

► Stabile



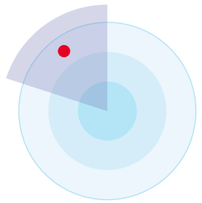
Political Influence
Le correnti politiche possono influenzare decisioni tecnologiche o economiche, ad esempio nella scelta dei fornitori di tecnologia. Da ciò possono nascere nuovi rischi.

▲ In aumento



Big Data Analytics
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



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 attacchi su commissione di diversi Paesi e gruppi politici 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

Conclusioni

Un’efficace cyberresilienza può essere attuata solo in modo interdisciplinare e intersettoriale. A tal fine è d’aiuto il seguente modello in cinque fasi:

1. **Identify**
   L’identificazione comprende l’analisi dei dati disponibili, della loro rilevanza ai fini della protezione nonché la loro memorizzazione ed elaborazione. Altrettanto importante è conoscere i potenziali rischi e minacce, nonché garantire la protezione nella catena di fornitura.

2. **Protect**
   Il personale a tutti i livelli gerarchici deve essere formato e sensibilizzato sul tema della cybersicurezza. Anche i programmi bug bounty e gli attacchi red teaming contribuiscono a rafforzare la resilienza. Inoltre, è consigliabile integrare nuove filosofie di sicurezza, come zero trust.

3. **Detect**
   Il monitoraggio continuo della propria infrastruttura e della rete interna è essenziale. Inoltre è utile una maggiore automatizzazione del Security Operations Center.

4. **Respond**
   Reagire rapidamente in caso di incidenti di sicurezza è estremamente importante. Anche gli incidenti mancati dovrebbero essere riconosciuti e documentati per poterne trarre utili conclusioni. Occorrerebbe inoltre sviluppare e formare un sistema operativo di gestione delle crisi.

5. **Recover**
   Una strategia di comunicazione ben strutturata in caso di crisi aiuta a mantenere la fiducia. Si raccomandano anche piani di Service e Business Continuity per garantire un esercizio impeccabile.

La sicurezza fisica non deve essere dimenticata, anche se spesso viene trascurata nell’ambito della cybersicurezza. Gli attacchi fisici possono mettere a repentaglio la resistenza (resilienza) delle aziende alle minacce informatiche.

Per esempio, fenomeni atmosferici estremi come siccità, caldo estremo, inondazioni e periodi di freddo intenso possono provocare danni all’infrastruttura con ripercussioni sulla stabilità dei cyberservizi, sia a livello nazionale che internazionale. Viceversa, anche gli incidenti informatici possono avere gravi ripercussioni su settori fisici. Per questo è importante tenere conto sia della sicurezza fisica che di quella informatica e adottare misure adeguate per garantire la resilienza delle aziende.

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
Copyright	© Aprile 2024 by Swisscom (Svizzera) SA, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Stampa	OK DIGITALDRUCK AG, Zurigo
Tiratura	200 copie

In qualità di «Innovator of Trust», Swisscom rende possibile e progetta il futuro digitale. Grazie a prodotti e servizi innovativi e alla fiducia della clientela si crea un'esperienza cliente unica con un impatto duraturo sull'ambiente e sulla società. In Svizzera e in tutto il mondo.

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

Stai cercando un lavoro nel settore della sicurezza presso Swisscom? Allora dai un'occhiata qui e invia la tua candidatura: swisscom.ch/securityjobs

#BeTheStrongestLink