swisscom

# Cyber Security Threat Radar
# 2021/2022

Rivalutare sempre i rischi e il contesto

# Sommario





*«Solo una Security perfettamente adeguata alle esigenze degli utenti può adempiere alla propria funzione e assicurare la resilienza necessaria a medio e lungo termine.»*

# Cyber Security Threat Radar

Ciò che fino a poco tempo fa era impensabile, dal 24 febbraio è una tragica realtà. **La guerra in Europa sta cambiando il nostro mondo.**

Con lo scoppio della guerra in Ucraina, il ruolo e l'importanza dei (social) media sono apparsi in tutta la loro chiarezza. Resoconti allarmanti, notizie false e dichiarazioni virtuose si alternano continuamente a una subdola disinformazione.

Di fatto, dall'inizio dell'invasione russa dell'Ucraina molti rischi e minacce hanno messo in allerta governi, organizzazioni e aziende ancora di più di quanto sia avvenuto negli ultimi due anni con la pandemia. La tensione si ripercuote sull'intera società.

Ma c'è una buona notizia: nonostante la situazione difficile, nell'infrastruttura di rete svizzera finora non è stato registrato alcun aumento degli attacchi.

Naturalmente i criminali informatici cercano di sfruttare la guerra in Ucraina per le loro attività illegali, ad esempio con tentativi di phishing ad hoc o richieste di donazioni contraffatte. Purtroppo questa è una pratica comune quando accadono eventi di grande portata. Il numero di crimini informatici rimane quindi a un livello costantemente elevato, a cambiare sono solo i pretesti utilizzati per colpire le vittime.

Mi auguro che questa edizione di Cyber Security Threat Radar 2021/2022 vi offra spunti utili sul tema della cybersicurezza e vi aiuti a sviluppare le vostre attività legate alla sicurezza nella vostra organizzazione o azienda.

**Philippe Vuilleumier**
Head of Group Security
Swisscom (Svizzera) SA

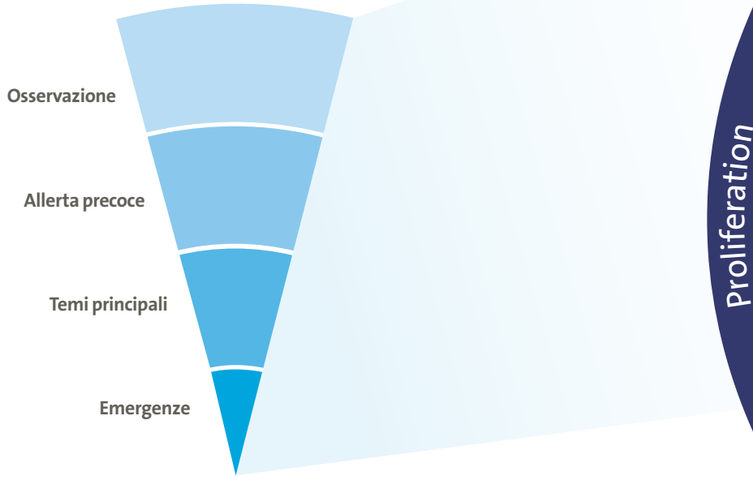
Il motto del Cyber Security Threat Radar dell'anno scorso «Le situazioni eccezionali richiedono misure eccezionali quanto a sicurezza, protezione e consapevolezza dei rischi» non ha perso rilevanza, al contrario: è sempre più attuale. In un periodo di sconvolgimenti come quello che stiamo vivendo è importante mantenere tutto sotto controllo, per adottare le misure giuste in modo tempestivo.

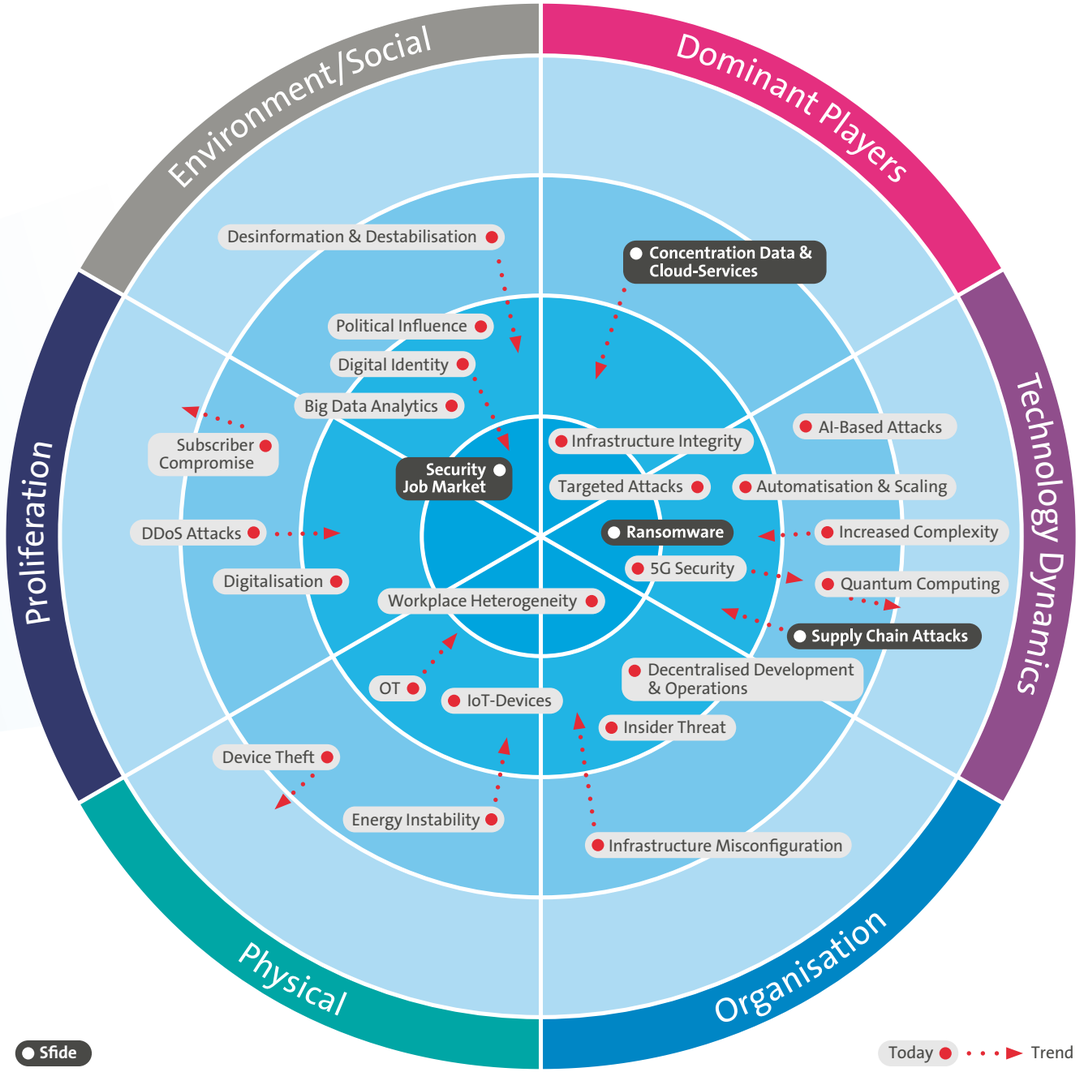
Al centro di tali misure vi sono le persone. Ovviamente le tecnologie costituiscono elementi insostituibili del sistema di sicurezza. Ma da sole non garantiscono alcuna protezione. Per questo raccomando caldamente di mettere le persone al centro di tutte le riflessioni, soluzioni e misure relative alla sicurezza. Solo una Security perfettamente adeguata alle esigenze degli utenti può adempiere alla propria funzione e assicurare la resilienza necessaria a medio e lungo termine.

