swisscom

Cyber Security Threat Radar
2022/2023

Vivere la Security by Design

Sommario

«Integrare sin dall'inizio e in modo propositivo la sicurezza nel pensiero aziendale ponendo i collaboratori al centro dell'attenzione – questo è ciò che intendiamo per Security by Design e Human Centered Security. Solo così potremo tenere le nostre aziende al sicuro.»

Cyber Security Threat Radar

I rischi informatici sono destinati a rimanere?

La minaccia rappresentata dai rischi informatici si mantiene su un livello molto elevato. Per migliorare la resilienza informatica nella propria azienda, è imperativo adottare una visione olistica della cibersicurezza e della sicurezza informatica. Non è consigliabile raggirare le crisi o sperare che la situazione di minaccia torni alla normalità. Piuttosto, è opportuno prepararsi contemplando tutti i possibili scenari di crisi, così che in caso di emergenza possano essere affrontati nel modo più adeguato riducendo al minimo i danni. I rischi informatici e multipli che stiamo attualmente affrontando sono destinati a rimanere; il loro impatto è ben visibile e palpabile in molti Paesi di tutto il mondo e sussiste il pericolo che i danni collaterali li rendano ancora più imprevedibili.

Ormai risulta piuttosto evidente che la cibersicurezza non è solo responsabilità dei reparti IT, ma riguarda tutte le aree di un'azienda. Una solida gestione della continuità operativa fa parte di un sistema di rischio tanto quanto un'IT di servizio stabile. Oltre alle precauzioni tecniche, anche dei collaboratori ben addestrati e attenti svolgono un ruolo centrale: la massima resilienza, infatti, può essere raggiunta solo grazie a questa combinazione.

Questo Cyber Security Threat Radar si propone di aiutare a identificare i rischi informatici centrali nella propria azienda e a combatterli in modo appropriato. Esso funge da linea guida per creare una consapevolezza uniforme del problema della sicurezza informatica e per instaurare un piano di sicurezza completo.

È un documento di riferimento per le organizzazioni più diverse e getta le basi per una sicurezza informatica efficace e quindi per il successo di ogni azienda nel mondo digitale.

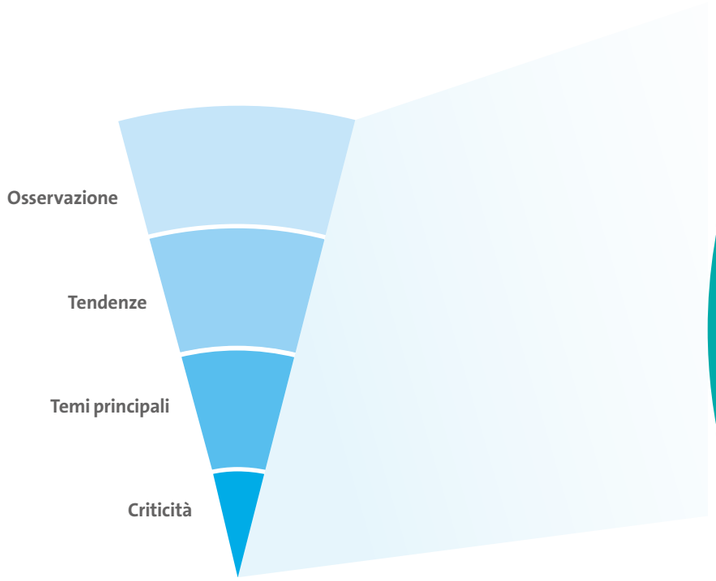
Marco Wyrsch
Head of Group Security
Swisscom (Schweiz) AG

«La guerra in Europa sta cambiando il mondo», diceva Philippe Vuilleumier, il mio predecessore come Head of Group Security presso Swisscom, nel messaggio di benvenuto al Cyber Security Threat Radar dello scorso anno. E anche un anno dopo, la sua affermazione non ha perso affatto di attualità, poiché la guerra tiene ancora il mondo con il fiato sospeso. Gli effetti si fanno sentire in molti modi: possibile penuria di elettricità, penuria di gas, spostamento delle attività belliche nel ciberspazio, atti di sabotaggio contro infrastrutture critiche, una gran quantità di notizie false e una copertura mediatica capillare su tutti i canali. Dalla situazione attuale risulta chiaro che in tempi di multicrisi la sicurezza logica e quella fisica vanno di pari passo. A maggior ragione occorre essere più consapevoli dei rischi. In tempi incerti, l'interazione tra persone, processi e tecnologie costituisce la base per creare resilienza e stabilità in un'azienda.

