QBE
At the heart of it

Copertura digitale

Prevedere le interruzioni tecnologiche in un clima dominato dal crimine informatico

Tre cose da ricordare:

1. Come l'adozione del cloud e dell'intelligenza artificiale può aumentare l'efficienza, ma anche esporre le aziende a maggiori rischi.

2. Come gli attori delle minacce cyber si stanno evolvendo, utilizzando nuovi strumenti e vecchie tattiche per attaccare le aziende.

3. Come le aziende possono gestire i rischi associati alla tecnologia, affinché la resilienza sia incorporata nella pianificazione e non applicata successivamente.

L'adozione dell'IA e le potenzialità delle piattaforme cloud stanno trasformando il business – ma la velocità e la portata di questo cambiamento repentino offrono terreno fertile per ransomware, frodi e interruzioni causate da terze parti

Il passaggio a piattaforme cloud pubbliche, private e ibride sta efficientando i processi, favorendo l'automazione e supportando l'adozione dell'intelligenza artificiale (IA). Questi progressi permettono vantaggi competitivi, ma vanno collocati in un contesto di minacce in rapida evoluzione. Man mano che aumenta la dipendenza delle aziende dai servizi cloud, aumentano anche le vulnerabilità che gli hacker possono sfruttare, come controlli carenti sull'identità, errori di configurazione e dati non protetti adeguatamente.

L'intelligenza artificiale generativa (GenAI) ha come effetto collaterale quello di amplificare le vulnerabilità e i rischi cyber, permettendo agli attori malevoli di agire con maggiore velocità e precisione e abbassando le barriere tecniche per i criminali informatici alle prime armi. I sempre più numerosi hacker che utilizzano la GenAI per violare i sistemi di sicurezza espongono le aziende a interruzioni operative che possono avere ripercussioni finanziarie, reputazionali e potenzialmente anche normative. Le minacce legate all'uso della GenAI si sono già concretizzate in truffe deepfake±, frodi di identità e attacchi di phishing† automatizzati. Gli episodi di ransomware continuano ad aumentare di conseguenza,con l'IT-ISAC che ha registrato 1.537 attacchi ransomware nel primo trimestre 2025, rispetto ai 572 del primo trimestre 2024, e le interruzioni che ne derivano rappresentano ormai un rischio fondamentale per le organizzazioni dipendenti da terze parti, inclusi i fornitori cloud.

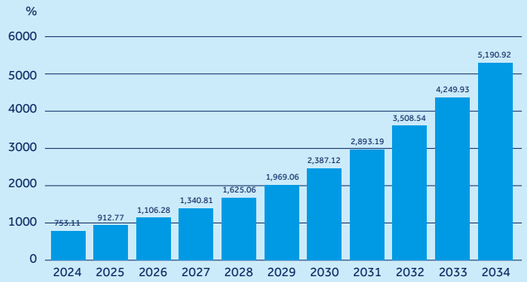
Glossario

± **Deepfake:** tecnologia basata sull'IA usata per produrre contenuti video o audio artificiali che appaiono convincenti e realistici.

† **Phishing:** tentativo di ottenere informazioni riservate e confidenziali dagli utenti di internet, come nomi utente, password e dati delle carte di credito. I cybercriminali inviano solitamente e-mail o contattano le vittime tramite messaggistica istantanea, fingendosi corrispondenti legittimi o ufficiali. Queste e-mail o messaggi di phishing spesso contengono link infetti da malware.

È essenziale un approccio proattivo, incentrato sulla resilienza. Le aziende devono integrare la gestione del rischio nei propri sistemi tecnologici, anticipare le vulnerabilità delle terze parti e incorporare nei processi la pianificazione della continuità operativa.

Figure 1: Valore previsto del mercato globale del cloud computing per anno (miliardi di USD)



Control Risks – Fonte: Precedente ricerca[1]

L'ampia diffusione del cloud rende urgente il controllo dei rischi associati. Si prevede che il mercato globale superi i 5.000 miliardi di USD entro il 2034, rispetto ai 912 miliardi del 2025.[2] Con il trasferimento di infrastrutture e dati sui server cloud da parte di un numero crescente di organizzazioni, quei server diventeranno obiettivi preziosi. Gli alert cloud ad alta gravità sono aumentati del 235% nel corso del 2024 rispetto all'anno precedente[3], riflettendo sia l'impennata nell'adozione del cloud sia la crescente capacità degli attori malevoli.

La maggior parte degli attacchi ospitati nel cloud si concentra sul Business Email Compromise (BEC).[4] I criminali informatici sfruttano piattaforme come Microsoft 365 per lanciare campagne di phishing BEC, che possono consentire il controllo degli account o il furto di credenziali, utilizzando una piattaforma cloud affidabile invece di domini falsificati (typosquatted‡) o email contraffatte[5] (spoofing). Questo significa che tali attacchi possono essere portati a termine senza attivare molte delle misure di sicurezza comuni. Inoltre, attori legati a stati nazionali e gruppi cybercriminali sofisticati stanno privilegiando minacce specifiche al cloud per colpire le infrastrutture digitali.

