Attività connesse: la dipendenza digitale aumenta il rischio

QBE

Introduzione

Le persone e le organizzazioni di tutto il mondo fanno sempre più affidamento sulle tecnologie digitali. I computer e gli strumenti che utilizzano l'intelligenza artificiale (IA) consentono di automatizzare attività semplici e complesse, mentre grazie ai dispositivi Smart fabbriche, veicoli e altre apparecchiature possono essere collegate a Internet.

I mercati tecnologici globali cresceranno in modo esponenziale nei prossimi cinque anni. Si prevede che il mercato dell'AI-as-a-service crescerà di ben nove volte, passando da circa 200 miliardi di dollari a 1.850 miliardi di dollari, quello del software-as-a-service di tre volte, toccando gli 850 miliardi di dollari, e quello dell'infrastruttura-as-a-service di cinque volte, per un valore pari a 532 miliardi di dollari, a dimostrazione della portata delle opportunità offerte dalle tecnologie digitali emergenti.

Allo stesso tempo però questo allargherà il campo dei criminali informatici, che rubano dati riservati per estorcere e frodare aziende di qualsiasi dimensione e settore, e di altri malintenzionati che usano la tecnologia per destabilizzare i competitor oppure imporre le proprie strategie ideologiche.

Interruzione tecnologica globale

L'interruzione di massa dei sistemi che eseguono il Falcon Sensor di CrowdStrike, avvenuta il 19 luglio scorso, ha mostrato l'interdipendenza e la vulnerabilità dei sistemi tecnologici globali. A causa dell'interruzione del servizio, le aziende Fortune 500 hanno subito un danno stimato di 5,4 miliardi di dollari e di 25 miliardi di dollari in valore azionario - senza contare Microsoft.

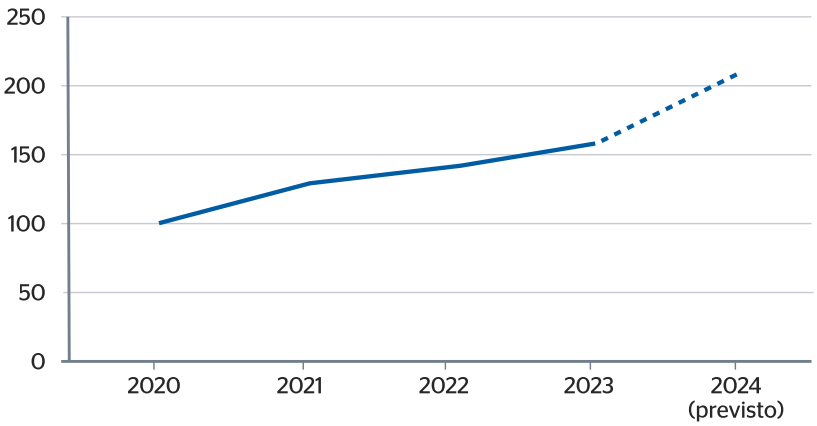
L'aggiornamento dei contenuti difettosi di CrowdStrike ha messo fuori uso circa 8,5 milioni di computer Windows (meno dell'1% di tutti i dispositivi di questo tipo in circolazione), mettendo in crisi qualsiasi settore in tutto il mondo ma soprattutto l'aviazione, i trasporti e la sanità. I criminali informatici hanno colto l'occasione per lanciare campagne di phishing ingannevoli che rimandavano a CrowdStrike, cercando di compromettere i sistemi, rubare dati ed estorcere denaro alle vittime. Anche se in questo caso si è trattato di un errore piuttosto che di un attacco intenzionale, molti incidenti informatici di questa portata sono e saranno deliberati.

A giugno 2017, l'attacco informatico di massa NotPetya era mirato alle organizzazioni ucraine, ma alla fine si allargò anche nel resto d'Europa, in Nord America e nella regione Asia-Pacifico. Questo malware, mascherato da ransomware, colpì settori critici come i trasporti, la logistica e le spedizioni, causando danni stimati per 10 miliardi di dollari. Sebbene abbia colpito un numero molto inferiore di dispositivi rispetto all'incidente di CrowdStrike, la sua natura intenzionale ha provocato danni di dimensioni maggiori.

Con l'aumento delle interdipendenze tecnologiche, ci aspettiamo che un numero crescente di incidenti informatici possa danneggiare più aziende con un unico attacco, il che significa che le aziende avranno maggiori probabilità di subire un evento dannoso. Si prevede inoltre che aumenteranno gli attacchi mirati ad aziende specifiche, al fine di estorcere riscatti o destabilizzare competitor.

