

Swiss Finance Institute Roundups

I principi fondamentali della sicurezza informatica

Editoriale



Secondo le proiezioni, le minacce informatiche costeranno oltre 10'000 miliardi di dollari nel 2025, diventando una delle sfide fondamentali di questo decennio. In questo *Roundup SFI*, esperti del mondo accademico e dell'industria esaminano le vulnerabilità più critiche e le risposte prioritarie. Il settore finanziario rimane particolarmente vulnerabile a causa di sistemi *legacy* vecchi di decenni e di effetti a cascata su reti di pagamento interconnesse. Piuttosto che relegare la sicurezza informatica ai dipartimenti IT, i consigli di amministrazione devono considerarla una preoccupazione strategica che richiede investimenti continui e un cambiamento culturale, in cui ogni dipendente comprenda il proprio ruolo di difesa. Mentre le bande di *ransomware* e gli attori sponsorizzati dagli Stati si confondono e i fornitori di servizi *cloud* centralizzati creano pericolosi punti di guasto, il percorso da seguire richiede non solo di migliorare la tecnologia, ma anche di ripensare a come bilanciare l'efficienza con la resilienza nel nostro mondo iperconnesso.

Vi auguriamo una lettura istruttiva e stimolante.

A handwritten signature in blue ink, appearing to read 'F. Degeorge', with a horizontal line underneath.

Prof. François Degeorge
Managing Director

Collaboratori



Alain Beuchat

Alain Beuchat è stato *Chief Information Security Officer* di Lombard Odier, responsabile della resilienza informatica, della strategia di sicurezza informatica e della conformità normativa dell'organizzazione, fino al suo pensionamento nel giugno 2025. È anche membro dello *Swiss Academy of Engineering Sciences' (SATW) Cybersecurity Advisory Board*. Ha conseguito un *Master of Science in Electrical Engineering* presso l'EPFL, il Politecnico Federale di Losanna.



Olivier Scaillet

Olivier Scaillet è Senior Chair SFI e Professore di Finanza e Statistica presso l'Università di Ginevra. La sua ricerca si concentra sulla teoria econometrica e sulle sue applicazioni in campo finanziario e assicurativo. Oltre al suo lavoro accademico, condivide le sue competenze in materia di gestione del rischio e modellazione con diverse banche in Svizzera. Ha conseguito un Dottorato di ricerca in Matematica applicata presso l'*Université Paris Dauphine*.



Marc Henauer

Marc Henauer è *Senior Political and International Affairs Officer* presso l'Ufficio federale della cibersicurezza (UFCS). In precedenza, ha diretto lo *Swiss MELANI Operation and Information Centre*, dove ha coordinato il monitoraggio delle minacce informatiche e ha migliorato la conoscenza della situazione informatica in Svizzera. Presso l'UFCS si occupa dello sviluppo di politiche nazionali e internazionali in materia di sicurezza informatica. Ha conseguito un *Master of Arts in Foreign Service and National Security Studies* presso la *Georgetown University*.



Beat Schär

Beat Schär è *Head of IT Security and Architecture* presso la Banca Nazionale Svizzera (BNS), dove supervisiona la progettazione e l'attuazione di strutture informatiche sicure, allinea la strategia di sicurezza informatica dell'istituto agli standard normativi nazionali e internazionali e contribuisce agli sforzi interdipartimentali per la salvaguardia dei sistemi critici. Ha conseguito un *Master of Applied Science in Information Technology and Electrical Engineering* presso l'ETH di Zurigo, il Politecnico Federale di Zurigo.



Anastasia Kartasheva

Anastasia Kartasheva è membro della facoltà SFI e Professore associato presso la Scuola di Finanza, nonché Direttore dello *Swiss Institute for International Economics and Applied Economic Research* dell'Università di San Gallo. Prima di assumere l'attuale incarico, ha lavorato come economista presso la Banca dei Regolamenti Internazionali (BRI). Ha conseguito un Dottorato di ricerca in Economia presso l'*Università di Tolosa*.



Fabian Schär

Fabian Schär è membro della facoltà SFI e Professore assistente di *Distributed Ledger Technology and Fintech* presso l'Università di Basilea. È ricercatore ospite del Fondo Monetario Internazionale (FMI), consulente tecnico del *Committee of Payments and Markets Infrastructure* e un esperto invitato da numerose banche centrali, dalla Banca dei Regolamenti Internazionali (BRI), dal Consiglio per la stabilità finanziaria e dal G20. Ha conseguito un Dottorato di ricerca in Economia presso l'Università di Basilea.

Ottobre 2025 (interviste del settembre 2025)

Questa versione è una traduzione della versione originale in inglese. La versione originale è disponibile su <https://www.sfi.ch/rndp-hcs25>

I fatti essenziali

Che cos'è la sicurezza informatica e com'è strutturata?

► **Beat Schär:** La sicurezza informatica si riferisce alla protezione dei sistemi informatici (*Information Technology – IT*), delle reti e dei dati da accessi non autorizzati, danni o interruzioni. Mentre le basi tecniche, come la protezione della confidenzialità, dell'integrità e della disponibilità, sono comuni a tutte le organizzazioni, le priorità e i rischi specifici dipendono dalla natura dell'azienda. Per esempio, un gestore patrimoniale dipende dalla sicurezza dei dati dei clienti; una banca centrale richiede la sicurezza, la disponibilità e l'indipendenza del sistema; un produttore si affida all'integrità delle linee di produzione automatizzate; e un negozio online ha bisogno di un'elaborazione sicura dei pagamenti e del tempo di funzionamento durante il traffico di punta. Nell'economia odierna, quasi tutti i settori si basano su sistemi informatici interconnessi, rendendo la sicurezza informatica una preoccupazione strategica fondamentale, seppure con le dovute differenze da un'azienda all'altra.

► **Alain Beuchat:** La confidenzialità, l'integrità e la disponibilità sono alla base della sicurezza informatica. Sono profondamente interconnesse: è normale vedere compromessi, tensioni e fallimenti complementari o a cascata tra di loro. La confidenzialità protegge l'identità di un utente e garantisce che possa accedere ai dati giusti. L'integrità protegge i dati e i sistemi da modifiche non autorizzate. La disponibilità garantisce che gli utenti possano accedere ai dati e all'infrastruttura quando ne hanno bisogno. Gli attacchi informatici possono colpire tutte e tre le componenti: gli attacchi di *phishing* cercano di ottenere le credenziali di accesso, consentendo agli hacker di accedere ai dati senza autorizzazione. Gli attacchi con richiesta di riscatto mirano a compromettere l'integrità e la confidenzialità dei dati. Gli attacchi *DDoS* (*Distributed Denial-of-Service* – Attacco distribuito di negazione del servizio) inondano i server, rendendo i siti web non disponibili per gli utenti legittimi. Per mettere in pratica queste tre componenti della sicurezza informatica, le organizzazioni adottano controlli di sicurezza stratificati, come crittografia, gestione degli accessi, protezione da *DDoS* e *malware*, monitoraggio dei sistemi e piani di risposta agli incidenti che affrontano in modo specifico i rischi di confidenzialità, integrità e disponibilità.

Come si inserisce la sicurezza informatica nel più ampio puzzle della sicurezza?

► **Fabian Schär:** Non appena due pezzi di hardware o software interagiscono, diventano vulnerabili agli attacchi e la sicurezza informatica deve intervenire. La sicurezza, nel suo senso più ampio, consiste nel proteggere dalle minacce. Queste minacce possono assumere molte forme: fisiche, digitali, emotive o istituzionali. Sebbene la sicurezza informatica si concentri sulla difesa dei sistemi informatici e dei dati dagli attacchi digitali, essa ha un effetto a catena su altre aree della sicurezza, tra cui la sicurezza nazionale, la sicurezza economica e la sicurezza personale.

► **Marc Henauer:** In sostanza, la sicurezza informatica riguarda la gestione di diversi tipi di rischio nell'economia e nella società. Vale la pena notare che la sicurezza informatica non è un livello aggiuntivo di processi che qualcuno può scegliere di adottare; piuttosto, cambia il modo in cui vengono eseguiti i processi esistenti. Per esempio, in passato le informazioni critiche venivano inviate per lo più tramite lettere sigillate o telegrafi. Ora vengono inviate attraverso sistemi di messaggistica istantanea. La sicurezza informatica non ha creato la messaggistica in sé, ma ha modificato il modo in cui viene usata oggi per garantire che rimanga sicura.

► **Olivier Scaillet:** Nel settore bancario, il Comitato di Basilea per la Vigilanza Bancaria (*Basel Committee on Banking Supervision – BCBS*) offre una guida utile classificando i rischi in tre categorie principali: rischi di credito, rischi di mercato e rischi operativi. Il rischio informatico rientra nei rischi operativi. Tuttavia, si distingue per l'intento malevolo, la maggiore probabilità che si verifichi, il potenziale di interruzione nascosta e prolungata e la capacità di diffondersi attraverso l'interconnessione digitale. Queste caratteristiche dimostrano che i tradizionali quadri di riferimento per il rischio operativo sono insufficienti. Il rischio informatico richiede strategie dedicate e lungimiranti in termini di supervisione gestionale, progettazione normativa e assicurazione del rischio.

► **Anastasia Kartasheva:** Dal punto di vista assicurativo, il rischio di sicurezza informatica è considerato anche un rischio operativo a causa del suo impatto sulla confidenzialità, l'integrità e la disponibilità dei dati, nonché sull'infrastruttura informatica. Questi rischi possono comportare accessi non autorizzati, con conseguenti violazioni dei dati, attacchi di malware ed errori interni al sistema che compromettono la sicurezza dei dati. A differenza di altri rischi, come il rischio sanitario o il rischio di una catastrofe naturale, lo sviluppo di metodi per trasferire i rischi di sicurezza informatica è stato limitato. Di conseguenza, le aziende dispongono di una protezione assicurativa minima contro i rischi di sicurezza informatica, la qual cosa le lascia in gran parte a cavarsela da sole quando devono affrontare le conseguenze di un attacco.

Come si differenziano gli attacchi informatici tra attori opportunistici e mirati?