1 precedenceresearch.com/cloud-computing-market
2 precedenceresearch.com/cloud-computing-market
3 unit42.paloaltonetworks.com/2025-cloud-security-alert-trends
4 ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index
5 guardz.com/blog/sophisticated-phishing-campaign-exploiting-microsoft-365-infrastructure

Glossario

‡ **Typosquatting:** pratica di registrare versioni comunemente errate di domini legittimi per diffondere malware tramite link in e-mail di phishing o mediante download automatici. Ad esempio, una variante del dominio legittimo example.com potrebbe essere registrata dolosamente come exxample.com.

** **Email spoofing:** tecnica con cui un aggressore falsifica l'indirizzo del mittente in un'e-mail per mascherarne la vera origine, facendo sembrare che provenga da una fonte affidabile.

Doppia esposizione: ransomware e phishing

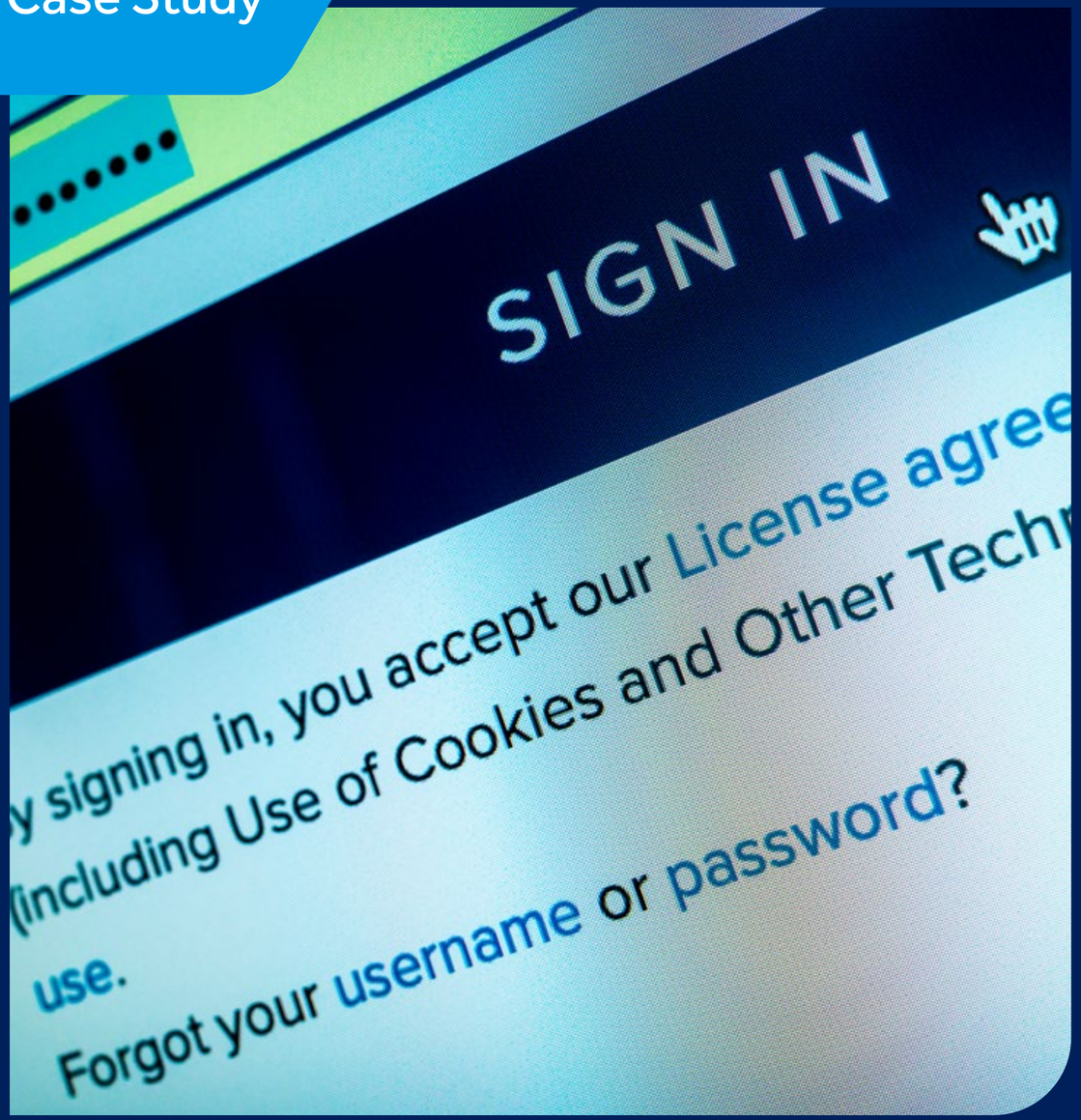
Quasi la metà dei dati aziendali archiviati nei server cloud è classificata come sensibile,[6] il che li rende particolarmente appetibili per gli operatori di ransomware. Le nuove varianti di questi malware sono progettate per individuare e colpire strumenti di collaborazione basati su cloud, e gli aggressori sono sempre più in grado di muoversi lateralmente tra sistemi on-premises e cloud, criptando o esfiltrando dati lungo il percorso.[7]

Il phishing resta il principale punto di accesso, rappresentando il canale tramite cui è stato perpetrato un terzo delle intrusioni nel 2023 e nel 2024.[8] Spesso gli aggressori ricorrono a tecniche di phishing per rubare credenziali attraverso attacchi adversary-in-the-middle (AITM)‡. Gli attori delle minacce hanno inoltre ottenuto successo nello sfruttare vulnerabilità delle applicazioni cloud, utilizzando credenziali legittime rubate e accedendo a utenti privilegiati o conti di servizio.