# Quadro della situazione – le minacce al radar

Nel momento in cui sono necessarie, poter contare su strategie e procedure di sicurezza consolidate e verificate aiuta a gestire gli imprevisti, i cosiddetti «cigni neri». In combinazione con una coerente cultura della sicurezza e trasparenza sugli errori e con una buona formazione dei collaboratori, formano la base della resilienza di un'organizzazione.

Affinché le reazioni siano adeguate, bisogna riconoscere per tempo le potenziali minacce e gestirle sistematicamente. Per dare una rappresentazione delle minacce e della loro evoluzione, utilizziamo il noto Cyber Security Threat Radar.



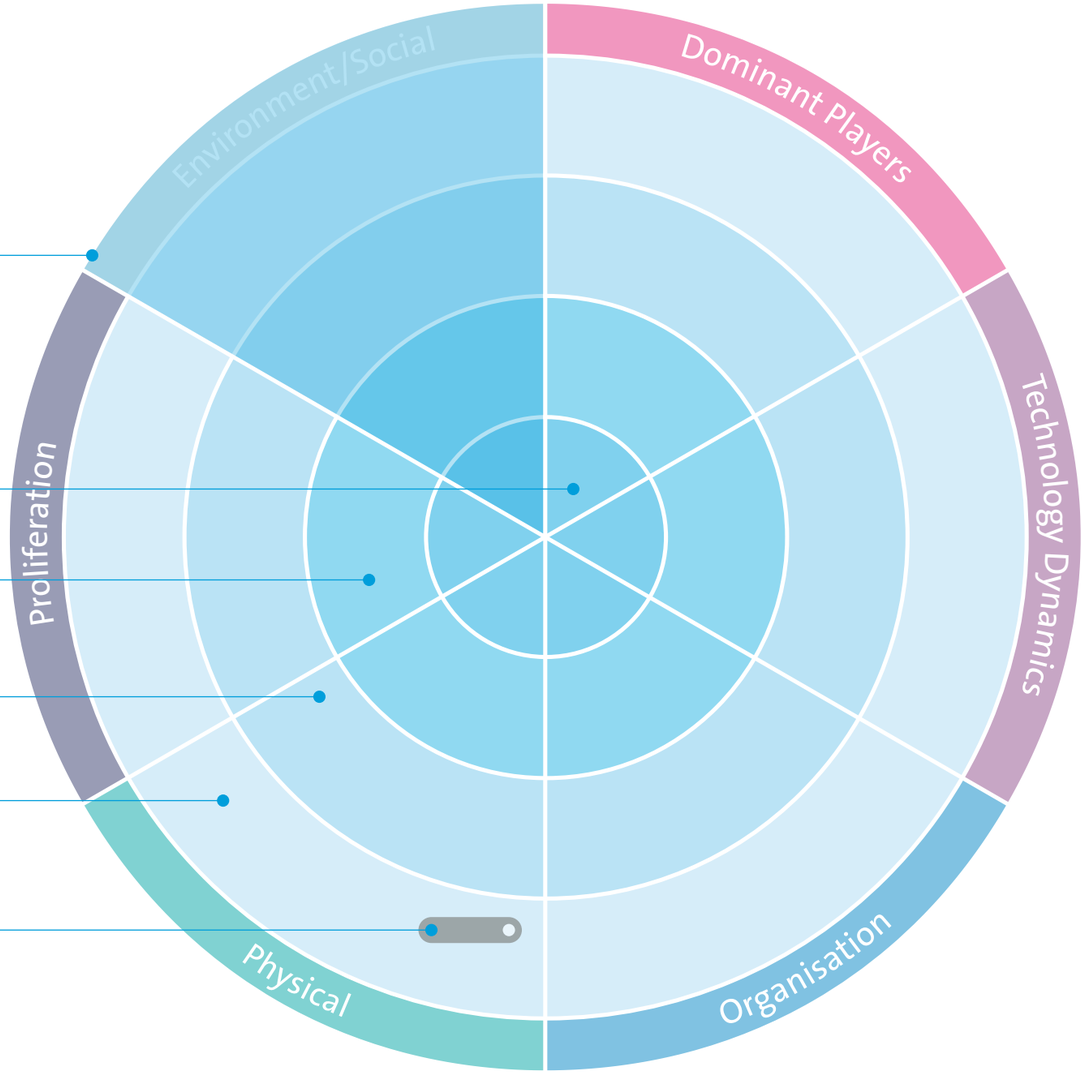
# Metodo

Il Threat Radar è diviso in sei **segmenti** che delimitano i diversi ambiti delle minacce. In ogni **segmento**, le relative minacce possono essere assegnate a uno dei quattro cerchi concentrici. I cerchi indicano l'attualità della rispettiva minaccia e quindi anche l'approssimazione della valutazione della minaccia. Più la minaccia è vicina al centro del cerchio, più è concreta e tanto più importanti sono le contromisure necessarie.

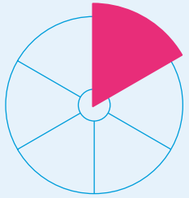
**Definiamo i cerchi come:**

- **Emergenze** per minacce già reali e controllate con un impiego relativamente importante di risorse.
- **Temi principali** per minacce che sono già comparse occasionalmente e vengono controllate con un impiego normale di risorse. Spesso sussistono processi regolati per contrastare in modo efficiente queste minacce.
- **Allerta precoce** per minacce non ancora comparse o che attualmente mostrano solo un'azione ridotta. Sono stati avviati dei progetti per contrastare tempestivamente una futura crescente importanza di tali minacce.
- **Osservazione** per minacce che compariranno solo tra qualche anno. Non vi sono misure concrete per gestire queste minacce.