Quadro della situazione – radar delle minacce

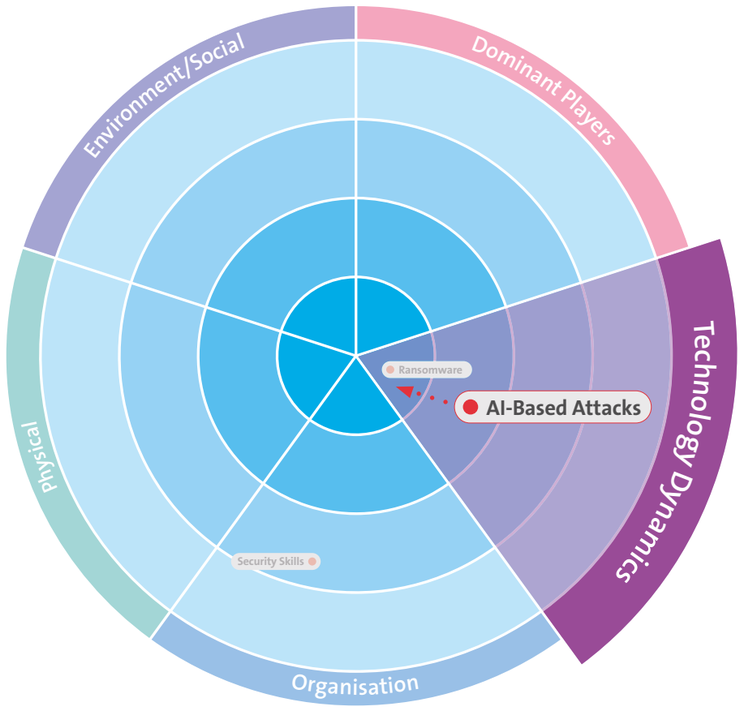
Poter attingere, al momento opportuno, a strategie e procedure di sicurezza consolidate e testate ci aiuta a meglio affrontare gli imprevisti – i cosiddetti «cigni neri». Abbinandovi una cultura della sicurezza coerente, trasparenza degli errori e collaboratori ben addestrati, gettiamo le basi per la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



Sfide e tendenze

AI-Based Attacks: il lato oscuro del progresso tecnologico



Di che cosa si tratta?

Gli AI-based attack (AI sta per artificial intelligence) sono attacchi informatici che si avvalgono delle tecnologie di intelligenza artificiale per rendere gli attacchi più efficaci ed efficienti o per aggirare le difese esistenti.

Gli attacchi basati sull'intelligenza artificiale non sono certo un fenomeno nuovo, ma negli ultimi mesi gli strumenti a disposizione hanno mostrato un vero e proprio salto evolutivo. Strumenti come il Large Natural Language Model AI ChatGPT, introdotto nel novembre 2022, dimostrano in modo sorprendente come, ad esempio, gli attacchi di phishing possano essere significativamente migliorati in termini di qualità o utilizzati per rilevare lacune nei codici dei programmi. Attualmente, il tema dell'intelligenza artificiale è molto presente nei media e il suo abuso per la creazione di malware / codici dannosi e campagne di phishing aumenterà sicuramente in futuro. Sebbene ne stiamo già osservando e analizzando lo sviluppo, attualmente non rappresenta ancora una criticità.

Come evolverà questa sfida?

Tra i primi sviluppi, ci aspettiamo una crescente fusione di attacchi mirati con e-mail di phishing generate dall'intelligenza artificiale. Un'AI basata su un modello linguistico può sviluppare una trama convincente riallacciandosi a una conversazione di posta elettronica esistente e collegarla in modo ingegnoso a un attacco di phishing o di social engineering. Attraverso un'adeguata automazione è possibile lanciare campagne di phishing mirate con e-mail contestuali perfettamente individualizzate.

Un'altra evoluzione nell'uso dannoso dell'intelligenza artificiale basata su modelli linguistici è la loro capacità di scansionare i codici dei programmi per individuare lacune e programmare malware mirati, inclusi vettori di attacco idonei. Il know-how necessario per chi sferra attacchi complessi continua quindi a diminuire.

Inoltre, la rapida evoluzione delle intelligenze artificiali che generano immagini e video consente attacchi deep-fake e campagne di disinformazione difficilmente identificabili con mezzi convenzionali.

Come affrontare la sfida in modo efficace?