6 cpl.thalesgroup.com/resources/webinars?commid=615147&bt_tok=%7b%7bRecipient.ID%7d%7d
7 microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments
8 ibm.com/new/announcements/x-force-cloud-threat-landscape

Glossario

‡ **Adversary-in-the-middle (AITM) attack:** noto anche come man-in-the-middle (MITM) attack, indica la situazione in cui un attore malevolo si inserisce in una conversazione tra l'utente (vittima) e il sistema. La posizione dell'aggressore gli consente di intercettare, inviare e ricevere dati destinati a uno degli interlocutori legittimi o che non erano affatto destinati a essere trasmessi.



Okta, 2023

Il fornitore di single sign-on (SSO) Okta è stato compromesso quando un gruppo di aggressori non identificati ha rubato credenziali ottenendo accesso al suo sistema di gestione dei ticket di supporto. Sono stati sottratti dati sensibili, tra cui cookie e token di sessione, consentendo l'impersonificazione di utenti validi.

Un cliente, 1Password – un gestore di password con oltre 100.000 utenti business – ha rilevato attività sospette sul proprio account Okta (usato per applicazioni interne) il 29 settembre, interrompendo immediatamente l'attività e avviando un'indagine.[9] Okta non ha notificato a 1Password la violazione fino al 19 ottobre, ben 16 giorni dopo, nonostante un altro cliente, BeyondTrust, avesse segnalato a Okta una violazione già il 2 ottobre.[10]

In totale, 134 clienti business di Okta sono stati colpiti e la società ha subito una perdita di 2 miliardi di USD in valore di mercato.[11,12]

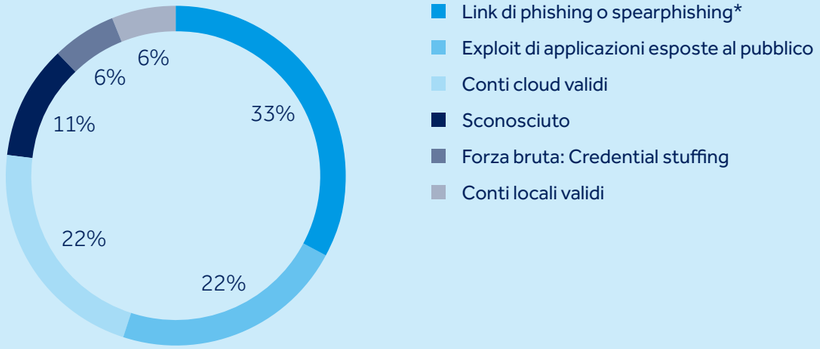
9 arstechnica.com/security/2023/10/1password-detects-suspicious-activity-in-its-internal-okta-account
10 portnox.com/blog/cyber-attacks/unpacking-the-okta-data-breach
11 nightfall.ai/blog/okta-data-breach-what-happened-impact-and-security-lessons-learned
12 cnbc.com/2023/10/23/okta-hack-wipes-out-more-than-2-billion-in-market-cap.html

Supply chain e dipendenze da terze parti

La crescente convergenza tra archiviazione e gestione dei dati ha reso i fornitori terzi un obiettivo particolarmente attraente per i criminali informatici di qualsiasi livello, dal momento che i dati stanno acquisendo sempre più valore nei marketplace del cybercrimine, e un singolo fornitore compromesso può mettere a rischio contemporaneamente anche centinaia di aziende.

Entro il 2025, il volume dei dati archiviati a livello globale dovrebbe raggiungere i 200 zettabyte (200 mila miliardi di gigabyte) tra infrastrutture IT private e pubbliche, infrastrutture di servizio, data center cloud pubblici e privati, dispositivi personali e dispositivi IoT.[13] La metà di questi dati sarà archiviata nel cloud, rispetto al 43% nel 2024[14], a una stima del 15% nel 2020[15] e a solo il 10% nel 2015.[16] Questa concentrazione di dati preziosi rende i fornitori di servizi cloud e di archiviazione particolarmente appetibili per gli aggressori.

Figure 2: Attacchi agli ambienti cloud, per vettore di accesso iniziale (2022-24)



Control Risks – Fonte: IBM[17]

13 cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/
14 storagenewsletter.com/2023/01/25/43-of-data-to-be-stored-in-public-cloud-by-2024-on-average/
15 gartner.com/en/documents/3989101
16 statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/
17 ibm.com/new/announcements/x-force-cloud-threat-landscape

Glossario

* **Spearphishing:** forma più mirata di phishing che si concentra su gruppi specifici di persone che condividono una caratteristica comune. Ad esempio, possono lavorare nella stessa azienda, frequentare la stessa università, usare gli stessi servizi finanziari o istituti, o acquistare dagli stessi siti web.