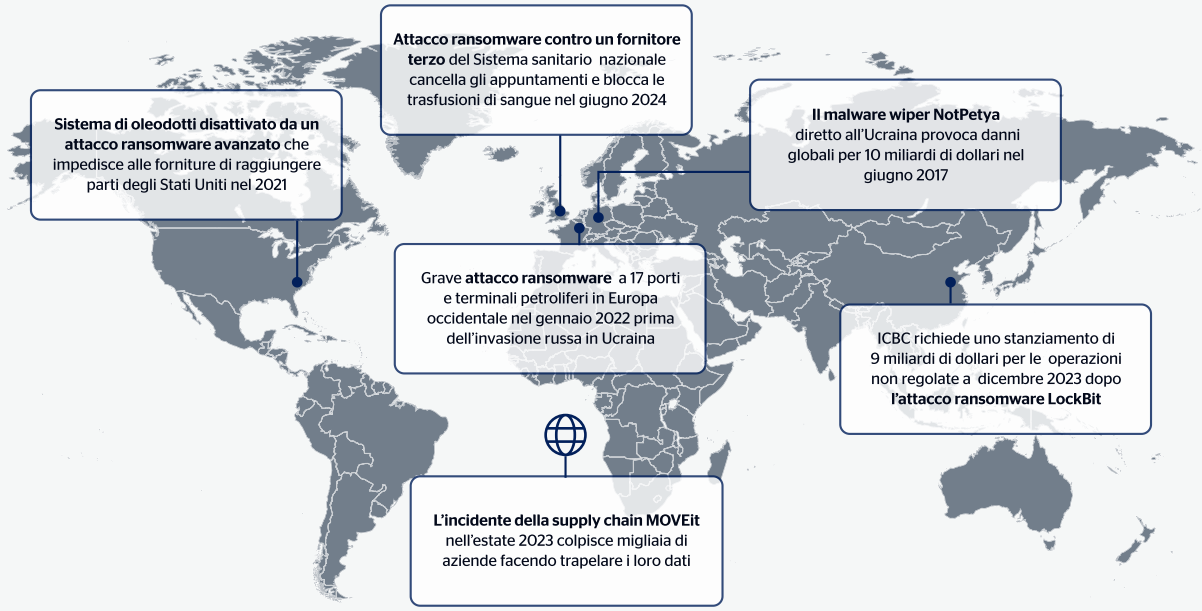
> Il disservizio di CrowdStrike ha provocato alle aziende Fortune 500 un danno stimato di 5,4 miliardi di dollari e una perdita di valore azionario di 25 miliardi di dollari.

Numero di attachi informatici distruttivi e dannosi registrati a partire dal 2020



Fonte: Control Risks

Episodi significativi di minacce informatiche dannose a partire dal 2017



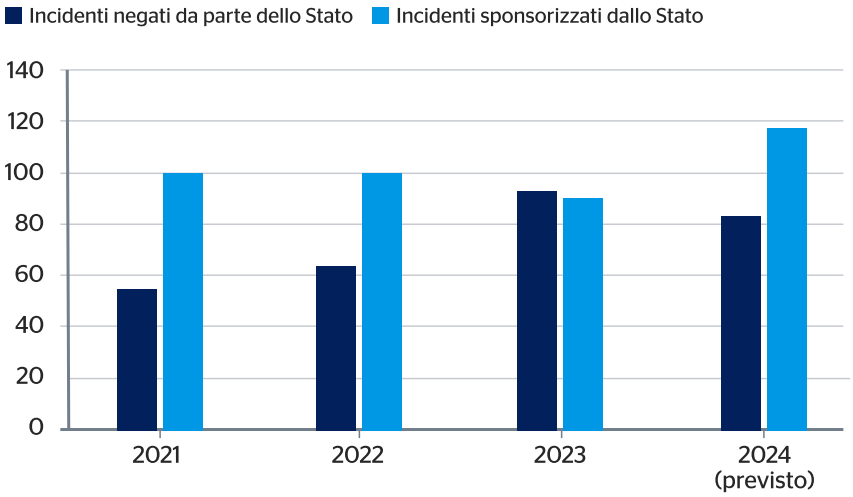
Attacchi spillover

La crescente rivalità geopolitica sta rendendo il mondo sempre più multipolare. Stanno aumentando gli attacchi perpetrati da criminali legati agli Stati e diretti contro infrastrutture critiche nazionali (critical national infrastructure, CNI), ad esempio attraverso il ransomware. Questi attacchi possono essere determinati da eventi geopolitici, come i conflitti in corso tra Israele e Hamas o tra Ucraina e Russia, manifestandosi come attacchi di criminali informatici o attivisti diretti dallo Stato contro entità in settori strategici, come quello energetico.