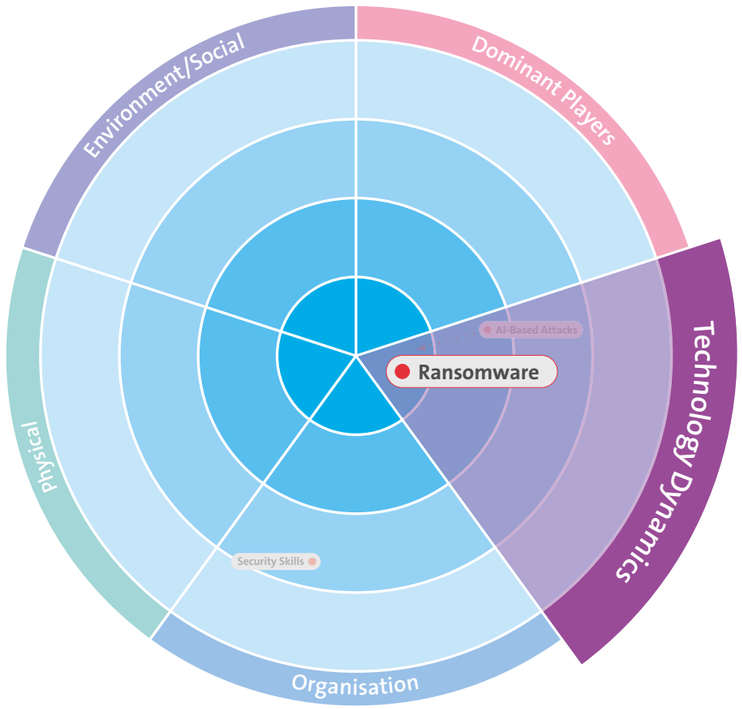
Le tecnologie di intelligenza artificiale (AI) possono essere utilizzate dagli hacker, ma allo stesso tempo l'AI offre anche a chi deve tutelarsi modi più efficaci per rilevare e difendersi dagli attacchi informatici, ad esempio per riconoscere testi, immagini e video generati da un'AI. Modelli quali Zero Trust per l'accesso controllato in modo granulare e autenticato a dati e risorse aiutano a ridurre l'area di attacco delle aziende. Ma anche best practice di sicurezza consolidate come l'autenticazione a più fattori, DevSecOps, la gestione delle vulnerabilità e delle patch e la consapevolezza della sicurezza tra i collaboratori aiutano a prevenire gli attacchi informatici, non solo basati sull' intelligenza artificiale, ma in generale.

«Le tecnologie di intelligenza artificiale evolvono rapidamente ed è importante sapere che non sono buone o cattive di per sé; piuttosto, sono uno strumento che può essere utilizzato per entrambi gli scopi. La vera sfida sta nel continuare a rafforzare le difese in modo che anche gli attacchi basati sull'intelligenza artificiale possano essere respinti con successo in futuro, sempre più con l'aiuto di un'intelligenza artificiale ‹buona›.»

Florian Leibenzeder
Responsabile Swisscom Security Operation Center

Sfide e tendenze

Ransomware: estorsione attraverso il furto di dati invece della «sola» cifratura



Di che cosa si tratta?

Il ransomware è un tipo di malware (software dannoso) che, dopo aver infettato un computer, un server o una rete, cifra i dati rendendoli inutilizzabili. La vittima ottiene la chiave di decodifica necessaria per ripristinare i dati solo dietro il pagamento di un riscatto («ransom»). L'anno scorso, questa forma di attacco è stata nuovamente riconosciuta come una sfida acuta e affrontata separatamente nel Cyber Security Threat Radar.

Da allora, molte aziende e organizzazioni si sono aggiornate ed evolute dal punto di vista tecnico; quindi, vengono pagati sempre meno riscatti a causa di questo tipo di attacchi. Gli hacker vengono prontamente bloccati quando effettuano il tentativo di cifratura o è comunque possibile recuperare i dati in altro modo. Essendo sempre più difficile, ad esempio, rendere inutilizzabili i backup, gli hacker ricorrono sempre più spesso all'esfiltrazione dei dati e alla minaccia di pubblicarli. A differenza dei dati cifrati, che possono essere ripristinati dal backup, nel caso dei dati esfiltrati è quasi impossibile impedirne la pubblicazione senza pagare un riscatto.

Gli hacker hanno una motivazione finanziaria. Gli attacchi ransomware e il conseguente furto di dati sono il modo più semplice e diretto per trarre guadagno da un'infrastruttura aziendale compromessa. Solitamente, la somma richiesta dipende dalle dimensioni dell'azienda e ammonta a circa il tre per cento del fatturato; tuttavia, è doveroso puntualizzare che l'importo del riscatto è spesso solo una frazione del danno finanziario cagionato dall'attacco.

Sebbene non esistano statistiche ufficiali sull'importo dei pagamenti effettuati, le stime suggeriscono un rendimento medio di 950 000 franchi per ogni attacco riuscito.

A livello globale, si stima che entro il 2031 i danni economici causati da attacchi ransomware potrebbero superare i 240 miliardi di franchi.

La prospettiva di guadagni facili attraverso simili attacchi porta a una crescente professionalizzazione degli hacker. In tale contesto, si parla addirittura di cosiddetti «Unicorn ransomware». Da varie fonti, ad esempio Conti Leaks, è noto che molti hacker dispongono oramai di risorse finanziarie simili a quelle di una start-up IT ben finanziata.

In alcuni casi, impiegano sviluppatori e hacker fissi che offrono alle vittime un'«assistenza clienti» a più livelli. Si avvalgono di metodi di sviluppo agili potenziando progressivamente il modello di business e l'infrastruttura. Mantengono anche propri programmi di Bug Bounty, grazie ai quali i criminali informatici ricevono informazioni sulle falle di sicurezza nella loro infrastruttura IT.

