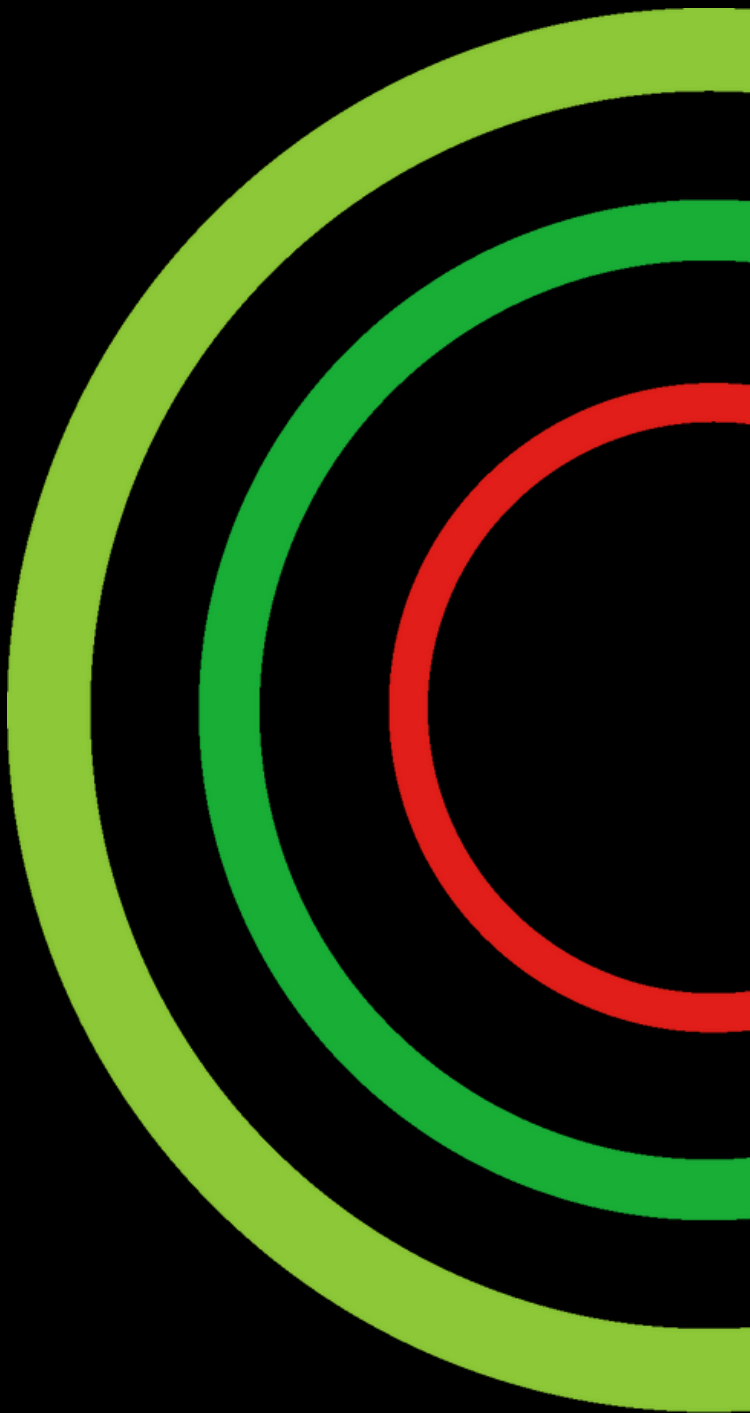
CYBERGON elmec

2025

Data Gathering

Report annuale sullo stato della cyber security in Italia nel 2024



CONTENUTI

INTRODUZIONE E METODOLOGIA DELLA RICERCA

Secondo il **Rapporto Clusit 2025**, l'andamento degli incidenti cyber in Italia e nel mondo è ancora in crescita, soprattutto per quanto riguarda gli attacchi con conseguenze gravi. **A livello globale i casi sono aumentati del 27%, mentre in Italia del 15%.**

Gli strumenti di attacco si sono evoluti e sono diventati facilmente accessibili grazie all'impiego dell'AI generativa e ai modelli "as-a-service". L'Intelligenza Artificiale permette di **generare codici più sofisticati** anche senza possedere delle capacità di sviluppo avanzate. Inoltre, ha **migliorato la qualità dei vettori con cui vengono diffusi i malware**, come e-mail di phishing e siti web contraffatti, rendendo i contenuti malevoli più difficili da riconoscere. Anche il **Malware-as-a-Service** si muove questa direzione, in quanto criminali informatici con competenze tecniche limitate possono acquistare malware dagli sviluppatori per poi diffonderli nella propria rete.

I dati raccolti nel 2024 durante **le nostre attività di monitoraggio e risposta rispecchiano il trend del settore**: il 70% degli incidenti con conseguenze gravi che abbiamo gestito sono stati generati da e-mail di phishing e attacchi ransomware. Andamento confermato anche dall'analisi del nostro antispam che segnala campagne di phishing e allegati sospetti come le principali cause di blocco delle comunicazioni.

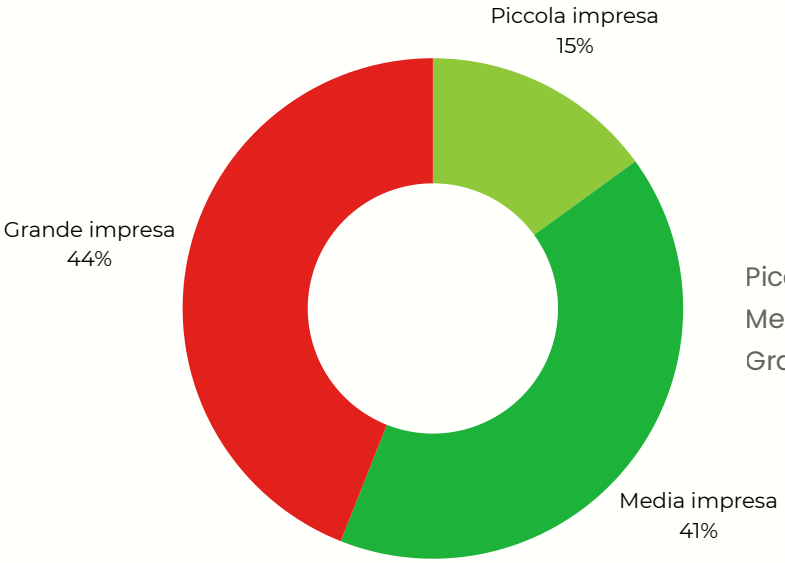
INTRODUZIONE E METODOLOGIA DELLA RICERCA

Dopo una panoramica sul nostro dataset di riferimento relativamente a dimensioni e settore aziendale, in questa edizione del Data Gathering presentiamo un'**analisi dell'andamento delle minacce intercettate** nel corso dell'anno passato con una distinzione tra anomalie, incident e un **focus più specifico sugli episodi che hanno avuto un impatto critico sul business delle aziende colpite**. Rispetto alle edizioni precedenti, abbiamo aggiunto anche **informazioni su vulnerabilità, patching e antispam**. Infine, concludiamo con le **previsioni per il 2025** correlate con quanto rilevato nei primi mesi dell'anno e con le novità emergenti nel settore cyber.