Il settore dell'energia è uno di quelli più presi di mira dagli attacchi cyber spillover.

Le sovvenzioni degli Stati a questi attivisti informatici sono fatte in modo da poter negare la propria responsabilità e proteggersi dall'attribuzione o da sanzioni diplomatiche. Le organizzazioni CNI sono obiettivi ambiti per le minacce spillover, poiché gli autori delle minacce ritengono di poterle danneggiare senza necessariamente provocare una risposta sul campo di battaglia. Stanno proliferando anche unità di spionaggio mascherate da gruppi di ransomware mossi per scopi finanziari che prendono di mira la proprietà intellettuale e i dati aziendali sensibili.

Numero di attacchi proxy non statali significativi e di campagne registrate legate allo Stato a partire dal 2021



Fonte: Control Risks

Attacchi ransomware legati alla Russia contro 17 terminali petroliferi europei, prima dell'invasione dell'Ucraina

A gennaio 2022, una serie di attacchi ransomware su larga scala ha preso di mira alcuni terminali portuali in Belgio, Germania e Paesi Bassi. Gli attacchi, che con ogni probabilità hanno avuto origine da autori spalleggiati dalla Russia, hanno messo fuori uso i sistemi informatici, compromettendo le operazioni di carico dei prodotti petroliferi nei porti. Gli attacchi sono stati condotti tre settimane prima dell'invasione dell'Ucraina da parte della Russia, dimostrando come gli attacchi spillover prendano di mira anche settori e territori secondari.

Nel 2023 gli attacchi ransomware sono aumentati del 74% rispetto all'anno precedente.

Facttori che determinano l'aumenti delle minacce informatiche

Geopolitica

Le tensioni tra Stati Uniti e CIna, il crescente multipolarismo e i conflitti in corso provocano ricadute dirompenti a livello globale, con vittime intenzionali e involontarie

Ransomware

Le bande di criminali informatici sono più attive e nocive che mai, con un vilume di attacchi più elevato, ricavi enormi e richieste di riscatto più elevate

Third-party threats

I fornitori de infrastrutture, i servizi software, gli host di dati e le tecnologie sono la prima linea del fronte informatico e rappresentano sempre più spesso i beragli prioritari

Technology

I progressi dell'IA introducono rapidamente nuovi rishi, mentre l'aumento della connettività e dell'interdipendenza accresce la superficie di attacco in continua espansione

Control Risks

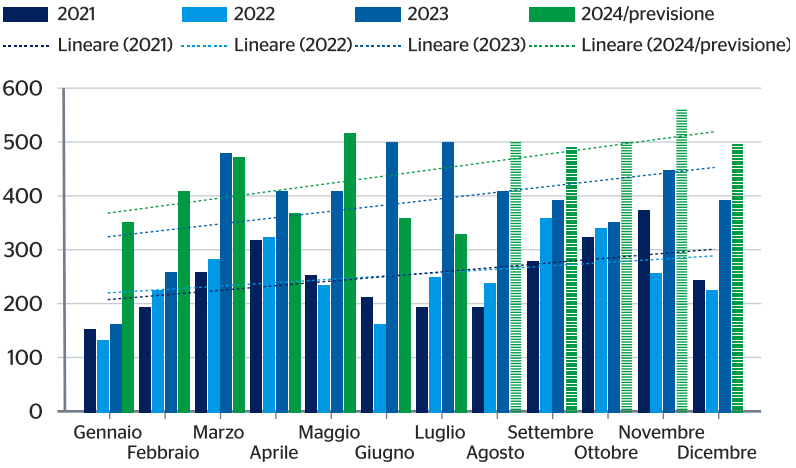
Ransomware

Aumenta la redditività per effetto dell'aumento del numero di attacchi

Gli attacchi ransomware nel 2023 sono aumentati del 74% rispetto al 2022 e il totale dei riscatti pagati dalle vittime ha superato il miliardo di dollari a livello globale. Dopo che le forze dell'ordine hanno smantellato il gruppo Hive nel 2022, infatti, l'ecosistema dei criminali informatici si è frammentato e il codice del ransomware è stato diffuso, consentendo anche a gruppi con capacità inferiori di condurre attacchi.