► **Alain Beuchat:** La maggior parte degli attacchi informatici sono opportunistici, non mirati. Gli aggressori scrutano Internet alla ricerca di note vulnerabilità, le sfruttano e poi scoprono chi è la vittima. Una volta ottenuto l'accesso, gli aggressori – che spesso lavorano su più livelli – decidono l'importo del riscatto in base alle dimensioni e alla sensibilità della vittima. Deve essere doloroso, ma non così tanto da impedire alla vittima di

pagare. Gli attacchi mirati sono diversi e comportano una sorveglianza a lungo termine, un intento strategico e spesso motivazioni geopolitiche. Queste operazioni, spesso legate ad attori statali, possono richiedere mesi o addirittura anni di preparazione e in genere si concentrano su agenzie governative o infrastrutture critiche. Entrambi i tipi di minacce coesistono e la comprensione della loro logica è fondamentale per mappare i rischi e pianificare le risposte. Una difesa forte inizia con il sapere non solo come operano gli aggressori, ma anche perché.

Quali dati recenti illustrano meglio la portata delle minacce informatiche di oggi?

► **Olivier Scaillet:** Gli esperti prevedono che il costo globale della criminalità informatica supererà i 10'000 miliardi di dollari entro il 2025, con un enorme balzo rispetto ai 3'000 miliardi di dollari del 2015. Sebbene queste cifre sbalorditive siano difficili da confermare, sottolineano l'enorme portata del problema e il suo allarmante tasso di crescita. Con gli attacchi informatici e la vulnerabilità generale in aumento, alcune proiezioni indicano che il costo potrebbe raggiungere i 25'000 miliardi di dollari entro il 2027. Di conseguenza, la sicurezza informatica e il rischio informatico sono diventati una delle principali preoccupazioni di governi, aziende e privati.



Quali sono i recenti incidenti di sicurezza informatica che secondo lei illustrano meglio lo stato del settore?

► **Olivier Scaillet:** Uno degli attacchi più dannosi è probabilmente l'attacco *NotPetya* del 2017. Da un punto di vista del rischio operativo, ha costretto le aziende colpite a chiudere per settimane, interrompendo la loro capacità di produrre beni e servizi. Questo effetto a catena ha colpito i loro clienti, che hanno subito perdite significative, quattro volte superiori a quelle delle aziende direttamente colpite. Questi rischi operativi sono stati più gravi per i clienti con pochi fornitori alternativi o per quelli che si affidano a prodotti altamente specializzati. Da un punto di vista del rischio reputazionale, la violazione ha portato i clienti a interrompere gradualmente i rapporti commerciali con le aziende direttamente colpite. Anche un anno dopo l'attacco, i clienti erano più propensi a tagliare i ponti con queste aziende, mostrando un'erosione a lungo termine della fiducia e dell'affidabilità. I clienti hanno ristrutturato le loro catene di fornitura per collaborare con aziende con profili di sicurezza informatica più solidi, la qual cosa indica che l'attacco ha danneggiato la reputazione dei fornitori colpiti come partner commerciali affidabili. L'attacco *NotPetya* è uno degli attacchi più sofisticati mai avvenuti e sottolinea le conseguenze diffuse che tali attacchi possono avere nel tempo.

► **Anastasia Kartasheva:** La chiusura di *Colonial Pipeline* nel 2021 è un esempio da manuale. L'azienda, che fornisce quasi la metà del carburante consumato sulla costa orientale degli Stati Uniti, ha subito un attacco *ransomware*. Per precauzione, ha chiuso i suoi sistemi. Nonostante il pagamento di un riscatto di circa 4.4 milioni di dollari in *Bitcoin* il giorno successivo all'attacco, ci è voluta quasi una settimana per riprendere il servizio completo, con conseguenti carenze di carburante in diversi Stati, la corsa alle scorte e prezzi ai distributori aumentati fino a 10 centesimi al gallone. L'impatto di un attacco come questo, che sfrutta una sola password compromessa in un'infrastruttura critica, può essere notevole, con ripercussioni sulla vita di milioni di persone. È inoltre essenziale considerare il "piccolo" costo del riscatto, rispetto ai costi economici e sociali totali associati alla chiusura.

► **Marc Henauer:** L'attacco *Viasat*, avvenuto lo stesso giorno dell'invasione dell'Ucraina da parte della Russia nel 2022, mirava a interrompere le comunicazioni satellitari utilizzate da migliaia di ucraini, tra cui agenzie militari e governative. Questo attacco, mirato all'Ucraina, ha avuto effetti di ricaduta ben al di là di quanto si potesse prevedere. La portata dei danni collaterali è stata vasta, con circa 6'000 turbine eoliche malfunzionanti in Germania, utenti di banda larga fissa in tutta Europa che hanno subito interruzioni e hanno dovuto sostituire l'hardware, e utenti di telefonia satellitare in Marocco e nel Regno Unito che hanno avuto problemi di connettività.

► **Alain Beuchat:** L'incidente di *CrowdStrike* del 2024, causato da un aggiornamento di routine del software, ha provocato la cancellazione di oltre 5'000 voli, il rinvio di procedure non urgenti da parte degli ospedali e l'interruzione dell'attività bancaria online da parte delle banche di tutto il mondo. Sebbene non vi siano prove che l'incidente di *CrowdStrike* sia stato causato da un'attività dolosa, la sua portata di perturbazioni supera quella di qualsiasi altro attacco informatico mai avvenuto e mette in evidenza la vulnerabilità dei sistemi informatici centralizzati. Questi incidenti sottolineano l'interdipendenza dei nostri sistemi informatici: un guasto, sia esso intenzionale o accidentale, può avere un impatto non solo su un singolo computer, ma anche sul funzionamento di un dispositivo collegato a una rete informatica a molti fusi orari di distanza. Oltre agli incidenti sopra citati, continuiamo a osservare un elevato volume di attacchi informatici che colpiscono le organizzazioni e i loro fornitori terzi. Molte di queste violazioni derivano dall'assenza di pratiche fondamentali di sicurezza informatica, come la gestione incoerente delle correzioni di sicurezza o la mancanza di autenticazione a più fattori.



Concetti fondamentali

Come sono strutturate e attuate le funzioni di sicurezza informatica?

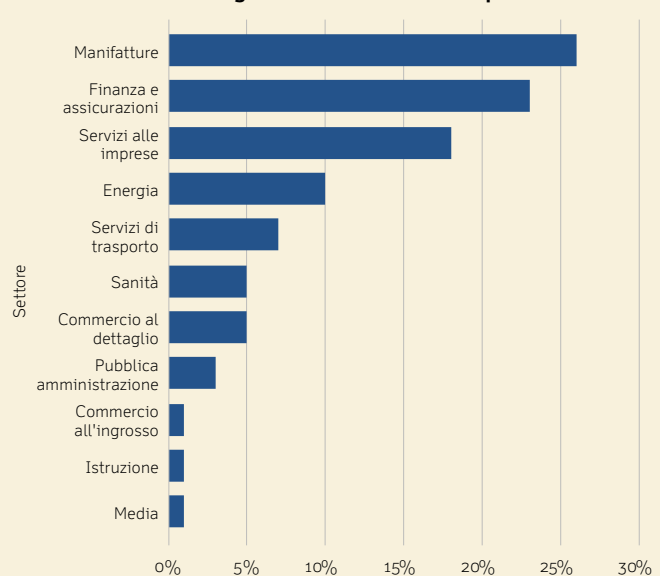
► **Beat Schär:** La gestione del rischio informatico è spesso organizzata in tre linee di difesa: proprietà del rischio, supervisione del rischio e audit indipendente. La prima, la proprietà del rischio, comporta l'identificazione, la valutazione e la mitigazione dei rischi di sicurezza informatica legati al contesto specifico dell'azienda. Gli specialisti interni di sicurezza informatica di solito sostengono queste attività. La seconda, la supervisione del rischio, prevede il monitoraggio dell'effettiva identificazione e gestione dei rischi. Questa responsabilità spetta di solito al dipartimento del rischio all'interno dell'azienda. Il terzo, l'audit indipendente, fornisce una valutazione esterna dei controlli di sicurezza informatica, delle politiche e delle pratiche di gestione del rischio. Questo approccio a tre livelli riduce al minimo le aree non monitorate, garantisce controlli ed equilibri tra le funzioni organizzative e allinea la gestione del rischio informatico a standard più ampi di *governance* e conformità.

Chi sono i principali aggressori e le vittime primarie degli attacchi informatici?

► **Marc Henauer:** Gli aggressori sono molto razionali e opportunisti e prendono di mira vittime che non possono permettersi una sicurezza di alto livello ma che hanno risorse finanziarie sufficienti per pagare il riscatto. Tra le loro vittime c'è praticamente chiunque sia connesso a una rete, dalle grandi aziende e agenzie governative alle piccole imprese, agli istituti scolastici, agli istituti di ricerca, alle organizzazioni non profit, alle ONG e ai singoli individui. Chiunque disponga di infrastrutture e dati di valore, oltre che di risorse finanziarie, può diventare un bersaglio. Un esempio significativo è la violazione della rete di un casinò avvenuta nel 2017, in cui gli hacker hanno sfruttato un termometro da acquario, collegato a Internet e scarsamente protetto, per estrarre 10 GB di dati dal database dei grandi scommettitori del casinò. Questo incidente è diventato un classico esempio di come anche il più banale dei dispositivi intelligenti possa diventare una porta d'accesso a informazioni sensibili se non adeguatamente protetto.

► **Anastasia Kartasheva:** Esiste una rete complessa di aggressori e vittime, che non operano tutti sullo stesso campo di battaglia. Per quanto riguarda gli aggressori, in genere vediamo Cina, Corea del Nord e Russia come attori principali a livello di Stati nazionali, con schemi intricati guidati da motivazioni strategiche, politiche o finanziarie. A livello individuale, gli hacker sono spesso adolescenti, soprattutto americani, che parlano correntemente l'inglese e sono abili nell'ingegneria sociale. Le loro azioni tendono a essere aggressive e a concentrarsi su specifici settori economici per settimane intere, con obiettivi che vanno dal prestigio all'attivismo al guadagno finanziario. Dobbiamo ricordare che anche i dipendenti possono rappresentare una minaccia importante per la sicurezza informatica e causare danni considerevoli, sia intenzionalmente sia per negligenza. Per quanto riguarda le vittime, le agenzie governative e gli operatori di infrastrutture critiche sono gli obiettivi principali degli hacker statali, mentre le istituzioni finanziarie e gli individui sono generalmente vittime di criminali informatici con motivazioni finanziarie. Nel frattempo, le aziende, i media e le istituzioni governative sono prese di mira da hacker ideologici o *hacktivisti*.

Distribuzione degli attacchi informatici per settore



Nota: Questa figura mostra la distribuzione degli attacchi informatici nei vari settori nel 2024.