Alcuni hacker ascrivono grande importanza alla loro popolarità. Con una campagna di guerrilla marketing, ad esempio, un gruppo di hacker ha esortato gli utenti a farsi tatuare il logo Lockbit dietro un compenso di 1000 dollari. A seguito dell'appello, Internet è stato inondato di foto ritraenti persone appena tatuate con il logo della cybergang.

Come evolverà questa sfida?

Il ransomware è e rimane un argomento caldo. Prevediamo un aumento significativo delle estorsioni multiple, ovvero la combinazione di più forme di attacco come ransomware, furto di dati e Denial of Service, poiché questa forma di attacchi ransomware si è già consolidata tra i criminali informatici. Anche i provider di Managed Service sono sempre più nel mirino degli hacker. L'esperienza dimostra che sono propensi a pagare i riscatti e anche i loro clienti possono essere attaccati direttamente per trarre ancora più profitto dall'attacco.

La maggiore sfida per il futuro consiste nella crescente specializzazione degli hacker e nella conseguente complessità dei loro attacchi. Già adesso la principale minaccia è rappresentata dalle cosiddette offerte ransomware-as-a-service: i gruppi ransomware non penetrano più direttamente nelle aziende, ma noleggiano ad altri hacker il loro software dannoso di cifratura e l'infrastruttura di server e di supporto. Il riscatto ricevuto viene quindi diviso «fraternamente» tra gli hacker e il gruppo ransomware. Ci sono «Initial Access Brokers» specializzati nell'infiltrarsi nelle aziende e quindi vendere le opzioni di accesso acquisite.

L'accesso iniziale può essere ottenuto sia a livello umano che a livello di infrastruttura: a livello di infrastruttura, i server accessibili pubblicamente vengono attaccati tramite vulnerabilità note o exploit zero-day. Spesso, gli exploit zero-day non sono più sviluppati internamente, ma acquistati da terze parti.

Per quanto riguarda il «livello umano», gli hacker sferrano l'attacco attraverso campagne di (spear) phishing mirate contro gli utenti finali di un'azienda. Altri gruppi ransomware contattano direttamente i collaboratori delle potenziali vittime e tentano di corromperli con ingenti somme di denaro. Anche gli attacchi alle infrastrutture private dei collaboratori stanno diventando sempre più frequenti, come mostra il recente attacco a LastPass: dopo aver violato la rete domestica di un amministratore di sistema, i cyber criminali sono riusciti ad impossessarsi delle credenziali VPN dell'azienda.

Come affrontare la sfida in modo efficace?

La misura di protezione più importante è seguire le Best Practice consolidate, fra cui rientrano i seguenti accorgimenti:

- gestire le vulnerabilità e le patch
- utilizzare moderne soluzioni di backup protette da air-gap, effettuare regolari backup (offline) e regolari test del lavoro di ripristino
- creare Security Awareness all'interno dell'azienda
- utilizzare sistematicamente l'autenticazione a più fattori (MFA) e combattere l'MFA fatigue
- assicurare un monitoraggio capillare della sicurezza informatica tramite Endpoint Detection and Response (EDR)
- impiegare team di sicurezza specializzati come Security Operation Center (SOC) e Cyber Security Incident Response Team (CSIRT)
- segmentazione della rete e concetto di zone di sicurezza
- definire processi di Incident Response e di comunicazione in caso di crisi ed effettuare formazioni periodiche sui possibili scenari di crisi

«Dato che gli hacker si stanno perfezionando sempre di più, può essere molto utile difendersi affidandosi a società specializzate e a team esterni di esperti.»

Tim Trinkl
Senior Security Analyst & Incident Responder B2B

Sfide e tendenze

Security Skills: prevenire la penuria di lavoratori qualificati e la perdita di know-how

Di che cosa si tratta?

Indipendentemente dalle loro dimensioni, molte aziende affrontano spesso la stessa sfida: i team addetti alla sicurezza informatica sono a corto di personale e/o semplicemente sovraccarichi di lavoro. Il crescente numero di incidenti di sicurezza, la sfida nel dare loro priorità e la penuria di lavoratori qualificati possono sopraffare le aziende, incrementando i rischi. Per tenere il passo con i criminali informatici, le aziende non hanno necessariamente bisogno di più budget, ma di collaboratori competenti in materia di sicurezza informatica. Ed ecco due vettori di attacco discussi nel Cyber Security Threat Radar: Security Skills e Infrastructure Misconfiguration. La carenza di competenze e di personale fa aumentare esponenzialmente i rischi informatici legati ai componenti delle infrastrutture mal configurati.

Negli ultimi anni le università, le scuole universitarie professionali e altri istituti di formazione hanno notevolmente ampliato i loro corsi di studio, ma il settore non riesce ancora a soddisfare l'attuale elevata domanda di specialisti della sicurezza informatica.

In una costante lotta alla ricerca di talenti, un'azienda può spendere tutte le sue risorse finanziarie nel tentativo di attingere a un mercato del lavoro «esaurito». Un'altra opzione è quella di guardare al proprio interno e investire nella formazione di base e continua dei propri collaboratori. Con l'aumentare del numero e della complessità degli attacchi da parte di criminali informatici governativi e privati, la carenza globale di esperti di sicurezza informatica è già dolorosamente sentita in molte aziende e organizzazioni.