Esempio

MURKY PANDA, 2023-in corso

MURKY PANDA, un attore di minaccia prolifico legato a uno stato nazionale in Cina, è stato scoperto mentre sfruttava vulnerabilità zero-day nei fornitori di software-as-a-service (SaaS) per ottenere accesso alle loro reti. Il gruppo è in grado di superare le difese e restare invisibile all'interno dei sistemi dei clienti per lunghi periodi, beneficiando così di un accesso prolungato a dati riservati. MURKY PANDA ha inoltre compromesso un fornitore di soluzioni cloud Microsoft, abusando dei privilegi amministrativi delegati destinati al personale IT e tecnico.[18]

Il gruppo rappresenta una minaccia seria per enti governativi, tecnologici e di servizi professionali in Nord America, in particolare per le azioni di compromissione di fornitori con accesso a informazioni sensibili. Gli ambienti cloud sono estremamente vulnerabili alle capacità avanzate di MURKY PANDA e alla sua conoscenza della logica applicativa personalizzata, che consente di sfruttare le funzionalità delle applicazioni anziché basarsi esclusivamente su vulnerabilità tecniche.

18 crowdstrike.com/en-us/blog/murky-panda-trusted-relationship-threat-in-cloud

Attori statali

I gruppi legati a stati nazionali stanno sfruttando sempre più le vulnerabilità nei sistemi cloud.

GenAI: difesa o arma?

La GenAI sta rimodellando lo scenario delle minacce informatiche. Il suo utilizzo e i marketplace sono destinati a crescere nei prossimi cinque anni in Nord America e in Europa, poiché gli strumenti GenAI apportano benefici di produttività in moltissimi settori.

- ChatGPT conta 755 milioni di utenti attivi e Microsoft Copilot 88 milioni nel 2025.[19]
- Gli utenti di ChatGPT sono aumentati del 33% tra dicembre 2024 e febbraio 2025.[20]
- Il 78% delle organizzazioni utilizza l'IA in almeno una funzione aziendale nel 2025, rispetto al 55% nel 2024.[21]
- Il 20-40% dei dipendenti utilizza attivamente l'IA nelle proprie mansioni, in particolare nella programmazione.[22]

Contemporaneamente, l'uso improprio della stessa tecnologia per frodi ed estorsioni si è affermato come una minaccia diffusa. La frode resa possibile dai deepfake, in cui i cybercriminali impersonano dirigenti, membri dei consigli di amministrazione e figure pubbliche utilizzando voci, video e immagini sintetiche, rappresenta un'evoluzione particolarmente allarmante.

Queste tattiche vengono impiegate per ingannare i dipendenti inducendoli a trasferire ingenti somme di denaro su conti non autorizzati controllati da reti criminali. Nel 2024, i deepfake sono stati utilizzati in quasi il 10% degli attacchi informatici andati a segno, con perdite finanziarie comprese tra 250.000 USD e oltre 20 milioni di USD. [23]

19 firstpagesage.com/seo-blog/chatgpt-usage-statistics
20 demandsage.com/chatgpt-statistics
21 sqmagazine.co.uk/ai-tools-usage-statistics
22 sqmagazine.co.uk/ai-tools-usage-statistics
23 Control Risks

Esempio

Società senza nome di Singapore, 2024

Un dipendente di una multinazionale a Singapore è stato ingannato da un cyber criminale che si spacciava per il CFO. Convinto che la videochiamata fosse autentica, il dipendente ha autorizzato un trasferimento di quasi 500.000 USD.[24] Sebbene il denaro sia stato rintracciato e bloccato dalle forze di polizia di Singapore e Hong Kong, l'incidente ha comportato costi significativi di risposta e di remediation.

24 channelnewsasia.com/singapore/deepfake-scam-impersonate-ceo-company-finance-director-5048706

Gli aggressori sponsorizzati da Stati usano inoltre la GenAI per scrivere codici malevoli, sfruttando i large language model (LLM) per condurre attività di ricognizione e ampliare le operazioni di malware. Tali attori possono anche prendere di mira gli LLM utilizzati dalle aziende per funzioni interne, causando interruzioni e problemi di integrità che compromettono le operazioni.

I gruppi di cybercriminali stanno sfruttando sempre più la GenAI e le tecnologie deepfake per condurre attacchi a fini finanziari su scala globale e trasversale ai settori. La GenAI è in grado di creare modelli di phishing efficaci o condurre campagne di social engineering altamente sofisticate e con grande rapidità. Criminali informatici con competenze limitate hanno utilizzato l'IA per supportare lo sviluppo di script e la scrittura di malware.[25] Sta aumentando la probabilità che le aziende debbano affrontare un aumento di attacchi da parte di gruppi precedentemente considerati troppo inesperti dal punto di vista tecnico o troppo poveri di risorse per rappresentare una minaccia concreta.[26] Solo tra gennaio e aprile 2025 i casi di estorsione tramite ransomware resi pubblici sono aumentati del 54% rispetto allo stesso periodo dell'anno precedente.[27]