Fonte: IBM X-Force

Quali sono i vettori di attacco informatico attualmente più diffusi e come sono evoluti?

► **Fabian Schär:** Con l'ascesa dell'intelligenza artificiale, l'ingegneria sociale è diventata sempre più sofisticata. Gli hacker utilizzano più dati e modelli più avanzati per creare attacchi mirati e sofisticati. Sono finiti i tempi degli errori evidenti, come quelli di battitura e di grammatica. Anche gli attacchi alla catena di approvvigionamento sono evoluti: gli hacker si sono infiltrati in molte organizzazioni prendendo di mira i loro fornitori di software. L'attacco *SolarWinds*, che si ritiene sia legato al governo russo, è un esempio emblematico. In questo caso, gli hacker hanno inserito un codice dannoso in un aggiornamento software affidabile, ottenendo l'accesso a migliaia di obiettivi di alto profilo, tra cui agenzie governative statunitensi e aziende Fortune 500. Il rischio di attacchi informatici cresce di giorno in giorno, man mano che i software e le aziende diventano sempre più connessi e che ci affidiamo sempre più a soluzioni cloud e a servizi di terzi.

Quali sono le motivazioni che spingono le diverse categorie di attori delle minacce, dagli attori nazionali agli hacktivist, a lanciare attacchi informatici?

► **Anastasia Kartasheva:** Le motivazioni sono molteplici. L'attuale instabilità del panorama globale ha reso evidente che la propaganda, la disinformazione durante le elezioni e gli attacchi alle infrastrutture vitali vengono utilizzati per ottenere vantaggi politici o militari. Anche il sabotaggio industriale è una delle principali preoccupazioni, in particolare per le aziende con un'ampia presenza internazionale che hanno un controllo meno diretto sui propri dipendenti, sono più vulnerabili alle operazioni e alle catene di fornitura globali e devono navigare in molteplici e complessi sistemi normativi. Affrontare queste diverse minacce è una sfida continua che presenta numerose difficoltà, tra cui la collaborazione con le terze parti giuste, l'acquisizione di competenze tecniche, la formazione del personale e la gestione delle minacce interne.

► **Fabian Schär:** È importante anche considerare l'orizzonte temporale. Gli attacchi con orizzonti a breve termine sono per lo più motivati da guadagni finanziari, mentre quelli con orizzonti a lungo termine hanno motivazioni strategiche o politiche. L'attacco informatico e l'esplosione di migliaia di cercapersone e *walkie-talkie* di Hezbollah lo scorso anno, che ha ucciso oltre 40 persone e ne ha ferite più di 3'500, evidenzia quanto sofisticati e ben pianificati possano essere questi attacchi. Al giorno d'oggi, quasi ogni dispositivo elettronico può essere vulnerabile a un incidente informatico.

Quali principi fondamentali guidano oggi un'efficace governance della sicurezza informatica?

► **Beat Schär:** La sicurezza informatica è una responsabilità quotidiana e costante. Adottando un approccio basato sul rischio, le aziende possono mettere in pratica un'efficace governance della sicurezza informatica. Per iniziare, devono condurre una valutazione approfondita del rischio per ottenere una comprensione completa delle vulnerabilità, degli asset e dell'esposizione alle minacce informatiche. Una volta effettuata la valutazione del rischio, il management deve dare priorità alle misure di sicurezza, intraprendere le azioni necessarie e accettare la responsabilità generale delle proprie decisioni. Una comunicazione interna aperta è fondamentale per promuovere la buona condotta di tutto il personale e per garantire che sia consapevole delle potenziali minacce e dei comportamenti attesi. Le valutazioni dei rischi dovrebbero poi essere aggiornate regolarmente, sulla base delle valutazioni delle minacce informatiche e della crescita dell'azienda.

► **Marc Henauer:** Secondo il diritto civile svizzero, il consiglio di amministrazione e il comitato esecutivo sono responsabili della gestione del rischio. Anche se c'è ancora margine di miglioramento, le aziende stanno diventando più consapevoli dei rischi informatici che devono affrontare. Tuttavia, è difficile dire quali aziende siano all'avanguardia e quali stiano rimanendo indietro. Da un lato, alcune piccole e medie imprese, soprattutto quelle fortemente automatizzate o digitalizzate, hanno una grande esperienza in questo settore. Dall'altro, alcune grandi aziende hanno subito perdite e interruzioni significative. Per esempio, nel 2017 la compagnia di navigazione danese Maersk ha avuto gravi problemi di capacità in tutte le sue operazioni globali a causa del cyberattacco NotPetya, mentre si stima che il gigante farmaceutico Merck abbia perso circa 900 milioni di dollari in termini di mancate vendite, interruzioni operative e costi di recupero. Nel mondo della sicurezza informatica, la portata non è tutto. Che siate attaccanti o difensori, spesso sono l'agilità e l'ingegno a darvi un vantaggio, la qual cosa ci ricorda che le dimensioni da sole non garantiscono la vittoria.

Quali possono essere gli impatti di gravi violazioni della sicurezza informatica?

► **Olivier Scaillet:** Le violazioni della sicurezza informatica su larga scala possono avere conseguenze di vasta portata. Uno studio sulle principali società statunitensi quotate sul mercato pubblico ha rilevato che nel breve periodo gli attacchi informatici comportano una riduzione dei rendimenti, un aumento del volume degli scambi, una riduzione della liquidità e un ampliamento degli *spread bid-ask*. Tuttavia, col tempo, queste aziende tendono ad aumentare i loro investimenti in sicurezza informatica, mentre il loro valore di mercato e la loro performance complessiva rimangono relativamente stabili. Le ricerche condotte sugli istituti finanziari dimostrano che gli attacchi informatici possono comportare perdite fino al 50% del reddito netto annuale, a causa dei costi finanziari diretti, delle interruzioni operative e dei danni alla reputazione. Inoltre, alcune violazioni possono avere un effetto a catena sui mercati finanziari, aumentando il rischio sistemico.

► **Anastasia Kartasheva:** Il danno alla reputazione è una delle principali preoccupazioni, soprattutto quando vengono compromessi dati sensibili. La portata delle informazioni esposte può essere enorme, e spazia dai dati fiscali e dalle dichiarazioni dei redditi alle storie mediche, agli identificatori biometrici, ai dati di localizzazione e alla proprietà intellettuale. Anche se l'impatto varia, i costi dei danni alla reputazione e delle controversie legali sono spesso tra i più elevati. È fondamentale riconoscere quanto le aziende siano interconnesse: gli incidenti informatici raramente rimangono isolati e possono avere effetti di vasta portata, difficili da controllare. Alla fine, ogni azienda deve non solo gestire la propria sicurezza informatica, ma anche decidere

se valga la pena pagare un riscatto quando è sotto attacco, considerando le potenziali conseguenze del rifiuto di pagare.

► **Fabian Schär:** L'impatto, spesso trascurato, di un attacco informatico è di ordine psicologico: l'ansia. Così come una persona può sentirsi a lungo a disagio dopo un'effrazione fisica, anche dopo che le serrature sono state cambiate, un disagio simile può persistere dopo una violazione della sicurezza informatica. Quando un hacker si infila nei sistemi informatici di un'organizzazione, il senso di violazione può rimanere anche dopo l'adozione di misure preventive più severe. Questo dubbio persistente – cioè se si verificherà un altro attacco – può influenzare in maniera sottile il comportamento, la fiducia e il processo decisionale all'interno dell'organizzazione.

► **Beat Schär:** Gravi violazioni della sicurezza informatica possono avere importanti conseguenze operative, finanziarie e di reputazione. Nel settore finanziario, un incidente grave può mettere a repentaglio la reputazione normativa ed erodere la fiducia del pubblico. In Svizzera, per esempio, l'Autorità federale di vigilanza sui mercati finanziari (FINMA) ha l'autorità di revocare le licenze bancarie nei casi in cui gli istituti non soddisfino i requisiti di gestione del rischio, compresi quelli legati alla sicurezza informatica. Negli Stati Uniti, gli approcci normativi continuano a evolvere, con discussioni sull'equilibrio tra informazioni obbligatorie e pratiche di sicurezza informatica efficaci. Alcune associazioni del settore hanno espresso il timore che alcune norme possano involontariamente complicare la risposta agli incidenti. Nonostante i pareri discordanti, generalmente la regolamentazione mira a migliorare la resilienza e la responsabilità dell'intero sistema.



DATA BREACH!

Quali sono le sfide e gli incentivi legati alla condivisione inter-organizzativa delle informazioni sulle minacce?

► **Fabian Schär:** In parole povere, la risposta è "fiducia". È logico che le aziende collaborino sulla sicurezza informatica e condividano le loro migliori pratiche, ma farlo significa rivelare molto del loro funzionamento interno in un panorama competitivo in cui alleati e rivali sono spesso gli stessi. Un progetto guidato dal governo, in cui le informazioni vengono condivise in modo più anonimo e consolidato, potrebbe essere migliore degli scambi diretti a livello individuale.

► **Alain Beuchat:** Avere le informazioni giuste è fondamentale, perché ciò aumenta la consapevolezza e aiuta le organizzazioni a valutare il rischio di essere un potenziale bersaglio e a prepararsi alle varie minacce. Esistono due canali principali per acquisire queste informazioni: si possono acquistare da terzi, il che consente di adattare la ricerca delle informazioni alla propria organizzazione, oppure si possono condividere le informazioni tra i partner di mercato attraverso l'*Open Source Intelligence (OSINT)*. L'utilizzo di una combinazione dei due canali è l'approccio più efficace. Un altro aspetto importante è la creazione di relazioni di fiducia attraverso questi scambi; tali relazioni consentono la condivisione rapida ed efficace di informazioni rilevanti in caso di attacco informatico.

► **Anastasia Kartasheva:** Un importante passo avanti per migliorare la condivisione delle informazioni sul rischio informatico a livello internazionale è stata la creazione nel 2018, da parte del Consiglio per la stabilità finanziaria, di un lessico che definisce i termini informatici. Con una comprensione comune delle differenze tra allerte, attacchi, eventi, incidenti, rischi e minacce, è diventato possibile raccogliere e confrontare i dati. Tuttavia, le informazioni informatiche possono anche dare un vantaggio agli aggressori informatici, che sono molto intelligenti e utilizzano varie tattiche per raccogliere informazioni sui loro potenziali bersagli. Per esempio, la nostra amministrazione locale conserva una grande quantità di dati sensibili, tra cui il patrimonio dei nuclei familiari. Un attacco mirato basato sul furto dei dati fiscali di una famiglia specifica è sicuramente più redditizio di un attacco casuale. La sicurezza complessiva si basa sulla forza dell'anello più debole.