DATA SET

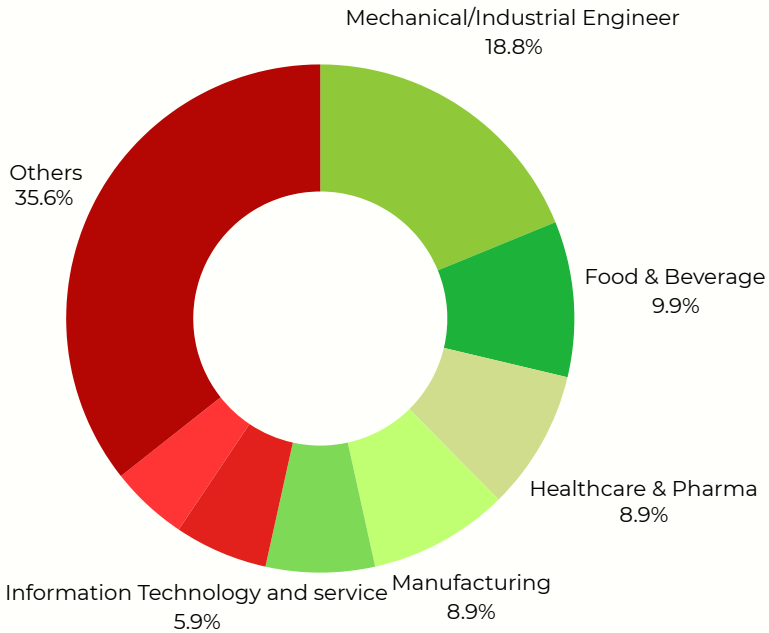
I dati raccolti provengono dal nostro pool di clienti composto da **173 aziende capogruppo** attive in diversi settori merceologici.
Rispetto all'anno precedente, il dataset preso in esame si è ampliato e prende in considerazione circa **54.000 asset IT** suddivisi in hardware, come dispositivi personali, server, router e firewall, e software, ovvero tutte le applicazioni e i programmi utilizzati da un'azienda per lo svolgimento delle proprie attività.

Dimensione aziendale



Piccole aziende: <50 dipendenti
Medie aziende: 50-200 dipendenti
Grandi aziende: >200 dipendenti

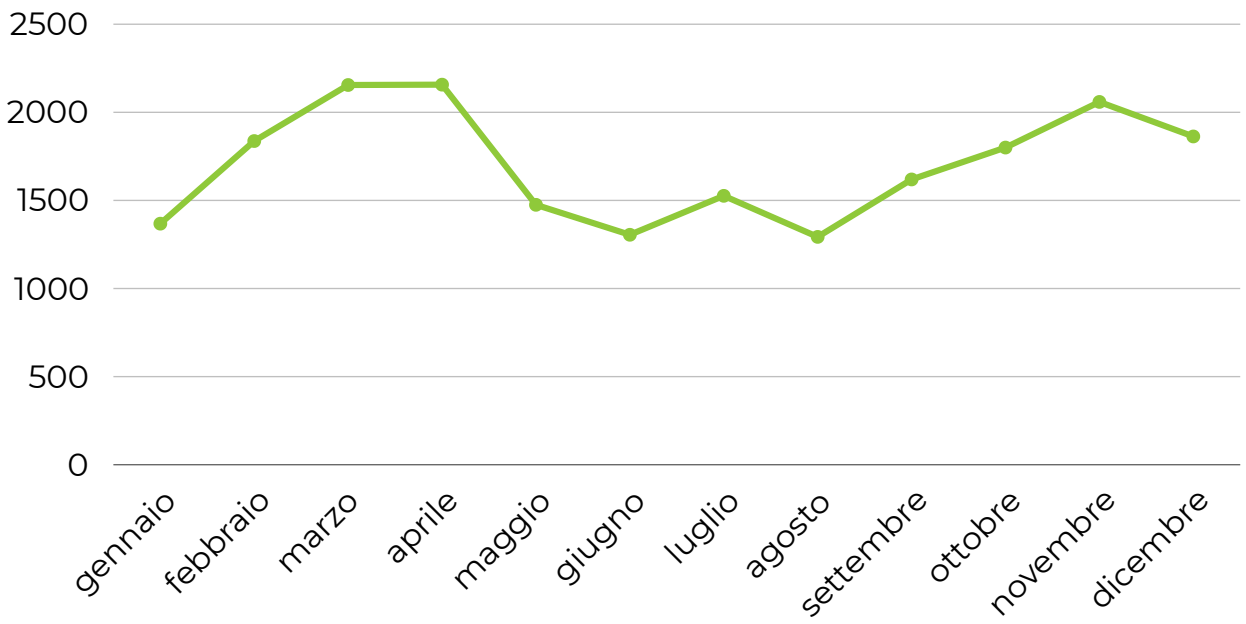
Settore Merceologico



INCIDENT E ANOMALIE

Durante le attività di monitoraggio svolte nel corso dell'anno, i nostri sistemi hanno rilevato circa 20.500 anomalie e oltre 13.000 incident.