Inoltre, le **minacce** contrassegnate dai punti citati mostrano una **tendenza.** Questa può essere in aumento, in diminuzione o stabile nella propria criticità. La lunghezza del raggio della tendenza indica la velocità di trasformazione attesa della criticità della minaccia.

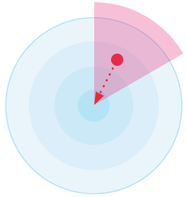


# Dettagli, tendenze e confronto rispetto all’anno precedente



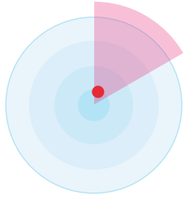
## Dominant Players

**In questo segmento vengono raccolte le minacce derivanti da interdipendenze di produttori, servizi o protocolli dominanti.**



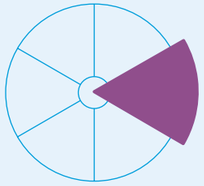
**Concentration Data & Cloud Services**
La forte centralizzazione dei dati nel cloud comporta un rischio di accumulazione. L’interruzione di un servizio centralizzato può avere effetti a livello mondiale.

▲ In aumento (maggiori dettagli a pagina 28)



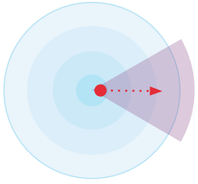
**Infrastructure Integrity**
All’interno di componenti fondamentali di infrastrutture critiche possono essere state integrate per negligenza o volutamente delle falle che mettono in pericolo la sicurezza del sistema.

► Nessuna variazione



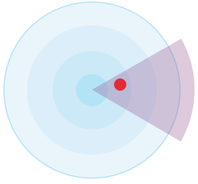
# Technology Dynamics

**Questo termine indica minacce che derivano dalla rapidissima innovazione tecnologica e che, da un lato, forniscono nuove opportunità agli hacker, mentre dall'altro creano nuove minacce dovute allo sviluppo stesso.**



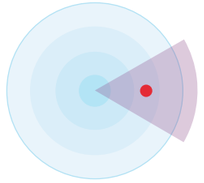
**5G Security**
Il 5G è una tecnologia di comunicazione mobile ancora giovane. La sua introduzione porterà con sé, oltre a numerose opportunità, anche minacce ancora sconosciute.

▼ In calo



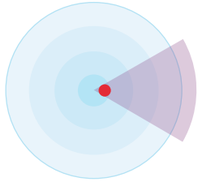
**Automatisation & Scaling**
La maggiore automazione dei processi operativi tecnici avrà un impatto più importante in caso di attacchi compiuti con successo o configurazioni errate.

► Nessuna variazione



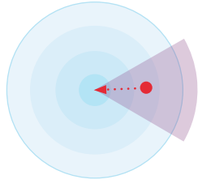
**Quantum Computing**
I computer quantistici possono rendere inutilizzabili le procedure crittografiche esistenti, poiché riescono a neutralizzarle in pochissimo tempo.

▼ In calo



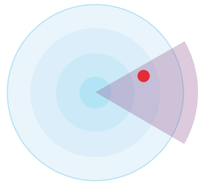
**Ransomware**
Dati critici vengono cifrati su vasta scala e decifrati (eventualmente) in cambio di un riscatto.

▲ In aumento (maggiori dettagli a pagina 32)



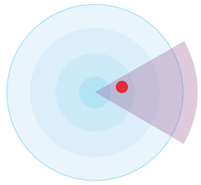
**Increased Complexity**
È in continua crescita la complessità dei sistemi, in particolare oltre i confini tecnologici e aziendali. In un contesto Multi Cloud e Hybrid Cloud, gli ambienti IT con diversi provider cloud diventano sempre più complessi. L'esposizione al rischio aumenta di conseguenza e la ricerca dell'errore diventa sempre più difficile.

▲ In aumento



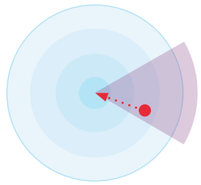
**AI-Based Attacks**
Gli attacchi tramite intelligenza artificiale (AI) sono più specifici e dunque più difficili da riconoscere. Utilizzando l'AI gli attacchi possono essere eseguiti in modo più efficiente su vettori classici come ad es. ransomware, phishing, spear-phishing e in certi casi anche in nuovi scenari come ad es. deep fakes, disinformazione ecc.

► Nessuna variazione



**Targeted Attacks (APTs)**
Attacchi mirati e complessi che perseguono un obiettivo concreto. Figure chiave vengono identificate e attaccate in modo mirato direttamente o indirettamente (lateral movement) per ottenere informazioni rilevanti o creare il massimo danno possibile. Un aspetto importante è la persistenza, ovvero il fatto che gli hacker agiscono quanto più a lungo possibile senza essere scoperti.

► Nessuna variazione



**Supply Chain Attacks**
Gli attacchi alla catena di fornitura mirano a sfruttare i rapporti d'affari e di fiducia tra un'azienda e parti esterne. Questi rapporti possono comprendere partnership, relazioni con i fornitori o l'utilizzo di software di terzi.

▲ In aumento (maggiori dettagli a pagina 36)



# Organisation

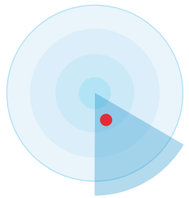
**Con il termine «organizzazione» vengono indicate le minacce che si basano sulle modifiche nelle organizzazioni o che sfruttano i punti deboli al loro interno.**

**Workplace Heterogeneity**
Oltre alle numerose opportunità che i nuovi modelli di lavoro portano con sé, l'impiego incontrollato di tali modelli come ad es. «Bring Your Own Device» (BYOD) oppure il maggiore impiego di postazioni di lavoro remote comporta una maggiore esposizione al rischio.

► Nessuna variazione

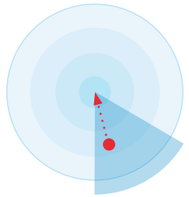
**Decentralised Development & Operations**
I classici settori di sviluppo sono «in via d'estinzione», lo sviluppo di applicazioni si avvicina alle Business Unit e al contempo si riducono i cicli delle release. Il controllo e la gestione della sicurezza diventano di conseguenza più difficili.

► Nessuna variazione



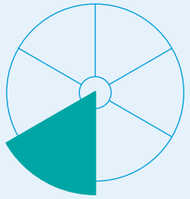
**Insider Threat**
Partner o collaboratori manipolano, usano in modo illecito o vendono per negligenza o intenzionalmente informazioni.