► **Marc Henauer:** In Svizzera, a livello nazionale, la recente Ordinanza sulla sicurezza informatica impone agli operatori delle infrastrutture critiche di segnalare gli attacchi informatici all'Ufficio federale della cibersicurezza (UFCS) entro 24 ore dalla scoperta e di presentare un rapporto completo entro 14 giorni. Questa norma rappresenta un notevole passo avanti per migliorare la visibilità di tali incidenti. L'Ordinanza riguarda attualmente le aziende di trasporto pubblico, i fornitori di energia, le autorità federali, statali e locali, gli ospedali e i fornitori di acqua potabile, oltre ad altri settori come quello finanziario. Qualsiasi attacco che comprometta la riservatezza, l'integrità, la disponibilità o la tracciabilità delle informazioni deve essere segnalato, compresi i malware installati con successo su un sistema, i cavalli di Troia di criptaggio, gli attacchi DDoS e l'accesso non autorizzato ai sistemi informatici attraverso le vulnerabilità della sicurezza. L'UFCS analizza queste segnalazioni e fornisce il supporto necessario. Traendo spunti da questi dati, otterremo una migliore comprensione del panorama globale delle minacce. Saremo in grado di identificare sin dall'inizio gli schemi degli attacchi alle infrastrutture critiche e di allertare tempestivamente altre potenziali vittime, consentendo loro di adottare misure preventive e difensive adeguate. Sebbene sia ancora troppo presto per valutare i benefici di questo processo, sono fermamente convinto che questo cambiamento normativo verso una migliore condivisione delle informazioni porterà a molti successi.

Incidenti informatici segnalati all'Ufficio federale della cibersicurezza



Nota: Questa figura mostra il numero settimanale di incidenti informatici segnalati all'Ufficio federale della cibersicurezza (UFCS) da gennaio 2024 a settembre 2025.

Fonte: Ufficio federale della cibersicurezza (UFCS)

Esposizione digitale

Come dovrebbero essere ripartiti i costi e le responsabilità della sicurezza informatica tra il settore pubblico e quello privato?

► **Anastasia Kartasheva:** Come la sicurezza tradizionale, la sicurezza informatica ha notevoli ricadute che spesso si ripercuotono sull'economia generale. Tuttavia, sarei cauta nel suggerire che il settore pubblico debba finanziare la sicurezza informatica, a causa del potenziale rischio morale che ne potrebbe derivare. C'è una grande differenza tra il permettere al governo di regolamentare l'edilizia in aree a rischio di calamità, per esempio, e la supervisione della sicurezza informatica. Ogni azienda deve definire la propria strategia e decidere quanto è disposta a investire per ridurre i propri rischi.

► **Marc Henauer:** Il mondo online è fondamentalmente un'estensione del mondo fisico, con i suoi aspetti positivi e negativi. Come nella vita reale, il governo ha la responsabilità di provare a creare un ambiente migliore e più sicuro. Tuttavia, non è tenuto a raggiungere pienamente questo scopo ambizioso, né può essere biasimato per non averlo fatto. Proprio come nel mondo reale ci si aspetta che le persone chiudano le porte di casa e assicurino le proprie abitazioni, spetta ai privati e alle aziende proteggere il proprio ambiente digitale con misure di sicurezza informatica adeguate.

► **Fabian Schär:** Per ottenere i migliori risultati, ogni parte dovrebbe concentrarsi sulla propria area di competenza. Il settore pubblico dovrebbe dare la priorità alla protezione delle infrastrutture vitali, indipendentemente dalla proprietà, mentre il settore privato deve garantire la continuità delle operazioni a livello sia aziendale sia industriale. Il ruolo del regolatore è quello di fornire linee guida chiare sui requisiti minimi e sulla direzione generale dell'economia. È inoltre essenziale incoraggiare la collaborazione e la condivisione tra le varie parti, compresi gli accademici, le aziende e le agenzie governative, in qualsiasi formato funzioni meglio.

Quali tendenze del mercato – come le fusioni, le acquisizioni e l'ascesa delle soluzioni *one-stop cloud* – rivelano in che modo il settore sta rispondendo alle minacce informatiche?

► **Beat Schär:** La spinta al consolidamento, sia attraverso le fusioni, sia affidandosi a pochi fornitori cloud dominanti, riflette il tentativo di razionalizzare le organizzazioni e i sistemi informatici. Un numero minore di sistemi semplifica la gestione, ma concentra anche i rischi, rendendo la vita più facile non solo agli utenti, ma anche agli aggressori. Le soluzioni cloud, per quanto efficienti e scalabili, comportano sfide quotidiane per la sicurezza a causa delle loro configurazioni complesse e sono al

centro di minacce che evolvono continuamente. La diversificazione dei sistemi o l'esecuzione di cloud paralleli migliorano la resilienza, ma queste misure sono costose e difficili da gestire. Poiché una manciata di fornitori domina sempre di più il mercato, questa centralizzazione crea una pericolosa dipendenza: se un fornitore fallisce o viene violato, le conseguenze potrebbero essere enormi. In definitiva, che si tratti di integrazione o di diversificazione, ogni approccio comporta i suoi propri compromessi in termini di sicurezza informatica.

In che modo l'esposizione al rischio della sicurezza informatica varia tra il settore finanziario e quello non finanziario?

► **Marc Henauer:** Le banche sono state all'avanguardia nell'integrare l'informatica nelle loro attività principali, già a partire dagli anni '50. Inizialmente i computer sostenevano la gestione dei registri contabili, ma col tempo si sono aggiunte funzioni critiche come il *batch processing*, la messaggistica finanziaria sicura, gli sportelli bancomat, l'online banking e il trading elettronico. Questa adozione precoce ha creato infrastrutture frammentate e pesanti. Tuttavia, il settore finanziario tende ad adottare cicli di sostituzione strutturati in modo più coerente rispetto a molte industrie non finanziarie. I sistemi informatici nei settori finanziari e non finanziari tendono a crescere organicamente, spesso senza un piano d'azione a lungo termine o un quadro normativo che definisca quali infrastrutture includere nel decennio successivo.

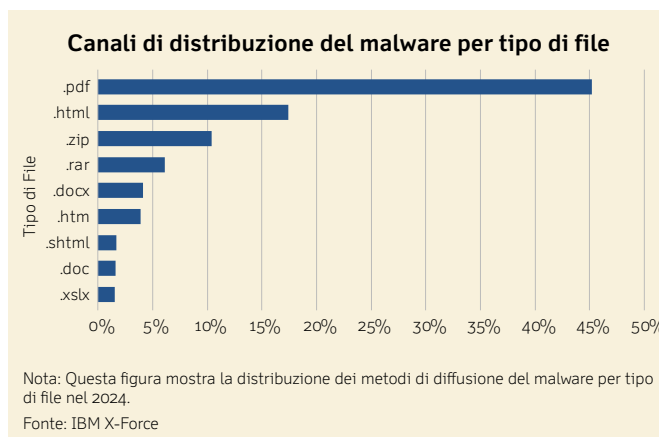
In che modo le organizzazioni hanno migliorato la loro preparazione agli attacchi informatici e quali sfide rimangono?

► **Alain Beuchat:** Le aziende hanno compiuto progressi notevoli nell'istituzione di protocolli di base per l'igiene informatica e nella scelta degli strumenti di sicurezza adeguati. In teoria, le basi sono chiare: applicare tempestivamente una correzione di sicurezza alle vulnerabilità note, usare la protezione anti-malware e il monitoraggio, applicare l'autenticazione a più fattori e garantire che i backup siano archiviati in modo sicuro. In realtà, però, questi passi apparentemente semplici sono difficili da effettuare su larga scala. La sfida sta nel farlo in modo coerente su tutti i sistemi. A rendere difficile la difesa informatica dal punto di vista operativo non è tanto la mancanza di conoscenze, quanto la pura e semplice complessità di applicare le difese su reti di grandi dimensioni. Errori umani, processi frammentati e ritardi nell'aggiornamento continuano a creare vulnerabilità, anche quando le difese sono attive. La vera preparazione non consiste tanto nel disporre della giusta lista di controllo, quanto nell'applicarla in modo coerente e rapido.

► **Olivier Scaillet:** Con l'aumento della complessità e dei costi delle misure di sicurezza informatica, i reparti informatici si trovano ad affrontare una crescente pressione per fornire valore. Le organizzazioni devono decidere saggiamente cosa proteggere, come proteggere e cosa possono permettersi di non proteggere, decisioni intrinsecamente gravate da rischi e incertezze. Allo stesso tempo, il management e i consigli di amministrazione devono rimanere vigili, poiché gli incidenti informatici comportano notevoli implicazioni di governance. Le ricerche dimostrano che gli attacchi riusciti aumentano la probabilità di *turnover* dei dirigenti, in particolare dei Chief Investment Officer e dei Chief Information Security Officer, e possono persino indurre cambiamenti a livello di consiglio di amministrazione quando si evidenziano lacune nella supervisione o nella preparazione. Queste sfide sottolineano che non sono solo gli enti normativi, ma anche gli azionisti a ritenere la leadership responsabile dei fallimenti della sicurezza informatica.

► **Beat Schär:** Gli attacchi sponsorizzati dagli Stati stanno diventando sempre più sofisticati. Gli hacker stanno introducendo un codice maligno negli aggiornamenti software di fornitori terzi fidati, il che rappresenta un modo discreto per colpire un'ampia gamma di vittime. Questi attacchi dimostrano come partner fidati possano diventare una minaccia e sottolineano l'importanza dei principi dell'architettura *zero-trust* e di una rigorosa gestione del rischio da parte di terzi. Poiché questi attacchi sono molto complessi, le possibilità di individuarli tempestivamente o di evitarli sono molto basse. Questa complessità sottolinea la necessità di una vigilanza continua, di una modellazione proattiva delle minacce e di simulazioni basate su scenari per testare e migliorare la resilienza dell'organizzazione.

► **Marc Henauer:** Il management deve comprendere che le competenze in materia di sicurezza informatica sono altamente specializzate e richiedono tempo e impegno per comprendere le implicazioni e riconoscere gli scenari. Ogni dipendente ha un ruolo nella sicurezza informatica, quindi la formazione del personale è fondamentale. Per quanto riguarda la comunicazione, non bastano una comunicazione esterna e una interna dall'alto verso il basso, ma servono anche canali efficaci che consentano agli utenti finali di segnalare problemi informatici sospetti dal basso verso l'alto. In definitiva, la preparazione alla sicurezza informatica deve essere incorporata nell'intera cultura organizzativa e non limitarsi al reparto informatico.