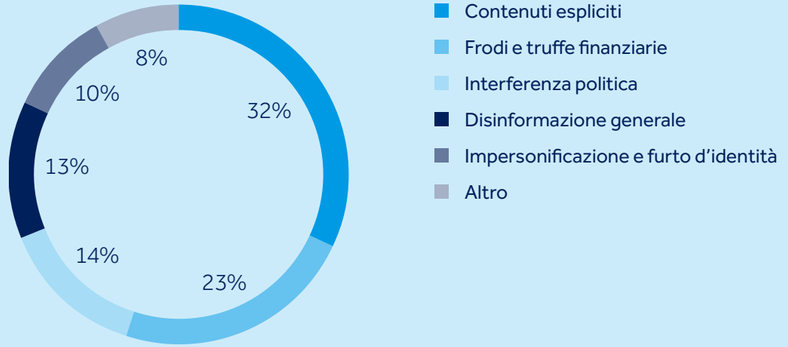
25 hp.com/us-en/newsroom/press-releases/2024/ai-generate-malware.html
26 anthropic.com/news/detecting-countering-misuse-aug-2025
27 Control Risks

Amazon, 2025

Un hacker etico ha evidenziato gravi vulnerabilità nell'estensione Q di Amazon per Visual Studio Code presentando una pull request malevola. Utilizzando soltanto un account GitHub non privilegiato, all'hacker sono state concesse inavvertitamente credenziali di livello amministrativo. Questo accesso gli ha consentito di istruire l'assistente a ripristinare le impostazioni di fabbrica, cancellare i file system locali ed eliminare i database delle risorse cloud. L'aggressore, che ha descritto l'esercizio come un'esposizione del "teatro della sicurezza IA" di Amazon, non ha avuto bisogno di malware sofisticati per riuscire nell'attacco – evidenziando le debolezze nell'architettura e nei controlli di sicurezza delle terze parti.[28] Sebbene nessun dato sensibile sia stato distrutto, l'incidente potrebbe ispirare attacchi simili ai servizi di sicurezza e di assistenza basata su IA di Amazon.

28 404media.co/hacker-plants-computer-wiping-commands-in-amazons-ai-coding-agent

Figure 3: Tipologia di contenuti negli attacchi deepfake, T1 2025



Control Risks – Fonre: Resemble AI[29]

Il costo della compromissione

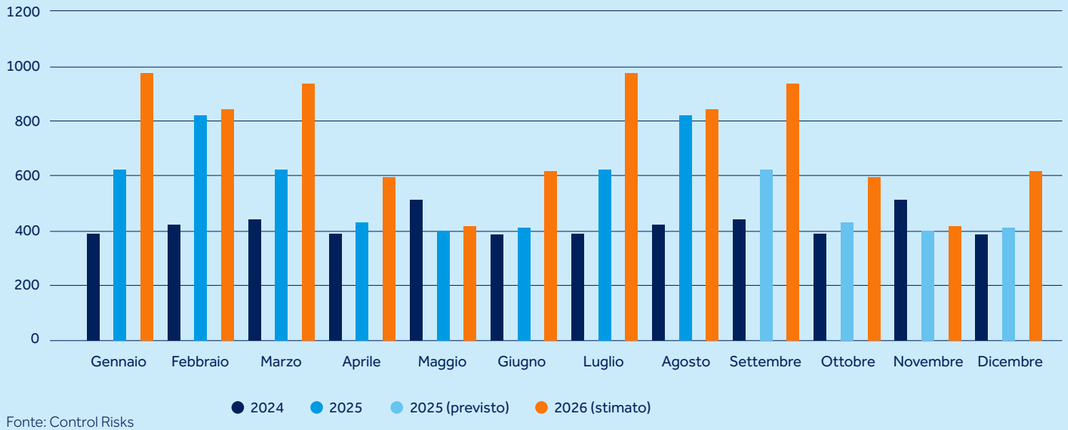
Gli attacchi ransomware possono causare perdite finanziarie, danni alla reputazione e persino azioni legali, non solo per l'azienda colpita, ma anche per i fornitori e i loro clienti. La diffusione dell'adozione dei servizi cloud e di altre tecnologie emergenti ha coinciso negli ultimi anni con un costante aumento dell'attività ransomware. Un esempio è la vasta ondata di attacchi contro organizzazioni del settore retail e finanziario guidata dal gruppo cybercriminale Scattered Spider nel Regno Unito, nel maggio 2025. Il gruppo si è avvalso di tecniche avanzate di social engineering e phishing per introdursi nei sistemi, impersonando piattaforme affidabili tramite domini typosquatted di fornitori SaaS terzi e kit di phishing che inducevano le vittime a cedere credenziali e dati di sessione.[30]

29 resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf
30 reliaquest.com/blog/scattered-spider-cyber-attacks-using-phishing-social-engineering-2025

Le organizzazioni di tutto il mondo continuano a subire gravi interruzioni a causa di malfunzionamenti delle terze parti.. Negli ultimi due anni numerosi settori sono stati colpiti da blackout di massa e incidenti informatici originati da terze parti. Uno dei più rilevanti è stato l'aggiornamento difettoso del Falcon Sensor di CrowdStrike nel 2024, che ha interessato circa 8,5 milioni di dispositivi Windows. Sebbene ciò rappresentasse meno dell'1% di tutte le macchine Windows, l'interruzione ha avuto conseguenze globali, con sanità, aviazione e altri trasporti tra i settori più colpiti.