► Nessuna variazione



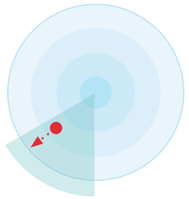
**Infrastructure Misconfiguration**
Sfruttamento di componenti mal configurati delle infrastrutture e/o falle identificate ed eliminate tardivamente.

▲ In aumento



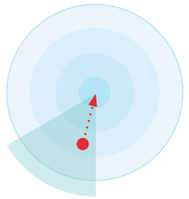
# Physical

**Questo termine indica gli attacchi alle infrastrutture nel cyberspazio che provocheranno sempre più danni nel mondo fisico. Ma sono comprese anche le minacce derivanti da un ambiente fisico e di regola orientate verso obiettivi fisici.**



**Device Theft**
Il furto o lo smarrimento di terminali quali smartphone, laptop ma anche di componenti IT importanti possono comportare la perdita di dati o compromettere la disponibilità dei servizi IT.

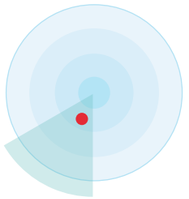
▼ In calo



**Energy Instability**
Attacchi a infrastrutture critiche come aziende che gestiscono le reti elettriche. L'affidabilità è fondamentale e il concetto di business continuity compare sempre di più anche nel dibattito sulla cyber-resilienza. La penuria di elettricità, i blackout (interruzione di corrente su vasta scala) o persino i blueout (interruzione della fornitura d'acqua su vasta scala) o simili sono punti importanti. I media riferiscono che la vulnerabilità delle infrastrutture critiche ai cyberattacchi è aumentata notevolmente.

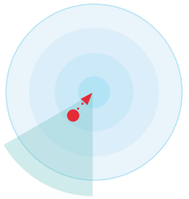
▲ In aumento





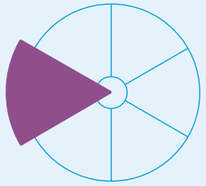
**IoT Devices**
Dispositivi con una protezione debole possono essere compromessi e sabotati. Potranno così essere limitati nella propria funzione, ad esempio in fatto di disponibilità o integrità dei dati.

► Nessuna variazione



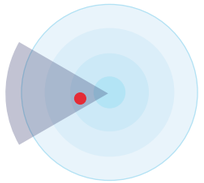
**Tecnologia operativa OT**
Per tecnologia operativa (OT) si intende l'uso di hardware e software per monitorare e controllare infrastrutture, dispositivi e processi fisici. I sistemi OT sono presenti in un'ampia gamma di settori ad alta intensità di capitale e svolgono tutta una serie di compiti che vanno dal monitoraggio delle infrastrutture critiche (CI) al controllo dei robot in un reparto di produzione. Esistono ancora molti sistemi di controllo protetti male o non protetti per gli impianti delle infrastrutture critiche.

▲ In aumento



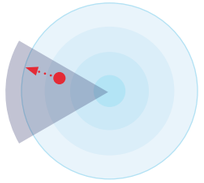
# Proliferation

**Nel segmento «Proliferation» sono comprese le minacce che sfruttano la sempre più semplice ed economica disponibilità di know-how e media IT. L'ampia diffusione comporta un maggior numero di aree di attacco e incrementa la disponibilità di strumenti di attacco.**



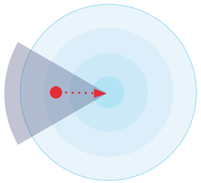
**Digitalisation**
Una crescente messa in rete del mondo reale e virtuale della vita privata e professionale comporta un maggior numero di vie di attacco. Anche il «New Work» e il passaggio all'home office aumentano i rischi informatici e la vulnerabilità dell'infrastruttura IT a causa di terminali non sicuri.

► Nessuna variazione



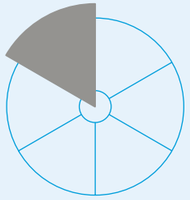
**Subscriber Compromise**
Il software dannoso accede ai dati privati degli utenti della rete mobile o viene utilizzato per attacchi all'infrastruttura IT o di telecomunicazione.

▼ In calo



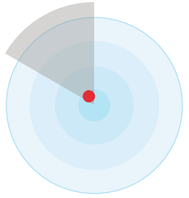
**DDoS Attacks**
Gli attacchi DDoS (Denial of Service) sono tentativi ostili di impedire il normale traffico dati di un server, di un servizio o di una rete target, inondando il bersaglio o l'infrastruttura circostante di traffico internet. Per essere efficaci, gli attacchi DDoS sfruttano diversi sistemi informatici compromessi come fonti del traffico dati dannoso. Le macchine utilizzate possono essere computer o altre risorse in rete come i dispositivi IoT. La grande diffusione di device quali ad es. i dispositivi IoT con una scarsa protezione porta a un aumento delle potenziali vittime delle botnet.

▲ In aumento



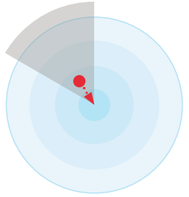
# Environment/Social

**In questo segmento rientrano le minacce che originano da cambiamenti socio-politici o che diventano più semplici e quindi più vantaggiose per gli hacker a causa di tali cambiamenti.**



**Security Job Market**
La richiesta di professionisti di Security è enorme e viene soddisfatta con molta difficoltà. Questo si traduce in una diminuzione del know-how disponibile per la lotta contro attacchi sempre più complessi e intelligenti.

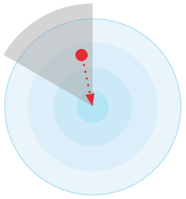
► Nessuna variazione (maggiori dettagli a pagina 24)



**Digital Identity**
Le identità digitali personali autenticate possono essere oggetto di furto o abuso, ad esempio per stipulare contratti a nome di terzi.

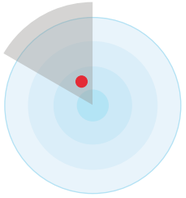
▲ In aumento





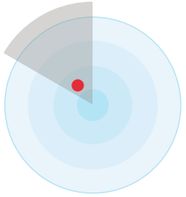
**Desinformation & Destabilisation**
La diffusione intenzionale di informazioni false può causare una destabilizzazione economica e sociale e viene utilizzata in modo mirato soprattutto negli scenari di crisi, sempre più spesso anche tramite il cyberspazio.

▲ In aumento



**Political Influence**
Le tendenze politiche possono influire sulle decisioni tecnologiche o economiche, per esempio attraverso la scelta di determinati fornitori di tecnologie. Ne possono scaturire nuovi rischi.