Quali sono le recenti tendenze di investimento nella sicurezza informatica che hanno influenzato maggiormente le pratiche del settore?

► **Marc Henauer:** C'è una crescente consapevolezza del fatto che i test continui sono fondamentali. Questi test devono riguardare sia gli aspetti tecnici sia quelli procedurali, comprese le simulazioni di attacco. Allargando il contesto dei test a un numero maggiore di esperti di sicurezza informatica, possiamo garantire che venga affrontata e migliorata anche la comunicazione, fondamentale per rassicurare terze parti, investitori e autorità di regolamentazione. L'intelligenza artificiale viene utilizzata sempre più spesso per migliorare le funzioni di sicurezza e simulare gli attacchi. L'investimento nella sicurezza informatica e il costo degli incidenti informatici stanno diventando sempre più evidenti nei bilanci, attraverso l'aumento delle spese operative e le conseguenze negative degli incidenti informatici.

► **Fabian Schär:** Oltre ai test, le istantanee e i backup multipli costituiscono una solida difesa contro i problemi di contaminazione e gli attacchi *ransomware* che potrebbero cancellare un intero sistema. Tuttavia, sembra che molte piccole e medie imprese, altamente suscettibili a questi rischi, non abbiano messo in atto un sistema di backup completo. Sebbene i backup e le istantanee non siano una soluzione completa per la sicurezza informatica, essi rappresentano un modo semplice ed economico per salvaguardare l'infrastruttura informatica da gran parte delle minacce odierne. Tuttavia, non proteggono da attacchi come l'estorsione dei dati o la doppia estorsione, in cui i dati vengono prima criptati e poi l'aggressore chiede un riscatto per mantenerli privati.

In che modo gli istituti finanziari decidono quanto investire nella sicurezza informatica e quali fattori influenzano queste decisioni?

► **Olivier Scaillet:** In parole povere, le decisioni di investimento nella sicurezza informatica dipendono da quanto le istituzioni finanziarie si percepiscono esposte al rischio di sicurezza informatica. Un'analisi delle società quotate negli Stati Uniti mostra che questa percezione è influenzata da diversi fattori, tra cui i passati attacchi informatici, le caratteristiche dell'azienda e del settore, la qualità della governance e le pressioni normative o di mercato. È interessante notare che le società con un rischio di sicurezza informatica più elevato tendono a sovraperformare i loro pari di circa il 10% all'anno, ma sottoperformano in modo netto quando i rischi informatici si materializzano. Questa differenza suggerisce che un fattore di rischio informatico distinto

esiste e viene valutato dal mercato. Le istituzioni finanziarie, dato il loro ruolo critico e la loro maggiore esposizione, devono riconoscere questa minaccia in evoluzione e garantire che i loro investimenti in sicurezza informatica siano proattivi e proporzionati al loro profilo di rischio.

► **Marc Henauer:** È probabile che le esperienze passate, il management e gli interessi del consiglio di amministrazione giochino un ruolo significativo in queste decisioni. Anche le autorità di regolamentazione finanziaria hanno un'influenza importante, in quanto stabiliscono i requisiti di base per le azioni da intraprendere. Un fattore chiave per migliorare la sicurezza informatica è la presenza di un piano a lungo termine che delinea gli investimenti finanziari effettuati nel tempo, consentendo al management di monitorare i progressi e le tappe fondamentali.



Quali sono le potenziali conseguenze di un attacco informatico ai sistemi di core banking o di messaggistica finanziaria?

Fabian Schär: Le banche commerciali devono assicurarsi di servire i propri clienti gestendo le transazioni finanziarie, come i pagamenti, 24 ore su 24. Le principali banche globali elaborano fino a 100 milioni di transazioni al giorno, tra cui bonifici, pagamenti con carta di credito e transazioni mobili. Quando il core banking di una grande banca viene preso di mira, si ha un impatto immediato sul mercato, causando un flusso irregolare di denaro sia nei mercati finanziari sia in quelli reali, finché non intervengono banche alternative. Il sistema primario di compensazione è la spina dorsale di ogni sistema finanziario. Qualsiasi problema con una rete di messaggistica o un sistema di regolamento, come SWIFT, TARGET2, Fedwire o il SIX Interbank Clearing System, può avere conseguenze di vasta portata e scatenare il panico nel settore finanziario e nel mondo reale, senza alcun riguardo per i confini internazionali.

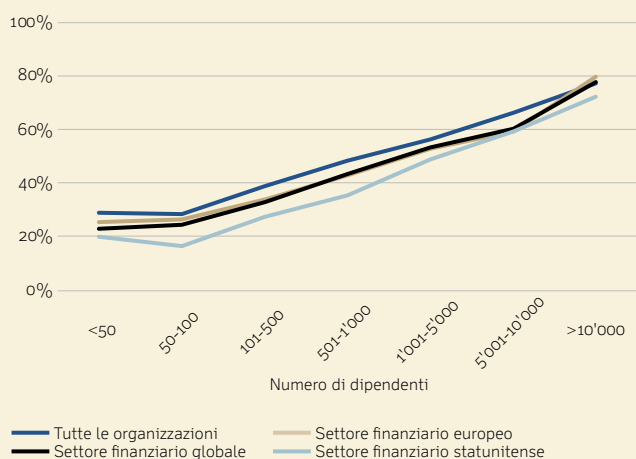
Come fanno le istituzioni finanziarie a quantificare i rischi informatici per una gestione efficace?

Beat Schär: Date le numerose parti in movimento e le incognite, una quantificazione accurata di questi rischi richiede un notevole sforzo supplementare e può fornire benefici limitati. Un approccio ampio e basato su scenari è probabilmente il modo più efficace per valutare la situazione e sembra essere lo standard. Poiché la comunicazione sulla sicurezza informatica è già complessa e la gestione quantitativa del rischio informatico è ancora agli inizi, è meglio mantenere gli aggiornamenti alla direzione chiari e concisi.

Quali rischi di sicurezza informatica sono introdotti dai fornitori di servizi terzi?

Alain Beuchat: L'utilizzo di fornitori di servizi terzi, che si tratti di venditori di cloud, di informatica esternalizzata o di fornitori di software, è diventato essenziale. Tuttavia, ciò aggiunge un nuovo livello di rischio che è sempre più difficile da gestire. Le autorità di regolamentazione si aspettano che applichiamo ai nostri fornitori lo stesso livello di controlli che effettuiamo all'interno della banca. In realtà, ciò significa verifiche continue, lunghi questionari sui fornitori e regolari *follow-up* per applicare gli standard al di là del nostro perimetro diretto. Con l'aumento dell'*outsourcing*, cresce anche la superficie di attacco. Per le istituzioni finanziarie, ciò rappresenta una duplice sfida: far rispettare i controlli alle parti esterne e mantenere la responsabilità interna.

Esposizione a vulnerabilità note e sfruttate (Known-Exploited Vulnerability – KEV) per dimensione d'impresa: economia nel suo complesso e settore finanziario



Nota: Questa figura mostra la percentuale di organizzazioni con almeno una vulnerabilità nota e sfruttata (Known-Exploited Vulnerability - KEV) rilevata nella propria infrastruttura nel 2023, suddivisa per dimensione aziendale. Include un benchmark che copre tutti i settori economici, insieme a dati aggregati per il settore finanziario globale e le sue componenti europee e statunitensi. Le categorie di dimensione aziendale sono definite in base al numero di dipendenti.

Fonte: Bitsight

Quali sono i limiti e i probabili sviluppi del mercato delle assicurazioni informatiche?

► **Beat Schär:** Valutare l'impatto di un attacco informatico è relativamente facile, ma determinare la probabilità di essere presi di mira è estremamente complesso. Questa complessità rende difficile valutare con precisione il rischio complessivo. Un approccio pratico consiste nel confrontare il proprio assetto di sicurezza informatica con quello dei colleghi del settore e puntare a superarlo: l'obiettivo, come in molte aree di gestione del rischio, è rimanere all'avanguardia. Detto questo, dobbiamo essere realistici: qualsiasi polizza assicurativa presenta delle lacune e l'assicurazione informatica non è da meno. Un'altra preoccupazione per un assicuratore è il rischio di concentrazione: alcuni fornitori di cloud rappresentano individualmente una quota sostanziale della capacità di elaborazione globale. Questo livello di concentrazione solleva seri interrogativi su come gli assicuratori possano gestire la loro esposizione al rischio sistemico in un ecosistema digitale così altamente interconnesso.

► **Alain Beuchat:** Il mercato delle assicurazioni informatiche sta maturando rapidamente, ma è così anche per la nostra consapevolezza dei suoi limiti e delle sue responsabilità. Negli anni passati, le polizze informatiche erano poco costose e vagamente coperte. Oggi gli assicuratori conducono una *due diligence* rigorosa, pongono domande tecniche dettagliate e sono pronti a contestare le richieste di risarcimento. La loro preoccupazione non è solo il costo, ma anche l'affidabilità. Se un attacco a un'azienda viene ricondotto a una macchina con configurazione errata o a un anti-malware obsoleto, gli assicuratori possono invocare esclusioni e ridurre i risarcimenti, indipendentemente dalle buone pratiche generali dell'azienda. In molti casi, le perdite di reputazione e di clienti, che danneggiano veramente, non sono affatto coperte dall'assicurazione. Con l'aumento dei premi e l'inasprimento delle esclusioni, alcuni istituti stanno iniziando a considerare l'assicurazione contro i rischi informatici come l'ultima risorsa, piuttosto che come una pietra miliare della loro strategia del rischio.