Questo ritorno del ransomware è continuato nel 2024, anno nel quale il numero di vittime pubblicamente dichiarate ha raggiunto il totale più alto degli ultimi tre anni *(*notare che il grafico in basso include MOVEit, un incidente del 2023 che ha generato un elevato volume di vittime. In termini reali, i numeri del 2024 sono significativamente più alti di quelli del 2023 se non si considera l'incidente MOVEit come un'anomalia).*

Numero di vittime di ransomware menzionate sui siti di fuga dati



Fonte: Control Risks

Numero di vittime nominate pubblicamente da gruppi di estorsione tramite ransomware e fughe di dati

2021	2022	2023	2024 (previsione)	2025 (previsione)
2.964	2.981	4.698	4.800	5.200

Fonte: Control Risks

> Le organizzazioni del settore sanitario che hanno subito attacchi ransomware nel 2023 sono state 389, il 35% in più rispetto al 2022.

Analisi settoriale

Nel 2023 gli attacchi ransomware hanno preso di mira soprattutto i settori manifatturiero, sanitario, informatico, didattico e governativo. In generale gli aggressori mirano sempre di più ai settori verticali, ma si concentrano sui comparti manifatturiero e sanitario, perché sono quelli in cui l'interruzione delle operazioni produce generalmente l'impatto più devastante.

Il ransomware rappresenta una minaccia estremamente pericolosa per le organizzazioni del settore manifatturiero e della produzione: il 65% delle aziende di questo comparto ha riferito di aver subito un attacco ransomware nel 2023, con un pagamento medio del riscatto pari a 2,4 milioni di dollari. Tra le vittime, il 62% ha pagato un riscatto per recuperare i dati rubati.

Non ci sono informazioni sufficienti per calcolare con precisione la richiesta media, poiché questa varia in modo significativo tra aree geografiche, settori e organizzazioni. Tuttavia, le organizzazioni di grandi dimensioni, altamente vulnerabili alle interruzioni operative, potrebbero trovarsi ad affrontare richieste di riscatto anche di decine di milioni di dollari, cifra che per le organizzazioni più piccole si aggirerebbe sulle centinaia di migliaia di dollari. Le aziende che si troveranno ad affrontare le richieste di riscatto più elevate saranno probabilmente quelle dei settori sanitario, governativo, informatico e delle comunicazioni e manifatturiero.

Anche le organizzazioni sanitarie sono molto ambite, così come quelle che detengono grandi volumi di informazioni di identificazione personale (personally identifiable information, PII) e di informazioni sanitarie protette (protected health information, PHI), nonché quelle che presentano requisiti di operatività critici. Il settore sanitario è sempre più preso di mira anche perché si tende a pensare che in materia di sicurezza informatica abbia una maturità relativamente minore rispetto ad altri. Il numero di organizzazioni sanitarie che hanno subito un attacco ransomware è passato da 214 nel 2022 a 389 nel 2023, con un'impennata dell'81,7%.

Big game hunting

I gruppi di ransomware utilizzano sempre più spesso tattiche di "big game hunting" ("caccia grossa"), individuando entità ad alto fatturato e di alto profilo da attaccare. Questa tattica consente ai gruppi di ransomware di incrementare il pagamento medio del riscatto attraverso richieste iniziali più elevate di quelle che una piccola e media impresa potrebbe permettersi, oltre a far leva sull'interruzione dell'operatività di un gran numero di clienti e/o clienti delle vittime.

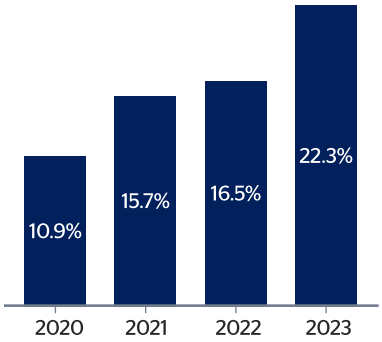
Negli ultimi anni le forze dell'ordine hanno conseguito importanti risultati nell'individuare e smantellare gruppi di ransomware, come dimostra l'eliminazione del ransomware Hive e le parziali eliminazioni dei prolifici gruppi LockBit e BlackCat. Questi gruppi hanno quindi cercato di massimizzare i pagamenti dei riscatti attraverso il "big game hunting" prima che le forze dell'ordine li raggiungessero e sequestrassero le loro risorse e infrastrutture. Il pagamento medio del riscatto nel 2023 è salito a 2 milioni di dollari rispetto ai 400.000 dell'anno precedente. La media è stata significativamente influenzata dal "big game hunting", in quanto alcuni aggressori hanno chiesto fino a 50 milioni di dollari, anche sela richiesta media di riscatto è rimasta invariata, intorno ai 300.000 dollari.

Gli autori delle minacce pensano inoltre che le grandi organizzazioni siano più propense a pagare un riscatto, perché l'interruzione delle operazioni risulterebbe anche più costosa. In media, il 61% delle aziende con un fatturato annuo di 5 miliardi di dollari paga un riscatto dopo un attacco, rispetto al 25% delle organizzazioni con un fatturato annuo inferiore a 10 milioni di dollari.