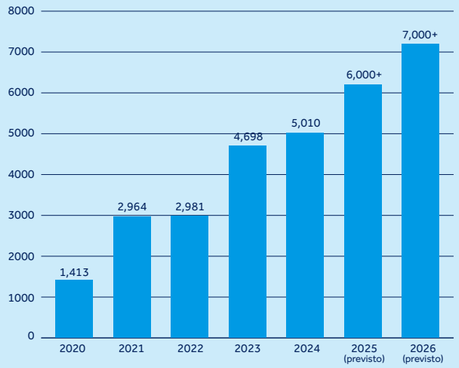
I cybercriminali hanno rapidamente sfruttato la situazione, lanciando campagne di phishing successive che utilizzavano esche legate a CrowdStrike per compromettere i sistemi, rubare dati ed estorcere denaro alle vittime. Sebbene l'incidente non fosse un attacco mirato, ha messo in evidenza l'impatto sistemico che tali malfunzionamenti possono avere sulle organizzazioni che dipendono dai SaaS per funzioni aziendali critiche. Episodi precedenti, come la campagna di vulnerabilità di massa MOVEit e il massiccio attacco informatico NotPetya, hanno dimostrato effetti a catena simili, danneggiando clienti a valle ben oltre il punto di compromissione originale.

Figure 4: Numero mensile previsto di vittime di ransomware elencate sui siti di data leak



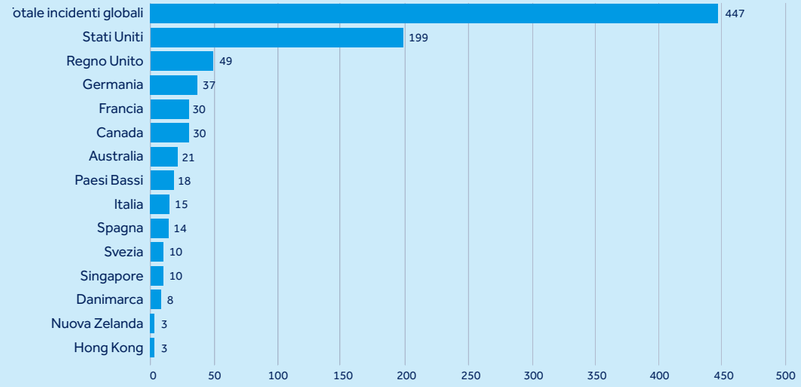
Fonte: Control Risks

Figure 5: Numero totale di vittime di ransomware citate nei siti di data leak (a livello globale)



Fonte: Control Risks

Figure 6: Numero di incidenti informatici significativi registrati per area geografica (agosto 2023 - agosto 2025)



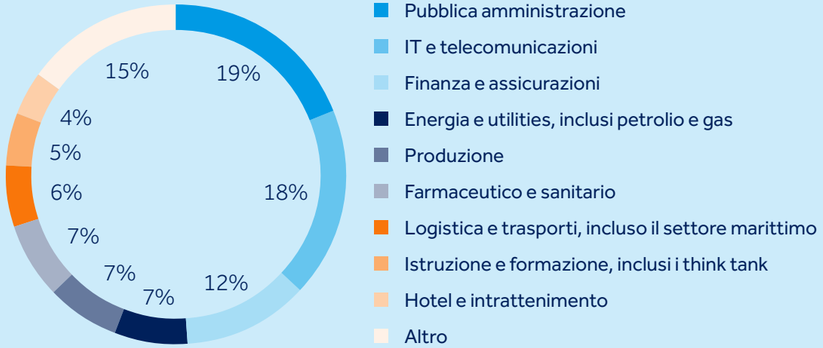
Fonte: Control Risks

Rackspace, 2022

Nel 2022, il gruppo di ransomware Play ha interrotto il servizio Hosted Exchange di Rackspace sfruttando una vulnerabilità zero-day di escalation dei privilegi in Microsoft Exchange. Almeno 27 clienti Hosted Exchange sono stati colpiti dopo che gli aggressori hanno ottenuto l'accesso iniziale tramite credenziali compromesse, bloccando l'accesso alle e-mail in tutte le loro organizzazioni.[31] Le conseguenze sono state significative: Rackspace è stata costretta a interrompere il proprio servizio Hosted Exchange, ha affrontato numerose cause legali da parte dei clienti ed è stata accusata di aver subito perdite per circa 11 milioni di USD.[32]

31 ir.rackspace.com/news-releases/news-release-details/update-recent-cybersecurity-incident
32 msspalert.com/news/rackspace-taking-losses-of-roughly-11-million-for-hosted-exchange-ransom-attack

Figure 7: Incidenti informatici che colpiscono i mercati chiave, per settore (agosto 2023 - agosto 2025)



Fonte: Control Risks

A livello globale, le organizzazioni affrontano rischi crescenti di inattività operativa, perdite finanziarie e danni reputazionali, mentre i criminali sfruttano una superficie d'attacco in continua espansione. L'uso sempre più diffuso di servizi di terze parti come cloud hosting, software esterni o strumenti di IA nelle operazioni quotidiane ha offerto agli attori delle minacce maggiori opportunità per colpire.