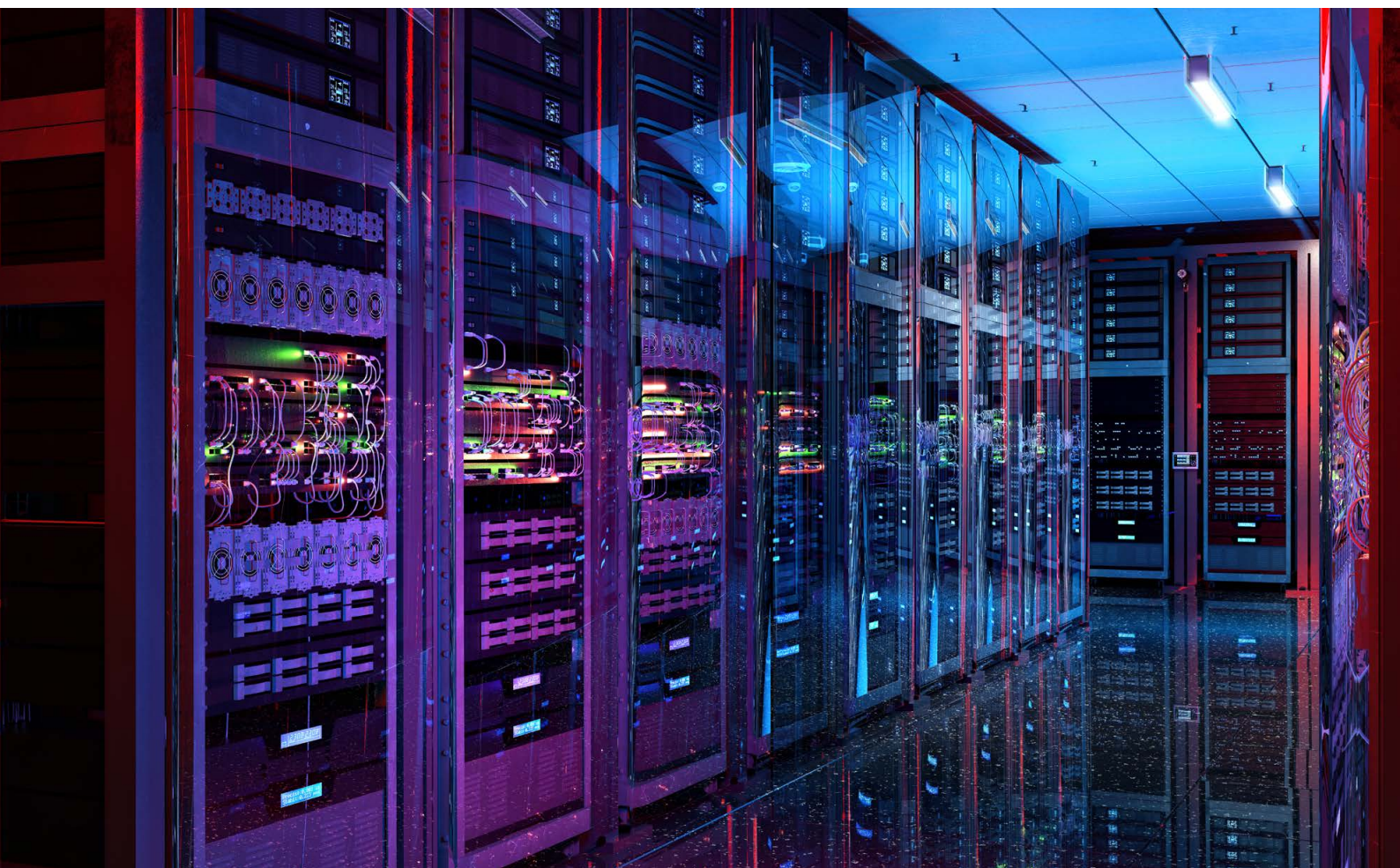
► **Anastasia Kartasheva:** I rischi informatici sono influenzati da una miscela di distribuzioni delle perdite a coda pesante, modelli incerti e informazioni disomogenee. A differenza dei rischi assicurabili tradizionali, gli eventi informatici possono essere mondiali, rapidi e deliberatamente adattivi, il che li rende particolarmente difficili da prevedere e modellare. Il loro costo elevato e la loro natura mutevole aggiungono ulteriore complessità. Queste caratteristiche pongono sfide importanti agli assicuratori, ma implicano anche che il mercato abbia un certo potenziale. Nuove soluzioni includono la creazione di intermediari che valutino la resilienza informatica di un'azienda, analogamente a quanto avviene per i rating sui mercati obbligazionari.

► **Olivier Scaillet:** Il mercato delle assicurazioni informatiche sta prendendo forma come settore a sé stante. Un modo per comprendere questa evoluzione è osservare l'equilibrio tra gli investimenti nella sicurezza informatica interna e il trasferimento del rischio attraverso l'assicurazione. Gli assicuratori ora non si limitano a offrire una copertura, ma aiutano le organizzazioni a gestire i rischi informatici direttamente o tramite terzi. Con lo sviluppo di questi modelli, mi aspetto una crescente pressione sulla ri-assicurazione, a causa dell'aumento dei costi e della complessità delle esposizioni informatiche. Questa traiettoria potrebbe infine portare a meccanismi di condivisione del rischio a livello globale, come sindacati assicurativi o mercati secondari per il rischio informatico, simili a quanto sta accadendo con i *catastrophe bond*. Questi meccanismi di condivisione del rischio consentirebbero agli investitori di negoziare titoli legati all'informatica e amplierebbero la capacità oltre le assicurazioni tradizionali.

In prospettiva, quali strategie avanzate dovrebbero adottare le istituzioni finanziarie per mitigare efficacemente gli attacchi?

► **Marc Henauer:** Le istituzioni finanziarie hanno una profonda conoscenza del panorama della sicurezza informatica e del funzionamento del sistema finanziario interconnesso, nonché delle sue potenziali vulnerabilità. Che sia grande o piccola, ogni banca può avere un effetto a catena sulla più ampia infrastruttura bancaria e finanziaria. Inoltre, esse sanno che i danni alla reputazione si ripercuotono su tutti. Se una banca viene gravemente colpita, l'intero settore finanziario ne risente. Non c'è alcun guadagno individuale da ottenere in questo caso. Questo fatto li spinge a collaborare in modo proattivo e a comunicare in modo aperto ed efficiente.

► **Olivier Scaillet:** In prospettiva, le istituzioni finanziarie devono adottare strategie di difesa avanzate e stratificate, come il rilevamento delle minacce alimentato dall'intelligenza artificiale, le strutture *zero-trust* e la formazione continua dei dipendenti, per stare al passo con minacce informatiche sempre più sofisticate. Ma oltre a proteggersi, le banche sono in una posizione unica per cogliere le opportunità di business emergenti nello spazio della sicurezza informatica. Man mano che il rischio informatico diventa un bene misurabile e prezioso, le istituzioni finanziarie possono assumere un ruolo guida nello sviluppo e nell'offerta di prodotti finanziari innovativi, come il *tranching* del rischio informatico sul modello dei *CDO* (*Collateralized Debt Obligations*). Strutturando il rischio in strati, che assorbono le perdite in base alla gravità, le banche possono facilitare la diversificazione basata sul mercato, offrire strumenti assicurativi informatici personalizzati e aiutare i clienti a coprire le esposizioni informatiche. In questo modo, passano dall'essere bersagli passivi a *market maker* attivi nell'economia del rischio informatico in evoluzione.



Frontiere

Le iniziative di finanza decentralizzata (*Decentralized Finance – DeFi*) rendono le cose più sicure o più vulnerabili dal punto di vista della sicurezza informatica?

► **Fabian Schär:** La finanza decentralizzata e quella centralizzata presentano profili di rischio di sicurezza informatica distinti, senza che nessuna delle due sia chiaramente superiore. Da un lato, i sistemi decentralizzati offrono alcuni vantaggi in termini di sicurezza, in particolare l'impossibilità per un singolo attore di alterare unilateralmente il registro pubblico, eliminando così molti vettori di attacco comuni nelle architetture centralizzate. D'altra parte, essi introducono vulnerabilità uniche. Per esempio, i sistemi DeFi si basano molto sulle chiavi private e se un utente perde o espone la propria, non ha alcuna possibilità di ricorso: i suoi asset possono essere rubati in modo irreversibile e gli aggressori possono persino usare la sua identità compromessa per creare nuovi *smart contracts*. L'attrattiva fondamentale della DeFi risiede nella sua assenza di necessità di fiducia, nei processi semplificati e nelle transazioni più veloci, caratteristiche che possono essere molto vantaggiose dal punto di vista commerciale. Tuttavia, l'assenza di intermediari sposta l'onere del rischio sull'individuo. Gli utenti devono non solo mettere al sicuro le loro chiavi, ma anche navigare in un sistema complesso in cui le protezioni comuni nella finanza tradizionale, come gli storni di transazioni o la risoluzione delle controversie, sono in gran parte assenti. In questo senso, la DeFi amplia la gamma di possibilità, ma introduce anche una nuova classe di rischi operativi e di sicurezza informatica che devono essere compresi e gestiti attivamente.

► **Olivier Scaillet:** Come in ogni innovazione tecnologica, ci sono lati positivi e lati negativi. Le ricerche hanno rilevato che gli attacchi ransomware sono il tipo di attacco informatico più comune, con un piccolo numero di bande di ransomware avanzato che domina la scena. Queste bande sono diventate società sofisticate con nomi elaborati, uffici, call center e operazioni di *franchising*. In genere ricevono i pagamenti dei riscatti in criptovalute e devono riciclare i proventi attraverso schemi complessi. Poiché il Bitcoin è tracciabile, gli aggressori preferiscono criptovalute più oscure, come *Monero* o *Zcash*. Secondo alcuni aneddoti, quando le vittime insistono per pagare in Bitcoin, le bande applicano un sovrapprezzo del 20%. È improbabile che si possa trovare una soluzione per evitare che le criptovalute vengano utilizzate per la criminalità informatica, poiché vietare l'uso delle criptovalute in un Paese ne eliminerebbe i vantaggi e lo porrebbe in una posizione di svantaggio tecnologico.

Quali sono le differenze in termini di rischi per la sicurezza informatica tra il denaro delle banche centrali, quello delle banche commerciali e gli asset digitali?

► **Anastasia Kartasheva:** Rubare denaro o asset elettronici è solo metà dell'opera. L'altra metà è incassare. La rapina alla Banca del Bangladesh del 2016 ne è un esempio lampante: gli hacker si sono infiltrati nel sistema informatico della banca centrale e hanno avuto accesso alla sua rete SWIFT per inviare false istruzioni di trasferimento per un totale di 951 milioni di dollari. Circa 81 milioni di dollari sono stati inviati nelle Filippine e poi riciclati attraverso una complessa e costosa rete di società di comodo e casinò. È interessante notare che i restanti trasferimenti, per un valore di oltre 850 milioni di dollari, sono stati scoperti perché un errore di battitura nel messaggio ha destato sospetti. Sebbene sia relativamente facile convertire asset non regolamentati come i Bitcoin in Paesi con una regolamentazione debole, farlo è un processo rischioso e oscuro, e l'utente finale probabilmente si ritrova con "soldi finti".

