

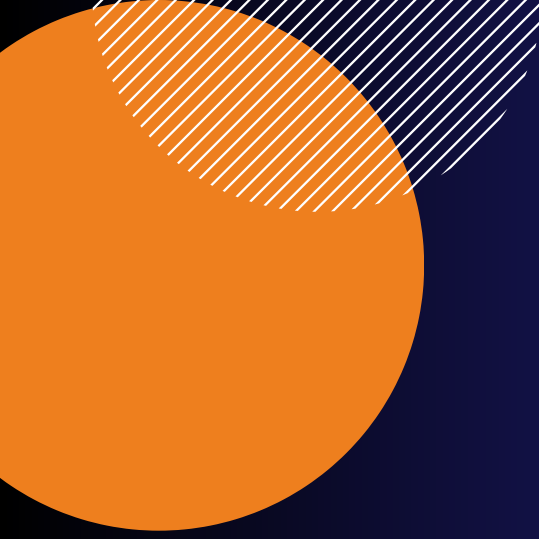


2024

CYBERSECURITY REPORT

“Cybersecurity isn’t just about technology; it’s also about processes, people, and governance”

 planetica



"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked."

Richard Alan Clarke



BREVE STORIA DEI RANSOMWARE

La tipologia di attacco più utilizzata negli ultimi anni è rappresentata dai ransomware, per questo motivo e per comprenderne meglio la fenomenologia ne riportiamo la storia. Inizialmente, i programmi dannosi erano noti come "virus informatici", ma col tempo sono emersi altri tipi di malware come i "worm" e i "macrovirus".

Successivamente sono comparsi anche keylogger, che registravano le attività dell'utente, e locker, che bloccavano l'accesso al sistema.

Nel corso degli anni, per identificare questo tipo di minacce, si è iniziato a usare il termine ombrello "Ransomware".

**2012:
CRYPTOLOCKER**

Uno dei primi ransomware ad aver avuto un grande impatto, CryptoLocker prendeva di mira i sistemi Windows e crittografava i file degli utenti, chiedendo un riscatto in Bitcoin per sbloccarli.

Simile a CryptoLocker, TorLocker prendeva di mira i sistemi Windows e crittografava i file degli utenti, ma utilizzava la rete Tor per la comunicazione e il pagamento dei riscatti.

**2013:
TORLOCKER**

**2014:
TESLACRYPT**

Questo ransomware attaccava i sistemi Windows e crittografava i file degli utenti, chiedendo un riscatto in Bitcoin o Litecoin per sbloccarli. TeslaCrypt era noto per la sua sofisticata tecnologia di crittografia e per le sue tattiche di negoziazione aggressive.

Ransomware più famoso, WannaCry, ha colpito centinaia di migliaia di computer in tutto il mondo nel 2017, sfruttando una vulnerabilità di Microsoft Windows.

Il ransomware ha causato miliardi di dollari di danni e ha dimostrato il potenziale devastante di questo tipo di attacco informatico.

**2015:
WANNACRY**

**2016:
PETYA**

Un altro ransomware worm altamente dannoso, Petya ha colpito nel 2016 principalmente le organizzazioni Ucraine. Simile a WannaCry, Petya ha sfruttato una vulnerabilità di Microsoft Windows per diffondersi e ha crittografato i file dei sistemi infetti, rendendoli inutilizzabili.

Una variante di Petya, NotPetya si è diffusa rapidamente in tutto il mondo nel 2017, causando danni ancora maggiori rispetto al suo predecessore. NotPetya ha preso di mira le organizzazioni in diversi settori, tra cui l'assistenza sanitaria, le finanze e il governo.

**2017:
NOTPETYA**

**2019:
SODINOKIBI**

Questo ransomware è diventato noto per i suoi attacchi mirati di alto livello contro grandi aziende, tra cui Norsk Hydro e Trafigura. Sodinokibi è stato anche utilizzato negli attacchi alla supply chain che hanno colpito aziende come JBS e Kaseya.

Altro gruppo ransomware molto attivo, Maze è noto per la sua sofisticata tattica di "doppia estorsione", che minaccia di pubblicare i dati rubati delle vittime se non viene pagato un riscatto.

**2020:
MAZE**

**2021:
CONTI**

Divenuto uno dei più prolifici e pericolosi al mondo, responsabile di attacchi contro diverse grandi aziende, tra cui Eni, Conti è noto per la sua abilità nell'eludere i sistemi di sicurezza e per le sue richieste di riscatto elevate.

Emerso come uno dei principali attori nel panorama delle minacce informatiche e responsabile di attacchi contro società come Vodafone e Accenture, LockBit è noto per la sua vasta gamma di tattiche di attacco e per la sua capacità di adattarsi alle nuove tecnologie di sicurezza.

**2022:
LOCKBIT**

**2023:
BLACKCAT**

Questo gruppo ransomware è relativamente nuovo, ma è già diventato uno dei più attivi al mondo. BlackCat è noto per i suoi attacchi mirati contro aziende di grandi dimensioni e per l'utilizzo di sofisticate tecniche di evasione.