Resilienza by design

Se l'adozione del cloud e l'integrazione dell'IA accelereranno al ritmo previsto, gli aggressori continueranno a sfruttare maggiori opportunità e punti di accesso, e le aziende resteranno vulnerabili agli attacchi. È essenziale disporre di una strategia solida per anticipare e resistere agli incidenti informatici, in particolare quelli derivanti da servizi di terze parti e ambienti cloud che oggi sostengono funzioni aziendali critiche.

Costruire resilienza significa integrare la gestione del rischio informatico nei cicli di vita della tecnologia fin dall'inizio. Ciò implica l'implementazione di solidi protocolli di gestione delle identità e degli accessi (IAM), l'esecuzione di audit di configurazione regolari e la crittografia dei dati sensibili in tutti gli ambienti cloud. Misure proattive come il monitoraggio continuo, la threat intelligence e i piani di risposta agli incidenti aiutano a rilevare e contenere le minacce prima che si intensifichino.

Le aziende dovrebbero inoltre valutare il livello di sicurezza dei propri fornitori terzi e stabilire protocolli chiari per la gestione del rischio lungo la supply chain. Adottando congiuntamente queste pratiche, le organizzazioni proteggeranno meglio le operazioni, preserveranno la continuità e manterranno la fiducia in un panorama informatico sempre più instabile.

Costruire resilienza significa integrare la gestione del rischio informatico nei cicli di vita della tecnologia. Questo implica protocolli solidi di gestione delle identità e degli accessi, audit regolari delle configurazioni e crittografia dei dati sensibili.

Esempio

Microsoft Azure, 2024

Nel luglio 2024, un attacco distributed denial-of-service (DDoS) ha interrotto l'operatività della piattaforma cloud Azure di Microsoft, mettendola offline per oltre otto ore. L'interruzione è stata causata da un picco di utilizzo che ha interessato Azure Front Door e la Content Delivery Network. Successivamente, un errore nell'implementazione delle difese ha amplificato l'impatto invece di contenerlo.[33]

33 forbes.com/sites/kateoflahertyuk/2024/07/31/microsoft-confirms-new-outage-was-triggered-by-cyberattack

Passaggi per costruire la cyber resilience

Le organizzazioni mature possono costruire una cyber resilience efficace attraverso diverse azioni:

Comprendere e indicizzare i profili di rischio per identificare asset critici, minacce e vulnerabilità e avere una visione chiara delle esposizioni organizzative.

Definire il livello di rischio organizzativo accettabile affinché la leadership possa stabilire chiari limiti di esposizione.

Dare priorità alle strategie di mitigazione del rischio che concentrino le risorse dove avranno il massimo impatto.

Prepararsi agli scenari peggiori con piani di contingenza e protocolli di ripristino collaudati.

Testare le capacità di gestione delle crisi sottoponendo a stress test il processo decisionale, la comunicazione e la risposta alla crisi.

Integrare il supporto delle terze parti nella strategia di cybersicurezza per fornire competenze nella gestione dei rischi residui.

Monitorare proattivamente le tendenze e adattare le difese informatiche per rimanere al passo con le minacce in evoluzione, le nuove tecnologie e le mutevoli esigenze aziendali.

Al cuore delle analisi degli assicuratori

Stefano Pompeo
Cyber Senior Underwriter

La nuova edizione del Cyber Resilience Report mostra che cloud e intelligenza artificiale stanno cambiando il modo in cui le aziende italiane affrontano la sicurezza informatica. I rischi evolvono rapidamente – ransomware, phishing e attacchi alle supply chain sono ormai una realtà anche per le PMI. Come sottoscrittori, osserviamo ogni giorno quanto sia importante investire nella resilienza cyber: non basta rispettare le regole, serve una strategia che coinvolga persone, processi e partner.

Solo così possiamo proteggere il business e costruire fiducia nel digitale.Mentre le aziende italiane accelerano l'adozione di infrastrutture cloud e strumenti basati sull'intelligenza artificiale, il panorama dei rischi si trasforma rapidamente. Le minacce descritte in questo report sono già attive e riflettono le tendenze che osserviamo quotidianamente nel mercato italiano. Per molti risk manager, la sfida non è solo quella di mitigare i rischi, ma anche di colmare il divario rispetto a esposizioni già esistenti, che evolvono con estrema rapidità.