L'attacco LockBit a ICBC dimostra la minaccia opportunistica del ransomware contro il settore finanziario

A novembre 2023, il gruppo di ransomware LockBit ha preso di mira il ramo dei servizi finanziari della Industrial and Commercial Bank of China (ICBC), con sede negli Stati Uniti, interrompendo le negoziazioni sul mercato dei Treasury (titoli di Stato) statunitensi. Ciò ha comportato il reindirizzamento forzato delle transazioni finanziarie e ha impedito a ICBC Financial Services di regolare le transazioni in Treasury per altri operatori di mercato, con la conseguenza che ICBC ha dovuto versare 9 miliardi di dollari alla sua filiale statunitense. Gli aggressori si sono probabilmente infiltrati nella rete della ICBC attraverso un box Citrix NetScaler senza patch che ha permesso loro di aggirare le misure di autenticazione.

Percentuale di incidenti informatici globali con impatto su fornitori IT terzi (2020-23)



Fonte: Control Risks

Compromissione della supply chain

Incidenti di terze parti

Si stima che almeno il 22% di tutte le violazioni della sicurezza informatica nel 2023 siano state una conseguenza di incidenti di terzi. Al fine di gestire il rischio proveniente da terze parti, difficile da mitigare, le organizzazioni devono adottare pratiche interne per rafforzare la propria resilienza in caso di violazioni esterne e per eseguire un follow-up mirato dopo gli incidenti più gravi, tenendo comunque conto delle caratteristiche del rischio, delle strategie di mitigazione e delle politiche assicurative dei loro fornitori IT terze parti.

Settori

Per i criminali informatici e gli autori delle minacce legati allo Stato, i fornitori di servizi IT, come le organizzazioni di software-as-a-service (SaaS), sono un obiettivo primario. Nel 2023, il 75% degli incidenti di terze parti è provenuto da attacchi a fornitori di servizi e software.

Quota di violazioni di terzi segnalate nel 2023 per settore

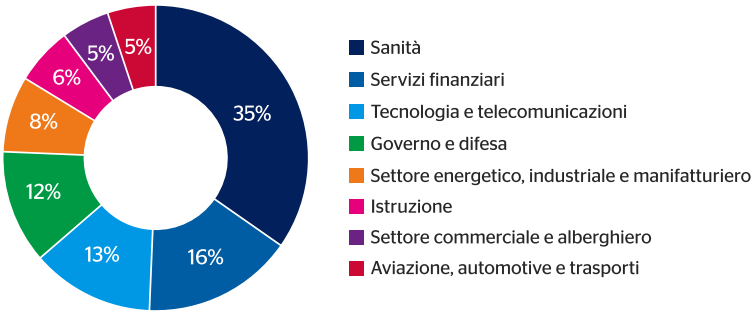


Grafico: Control Risks • Fonte: Scheda di valutazione della sicurezza

Oltre il 75% degli incidenti di terze parti è attribuibile a tre sole vulnerabilità della supply chain.

Gli attacchi "zero-day" possono essere più incisivi per i gruppi di ransomware

I gruppi di ransomware considerano le supply chain IT obiettivi ambiti, perché danno l'opportunità di colpire più aziende di diversi settori con un unico attacco. Inoltre, queste organizzazioni hanno operatività complesse, aspetto che può essere sfruttato nelle trattative per il riscatto. Nel 2023, il 64% delle violazioni di terze parti è stato collegato al gruppo ransomware Clop che sfrutta un bug zero-day (una vulnerabilità sconosciuta e senza patch in un sistema o dispositivo) e il 61% è stato attribuito alla vulnerabilità MOVEit, evidenziando come i rischi di terze parti possano trasformarsi in impatti diretti sui clienti della supply chain. Il grafico in basso mostra che oltre il 75% degli incidenti di terze parti nel 2023 è attribuibile a tre sole vulnerabilità della supply chain.