► Nessuna variazione



**Big data analytics**
Maggiori quantità di dati e migliori modelli di analisi possono essere sfruttati illecitamente per condizionare il comportamento delle persone. Le decisioni vengono sempre più delegate a sistemi autonomi. I dati dei «Big Data Lake» vengono impiegati in modo mirato per la disinformazione, fake news e analisi sociologiche e psicosociali, oltre che per la creazione di modelli di comportamento. Quest'ultima comporta una violazione della sfera privata.

► Nessuna variazione

# Sfide e trend

## Carenza di specialisti nel Security Job Market


### Di cosa si tratta?

Infrastrutture IT ibride sempre più decentrate, ambienti IoT e lavoro da remoto: i requisiti posti ai sistemi di sicurezza IT crescono, le minacce aumentano, ma gli specialisti scarseggiano. Le aziende dovrebbero combinare diverse misure per proteggere i dati e le reti e sviluppare know-how. L'automazione nonché la formazione e il perfezionamento rivestono altresì grande importanza.

Le attuali sfide poste alla sicurezza IT sono aggravate dalla carenza di specialisti qualificati. Il Global Risk Report 2022 del World Economic Forum (WEF) segnala la carenza di esperti di cybersicurezza anche a livello mondiale. Si stima che sul mercato del lavoro manchino circa tre milioni di professionisti.

L'International Information System Security Certification Consortium (ISC)² ha condotto un sondaggio sui possibili effetti della mancanza di personale esperto di cyber security. Il 32 % degli intervistati cita sistemi mal configurati come una possibile conseguenza. Una percentuale quasi uguale teme che non rimanga tempo sufficiente per un'adeguata gestione dei rischi o che venga tralasciato qualche aspetto importante. Il 27 % riferisce di non essere in grado di individuare tutte le minacce della rete. Un altro 27 % considera come un pericolo reale l'installazione e la configurazione di software eseguite in modo sbrigativo a causa della carenza di personale.

Lo studio «Situazione degli specialisti ICT: previsione del fabbisogno 2028» condotto da ICT-Formazione professionale Svizzera stima che entro il 2028 in Svizzera saranno richiesti circa altri 118 000 specialisti ICT. Per coprire questo fabbisogno ulteriore dovrebbero essere formate circa 36 000 persone in più rispetto a quanto avviene oggi. Si tratta di una sfida a livello macroeconomico e della politica di formazione che impone misure straordinarie. Le imprese di tutti i settori e l'amministrazione pubblica sono chiamate a creare nuovi posti di apprendistato e di studio in informatica e mediamatica.

Alla luce di tali cifre non c'è da stupirsi che le aziende abbiano difficoltà a trovare candidati adeguati e a trattenerli. Per coprire un posto vacante nel settore IT è necessario pubblicare vari annunci ed effettuare molti colloqui di candidatura, nel complesso servono in media sei mesi. Inoltre, soprattutto per le piccole e medie imprese risulta difficile non solo trovare gli specialisti, ma anche rimanere abbastanza attraenti nel lungo periodo e quindi fidelizzarli.

## Come evolverà questa sfida?

L'assunzione di specialisti IT è una sfida se non vi sono professionisti adeguati e qualificati a sufficienza. Molte aziende tentano pertanto di trattenere il personale già impiegato. Ma questa misura da sola non basta per eliminare il problema: la soluzione consisterà nel mantenere i collaboratori qualificati e automatizzare le attività quotidiane.

La difficoltà nel trovare i professionisti giusti con competenze in fatto di IT Security per la propria azienda aumenterà, poiché sono sempre di più le imprese (anche piccole) ad aver bisogno di esperti. Il cambiamento demografico aggraverà ulteriormente la situazione sul mercato del lavoro. Le aziende hanno sempre meno accesso a nuovi specialisti giovani. La «war for talent» è destinata a inasprirsi e le esigenze in materia di sicurezza cresceranno in generale. Gli scenari di crisi come la guerra in Ucraina aumenteranno e rafforzeranno la consapevolezza sulle questioni legate alla sicurezza nelle aziende e organizzazioni.

La penuria di esperti nel settore della cyber security si esplicherà su due fronti: da un lato con la mancanza di esperti digitali per lo sviluppo di soluzioni di IT Security, a fronte di attacchi informatici sempre più sofisticati e mirati. Dall'altro, nelle aziende mancheranno addetti alla sicurezza IT qualificati in grado di contrastare la crescente minaccia della cybercriminalità con misure adeguate.

La carenza di specialisti IT colpisce soprattutto le piccole e medie imprese (PMI), poiché i collaboratori qualificati preferiscono in genere le grandi società con modelli salariali interessanti e/o benefit sociali.

Per colmare la mancanza di personale, sempre più università offrono corsi di studio specifici in cyber security. Tuttavia, resta da appurare se ciò consenta di risolvere rapidamente i problemi strutturali. Per maturare il know-how necessario serve molto tempo e, oltre alla formazione teorica, occorre anche una certa esperienza pratica. Un approccio più promettente potrebbe essere quello pratico che vede le aziende con i rispettivi reparti specializzati e specialisti impegnarsi nella ricerca e nell'apprendistato. Inoltre, le imprese dovrebbero anche puntare sui collaboratori interessati, concentrandosi maggiormente sul loro perfezionamento nel settore della cyber security. Ma tutto ciò non sarà sufficiente, perlomeno a breve e medio termine, per colmare la carenza di personale e la conseguente lacuna di sicurezza. Nei reparti Security con carenza di organico non mancano solo le conoscenze specialistiche: spesso gli esperti sono oberati da un carico di lavoro enorme, il che naturalmente non è un presupposto sano per la propria cyber security.