Andamento anomalie

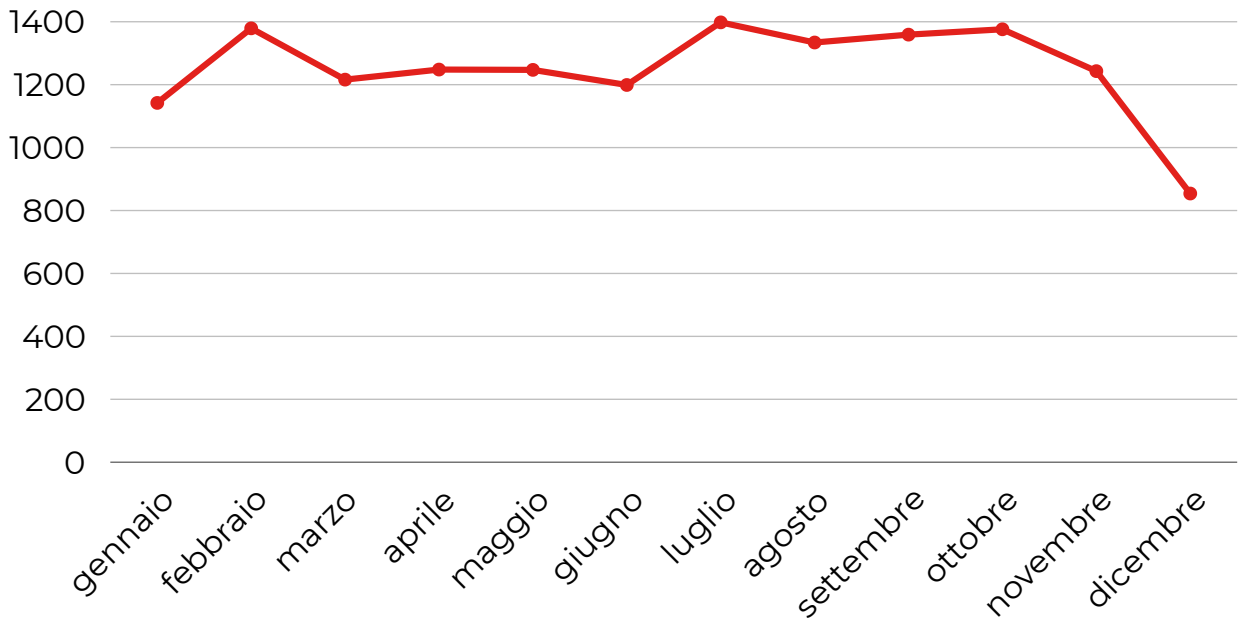


Con anomalia si intende una **segnalazione generata a seguito della rilevazione di un comportamento potenzialmente sospetto**, come per esempio dei log ad orari insoliti oppure molteplici accessi contemporanei dallo stesso account. Queste segnalazioni non sono necessariamente collegate a un attacco in corso, ma vanno analizzate a livello di SOC per definire se si tratta di effettive minacce oppure semplici comportamenti inusuali.

Come possiamo vedere dal grafico, l'**impatto degli alert gestiti dal SOC è direttamente proporzionale alle interazioni degli utenti**: nei mesi di maggiore attività abbiamo registrato dei picchi nelle segnalazioni, mentre quando il numero di utenti attivi è minore, come nei mesi estivi, la quantità di eventi gestiti si riduce.

INCIDENT E ANOMALIE

Andamento incident



Gli incident, invece, sono a tutti gli effetti dei **tentativi di violazione dell'infrastruttura IT rilevati dai sistemi di difesa**. Nella maggior parte dei casi si tratta di eventi con impatto minimo, come per esempio la ricezione di un file sospetto oppure la compromissione di un'utenza, facilmente arginabili e gestibili.

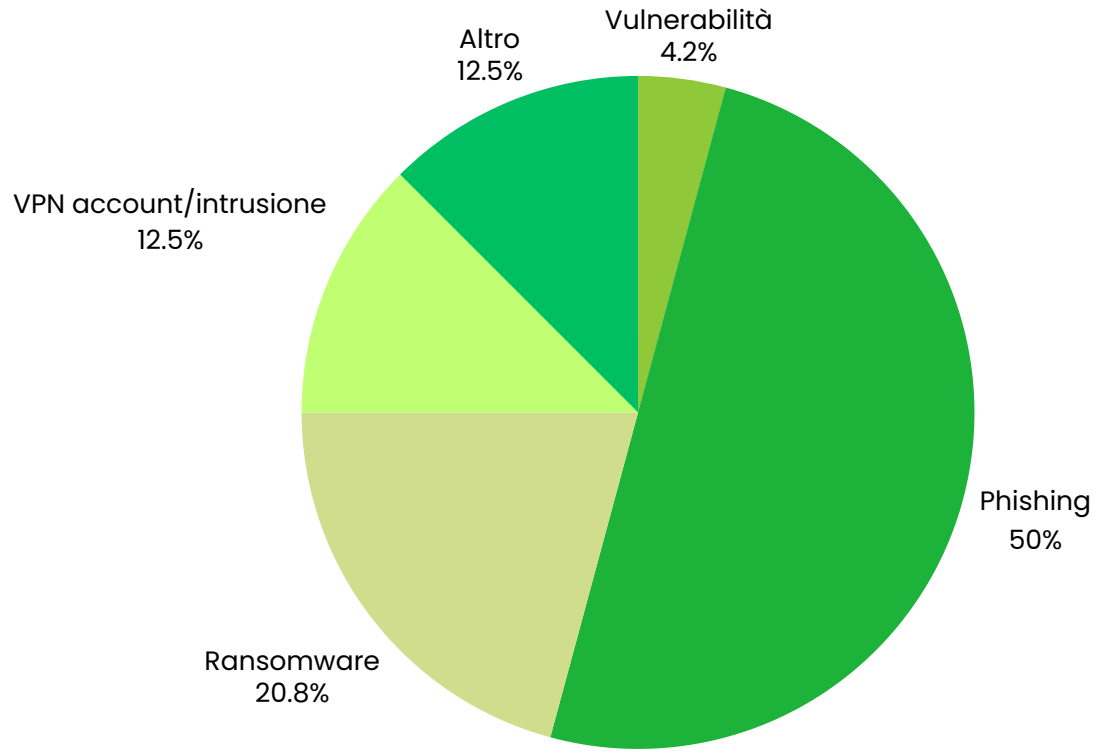
Facendo il paragone con il grafico relativo alla gestione delle anomalie che presenta picchi e decrescite collegati alle attività degli utenti, gli incidenti reali in ambito infrastrutturale seguono un **andamento costante, in quanto gli attaccanti sono sempre attivi**.

Rispetto ai 13.000 incident totali, **29 hanno avuto conseguenze significative sulle attività dell'azienda**, impattando la business continuity in maniera altamente critica.

INCIDENT E ANOMALIE

Incident con impatto grave

Per prima cosa facciamo una specifica su cosa rientra nel phishing e cosa nel ransomware. Classifichiamo come attacchi **phishing le campagne e-mail usate per rubare dati sensibili e credenziali, oppure che hanno sfruttato una casella compromessa per attività malevole,** come richieste di pagamento fraudolente o esfiltrazioni di dati. Non rientrano in questa categoria le **comunicazioni utilizzate per diffondere malware che classifichiamo come ransomware**: in questo caso il phishing è un mezzo per fare breccia nei sistemi di difesa, ma non il vettore con cui viene effettivamente condotto l'attacco. Infatti, **tra i punti di ingresso per un attacco ransomware ci sono siti web compromessi, vulnerabilità dell'infrastruttura, furto di credenziali VPN e**, per l'appunto, anche **campagne di phishing**.