Tuttavia, il problema non si limita alla carenza di specialisti nel campo della sicurezza informatica, ma interessa anche l'abbandono della professione da parte degli esperti del settore. Numerosi studi dimostrano che molti collaboratori attivi nella sicurezza informatica stanno prendendo in considerazione la possibilità di cambiare lavoro.

Come evolverà questa sfida?

«A causa delle tensioni geopolitiche e dell'instabilità macroeconomica, di violazioni di dati di alto profilo e di crescenti sfide alla sicurezza fisica, la sicurezza informatica sta diventando sempre più importante e la domanda di professionisti in questo settore è in aumento», afferma Clar Rosso, CEO di (ISC)² – International Information System Security Certification Consortium.

Molte aziende si affidano a piattaforme per specialisti informatici al fine di rafforzare in modo mirato la formazione di base e continua all'interno dell'azienda. Tuttavia, spesso in questi corsi manca un'integrazione adeguata del personale, che però necessita di crescenti competenze di sicurezza nei processi aziendali, di sviluppo e di innovazione. Domande su come rendere la formazione di base e continua così attrattiva da essere accettata dai collaboratori tecnici e utilizzata nelle attività quotidiane, o sulle possibilità per realizzare una campagna di formazione attiva nell'ambiente specialistico rimangono spesso senza risposta. All'offerta formativa vera e propria si aggiunge rapidamente la questione del giusto assetto organizzativo.

Molti candidati deplorano la mancanza di disponibilità nel processo di reclutamento lamentando, fra le altre cose, lunghi tempi di risposta alle candidature da parte delle aziende, regolamenti rigidi, fasce salariali bloccate e processi di assunzione poco trasparenti. Ciò suggerisce processi di reclutamento non professionali per alcune delle aziende criticate. Per essere percepito dai talenti informatici come un datore di lavoro attrattivo nel tempo, è auspicabile un rigoroso Employee Journey nel processo di reclutamento.

Come affrontare la sfida in modo efficace?

Migliorare le condizioni di lavoro: il denaro da solo non dà la felicità, ma è certamente un fattore decisivo. Oltre a una remunerazione adeguata, le aziende possono anche guadagnare punti in termini di ambiente di lavoro e di equilibrio tra lavoro e vita privata. Le possibilità qui sono molteplici: orari di lavoro flessibili, modelli di telelavoro, orario di lavoro ridotto con lo stesso stipendio ecc. Spetta poi alle singole aziende decidere di volta in volta quali opzioni sono realistiche o meno.

Adeguare le aspettative poste ai candidati: posizioni da esordiente o Junior con una laurea e almeno cinque anni di esperienza professionale non corrispondono alla realtà. Parecchie aziende dovrebbero riconsiderare le loro aspettative, altrimenti la ricerca di buoni collaboratori potrebbe risultare piuttosto complicata.

Offrire formazione continua e continuare a svilupparla internamente: attraverso opportuni corsi di formazione e di perfezionamento – dai training in azienda ai campi di addestramento DevSecOps, fino ai corsi universitari – i collaboratori possono acquisire le competenze di sicurezza necessarie e quindi assumere nuovi compiti. Affinché il proprio personale fruisca di queste opportunità, le imprese devono creare incentivi adeguati, ad esempio contribuendo ai costi di formazione.

Ricorrere all'outsourcing e ridurre il carico di lavoro: per ridurre il carico di lavoro nella sicurezza, alcune aree di responsabilità possono essere esternalizzate a fornitori di servizi specializzati. I fornitori di servizi esterni possono contribuire a colmare lacune specifiche nel know-how dell'azienda («knowledge gap»).

«Dobbiamo assolutamente colmare il divario di talenti nella sicurezza informatica. Per riuscirci dobbiamo abbattere le barriere all'accesso, trattenere il personale con un lavoro incentivante nel campo della cibersicurezza e garantire che i collaboratori rimangano fedeli all'organizzazione nel lungo termine. Anche la formazione mirata nell'ambiente DevSecOp interno supporta in modo proattivo la ‹battaglia per i talenti›.»