## Come affrontare adeguatamente questa sfida?

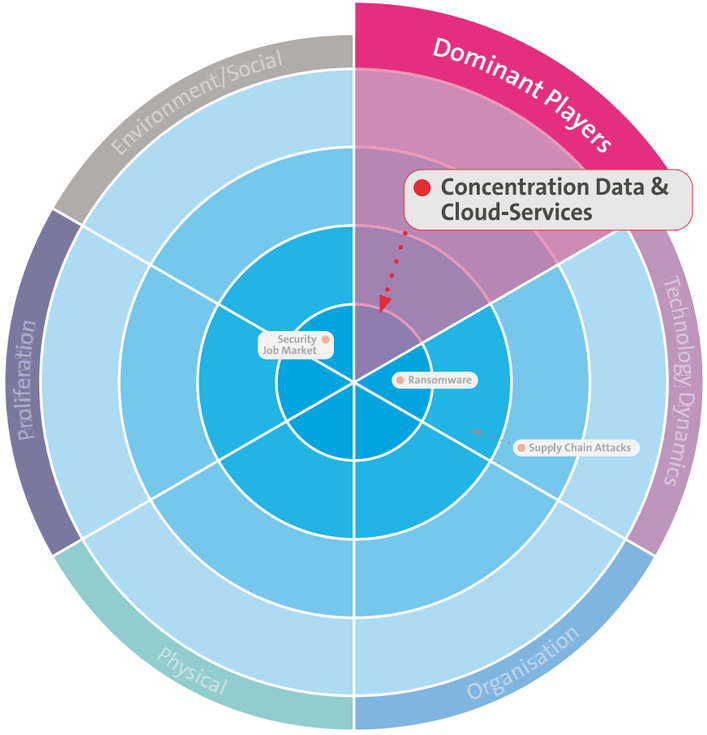
- Mantenere elevata l'attrattiva del datore di lavoro e fidelizzare i collaboratori all'azienda
- I talenti hanno bisogno di un sostegno pratico
- Investire nella formazione specialistica interna e istituire programmi di formazione interessanti
- Offrire possibilità di sviluppo nell'azienda e un'elevata occupabilità
- Utilizzare maggiormente i social media nel reclutamento e partecipare agli eventi del settore
- Utilizzare l'employer brand marketing e la rete dei collaboratori
- Istituire programmi junior o promuovere possibilità per profili junior (preparare i collaboratori futuri)
- Anche i programmi Bug Bounty interni permettono di trovare talenti
- Automazione dei processi standard e supporto software anche per i compiti più complessi
- Integrazione di un MSSP (Managed Security Service Provider) esterno

*«Non sempre sono necessari esperti con una formazione completa. Abbiamo avuto ottime esperienze con professionisti di settori affini (sviluppatori, amministratori di reti e simili) e giovani che vogliono perfezionarsi in questo campo una volta conclusa la formazione.»*

**Dimosthenis Georgokitsos**
Program Manager Cyber Security,
Recruiting & Education, Swisscom (Svizzera) SA

# Sfide e trend

## Hybrid Cloud e Multi Cloud in Concentration Data & Cloud-Services




### Di cosa si tratta?

In una soluzione Multi Cloud, un'azienda utilizza vari servizi cloud, spesso di fornitori diversi. Il Multi Cloud offre flessibilità e possibilità di scelta, ma comporta anche una certa complessità. La «giusta» soluzione cloud per la maggior parte delle aziende non è tuttavia né public né private, bensì una combinazione dei due.

Il Multi Cloud fa parte del percorso verso il cloud. Dopo una migrazione e/o l'onboarding di servizi cloud ci si rende conto che serve un altro cloud, per questioni di necessità. I motivi possono essere diversi, ad es. rischi, lock-in, servizi, progetti, team DevOps decentrati che utilizzano piattaforme cloud diverse. Di solito si tratta di un ambiente Multi Cloud Azure, GCP o AWS. I servizi sottostanti devono essere gestiti più volte, a scapito dell'efficienza. Una soluzione globale per più cloud può risolvere questo problema, ma la complessità generale rappresenta una nuova sfida.

Una strategia Multi Cloud comprende due o più piattaforme o provider di cloud computing. Alcuni esperti parlano di Multi Cloud solo quando un'azienda utilizza servizi con le stesse funzionalità di fornitori diversi, a differenza di una strategia in cui un'organizzazione opera una selezione per ciascun fornitore.

La maggior parte degli studi/esperti sottolinea le seguenti sfide:

- Gestione centralizzata degli accessi e delle identità lungo l'intero ciclo di vita
- Compliance
- Mancanza di visibilità e controllo (E2E)
- Sicurezza dei dati
- Maggiore complessità
- Lacune nelle conoscenze e competenze
- Possibilità di monitoraggio e protocolli non uniformi
- Sicurezza nella catena di fornitura
- Trasferimento della responsabilità per la sicurezza

## Come evolverà questa sfida?

La gestione centralizzata degli accessi e delle identità (Identity and Access Lifecycle Management) diventerà ancora più importante, poiché la necessità di sicurezza dei dati e compliance continuerà a crescere senza sosta. La questione della «visibilità end-to-end» deve essere chiarita al fine di preparare l'Incident Detection & Response.

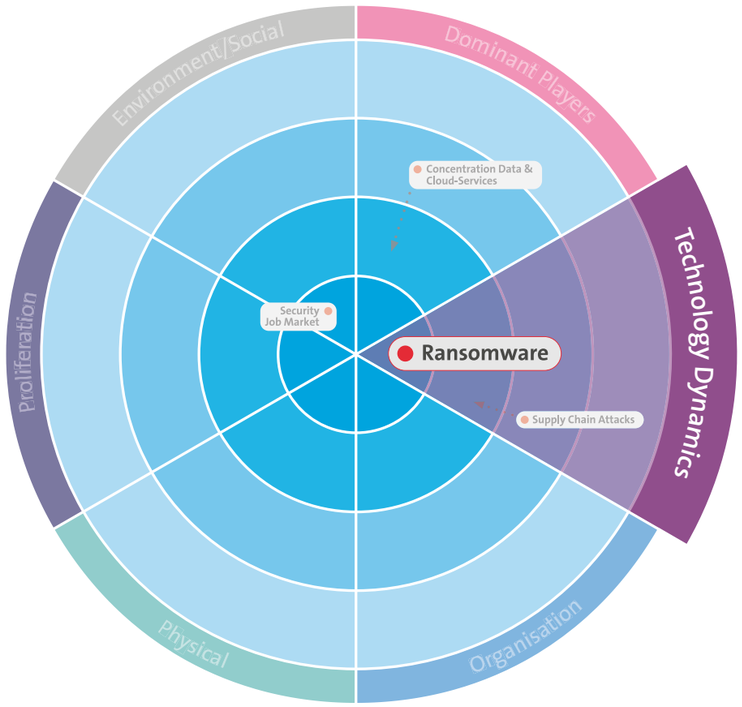
## Come affrontare adeguatamente questa sfida?

- Iniziare a riflettere per tempo sul Multi Cloud
- Un'architettura globale che permetta il passaggio dal cloud al Multi Cloud
- Impiegare un sistema per la verifica della situazione di sicurezza (Security Posture) e della compliance in tutti i cloud
- Monitorare globalmente le infrastrutture dei cloud e tracciare una panoramica centrale di tutti gli eventi rilevanti ai fini della sicurezza

*«Un ambiente Multi Cloud offre indubbi vantaggi. Tuttavia, occorre gestire correttamente la conseguente complessità in modo da tenere sotto controllo i rischi derivanti dall'aumento della superficie di attacco.»*

**Duilio Hochstrasser**
Security Specialist, Swisscom (Svizzera) SA

# Sfide e trend
## Ransomware




### Di cosa si tratta?

Il ransomware è un malware sviluppato per impedire a un utente o a un'organizzazione di accedere ai propri dati. I cyber criminali cifrano i file con il ransomware e chiedono un riscatto, mettendo le imprese in una posizione tale per cui pagare il riscatto appare il modo più facile ed economico per riottenere l'accesso ai propri dati. Talvolta, oltre alla cifratura si aggiunge anche il furto dei dati per mettere ulteriormente la vittima sotto pressione e indurla a pagare.