INCIDENT E ANOMALIE

Tra gli eventi critici che abbiamo gestito nel 2024, **il 50% è stato causato dal phishing**, strategia di attacco che è diventata più pericolosa grazie all'impiego di **strumenti di AI generativa**, che permettono di creare comunicazioni ben fatte e più credibili rispetto alle campagne graficamente e lessicalmente poco accurate degli anni precedenti.

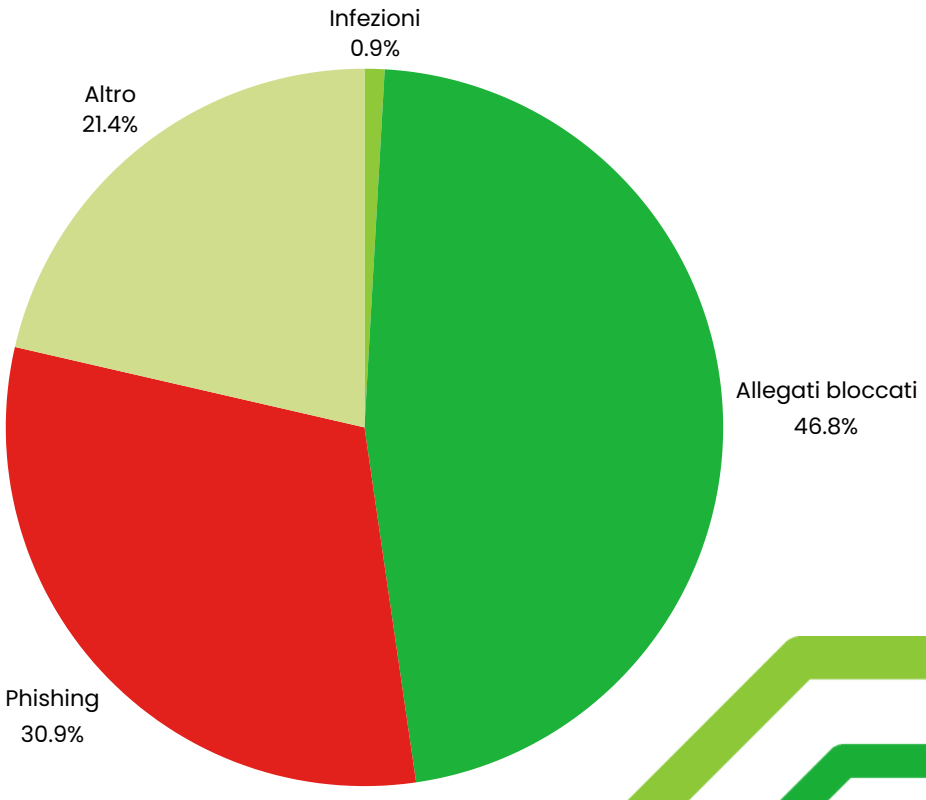
Al secondo posto troviamo i **ransomware** che restano un vettore di attacco ancora molto utilizzato sia per l'**impatto critico che hanno sulle attività di un'azienda** una volta andati a segno, sia perché sono facilmente accessibili anche da attori con competenze tecniche ridotte grazie alla **disponibilità di malware già pronti all'uso in modalità Ransomware-as-a-Service**.

PHISHING E COMUNICAZIONI MALEVOLE

Come mostrato nel capitolo precedente, le comunicazioni malevole hanno un peso importante negli attacchi informatici da noi analizzati.

Siamo andati quindi a esaminare i **dati raccolti dai nostri sistemi antispam** per avere un quadro più chiaro sulle comunicazioni malevole in entrata. Rispetto al campione di riferimento, composto da 200 domini appartenenti a 52 aziende, l'**11% delle e-mail processate sono state contrassegnate come sospette**.

Precisiamo che le e-mail segnalate dall'antispam non si sono necessariamente tradotte in un attacco, ma sono attività sospette su cui è opportuno fare delle riflessioni.



PHISHING E COMUNICAZIONI MALEVOLE

Escludendo dall'analisi le comunicazioni categorizzate come semplice spam, possiamo vedere che **la maggior parte delle mail segnalate conteneva allegati pericolosi**, possibili vettori di virus e malware, mentre **il 30% erano campagne phishing e whaling**, una tipologia di phishing che punta alle figure che ricoprono incarichi sensibili.

Per ridurre i rischi legati ai messaggi malevoli è importante educare il personale aziendale a **riconoscere le e-mail sospette e seguire buone abitudini** che possono contribuire a mitigare i tentativi di attacco. Alcuni comportamenti fondamentali sono: aggiornare le password frequentemente, non condividere mai le proprie informazioni personali e le credenziali di accesso agli account e non aprire allegati da mittenti sconosciuti.

Il dato sulle segnalazioni dell'antispam sottolinea come **la formazione agli utenti deve essere parte integrante della strategia di cyber security**. Infatti, il fattore umano può diventare una falla considerevole all'interno di un sistema di difesa ben strutturato.

Anche le **attività di Intelligence** hanno un ruolo importante per rafforzare le difese dell'azienda. Attraverso il **monitoraggio dei dati pubblicati sul dark web** è possibile scoprire eventuali esposizioni dell'azienda e anche alcune delle strategie di attacco in corso di sfruttamento, come nuove campagne phishing, siti contraffatti e malware sviluppati, così da riuscire a mettere in atto azioni correttive per prevenire e mitigare gli attacchi.