Marcus Beyer
Security Awareness Officer

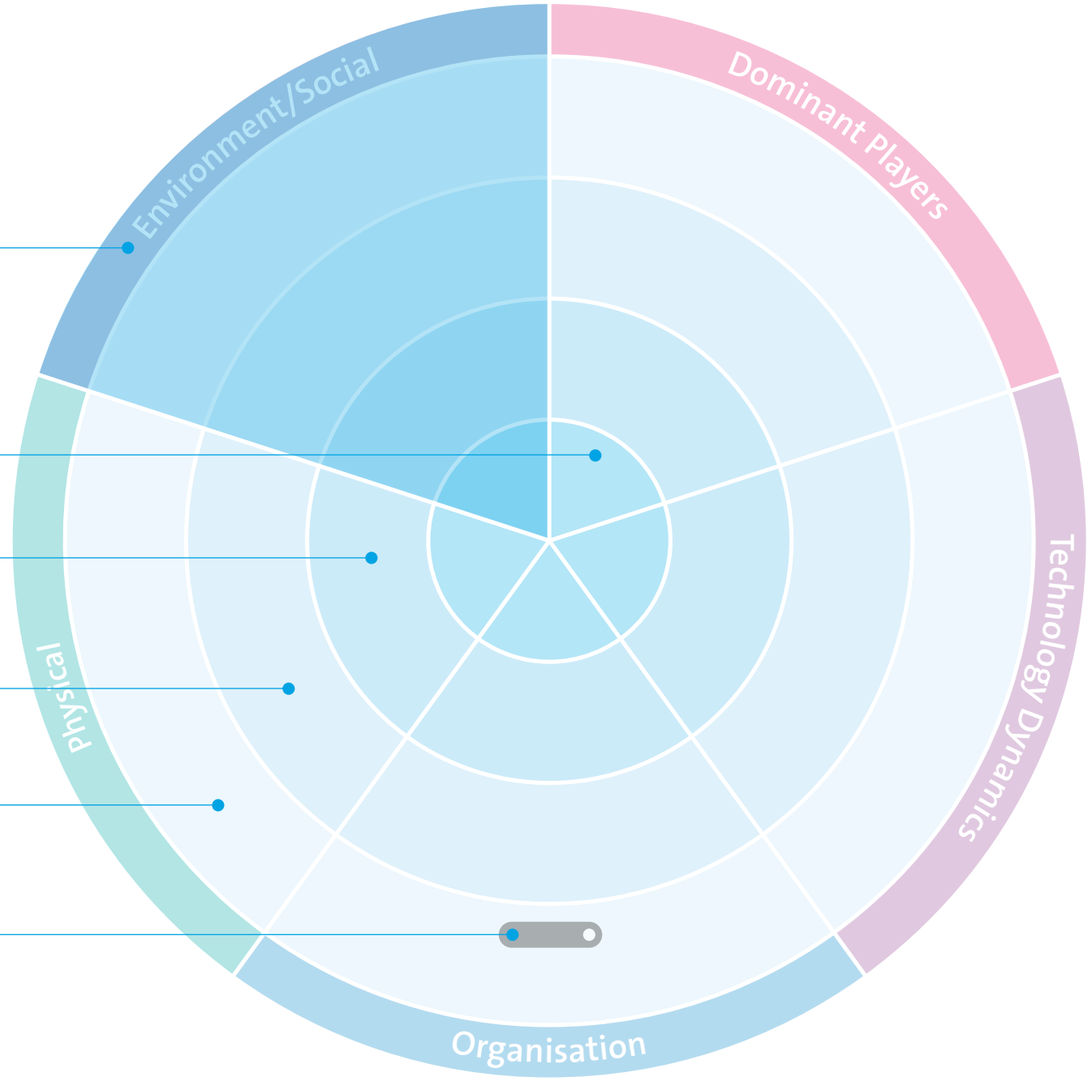
Metodica

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 quattro 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.

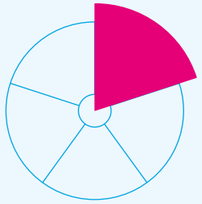
Descriviamo i cerchi come

- **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;
- **osservazione** per le minacce che si verificheranno solo tra qualche anno. Non esistono ancora misure concrete per affrontare 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.

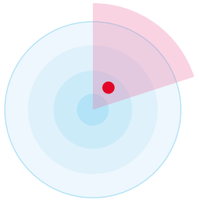


Dettagli comprensivi di tendenze e confronto con l’anno precedente



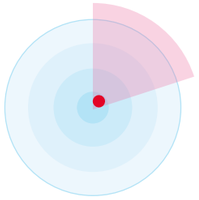
Dominant Players

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



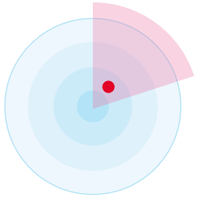
Concentration Data & Cloud Services
L’intensa centralizzazione dei dati nel cloud porta a rischi di accumulazione. Il guasto di un servizio o di un servizio centrale può avere ripercussioni in tutto il mondo.

▲ In aumento



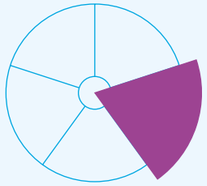
Infrastructure Integrity
In componenti essenziali delle infrastrutture critiche possono essere state inserite, per negligenza o in modo deliberato, vulnerabilità che mettono a repentaglio la sicurezza dei sistemi.

► Stabile



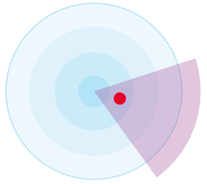
Legacy Protocols
Le dipendenze tra software fanno sì che si utilizzino ancora protocolli completamente obsoleti e vulnerabili (ad esempio NTLMv1, SMBv1, RC4), per cui singole applicazioni mettono a repentaglio la sicurezza di intere infrastrutture.