Il ransomware si è trasformato in breve tempo nella forma di malware più nota e visibile. Ogni anno causa in tutto il mondo costi superiori a 1 miliardo di dollari (Gartner). Poiché il ransomware è diventato un business redditizio per i criminali informatici e i metodi di attacco sono sempre più raffinati, anche i costi causati dagli attacchi continueranno ad aumentare. Fino a poco tempo fa, a finire nel mirino degli attacchi di ransomware erano soprattutto le grandi società, ma negli ultimi anni vengono colpite sempre di più anche le medie imprese.

Ai costi diretti del riscatto eventualmente pagato, che ammontano in media a 710 000 franchi nel caso di un attacco a una piccola impresa, si sommano i costi indiretti della mancata operatività durante le ore o i giorni in cui i sistemi sono bloccati. A questi si aggiungono i costi di riparazione o ripristino dei sistemi e i danni di immagine. Una cattiva reputazione può mettere a repentaglio l'esistenza stessa dell'azienda in poco tempo. Risollevare la reputazione costa un'enorme quantità di energia, tempo e denaro.

## Come evolverà questa sfida?

Questa tendenza prosegue inalterata. Fintanto che sistemi privi di patch o con accessi VPN/RAS senza autenticazione multifattore sono accessibili via internet e i collaboratori installano malware come Quakbot, vi è il rischio di un attacco ransomware. In considerazione delle campagne di malspam e phishing facilmente eseguibili e spesso riuscite, i criminali informatici non hanno affatto bisogno di sviluppare ulteriormente gli attacchi ransomware andati a segno. Non è da escludere che in futuro gli attacchi vengano maggiormente automatizzati oppure organizzati «As-a-Service». Le tecnologie deepfake e l'impiego dell'intelligenza artificiale renderanno questi attacchi ancora più difficili da individuare. Inoltre, sempre più hacker hanno iniziato non solo a cifrare i dati ma anche a minacciare le vittime di pubblicarli («double extortion»).

A partire dalla metà del 2023, le imprese in Europa dovranno segnalare gli attacchi ransomware. Pertanto si può ritenere che il numero degli attacchi resi noti pubblicamente aumenterà in modo significativo e quindi la popolazione ne avrà maggiore consapevolezza. Da ciò non si può tuttavia desumere se il numero degli attacchi varierà di conseguenza. Una cosa è certa: i ransomware non sono eventi di «forza maggiore» e in futuro anche i servizi cloud saranno presi di mira dai criminali informatici.

Al pari di altre società di settori affini, stiamo lavorando intensamente per migliorare la prevenzione e la protezione dai ransomware.



## Come affrontare adeguatamente questa sfida?

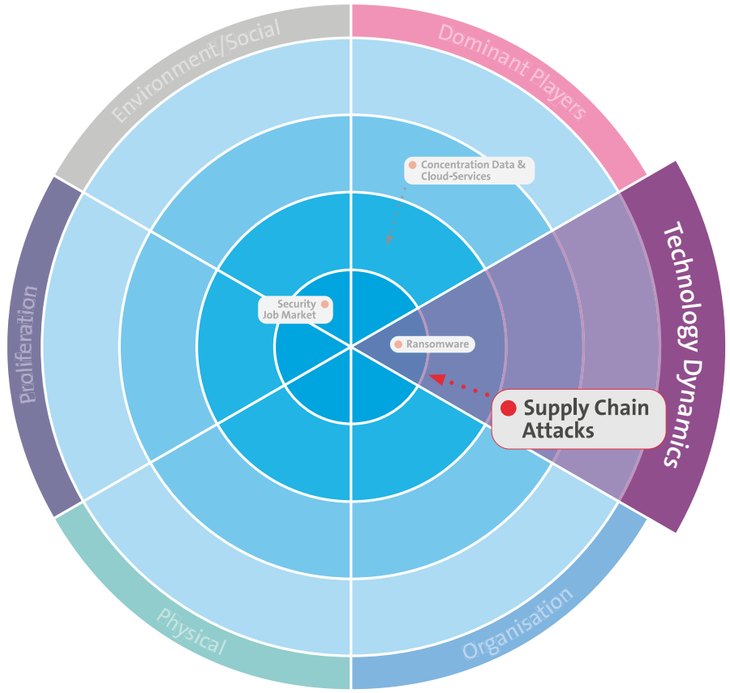
- Assicurarsi che i sistemi IT e le applicazioni software vengano gestiti correttamente nell'intera organizzazione
- Installare prontamente le patch per tutti i servizi internet (in particolare se le falle vengono già sfruttate)
- Effettuare regolarmente il backup (offline) di sistemi e dati (ed effettuare il recovery test per tali backup)
- Sviluppare un piano di comunicazione per le situazioni di crisi che tenga conto di operatori terzi, fornitori, partner, collaboratori e altri gruppi di interesse importanti
- Valutare la capacità dell'azienda (e del reparto IT) di reagire a un attacco e di far fronte a possibili interruzioni di sistema con l'ausilio di piani di incident response
- Assicurarsi che i collaboratori siano adeguatamente informati in merito alla cyber security e al pericolo di un attacco ransomware
- Proteggere i servizi RAS/VPN con l'autenticazione multifattore/Conditional Access
- Investire in un sistema EDR capillare e nel monitoraggio (ad es. dell'infrastruttura Active Directory) in modo da avere eventualmente l'opportunità di individuare tempestivamente l'attacco e bloccarlo
- Ridurre l'area di attacco

*«Gli autori degli attacchi ransomware sono opportunisti. Colpiscono dove si presenta un'opportunità, ovvero dove trovano un accesso.»*

**Thomas Röthlisberger**
Senior Security Analyst & Tech Lead Red Team, Swisscom CSIRT

# Sfide e trend

## Supplier Ecosystem and Dependencies/Supply Chain Security




### Di cosa si tratta?

Tutte le organizzazioni devono fidarsi in una certa misura delle altre imprese quando installano il software della rispettiva azienda nelle proprie reti ai fini della collaborazione. Un attacco alla catena di fornitura (Supply Chain) sfrutta questi rapporti di fiducia, ma anche la perdita di controllo dovuta alle interdipendenze tra le varie organizzazioni.