VULNERABILITÀ E PATCH

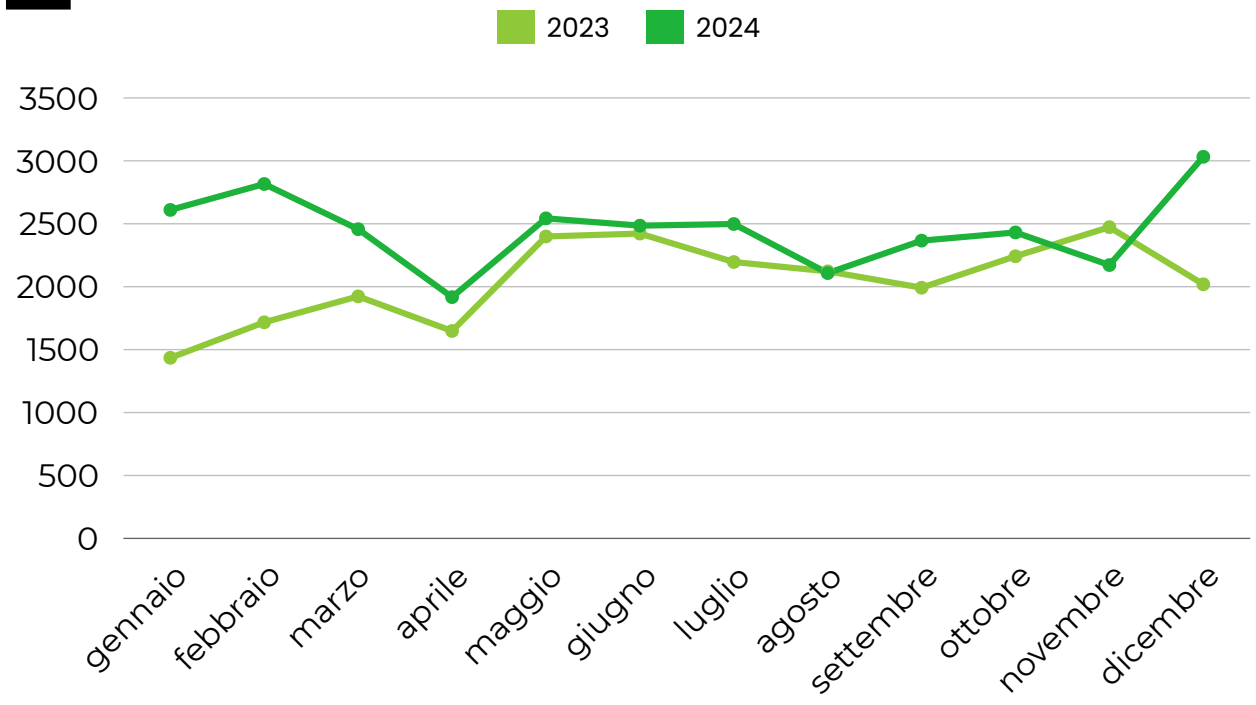
Tra gli incident da noi trattati nel 2024 abbiamo registrato anche dei casi di sfruttamento delle vulnerabilità (4%).

Si tratta di una tecnica di attacco complessa che richiede competenze avanzate per riuscire a **trovare dei difetti nei sistemi IT** legati ad errori di programmazione o configurazione, mancanza di aggiornamenti di sicurezza o conflitti tra software.

Secondo lo studio condotto da VulnCheck, **le vulnerabilità attivamente sfruttate nel corso del 2024 sono aumentate del 20%** e tra quelle critiche, il 23% è stato indicizzato come zero day. Prevalentemente le vulnerabilità sfruttate sono legate ai sistemi aziendali esposti su internet o a disposizione della supply chain. Ecco perché è importante **monitorare regolarmente l'esposizione aziendale**, ovvero quali sono i sistemi pubblicati e i dati facilmente accessibili dagli attaccanti, e **installare con tempestività le nuove patch disponibili** in modo da prevenire l'evoluzione degli attacchi.

Il numero di vulnerabilità tende a crescere di anno in anno a seguito del rilascio di nuove funzionalità per sistemi e applicativi esistenti, oltre che per il lancio di quelli nuovi. Proprio per questo, rispetto al 2023, **il numero di aggiornamenti completati nel 2024 è cresciuto del 19%**. Guardando questo lato da un punto di vista più ottimistico, un numero crescente di patch è direttamente proporzionale alla riduzione del perimetro di attacco sfruttabile dai criminali informatici.

VULNERABILITÀ E PATCH



I picchi nelle nostre attività coincidono con i picchi nella pubblicazione di nuove CVE a livello globale collegate ad eventi rilevanti per il settore della cyber security, come la condivisione di nuovi dati da parte di ShadowServer tra gennaio e febbraio, la conferenza RSA a inizio maggio e la pubblicazione di report di importanti realtà come F5 e CISA a luglio e DoD a ottobre.

Come spesso accade nel settore della cyber security, le nuove informazioni disponibili sono utili ad entrambe le parti, attacco e difesa. Per prioritizzare le attività di remediation e ottimizzare l'effort del reparto IT, è importante **monitorare le CVE pubblicate in correlazione con le informazioni sulle vulnerabilità attivamente in corso di sfruttamento** dai cyber criminali per campagne di attacco estese.

TEMPI DI FERMO E TEMPI DI RIPRESA

Dopo l'analisi dettagliata delle minacce rilevate dai nostri strumenti avanzati di monitoraggio e correlazione, torniamo al quadro generale con una riflessione sulle conseguenze legate a un attacco informatico andato a segno.

Prendendo in considerazione gli eventi critici, la continuità di business di un'azienda può risultare compromessa in modo più o meno impattante, fino al fermo totale delle attività.

Nella nostra esperienza, **il tempo di fermo in caso di attacco pervasivo varia tra i 7 e i 14 giorni**, mentre il tempo necessario **per recuperare almeno l'80% dell'operatività** è influenzato da diversi fattori, tra cui l'organizzazione e le attività svolte dall'azienda colpita e le procedure di remediation previste. Per questo, tale tempistica **può oscillare tra le 2 settimane e i 2 mesi**.

Sentiamo sempre più spesso parlare di **resilienza informatica**, ovvero la capacità delle aziende di preservare i processi core business anche a fronte di un attacco o di un incidente esteso. Anche le normative comuni si stanno concentrando su questo aspetto come tassello fondamentale per una strategia di difesa ben strutturata. Uno dei detti più diffusi nel settore della cyber security recita: "**non è questione di se, ma di quando**". Se la probabilità di un attacco informatico è così alta da essere quasi una certezza, le misure di remediation per **Business Continuity e Disaster Recovery devono diventare parte integrante dei sistemi di sicurezza** informatica così da riuscire a ripristinare tempestivamente le attività di business, limitando gli ingenti danni economici causati dal tempo di fermo.

GEOGRAFIA DEGLI ATTACCHI

↘

Passiamo ora all'analisi della provenienza di connessioni esplorative e tentativi di attacco a danno delle aziende nel nostro campione.

Connessioni esplorative

Le connessioni esplorative sono delle **ricognizioni che sondano il perimetro delle infrastrutture IT senza che si verifichino tentativi di attacco**. Solitamente gli attori di queste connessioni stanno cercando eventuali esposizioni o punti vulnerabili nei sistemi delle aziende.

La maggior parte delle connessioni esplorative del 2024 provengono dalla **Cina**, seguita da **Italia, Stati Uniti, Germania e Singapore**.