► Stabile



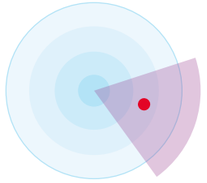
Technology Dynamics

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 agli hacker nuove opportunità di creare nuove minacce attraverso il proprio sviluppo.



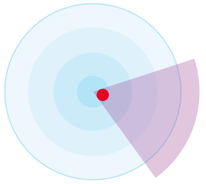
5G Security
Il 5G è una tecnologia di comunicazione mobile ancora recente. Oltre a molte opportunità, la sua introduzione comporterà anche nuove minacce.

► Stabile



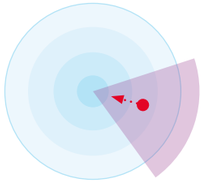
Quantum Computing
I computer quantistici possono rendere inutilizzabili le procedure crittografiche esistenti poiché riescono ad aggirarle in tempi molto brevi.

▼ In calo



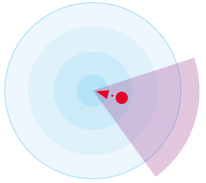
Ransomware
Dati critici vengono crittografati su larga scala e decriptati (forse) nuovamente contro il pagamento di un riscatto.

▲ In aumento



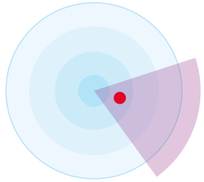
Increased Complexity
La complessità dei sistemi, in particolare quelli operanti al di là di confini tecnologici e aziendali, è in costante crescita. Soprattutto in ambito ibrido/multi-cloud con molti provider cloud, gli ambienti IT stanno diventando sempre più complessi, il che aumenta l'esposizione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

▲ In aumento



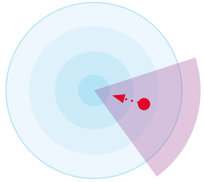
AI-Based Attacks
Gli attacchi che utilizzano l'intelligenza artificiale (AI) sono più mirati e quindi più difficili da riconoscere. L'intelligenza artificiale può essere utilizzata per sferrare attacchi più efficienti attraverso vettori classici quali ransomware, phishing, spear phishing e, occasionalmente,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

▲ In aumento



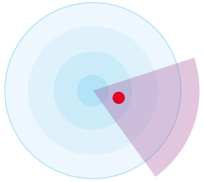
Targeted Attacks
Si tratta di attacchi mirati e complessi per raggiungere un obiettivo specifico. Le persone chiave sono identificate e prese di mira direttamente o indirettamente (es. Lateral Movement, Social Engineering) al fine di ottenere informazioni rilevanti o causare il massimo danno. Un aspetto 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



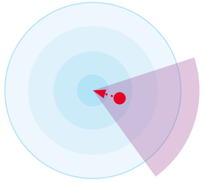
DDoS Attacks
Un attacco DDoS (Denial of Service) è un tentativo doloso di perturbare il normale traffico di dati di un server, di un servizio o di una rete target inondando di traffico internet l'obiettivo o l'infrastruttura circostante. Gli attacchi DDoS raggiungono la loro efficacia utilizzando più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

▲ In aumento



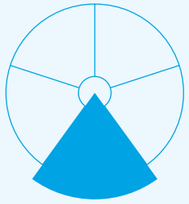
Supply Chain Attacks
Gli attacchi alla catena di fornitura mirano a sfruttare la relazione di fiducia e commerciale tra un'azienda e terze parti, come partenariati, rapporti di fornitura o l'utilizzo di software di terze parti.

▲ In aumento



Subscriber Compromise
Il software dannoso ottiene l'accesso ai dati privati degli 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 degli abbonati, mentre gli attacchi successivi hanno lo scopo di sottrarre e assumere illecitamente le loro identità digitali.

▲ 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 collaboratori 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.

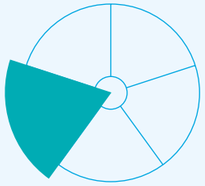
► Stabile

Security Skills
La complessità degli attacchi informatici e la crescente digitalizzazione rendono indispensabile disporre di competenze di sicurezza e impiegare professionisti informatici 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 specialisti.

▲ In aumento

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.

▲ In aumento



Physical

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

Device Theft
Il furto o altro tipo di smarrimento di terminali come smartphone e laptop o anche di componenti IT importanti può causare la perdita di dati o compromettere la disponibilità dei servizi IT.