Quota di incidenti di terzi nel 2023 per vulnerabilità

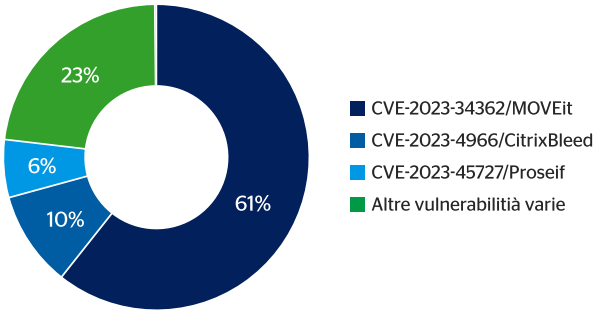
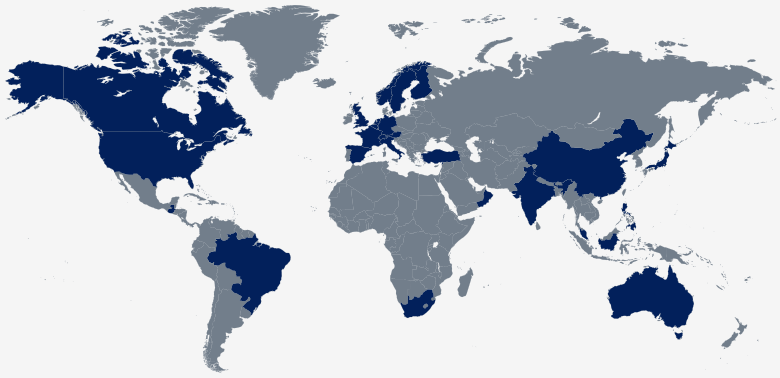


Grafico: Control Risks • Fonte: Scheda di valutazione della sicurezza

La campagna MOVEit dimostra che la violazione dei dati dei fornitori di servizi IT può avere un impatto di ampia portata

Dopo aver sfruttato una vulnerabilità zero-day nel servizio di trasferimento di file MOVEit a maggio 2023, il gruppo di criminali informatici Clop ha rubato file da organizzazioni ignare di essere esposte a tale minaccia. L'ondata di furti di dati e di estorsioni ha colpito almeno 2.180 organizzazioni e Clop ha probabilmente incassato oltre 100 milioni di dollari in pagamenti di riscatti.

Diffusione geografica delle vittime di MOVEit



Tecnologia

Minacce al cloud

Da quando le organizzazioni hanno adottato i servizi cloud, gli hacker hanno sviluppato strumenti e tattiche per ottenere un accesso più facile e persistente alle applicazioni basate su questa tecnologia, al fine di individuare possibili vulnerabilità. La navigazione attraverso le configurazioni in cloud consente di eludere i tipici protocolli di rilevamento, come l'analisi IP avanzata. Anche gli autori legati allo Stato e i criminali informatici più sofisticati si sono spostati nel cloud, trasferendo i dati nel proprio archivio cloud.

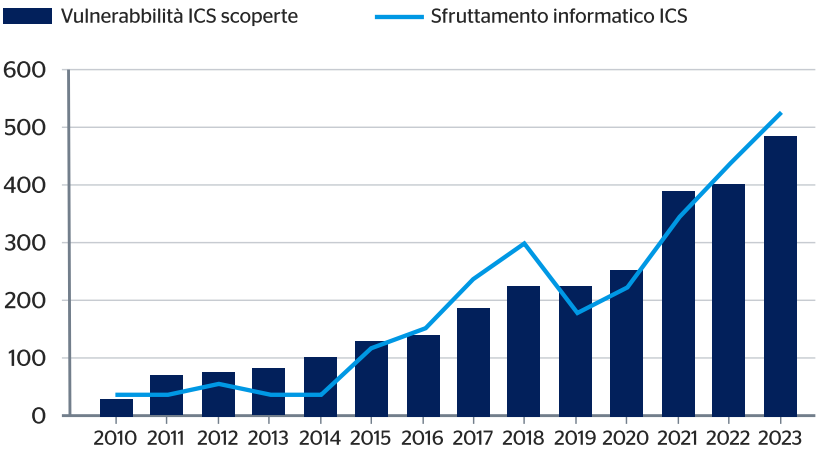
Tecnologia operativa e adozione dell'IoT

Gli attacchi ransomware contro le aziende del settore industriale sono aumentati del 50% nel 2023 rispetto al 2022. Il successo degli attacchi che colpiscono la tecnologia operativa (operational technology, OT), il software e l'hardware che monitora e controlla le apparecchiature industriali, deriva dal fatto che per queste aziende l'interruzione dell'operatività è finanziariamente più dannosa del riscatto.

L'ingegneria, l'industria manifatturiera e i servizi pubblici sono tutti obiettivi interessanti per gli attacchi indirizzati all'OT. Gli autori delle minacce, con capacità diverse, hanno preso sempre più di mira l'OT che utilizza controllori o dispositivi esposti a Internet. Una marcata proliferazione di dispositivi IoT (Internet of Things), hardware connessi in modalità wireless alle reti, ha probabilmente accentuato tali minacce, in particolare nei settori manifatturiero e dei servizi pubblici. Un'efficace segmentazione della rete e la limitazione o la completa rimozione delle porte esposte a Internet possono ridurre il rischio di un attacco dannoso.