Tentativi di attacco

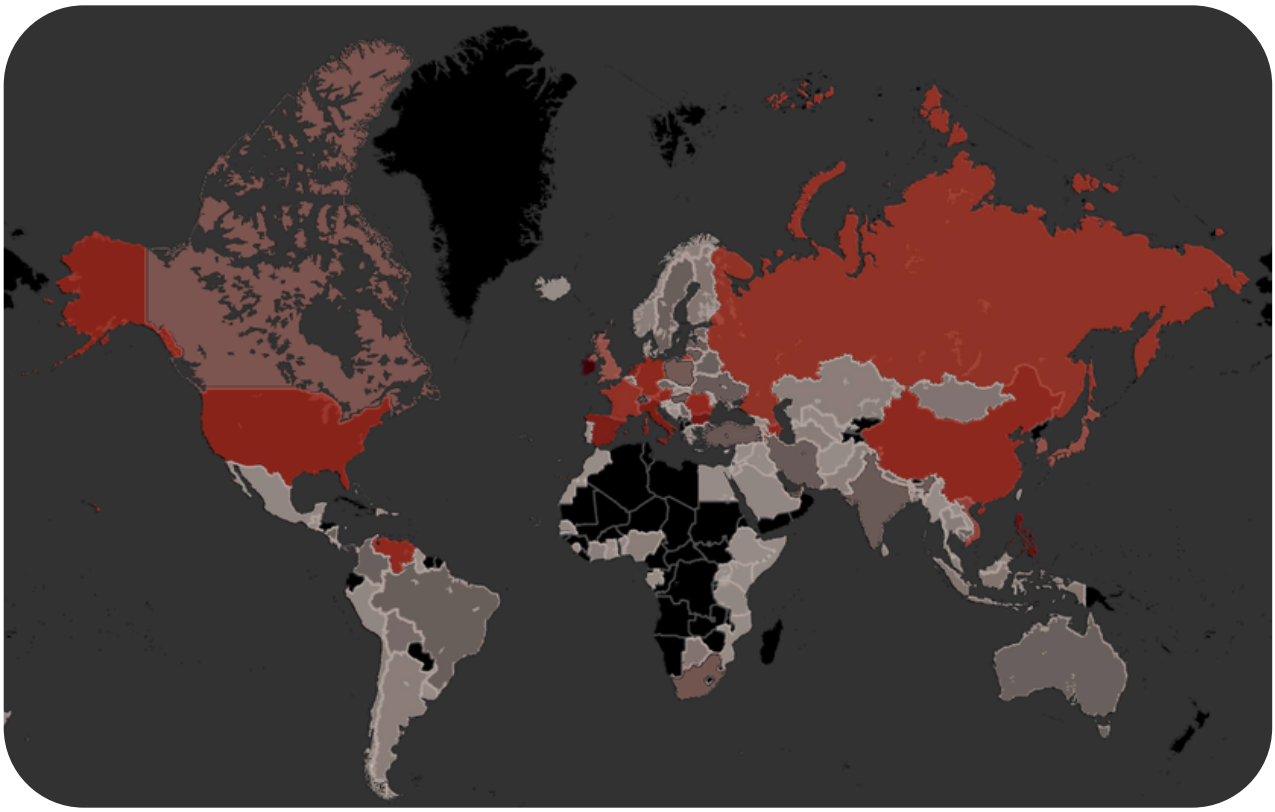
Analizzando più nel dettaglio la provenienza dei tentativi di attacco bloccati dai firewall, notiamo due trend interessanti.

Il primo è che **sono diminuiti i tentativi di attacco da Paesi emergenti e sono, invece, cresciute le connessioni provenienti dagli stati occidentali**. Questo perché le aziende di tutte le dimensioni stanno rafforzando i propri livelli di difesa e le organizzazioni criminali devono **sfruttare tecniche più sofisticate** per fare breccia nei sistemi di protezione. Per questo motivo ci si rivolge ad attori più competenti, in grado di mettere in atto attacchi più mirati. Inoltre, sempre più spesso gli **attacchi vengono sferrati attraverso grossi cloud provider** e quindi, con la crescita delle region europee, è in aumento anche il traffico continentale rispetto alle connessioni transoceaniche.

La seconda tendenza emergente, in continuità con la prima, riguarda la **crescita esponenziale delle attività malevole provenienti dall'Italia** rispetto al 2023, arrivando, nel caso delle piccole aziende, a contare il 98% degli attacchi totali. Possiamo supporre due motivazioni a spiegazione di questo dato. La prima riguarda il fatto che il mercato del **cyber crime italiano offre competenze tecniche a prezzi più contenuti** rispetto agli attori di altre nazioni occidentali. La seconda è legata alla **necessità degli attaccanti di utilizzare risorse locali per eludere i sistemi di difesa basati sulla sorgente delle connessioni**. Spesso, infatti, alcune realtà considerano attendibili le connessioni provenienti dai confini nazionali, e quindi, attaccando aziende italiane dall'Italia è possibile bypassare facilmente un primo livello di sicurezza.