In che modo l'intelligenza artificiale aggrava le minacce alla sicurezza informatica?

► **Anastasia Kartasheva:** L'intelligenza artificiale è un'arma a doppio taglio. Gli aggressori sono diventati molto più intelligenti. I giorni in cui si inviavano e-mail di massa con indirizzi casuali, errori di battitura e loghi mal progettati sono ormai lontani. Nel frattempo, i difensori possono sfruttare l'intelligenza artificiale per rafforzare il proprio team e automatizzare le loro difese. Il settore sta cercando di distribuire strumenti di intelligenza artificiale in tutto il sistema informatico. È fondamentale aumentare la consapevolezza delle minacce di oggi e di domani ed educare gli utenti ovunque.

► **Fabian Schär:** Il rapido sviluppo dei *deepfakes*, guidati dai sistemi di *deep learning*, è per me particolarmente preoccupante. L'unico meccanismo di difesa che mi viene in mente oggi è la firma crittografica. Oggi abbiamo migliaia di ore di video con politici di spicco a disposizione online. È relativamente semplice per un modello di intelligenza artificiale vestire i panni di quella persona e farle dire tutto ciò che si desidera. Credo che presto ci troveremo in un mondo in cui i discorsi non saranno più pronunciati di persona, ma saranno scritti e presentati da un sistema di intelligenza artificiale, con il messaggio firmato crittograficamente per garantirne l'autenticità.

Come fanno oggi le istituzioni finanziarie a gestire le minacce alla sicurezza informatica utilizzando l'intelligenza artificiale?

► **Fabian Schär:** È difficile per le società finanziarie rimanere all'avanguardia in questo gioco per due motivi principali. In primo luogo, la concorrenza è molto veloce. In secondo luogo, le banche hanno spesso una durata di vita lunga, il che significa che sono bloccate da sistemi *legacy* complessi che sono difficili da proteggere in modo efficace. L'intelligenza artificiale aiuterà sempre più le banche a rilevare attività sospette e a reagire più rapidamente. Tuttavia, gli aggressori sembrano avere la meglio in questo campo.

► **Olivier Scaillet:** Si stanno verificando diversi sviluppi interessanti. L'intelligenza artificiale offre numerosi vantaggi, come efficienza, scalabilità e adattabilità nella sicurezza informatica. Questi vantaggi facilitano l'identificazione di potenziali attività fraudolente basate su modelli di comportamento dei clienti, anticipano le minacce imparando dai dati storici e consentono sistemi di risposta automatizzati che isolano i problemi e riducono i tempi di risposta. Tuttavia, tutto ciò che sappiamo oggi dovrà essere modificato quando l'informatica quantistica diventerà il nuovo standard.

Qual è la tempistica realistica per la comparsa di minacce da parte dell'informatica quantistica?

► **Anastasia Kartasheva:** La potenza e la velocità di calcolo sono fondamentali nel mondo informatico. Alcuni esperti prevedono che gli attacchi più sofisticati provenienti dai computer quantistici diventeranno lo standard entro il prossimo decennio. Tuttavia, nonostante gli attacchi informatici siano, per definizione, condotti da computer, c'è sempre un elemento umano coinvolto. La capacità di calcolo non è l'unico fattore; sia gli aggressori sia i difensori dovranno migliorare le proprie competenze man mano che progrediamo.

Quali sono le misure specifiche che le istituzioni finanziarie dovrebbero adottare per prepararsi in futuro a una sicurezza informatica resistente ai quanti?

► **Fabian Schär:** Le banche devono sempre prepararsi alle sfide future. A mio avviso, devono migliorare la loro comprensione del sistema attuale e di quello emergente. L'attuale struttura informatica bancaria è un modello consolidato, nato negli anni '50 e sottoposto a numerose fusioni e acquisizioni. A differenza di molti altri settori, l'importanza di un sistema centralizzato è cruciale nel settore bancario e il problema del retaggio è sostanziale. J.P. Morgan Chase, per esempio, è il risultato di oltre 1'200 istituti precedenti.

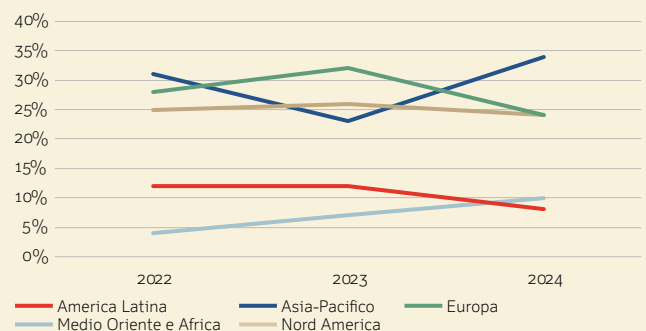
► **Olivier Scaillet:** I preparativi per un futuro quantistico prevedono diverse fasi. Innanzitutto, le banche devono compilare un inventario chiaro dei loro attuali blocchi crittografici per comprenderne la configurazione e le vulnerabilità. Poi viene la fase di sviluppo, in cui collaborano con i fornitori di sistemi e con i proprietari di sistemi interni per testare a fondo la nuova tecnologia quantistica. Poi c'è la fase di sostituzione della vecchia tecnologia con quella nuova. L'approccio attuale per affrontare i rischi della crittografia post-quantistica (*Post-Quantum Cryptography – PQC*), e le potenziali debolezze dei nuovi algoritmi resistenti alla PQC, consiste nel combinare i vecchi e i nuovi metodi adottando protocolli ibridi che applicano entrambe le tecnologie contemporaneamente.

Quanto sono marcate le differenze tra Paesi e settori in termini dei mezzi a loro disposizione per garantire la sicurezza informatica?

Fabian Schär: Le differenze tra Paesi e settori sono significative e spesso sono radicate nella storia, nella geografia e nella struttura istituzionale. Nel settore finanziario, per esempio, i centri finanziari più recenti godono spesso di un vantaggio strutturale: i loro sistemi sono stati costruiti nell'era dei mercati globali e del trading elettronico, consentendo basi informatiche più moderne. Al contrario, le banche storiche spesso si affidano a sistemi legacy, talvolta vecchi di decenni, che sono difficili e costosi da revisionare. Ciò crea complessi mosaici più difficili da proteggere e mantenere. A livello di Paesi, mentre il mondo occidentale gode generalmente di capacità di sicurezza informatica più forti, delle variazioni persistono. Alcuni Paesi attirano una maggiore attenzione geopolitica e sono quindi bersaglio più frequente di attacchi informatici, in particolare gli Stati Uniti. Altri, come la Svizzera, beneficiano di una posizione geopolitica più neutrale, di istituzioni ben finanziate e di una forte cooperazione tra pubblico e privato. Queste differenze determinano sia l'esposizione sia la resilienza di fronte all'evoluzione delle minacce.

Anastasia Kartasheva: La preparazione alla sicurezza informatica varia non solo a seconda del Paese, ma anche a seconda del settore, dell'azienda e dell'individuo, a seconda di come vengono definite chiaramente le responsabilità e di come vengono allineate le risorse. In alcune giurisdizioni, il settore pubblico ha assunto un ruolo guida stabilendo standard chiari, finanziando centri di coordinamento e facilitando la condivisione di informazioni sulle minacce. In altre, soprattutto nei mercati emergenti o nelle economie in transizione, le imprese sono spesso abbandonate a se stesse, con una guida o una chiarezza normativa limitata. Questa situazione porta a una protezione non uniforme: mentre alcune grandi aziende dispongono di difese di alto livello, altre, in particolare le imprese più piccole e le istituzioni statali, rimangono altamente vulnerabili a causa di budget limitati e sistemi frammentati. In definitiva, l'efficacia di un quadro di sicurezza informatica dipende tanto dalla governance nazionale e dalla maturità istituzionale, quanto dalla tecnologia o dalla spesa.

Distribuzione degli attacchi informatici per regione geografica



Nota: Questa figura mostra la distribuzione degli attacchi informatici nelle diverse aree geografiche dal 2022 al 2024. Nel 2024, i Paesi più colpiti all'interno di ciascuna regione sono stati gli Stati Uniti (86% del Nord America), il Giappone (66% dell'Asia-Pacifico), l'Arabia Saudita (63% del Medio Oriente e Africa), il Brasile (53% dell'America Latina) e il Regno Unito (25% dell'Europa).

Fonte: IBM X-Force

Come descriverebbe il ruolo degli standard internazionali negli impegni di sicurezza informatica transfrontalieri?

► **Marc Henauer:** Gli standard internazionali svolgono un ruolo cruciale nel consentire la cooperazione transfrontaliera in materia di sicurezza informatica, offrendo un linguaggio comune, aspettative condivise e parametri tecnici di riferimento per la gestione del rischio. Anche se l'attuazione varia a seconda delle regioni e dei settori, questi standard – come l'ISO 27001 (dell'*International Organization for Standardization*) e il *Cybersecurity Framework del National Institute of Standards and Technology (NIST)* degli Stati Uniti – aiutano a ridurre la frammentazione e consentono la collaborazione tra governi, settori e catene di approvvigionamento. Come la politica climatica, anche la sicurezza informatica ha bisogno di un allineamento globale in linea di principio, ma trasformarla in un'azione coordinata rimane una sfida complessa. Il vero progresso dipende da reciprocità e fiducia attraverso i confini e i settori, non

dall'imposizione di modelli adatti a tutti. Il rischio di perdere istituzioni chiave come il MITRE, un'organizzazione di ricerca senza scopo di lucro, che gestisce infrastrutture condivise come gli identificatori *CVE (Common Vulnerabilities and Exposures)*, rivela la fragilità dei sistemi centralizzati e sottolinea la necessità di approcci resilienti, distribuiti e cooperativi alla governance globale della sicurezza informatica.

► **Beat Schär:** Gli standard internazionali sono estremamente preziosi come punti di riferimento, in quanto aiutano le organizzazioni a valutare la propria posizione e a migliorare. L'esistenza di iniziative diverse tra settori e Paesi offre una ricca fonte di informazioni sulle sfide che gli altri affrontano e sulle soluzioni che applicano. Nel campo della sicurezza informatica, nessun singolo attore ha tutte le risposte: imparare continuamente gli uni dagli altri non è solo utile, è essenziale.