> Gli attacchi ransomware contro le aziende del settore industriale sono aumentati del 50% nel 2023 rispetto al 2022.

Numero di vulnerabilità in ICS vs incidenti che sfruttao le vulnerabilità ICS, 2010-23



Fonte: Control Risks

> Le aziende sfrutteranno sempre più l'IA generativa e le tecniche di automazione per identificare gli attacchi informatici.

IA

Da strumenti esclusivamente pre-programmati per compiti specifici che richiedono l'intervento umano, l'IA si sta sviluppando in IA a memoria limitata o IA ristretta, in grado di utilizzare insiemi di dati di massa per prendere decisioni. Oggi gli strumenti di IA generativa open-source possono scrivere il codice per un malware o migliorare molte delle tattiche tradizionali impiegate dagli autori delle minacce legati allo Stato e dai gruppi di criminali informatici, come gli attacchi di spear phishing e di malware.

Man mano che l'IA diventa più facilmente accessibile e i modelli linguistici di grandi dimensioni (large language models, LLM) proliferano, anche i criminali informatici dotati di minori capacità sono in grado di lanciare più rapidamente attacchi di grandi dimensioni. Questo aumento di capacità in termini di scala e frequenza sarà l'impatto più significativo sul panorama delle minacce informatiche.

I criminali utilizzano strumenti di IA generativa per creare deepfake di dipendenti e dirigenti conosciuti per frodare organizzazioni di tutte le dimensioni. All'inizio di quest'anno un'organizzazione globale ha perso 20 milioni di dollari a causa di un attacco deepfake. Questi schemi non sono nuovi, alcuni sono stati segnalati già nel 2019, ma la loro frequenza e le possibilità di successo stanno crescendo notevolmente e le competenze richieste per realizzarli diminuiscono con il miglioramento della tecnologia.

Al contrario, l'IA contribuisce però anche all'individuazione di comportamenti dannosi nelle reti aziendali, e prevediamo che continuerà a migliorare le capacità di sicurezza e difesa informatica. Le organizzazioni sfrutteranno sempre più l'IA generativa e le tecniche di automazione per identificare gli attacchi informatici in un panorama di minacce innovative, motivate e in continua evoluzione.

Diversificazione delle tecnologie

Il cloud e le tecnologie emergenti hanno fornito alle organizzazioni soluzioni infrastrutturali economicamente vantaggiose. Tuttavia, la maggiore adozione di infrastructure-as-a-service e AI-as-a-service ha aumentato la superficie di attacco degli autori delle minacce, offrendo maggiori opportunità di infettare più vittime con un solo incidente.

Questi sono solo alcuni degli esempi. L'aumento dei dispositivi IoT ha permesso di perpetrare attacchi informatici più dannosi che hanno avuto un impatto sui servizi pubblici essenziali, come la distribuzione dell'acqua. I progressi dell'IA generativa hanno permesso ai criminali informatici di creare deepfake di dirigenti per facilitare gli attacchi di social engineering. Gli autori delle minacce legati allo Stato e i cyberattivisti si rivolgono a soluzioni criminali informatiche per influenzare le elezioni o finanziare le campagne. Un'ampia gamma di aggressori sta sviluppando strumenti propri e sfruttando l'intelligenza artificiale per automatizzare la preparazione degli attacchi e perpetrare malware. L'adozione di tecnologie emergenti, con ritmi e dimensioni variabili a seconda del settore e della zona geografica, sta ampliando la superficie di attacco; al contempo, le organizzazioni cercano di farsi trovare pronte.

Gli attivisti colpiscono la tecnologia operativa e interrompono la fornitura d'acqua

A dicembre 2023, il gruppo di attivisti Cyber Av3ngers, legato all'Iran, ha attaccato un impianto idrico privato a Erris, in Irlanda. Sfruttando i controllori logici programmabili (programmable logic controllers, PLC) prodotti dall'azienda israeliana Unitronics, gli attacchi hanno provocato un'interruzione dell'acqua per due giorni ai residenti locali. I Cyber Av3ngers hanno rivendicato gli attacchi ai PLC come parte della loro campagna contro i prodotti e le organizzazioni israeliane nel contesto del conflitto tra Israele e Hamas.

Conclusione

L'interdipendenza tecnologica, promossa dai progressi dell'interconnettività, dell'intelligenza artificiale e delle tecnologie emergenti, ha aumentato la vulnerabilità agli attacchi informatici. L'instabilità dei conflitti globali, i cambiamenti geopolitici e il boom dell'economia criminale informatica sono tutti fattori ulteriori che potrebbero aumentare i rischi per le organizzazioni.