GEOGRAFIA DEGLI ATTACCHI

Grandi aziende



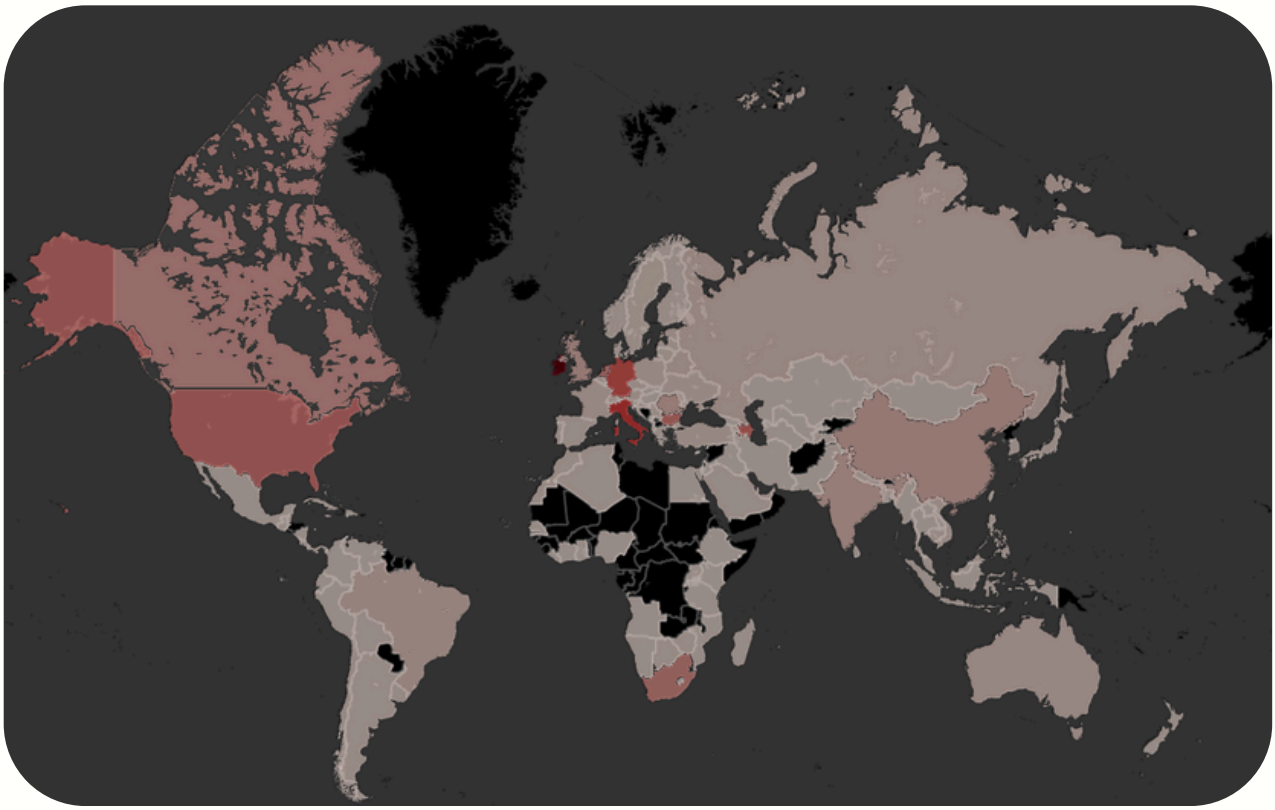
Come possiamo vedere nella mappa, la maggior parte dei tentativi di attacco ai danni delle grandi aziende proviene da **Paesi europei**. Inoltre, tra i primi posti in classifica si nota anche l'Azerbaijan, che conferma il trend di crescita iniziato nel 2023.
Come anticipato, la provenienza degli attacchi è influenzata da due fattori: il primo è che **i cyber criminali più esperti, in grado di penetrare nei sistemi di difesa di realtà strutturate, agiscono principalmente da Paesi sviluppati**; il secondo è collegato alla crescita dei **cloud provider con region in Italia e Europa,** come Azure, AWS e Oracle Cloud, che vengono utilizzati come punto di partenza per gli attacchi alle aziende italiane.

TOP 5

1. Spagna
2. Azerbaijan
3. Bulgaria
4. Italia
5. Romania

GEOGRAFIA DEGLI ATTACCHI

↘ Medie aziende



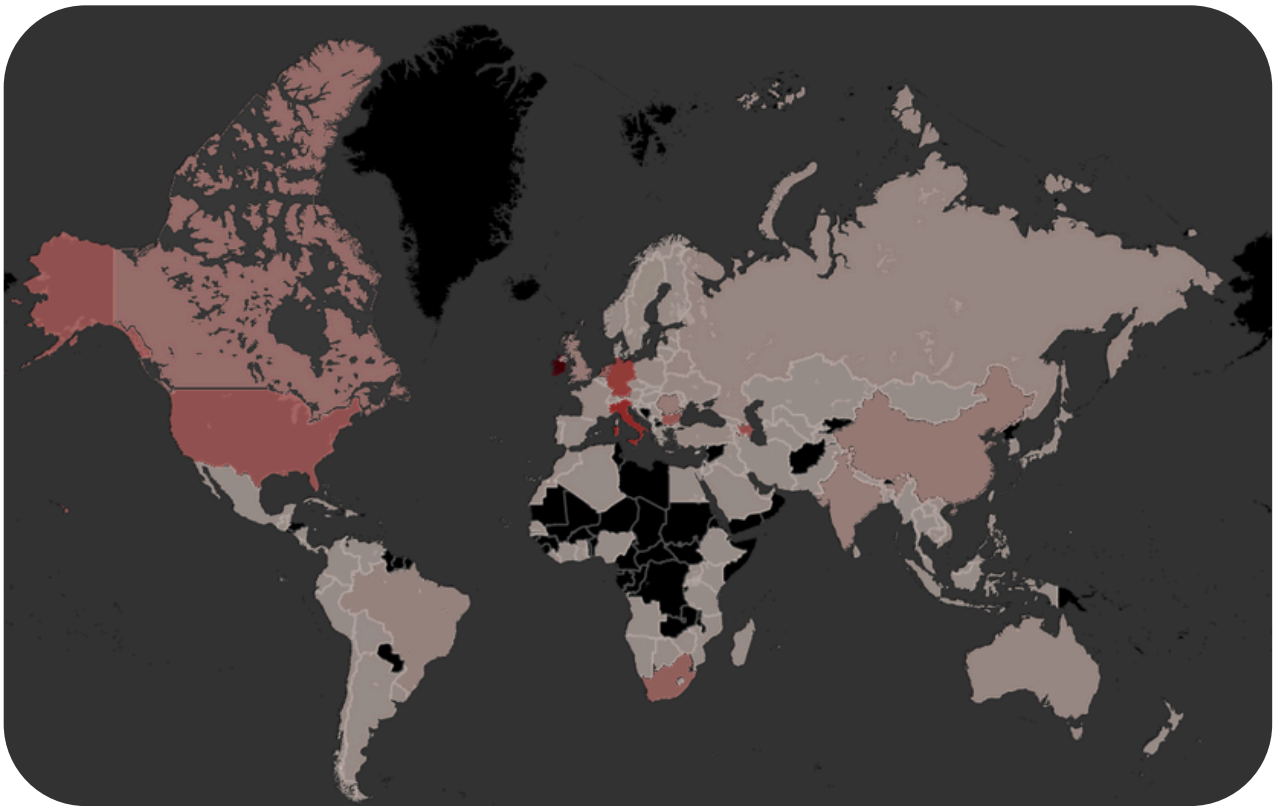
Situazione simile per le aziende di medie dimensioni colpite principalmente da attori malevoli provenienti da **Paesi europei** con l'**Irlanda**, Paese in cui sono collocati i principali data center AWS in Europa, solidamente in vetta alla classifica.
Questo dato ci mostra anche che i gruppi di cyber criminali esperti non si limitano più ad attaccare solo grandi realtà, ma hanno **esteso i loro tentativi di attacco anche verso aziende di medie e piccole dimensioni.**

TOP 5

1. Irlanda
2. Azerbaijan
3. Germania
4. Italia
5. Canada

GEOGRAFIA DEGLI ATTACCHI

↘ Piccole aziende



Anche verso le piccole aziende i tentativi di attacco provenienti da **Paesi europei** sono in aumento, con **l'Italia che nell'arco di un anno ha scalato la classifica con il 98% degli eventi malevoli intercettati**. Generalmente, il business delle piccole realtà si concentra sul territorio italiano. Per questo motivo, la maggior parte degli attori che hanno interesse a colpire queste aziende è italiana con base in Italia.