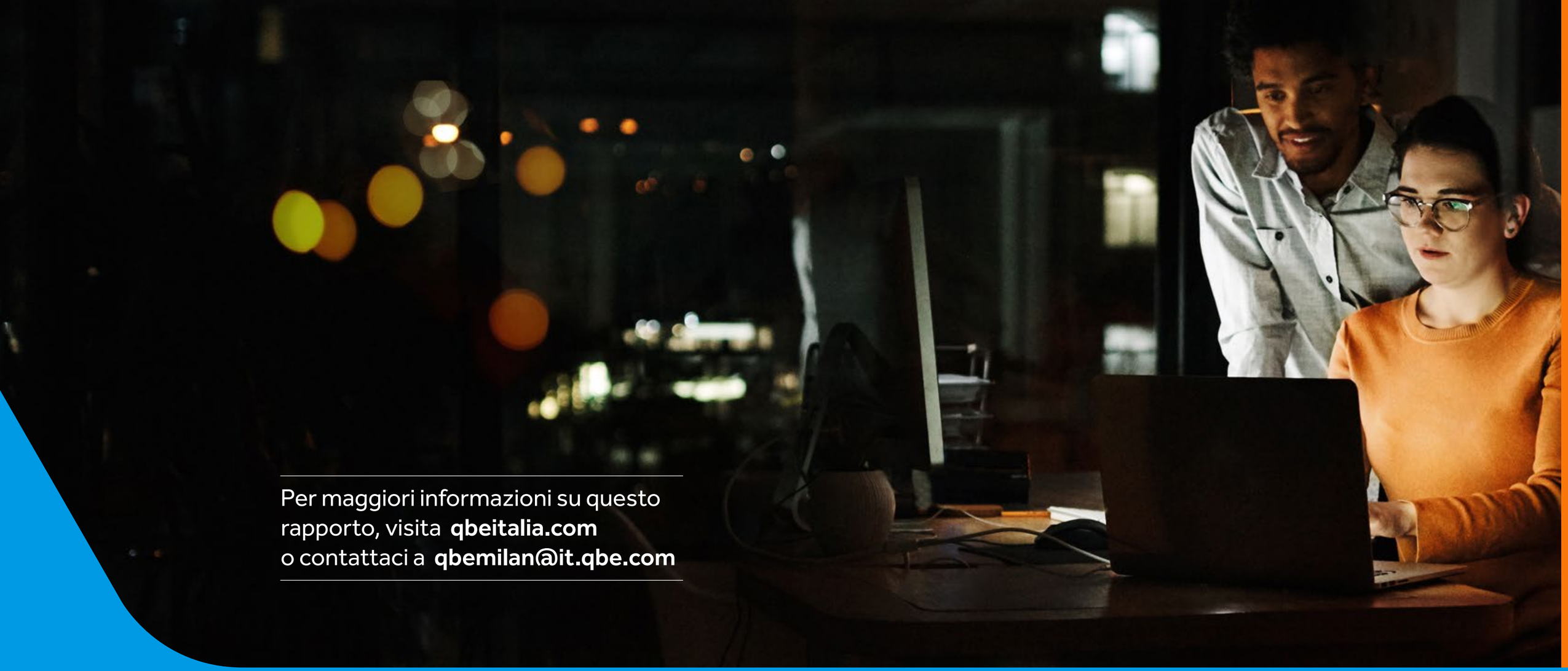
La minaccia alla supply chain continua a destare preoccupazione anche in Italia. L'esternalizzazione di processi aziendali può portare efficienze e risparmi, ma ogni fornitore connesso ai sistemi aziendali rappresenta un potenziale punto di vulnerabilità. Un'interruzione in un nodo critico può bloccare l'intera operatività. È quindi fondamentale mappare con precisione le connessioni esterne e valutare l'impatto di eventuali disservizi.

Copertura digitale: prevedere le interruzioni tecnologiche in un clima dominato dal crimine informatico

Nel nostro Paese, eventi come il caso CrowdStrike del luglio 2024 – che ha causato danni stimati in miliardi di euro a livello globale – hanno evidenziato quanto le interdipendenze tecnologiche siano pervasive e quanto sia urgente rafforzare la resilienza. Il 37% dei manager italiani ha dichiarato di aver potenziato le misure di protezione dopo quell'incidente.

Anche il quadro normativo italiano si sta evolvendo. Le aziende devono oggi confrontarsi con obblighi sempre più stringenti in materia di gestione degli incidenti, protezione dei dati e comunicazione verso stakeholder e autorità. La collaborazione con esperti legali, forensic IT e professionisti della comunicazione è diventata parte integrante della gestione del rischio cyber.

Per gli underwriter cyber, l'espansione delle superfici di attacco e l'evoluzione normativa richiedono una valutazione rigorosa della resilienza aziendale. Non basta più proteggere il perimetro: è necessario adottare un approccio "resilience by design", che includa governance strutturata, test di stress e architetture robuste. Le aziende che dimostrano una gestione del rischio solida e proattiva saranno valutate positivamente, con impatti diretti su condizioni di copertura e premi.



Per maggiori informazioni su questo rapporto, visita **qbeitalia.com** o contattaci a **qbemilan@it.qbe.com**

QBE Europe SA/NV
Rappresentanza Generale per l'Italia Via Melchiorre Gioia 8
20124 Milano, Italy
+39 02 3626 3500

QBEitalia.com

Questo resoconto è stato sviluppato per QBE da Control Risks

QBE
At the heart of it

963704/2510-IT