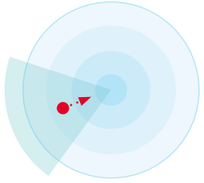
▼ In calo

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 aumento

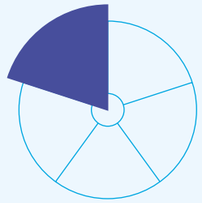
Unsecure IoT/OT Devices
Che si tratti di tecnologia operativa (OT) per monitorare e manovrare processi fisici, dispositivi e infrastrutture o di dispositivi IoT, l'internet delle cose è onnipresente. I compiti svolti sono i più disparati, dai più semplici ai più complessi, e spaziano dalle applicazioni 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



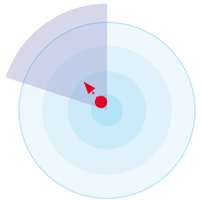
Targeted Sabotage
Si tratta di attacchi mirati a importanti infrastrutture critiche, impianti di distribuzione e linee che possono limitare notevolmente internet. Il sabotaggio mirato di linee nevralgiche in fibra ottica è in aumento, rappresenta un rischio e va monitorato. Le contromisure sono difficili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

▲ In aumento



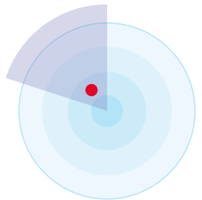
Environment/Social

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 gli hacker.



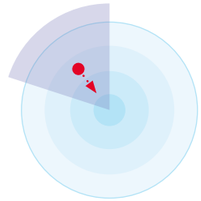
Security Job Market
La domanda di professionisti della sicurezza è enorme e molto difficile da soddisfare. Ciò comporta una diminuzione del know-how a fronte di attacchi sempre più complessi e intelligenti.

► Stabile



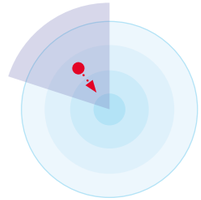
Digital Identity
Le identità digitali personali certificate possono essere utilizzate in modo improprio o rubate, ad esempio per concludere contratti a nome di qualcun altro.

▲ In aumento



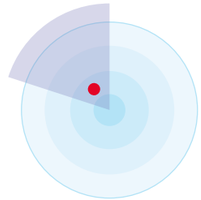
Disinformation & Destabilisation
La diffusione deliberata di informazioni false può causare instabilità economica e sociale ed è sempre più utilizzata in scenari di crisi anche attraverso il ciberspazio.

▲ In aumento



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.

► Stabile



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

Conclusioni

La Security by Design quale considerazione e integrazione coerente degli aspetti di sicurezza in tutte le fasi dello sviluppo di un software – dall' idea iniziale all'introduzione e all'utilizzo dei prodotti – non solo è sempre più importante, ma è anche la colonna portante di una sicurezza informatica stabile per aziende e organizzazioni.

In combinazione con un approccio alla sicurezza incentrato sull'essere umano, ovvero la sensibilizzazione regolare del personale in materia di sicurezza, le aziende diventano più sicure e sono meglio preparate ad affrontare situazioni di crisi incombenti.

Se ci si prende il tempo per identificare i possibili rischi, ben presto ci si accorge che la propria azienda è esposta ad ogni tipo di scenario di crisi immaginabile. Questi rischi devono essere affrontati e analizzati. Nascondere la testa nella sabbia non è certamente un'opzione sostenibile né consigliata.

Occuparsi dei rischi informatici è sicuramente impegnativo; tuttavia, è estremamente importante tenere sotto controllo l'intero apparato ed essere consapevoli dei rischi per la cibersicurezza in generale – e dei relativi rischi di subire un blocco.

Perciò, se i modelli di pensiero, i concetti e le tecnologie esistenti non forniscono più risposte soddisfacenti, è tempo di testare, introdurre e stabilire nuovi approcci, metodologie, ruoli e tecnologie. Il che richiede una visione ben ponderata, una strategia, coraggio e molta perseveranza.

Per le aziende, questo investimento nel futuro è una grande sfida. L'aspetto più difficile, che richiede l'onere maggiore e parecchia pazienza, è quello di riconsiderare e rielaborare i modelli di pensiero e i processi esistenti all'interno dei reparti informatici. Eppure, sono proprio questi cambiamenti ad essere talvolta essenziali per tutelare la propria azienda dalle minacce. Poiché è indubbio che i rischi informatici stanno evolvendo rapidamente e che soltanto le aziende che tengono il passo e dispongono di una sicurezza agile saranno adeguatamente protette contro la cibercriminalità anche in avvenire.

«L'interazione tra persone, processi e tecnologie costituisce la base per creare resilienza e stabilità in un'azienda in tempi incerti.»

Appunti

Sigla editoriale

Editore	Swisscom (Svizzera) SA, Group Security
Concetto/realizzazione	Agentur Nordjungs, Zurigo
Redazione	Swisscom (Svizzera) SA Marcus Beyer (Group Security) Manuel Bühlmann (Group Communications) Claudia Lehmann (B2B Communications)
Traduzione	Apostroph Bern AG
Copyright	© Maggio 2023 by Swisscom (Svizzera) SA, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Stampa	OK DIGITALDRUCK AG, Zurigo
Tiratura	200 copie

Swisscom è sempre all'avanguardia e progetta innovazioni affidabili sulle quali le persone possono crescere. In veste di «Innovators of Trust».

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

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

#BeTheStrongestLink