Domanda finale

Quale ruolo dovrebbero svolgere i consigli di amministrazione, i comitati di direzione e la normativa nel definire la governance della sicurezza informatica?

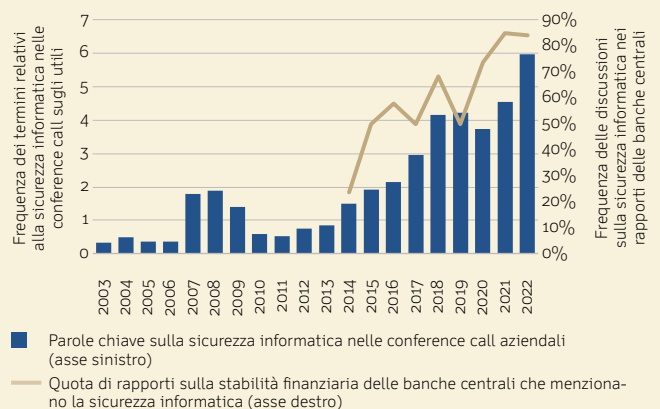
► **Alain Beuchat:** Le recenti normative svizzere richiedono l'approvazione delle strategie di sicurezza informatica da parte del consiglio di amministrazione (CdA). Tuttavia, l'impegno del CdA nella sicurezza informatica è più di un requisito di conformità: è sempre più una questione di sopravvivenza strategica. In altre parole, il coinvolgimento formale non sempre si traduce in una supervisione efficace. Molti membri dei CdA faticano a comprendere quanto le loro organizzazioni si affidino all'infrastruttura informatica, per non parlare della complessità della difesa informatica. Sebbene siano generalmente consapevoli dell'impatto che gli attacchi informatici possono avere, spesso grazie alla copertura mediatica, rimane difficile per loro collegare queste minacce alle vulnerabilità e alle realtà specifiche della propria organizzazione. Per colmare questo divario non bastano le riunioni informative. I membri dei CdA devono avere una conoscenza di base sufficiente per poter porre domande eloquenti, mettere in discussione i compromessi e capire cosa implica realmente il profilo di rischio della loro azienda. Finché i CdA non svilupperanno una maggiore conoscenza dell'informatica, la governance rimarrà indietro rispetto alla velocità della minaccia.

► **Olivier Scaillet:** Nel contesto svizzero, gli enti normativi come la FINMA svolgono un ruolo cruciale nel definire la governance della sicurezza informatica, specialmente nel settore finanziario. Mentre alcune istituzioni sono più avanti, grazie a risorse più forti o a una comprensione più approfondita dei rischi informatici, la regolamentazione rimane relativamente leggera in aree come le soluzioni cloud e le catene di fornitura. Un prossimo passo fondamentale sarebbe quello di chiarire i ruoli e le responsabilità di tutti i livelli di gestione in caso di fallimento della sicurezza informatica, la qual cosa contribuirebbe a promuovere una maggiore responsabilità da parte della direzione. Allo stesso tempo, i consigli di amministrazione e i comitati di direzione non devono vedere la sicurezza informatica solo come una questione tecnica delegata ai team informatici. I CdA devono essere regolarmente informati sia sugli incidenti sia sugli sviluppi più importanti e devono condurre esercitazioni di routine per assicurarsi di essere preparati a prendere decisioni valide una volta sotto pressione. La sicurezza informatica riguarda quasi tutti gli aspetti del mondo degli affari e della società, quindi i membri dei CdA hanno il dovere di impegnarsi tempestivamente e in modo proattivo, anziché aspettare che una crisi li costringa ad agire.

► **Anastasia Kartasheva:** E' essenziale disporre di un piano di emergenza ben sviluppato. Il piano deve affrontare questioni fondamentali, come la rapidità con cui i sistemi possono essere ripristinati, se l'aggressore vi ha ancora accesso, quali perdite potrebbero essere coperte da un'assicurazione per la sicurezza informatica e se potrebbero risultare sanzioni normative o multe. Non esiste una soluzione unica per tutti, ma la formazione proattiva della leadership aziendale sui rischi della sicurezza informatica è fondamentale.

► **Fabian Schär:** Come per molte altre cose, adottare misure ragionevoli può essere utile, ma spingersi troppo oltre può avere l'effetto opposto. Se i banner dei cookie obbligatori sui siti web ci hanno insegnato qualcosa, è che la conformità normativa spesso si limita a ripettare la forma, senza garantire davvero la protezione del tesoro. In definitiva, né le aziende né i singoli individui possono esternalizzare la responsabilità: la normativa stabilisce i requisiti minimi, non il livello a cui fermarsi, per una sicurezza informatica efficace.

Menzioni della sicurezza informatica da parte di imprese e banche centrali



Nota: Questa figura presenta due misure dell'attenzione istituzionale alla sicurezza informatica tra il 2003 e il 2022. Le barre mostrano la frequenza dei termini relativi alla sicurezza informatica (per esempio, sicurezza informatica, attacco informatico, minaccia informatica, perdita di dati, malware, ransomware) nelle relazioni sugli utili aziendali, standardizzati per 10'000 frasi (asse sinistro). La linea indica la percentuale di relazioni sulla stabilità finanziaria e relazioni annuali pubblicate dalle banche centrali del G20 che includono una discussione approfondita sulla sicurezza informatica (asse destro).

Fonti: Advisen, NL Analytics, e Fondo Monetario Internazionale (IMF)

In che modo, secondo voi la normativa sta influenzando la capacità del settore finanziario di gestire il rischio informatico?

► **Marc Henauer:** L'UFCS della Svizzera è fondamentale per incrementare la resilienza informatica del Paese. Il suo lavoro si concentra su quattro obiettivi principali: migliorare la comprensione delle minacce, consentire la prevenzione, ridurre al minimo l'impatto degli incidenti e proteggere i prodotti e i servizi digitali. Una recente pietra miliare è stata l'introduzione di un obbligo di segnalazione di 24 ore per gli attacchi informatici alle infrastrutture critiche, progettato per generare dati più accurati e ispirare una regolamentazione più intelligente. Questo nuovo obbligo di segnalazione porterà a informazioni più chiare sulle minacce, a un supporto più mirato e a una base più solida per la gestione del rischio informatico in un quadro nazionale coordinato. Sarà interessante vedere come questo requisito si svilupperà nel tempo.

► **Fabian Schär:** Sebbene sia difficile trarre conclusioni definitive, l'esperienza passata suggerisce che le normative sulla sicurezza informatica nel settore finanziario sono state generalmente efficaci. Tuttavia, anche i quadri normativi più solidi e le salvaguardie tecniche non possono eliminare il rischio dell'errore umano; la formazione e la consapevolezza continue sono quindi essenziali. In prospettiva, i requisiti di *reporting* obbligatorio e la maggiore trasparenza dei dati continueranno probabilmente a definire gli standard normativi, migliorando la nostra comprensione collettiva delle minacce informatiche. Tuttavia, il rispetto di scadenze rapide per il reporting, per esempio entro 24 ore, rimane una sfida, poiché le aziende hanno spesso bisogno di più tempo per valutare appieno la portata di un incidente, soprattutto quando si coordinano con parti esterne.

► **Olivier Scaillet:** Tutti nel settore finanziario sanno che dobbiamo concentrarci su quando avverrà il prossimo attacco e su come minimizzarne l'impatto, non sul fatto se avvenga o no. Anche se può sembrare frustrante, affrontare questa dura realtà permette alle aziende e al settore di prepararsi. All'interno delle aziende, si dovrebbe parlare onestamente della velocità di recupero dopo un attacco; tra le aziende, si dovrebbe parlare di come limitare i rischi comuni utilizzando una gamma più ampia di hardware e software. Sebbene le normative possano imporre molte di queste misure, esse hanno un potere limitato nell'indurre il settore ad adottare sistemi diversi. Sono preoccupato per la costante diminuzione del numero di fornitori e per la mancanza di un modo valido per invertire questa tendenza.

Quali sono le minacce emergenti alla sicurezza informatica che avranno un impatto più significativo sulla società nel prossimo decennio?

► **Fabian Schär:** Nei prossimi anni, i progressi dell'intelligenza artificiale, dei *big data* e dell'informatica quantistica porteranno la nostra sicurezza informatica a un livello superiore. Sono fermamente convinto che dovremmo sfruttare tutto il potenziale dei programmi di ricompensa per trasformare i "cattivi" in "buoni". Gli attacchi ransomware sono spesso motivati da un guadagno economico, quindi è logico che le aziende ricompensino le persone che contribuiscono a migliorare la loro sicurezza, piuttosto che pagare riscatti per rimanere a galla. Il gioco del gatto e del topo esiste fin dall'antichità e non c'è motivo di pensare che il futuro sarà diverso, solo che gli strumenti evolveranno.

► **Anastasia Kartasheva:** Nel prossimo decennio il settore finanziario si troverà ad affrontare una serie sempre più complessa di minacce alla sicurezza informatica, a causa della crescente interdipendenza digitale e dell'esposizione globale. Una sfida fondamentale sarà la verifica dell'identità di terze parti – imprese o individui – soprattutto a livello transfrontaliero, dove gli standard e le normative digitali sono diversi. Allo stesso tempo, la superficie di attacco si espanderà, grazie alla proliferazione di dispositivi connessi, al consolidamento dei sistemi informatici e alla diffusa adozione dei cloud. Queste tendenze, unite ai progressi dell'intelligenza artificiale, dell'apprendimento automatico e dell'informatica quantistica, incoraggeranno avversari più sofisticati. Insieme, imporranno un ripensamento fondamentale della fiducia, della verifica e della resilienza nella sicurezza informatica.



Swiss Finance Institute

Con il sostegno dei suoi fondatori – il settore bancario svizzero, la Confederazione svizzera e le principali università svizzere – lo Swiss Finance Institute (SFI) promuove in modo competitivo la ricerca e l'insegnamento di prim'ordine in ambito bancario e finanziario in Svizzera. Unendo l'eccellenza accademica all'esperienza pratica, l'SFI contribuisce al potenziamento della piazza finanziaria svizzera.

Editore e contatto

Dr. Cyril Pasche
Director Knowledge Exchange and Education
+41 22 379 88 25
cyril.pasche@sfi.ch

swiss:finance:institute

Walchestr. 9, CH-8006 Zurich, T +41 44 254 30 80
c/o University of Geneva, 42, Bd du Pont d'Arve, CH-1211 Geneva 4, T +41 22 379 84 71
www.sfi.ch