Inoltre, restano attivi in questa fascia anche gruppi provenienti da **nazioni in via di sviluppo** come Egitto e Panama. Questo perché i livelli di protezione delle piccole aziende sono meno avanzati e quindi, anche cyber criminali con competenze meno evolute riescono a violare i sistemi di difesa.

TOP 5

1. Italia
2. Germania
3. Olanda
4. Russia
5. Hong Kong

TREND 2025

Nei primi mesi del 2025 abbiamo rilevato un aumento considerevole di incidenti con impatto critico.

Tra gennaio e febbraio abbiamo gestito **9 eventi critici**, tra cui spiccano **4 attacchi ransomware e 2 campagne phishing**. Inoltre, abbiamo rilevato un **aumento del 300% delle rivendicazioni di gang criminali** sul nostro campione di aziende. Questo dato ci permette di fare delle riflessioni iniziali su cosa aspettarci in questo 2025.

Provenienza degli attacchi

Rispetto al 2024 abbiamo riscontrato delle **novità nella geografia degli attacchi**. Fanno la loro comparsa nella top 5 delle nazioni da cui provengono la maggior parte dei tentativi di attacco le Filippine, al secondo posto, e gli Stati Uniti, al quarto.

Per quanto riguarda le **Filippine**, non sappiamo per certo quale sia la causa di questa crescita, ma possiamo fare diverse ipotesi, tra cui l'attivazione di una nuova cellula di cyber criminali in questo stato, l'appoggio a sistemi IT presenti sul territorio come punto di partenza per gli attacchi, oppure lo sfruttamento di un'infrastruttura privata con sede nelle Filippine controllata illecitamente da attori malevoli.

Mentre, relativamente agli **Stati Uniti** possiamo supporre che, come nel caso dell'Irlanda, l'aumento delle attività sia legato alla presenza sul loro territorio di importanti cloud provider, tra cui Google, utilizzati come punto di partenza per i tentativi di attacco. Inoltre, non è da escludere l'influenza legata all'evoluzione della posizione di questo Paese in ambito geopolitico.

TREND 2025

Tipologia di attacco

Rispetto al 2024, l'andamento delle **campagne phishing resta stabile**, mentre sono in **crescita gli attacchi ransomware**.

Per quanto riguarda le campagne phishing, riteniamo che la stabilità del dato sia dovuta al fatto che attacco e difesa si stanno evolvendo di pari passo. Da un lato, le aziende stanno cercando di proteggersi dal phishing investendo nella **formazione degli utenti** e introducendo **misure di protezione dell'identità aggiuntive** come, per esempio, l'autentificazione a due fattori oppure l'uso di chiavi biometriche. Di contro, le campagne malevole sono diventate più efficaci grazie all'impiego di **strumenti di AI generativa** che rendono i contenuti delle comunicazioni più credibili.

Lato ransomware, sia a livello globale che nel nostro campione di aziende, c'è stato un **aumento delle rivendicazioni di gruppi di cyber criminali** che sfruttano i malware come strumenti di attacco. Molto spesso i gruppi più attivi agiscono dalla Russia o sono simpatizzanti, per questo riteniamo che l'aumento degli attacchi ransomware rivendicati sia una conseguenza delle tensioni geopolitiche.

TREND 2025

Aggiornamento normativo

Per quanto riguarda la crescita del numero di incidenti riteniamo che, oltre al progredire delle tecniche di attacco, il dato sia influenzato anche dalle **normative entrate in vigore tra la fine del 2024 e l'inizio del 2025**, tra cui DORA e NIS2, che impongono alle aziende, oltre che migliori standard di sicurezza, anche una **maggiore trasparenza in caso di incidenti informatici**.

In passato, spesso le aziende colpite da attacchi cyber nascondevano la notizia preoccupate per i danni reputazionali, oltre a quelli economici. Gli aggiornamenti normativi, in particolar modo **la NIS2, che introduce l'obbligo a partire dal 2026 di comunicare gli incidenti all'Agenzia Nazionale per la Cyber Security**, si stanno muovendo per promuovere la condivisione di informazioni tra le aziende e gli organi di sicurezza in modo da limitare la diffusione degli attacchi e velocizzare risposte e azioni correttive. Per questo motivo **prevediamo un trend di crescita nelle segnalazioni degli incidenti** per tutto il 2025, con un'ulteriore impennata nel 2026.

Gli obblighi di trasparenza non vanno assolutamente percepiti come potenziali rischi per l'immagine dell'azienda, ma, a nostro avviso, devono essere visti come un passo utile nella **lotta comune contro la criminalità informatica** e speriamo che diventino una best practice condivisa anche nei settori che al momento non sono stati coinvolti dagli obblighi normativi.

CONCLUSIONI

Per ricapitolare, nel 2024 abbiamo visto che attacco e difesa continuano a rincorrersi per tenere il passo l'uno dell'altro.

Da un lato **i sistemi di protezione delle aziende sono diventati più solidi**, anche a seguito degli obblighi imposti dalle nuove leggi europee, rafforzando monitoraggio, analisi, aggiornamenti e remediation. Di contro, **anche le tecniche di attacco si stanno facendo più sofisticate** grazie soprattutto all'utilizzo dell'AI che ha reso le campagne malevole più efficaci e accessibili. Infatti, nella maggior parte dei casi, gli eventi critici causati da ransomware e phishing sono partiti proprio da e-mail fraudolente.

Oltre al complesso quadro tecnologico, anche la geografia degli attacchi è in evoluzione con un **aumento delle attività malevole provenienti dall'Italia e da altri stati europei**. Inoltre, **la quantità di gruppi di cyber criminali attivi sta crescendo nel tempo** generando un aumento degli attaccanti e quindi degli attacchi.

Siamo di fronte ad **una nuova normalità in cui l'incidente informatico è parte della quotidianità**. La guerra cibernetica attualmente in corso non si fermerà fino a quando ci saranno interessi economici e politici. Le aziende di tutti i settori e dimensioni hanno innalzato il loro livello minimo di protezione e le tecnologie di difesa stanno diventando accessibili anche alle piccole realtà anche grazie alle novità normative che puntano a sensibilizzare maggiormente il board delle aziende.

In questo scenario, **la collaborazione tra enti pubblici, associazioni e aziende è cruciale** per innalzare il livello di difesa generale e contrastare il cyber crime.

Il seguente report è frutto di una ricerca approfondita di un pool di esperti.

CONTATTI

shockwave@cybergon.com

VISITA IL SITO

cybergon.com

LA NOSTRA SEDE

Via Pret 1
Brunello (VA), 21020, Italia