L'interdipendenza tra settori e aziende renderà tali rischi inevitabili, in quanto gli autori delle minacce hanno come priorità lo sviluppo di malware sofisticati per colpire gli ambienti OT o i fornitori terzi di servizi e software. L'IA e altre tecnologie continueranno a svilupparsi, contribuendo a ridurre e prevenire una serie di minacce che cercano di sfruttare l'interdipendenza tecnologica.

Una strategia di trasformazione digitale protetta dalle minacce future può essere un catalizzatore del successo. Le strategie di mitigazione del rischio devono considerare la crescente probabilità di incidenti informatici e promuovere una resilienza proattiva, implementando al contempo protocolli di risposta per reagire rapidamente agli attacchi informatici.

Allegati – Riferimenti principali

"Global ransomware threat expected to rise with AI, NCSC warns", ncsc.gov.uk
"2023 Ransomware Attack Report", blackfog.com
"Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline", chanalysis.comv
"#StopRansomware: CLOP Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability", cisa.gov
"Two-day water outage in remote Irish region caused by pro-Iran hackers", therecord.media
"NCC Group Releases Annual Cyber Threat Monitor Report 2023", nccgroup.com
"Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double", dni.gov
"The State of Ransomware 2024", sophos.com
"The State of Ransomware in Manufacturing and Production 2024", sophos.com
"Helping our customers through the CrowdStrike outage", blog.microsoft.com
"Dragos 2023 OT Cybersecurity Year in Review", dragos.com
"Global Third-Party Cybersecurity Breach Report", securityscorecard.com

L'9 ottobre 2024 è stata pubblicata una correzione per rettificare un dato errato nell'analisi settoriale a pag. 7. A livello globale, nel 2023, un totale di 389 organizzazioni sanitarie hanno dovuto affrontare attacchi ransomware (Control Risks, 2024).

Assicurazione contro le minacce informatiche di QBE

I prodotti informatici di QBE proteggono dai possibili rischi associati alla tecnologia digitale e forniscono un supporto fondamentale in caso di attacco informatico. L'offerta comprende QCyberProtect, una nuova polizza assicurativa globale contro le minacce informatiche che offre una copertura omogenea in tutto il mondo per le perdite derivanti dai rischi informatici esistenti ed emergenti, tra cui, a titolo esemplificativo, la sicurezza delle reti, la responsabilità per la privacy, le interruzioni delle attività IT e non IT e la perdita di reputazione.

Copertura su misura e servizio individuale

Per garantire la protezione, gli agenti assicuratori di QBE lavorano a stretto contatto con i clienti per creare una copertura adatta alle esigenze specifiche. Ci prendiamo il tempo necessario per conoscere l'attività e fornire una copertura su misura che protegga dai rischi informatici esistenti ed emergenti.

Aiutiamo a gestire i rischi

Non ci limitiamo a coprire i rischi, ma insegniamo a gestirli e a ridurli. Offriamo strumenti di supporto alla gestione del rischio, tra cui:

- QBE QCyberPrepare: una stanza di sicurezza online per aiutare i clienti a prepararsi nel caso di un incidente informatico.
- Accesso gratuito al QBE Cyber Risk Management Portal, che offre un'ampia gamma di informazioni sui rischi informatici e su come proteggersi.
- Accesso agli strumenti e ai servizi QBE, nonché sconti per una serie di Cyber Risk Management Services offerti dai nostri partner di fiducia.

Supporto in caso di crisi

QBE fornisce assistenza 24 ore su 24 in caso di un attacco informatico. Ciò potrebbe comportare la messa a disposizione di un team forense per capire come si è verificata la violazione informatica e come risolvere il problema, la consulenza legale per rispettare i requisiti normativi o la gestione di una dichiarazione ai media per ridurre al minimo l'impatto sulla reputazione.

Per ulteriori informazioni, visitare qbeitalia.com/prodotti/cyber/

Questo resoconto
è stato sviluppato
per QBE da
Control Risks

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

QBE Europe SA/NV, Rappresentanza Generale per l'Italia, Via Melchiorre Gioia 8 – 20124 Milano. R.E.A.
MI-2538674. Codice fiscale/P.IVA 10532190963 Autorizzazione IVASS n. I.00147 QBE Europe SA/NV è autorizzata dalla Banca Nazionale del Belgio con licenza numero 3093. Sede legale Boulevard Du Regent 37, BE 1000, Bruxelles, Belgio. N. di registrazione 0690537456.

641209/2405