L'attacco è indirizzato all'anello debole nella catena di fiducia. Se un'organizzazione dispone di una cyber security forte ma collabora con un fornitore con un basso livello di sicurezza, gli hacker prenderanno di mira quest'ultimo. Dopo essersi intrufolati nella rete del fornitore, gli hacker possono passare alla rete sicura sfruttando questo rapporto di fiducia. I disservizi dei fornitori mettono a rischio la fornitura di servizi dell'organizzazione, ad esempio a causa della mancanza delle prestazioni preliminari (inosservanza dei SLA da parte dell'organizzazione) oppure a causa di rischi diretti per l'organizzazione (ad es. compromissione di dispositivi di terzi a livello di software o reti interne).

Gli obiettivi principali degli attacchi alla catena di fornitura sono infatti i Managed Service Provider (MSP). I MSP hanno completo accesso alle reti dei relativi clienti e rappresentano quindi una risorsa inestimabile per i criminali informatici. Sfruttando il MSP, gli hacker possono facilmente estendere le loro attività alle reti dei clienti. Facendo leva sui punti deboli nella catena di fornitura, hanno una maggiore influenza e possono ottenere accesso a reti altrimenti molto più difficili da penetrare. In questo modo gli autori dell'attacco a Kaseya sono riusciti a infettare con ransomware moltissime organizzazioni.

Altri attacchi Supply Chain vengono eseguiti con un software che diffonde il malware ai clienti di un'azienda. Ad esempio gli autori dell'attacco a Solarwinds si sono intrufolati nel build server dell'impresa e hanno aggiunto una «back door» nell'aggiornamento di Orion, il programma di monitoraggio della rete di Solarwinds. Dopo aver inoltrato il codice di questo aggiornamento ai clienti, gli hacker sono riusciti ad accedere anche alle rispettive reti. Log4J ha inoltre mostrato che molte aziende non dispongono di conoscenze sufficienti sull'utilizzo di library e framework. Ciò va oltre i fornitori diretti e comprende anche i subfornitori o i sub-subfornitori.

## Come evolverà questa sfida?

Prevediamo un inasprimento di questo problema a seguito della crescente interconnessione con i fornitori (supporto da remoto, librerie, SaaS) e attacchi mirati per perturbare le catene di fornitura. Inoltre, oggi gli hacker sfruttano le falle scoperte in tempi molto più brevi.

## Come affrontare adeguatamente questa sfida?

- Concentrazione sui fornitori più importanti/critici
- Integrazione di tecniche DevSecOps nel ciclo di sviluppo dei software
- Riduzione al minimo dei dati scambiati con i partner
- Inventario dei rapporti di fornitura e valutazione dei loro effetti
- Osservazione continua dei principali fornitori e allestimento di continuity plan
- Creazione di alternative e soluzioni di ripiego per fornitori importanti

*«Utilizzando "Software Bills of Materials" (SBOM) comprovati è possibile controllare e verificare la composizione dei deliverable fino ai livelli di funzione, anche su più livelli. Questa pratica va eseguita sistematicamente anche per gli hardware, sia custom che standard. Alcune tecnologie integrano tale opzione già oggi.»*

**Oliver Jäschke**
Security Governance Manager, Swisscom (Svizzera) SA



# Conclusione

Pensavamo che con l'uscita graduale della pandemia avremmo ritrovato un po' di tranquillità, ma la guerra in Ucraina ha mostrato nuovamente la vulnerabilità del nostro mondo. Molti aspetti appaiono oggi ancora più fragili e incontrollabili.

A questo si aggiunge la scarsità di risorse sempre più evidente in molti reparti Security e IT. Il mondo si trova a fare i conti con i cosiddetti «wicked problem», ossia con problemi che, a causa di requisiti incompleti, contraddittori o mutevoli, sono difficili da individuare, non sempre si possono prevedere, pianificare e mitigare, e quindi di norma diventano difficili o impossibili da risolvere.

Lo scenario appare estremamente complesso e un po' sconfortante, ma non dobbiamo lasciarci scoraggiare. La digitalizzazione nelle aziende e organizzazioni avanza inesorabilmente. Quasi tutte le organizzazioni e imprese che non vi hanno già provveduto negli scorsi anni hanno in programma di esternalizzare i servizi e componenti IT nel cloud nel 2022. Temi quali il metaverso, Web 3.0, NFT e Blockchain caratterizzano l'attuale sviluppo del cyberspazio e danno motivo di speranza. Ora è importante non mollare, soppesare le opzioni e applicare una gestione attiva dei rischi.

In un mondo sempre più volatile, incerto, complesso e ambiguo dobbiamo concentrarci maggiormente sulla nostra gestione interna dei rischi. Cosa vale la pena proteggere? Chi o cosa minaccia i valori e gli asset della nostra organizzazione? Quale ruolo svolgono i servizi e componenti critici di terzi quali fornitori, operatori SaaS, servizi cloud ecc.?

Dobbiamo trasformare i collaboratori in alleati, chiedere ai dirigenti di assolvere una funzione esemplare, monitorare sistematicamente il rispetto delle regole e disposizioni e creare alleanze intersettoriali. Per opporre una difesa adeguata ai rischi e pericoli in continua evoluzione, la Security dev'essere agile.

*«Le persone rivestono un ruolo centrale nel sistema di sicurezza.»*

# Appunti



## Sigla editoriale


| | |
|---|---|
| **Editore** | Swisscom (Svizzera) SA, Group Security |
| **Concetto/realizzazione** | Agentur Nordjungs, Zurigo |
| **Redazione** | Swisscom (Svizzera) SA<br>Marcus Beyer (Group Security)<br>Manuel Bühlmann (Group Communications)<br>Claudia Lehmann (B2B Communications) |
| **Traduzione** | Textraplus AG |
| **Copyright** | © Maggio 2022 by Swisscom (Svizzera) SA, Group Security,<br>Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch |
| **Stampa** | OK DIGITALDRUCK AG, Zurigo |
| **Tiratura** | 200 copie |

# Nel mondo interconnesso senza pensieri

Al centro di tutte le nostre riflessioni in tema di sicurezza mettiamo le esigenze di collaboratori, clienti e partner. Sviluppiamo soluzioni, prodotti e servizi sicuri basati sulle reti e sui sistemi IT più moderni.

**Cerchi un lavoro in Swisscom nel campo della security?**
Allora dai un'occhiata qui e inviaci la tua candidatura:

swisscom.com/securityjobs

# #talkingaboutsecurity

**swisscom.ch/security**