E' emerso di recente come una seria minaccia, Hive è noto per la sua abilità nel negoziare con le vittime e per la sua disponibilità a collaborare con altri gruppi ransomware.

**2024:
HIVE**

SOMMARIO

1. Prefazione.....	6
2. Introduzione.....	9
3. Visione Cyber Italia vs Mondo.....	10
4. Visione Italia: caso Fastweb.....	17
4.1 Malware e botnet.....	18
4.2 Attacchi DDoS (Distributed Denial of Service).....	19
4.3 Servizi critici esposti su Internet.....	21
4.4 Blocklist.....	23
5. Affrontare lo skill shortage nella cybersecurity: sfide e opportunità...	25
5.1 Strategie e prospettive per mitigare il fenomeno.....	26
6. Speciale finanza: analisi del cybercrime finanziario	30
6.1 Caratteristiche del phishing.....	32
6.2 Financial Malware.....	34
6.3 Furto delle credenziali.....	37
7. Strategia di data security nell'era dell'IA generativa.....	39
8. Sicurezza Ibrida.....	49
9. Cloud adoption e Cloud-Native Application Protection Platform.....	55
9. Conclusioni.....	60
10. Bibliografia/Sitografia.....	62
11. Contatti.....	

PREFAZIONE

Il presente report, realizzato da Planetica grazie alle competenze interne in materia di cybersecurity, analizza i dati più rilevanti in materia di sicurezza informatica per il biennio 2023-2024 con un focus particolare sulla situazione globale. Anche quest'anno il quadro che emerge è preoccupante, con un numero di incidenti di sicurezza informatica in aumento rispetto all'anno precedente. Nonostante gli sforzi compiuti fino ad oggi, la nostra società non ha ancora raggiunto una capacità difensiva adeguata rispetto ad altri Paesi. Ciò è particolarmente evidente se consideriamo le competenze digitali, un settore in cui mostriamo ancora molte lacune a livello nazionale. Il nostro impegno per la sicurezza informatica deve essere rafforzato, a partire dall'investimento in competenze digitali e in formazione specialistica. Inoltre, è necessario un maggiore sostegno economico per garantire un'adeguata protezione dei sistemi. Solo attraverso un impegno congiunto e costante potremo affrontare le sfide poste dalla sicurezza informatica e garantire la tutela dei nostri sistemi e dei nostri dati. Occorre quindi pensare in modo innovativo tenendo conto dei seguenti aspetti:

- **Valutazione della sostenibilità a lungo termine degli investimenti in Cybersecurity:** investire in tecnologia digitale è fondamentale, ma è altrettanto importante valutare i costi a lungo termine associati all'aggiornamento e alla manutenzione di queste tecnologie per evitare l'obsolescenza e garantire la cybersecurity. Tuttavia, non tutti gli imprenditori e le pubbliche amministrazioni hanno le capacità e le risorse per calcolare con precisione questi costi.

- **Imporre limiti nel Far West digitale:** l'attuale scenario digitale ricorda il "Far West", con limitate regolamentazioni su chi può vendere e acquistare tecnologia. Questa mancanza di controlli può portare a un uso scorretto e a danni all'ecosistema e/o a terzi. Pertanto, è cruciale definire limiti e regolamentazioni per garantire un uso responsabile della tecnologia.
- **Responsabilizzare le persone che arrecano danni nell'ecosistema digitale:** nel "Far West" digitale, dove manca spesso una pianificazione degli investimenti, le persone che causano danni all'ecosistema digitale e/o a terzi devono essere ritenute responsabili.

Nonostante la complessità della situazione attuale, le istituzioni e il legislatore nazionali stanno svolgendo un ruolo importante cercando di gestire i fenomeni connessi alla sicurezza digitale.

Andrea Rivetti
Amministratore &
Equity Partner

Matteo Marco Marzan
Amministratore &
Equity Partner

INTRODUZIONE

Nel 2023, il mondo ha affrontato un ordine geopolitico polarizzato, molteplici conflitti armati, scetticismo e entusiasmo per le implicazioni delle tecnologie future e uno scenario di incertezza economica globale. In questo contesto complesso, **l'economia della cybersecurity è cresciuta in modo esponenzialmente più rapido** rispetto all'economia globale nel suo complesso e ha superato la crescita del settore tecnologico. Tuttavia, molte organizzazioni e paesi hanno sperimentato questa crescita in modi eccezionalmente diversi. È emersa una netta divisione tra le organizzazioni resilienti in termini di cybersecurity e quelle in difficoltà. Questa chiara divergenza delle competenze in termini di cybersecurity è aggravata dai contorni del panorama delle minacce, dalle tendenze macroeconomiche, dalla regolamentazione di settore, come DORA e l'AI Act, e dall'adozione anticipata di tecnologie da parte di alcune organizzazioni. Altri evidenti ostacoli, come il costo crescente dell'accesso ai servizi, agli strumenti, alle competenze e all'esperienza di cybersecurity innovativi, continuano ad influenzare la capacità dell'ecosistema globale di costruire uno spazio cibernetico più sicuro durante le transizioni. Nonostante questa divisione, molte organizzazioni segnalano chiari progressi in alcuni aspetti delle loro capacità cibernetiche. Le piccole e medie imprese (PMI), nonostante rappresentino la maggioranza degli ecosistemi di molti paesi, sono colpite in modo sproporzionato da questa disparità:

- Il numero di organizzazioni che mantengono la resilienza cibernetica minima vitale è diminuito del 30%. Mentre le grandi organizzazioni hanno dimostrato guadagni eccezionali in termini di resilienza cibernetica, le PMI hanno mostrato un calo significativo.
- Più del doppio delle PMI rispetto alle organizzazioni più grandi afferma di non avere la resilienza cibernetica per soddisfare i propri requisiti operativi critici.
- Il 90% dei 120 dirigenti intervistati al Meeting annuale del Forum economico mondiale sulla cybersecurity ha affermato che è necessaria un'azione urgente per affrontare questa crescente disuguaglianza cibernetica.

Le tecnologie emergenti renderanno sempre più gravose le sfide relative alla Cybersecurity, accelerando ulteriormente il **divario tra le organizzazioni più capaci e quelle meno preparate.**

Un esempio su tutti riguarda l'Intelligenza Artificiale di cui sappiamo ancora molto poco delle reali possibilità e dei pericoli associati, ad esempio è necessaria una comprensione di base delle implicazioni in relazione alla sicurezza di breve, medio e lungo periodo. Meno di un intervistato su dieci ritiene che nell'arco di due anni l'IA generativa darà vantaggi ai difensori rispetto agli attaccanti e circa la metà dei dirigenti afferma che gli sviluppi delle capacità avversarie (phishing, malware, deepfake) rappresentano l'impatto più preoccupante sulla cybersecurity.

La carenza di competenze e talenti in ambito Cyber continua ad essere un problema persistente per poter affrontare le sfide del contesto moderno.

VISIONE CYBER ITALIA VS MONDO

In questa sezione andremo ad illustrare gli incidenti di sicurezza di pubblico dominio avvenuti nel mondo nello scorso anno, confrontandoli con i dati raccolti nei 4 anni precedenti. Tra il 2019 e il 2023 sono stati rilevati 10.858 cyber attacchi con un +12% di crescita degli incidenti dal 2022 al 2023.

Negli ultimi 12 mesi, abbiamo avuto il numero più alto di incidenti di sempre, ovvero 2.779

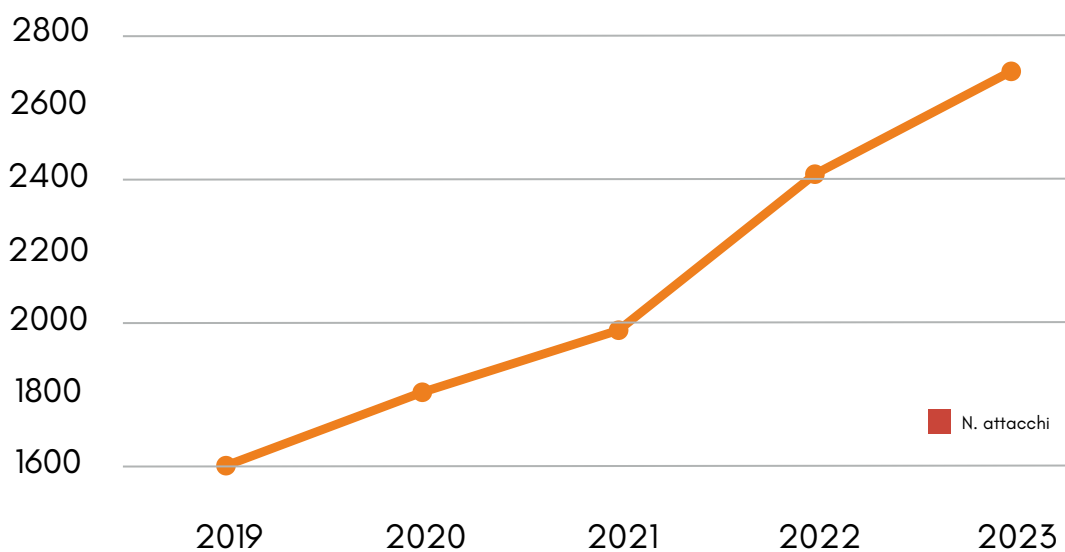


Figura 1 - Andamento dei cyber attacchi nel periodo 2019-2023 - Fonte: Rapporto Clusit 2024

È interessante notare che a partire dal 2019 il numero di incidenti ha superato le previsioni, e questa tendenza è rimasta stabile negli ultimi due anni, gli incidenti sono aumentati più velocemente di quanto ci si aspettava confermando quindi un costante peggioramento dello scenario globale. Come ulteriore elemento rafforzativo di questa tesi evidenziamo infatti che il picco massimo dell'anno, nonché peggior dato mai rilevato, è stato registrato a aprile 2023, con un numero di 270 attacchi.

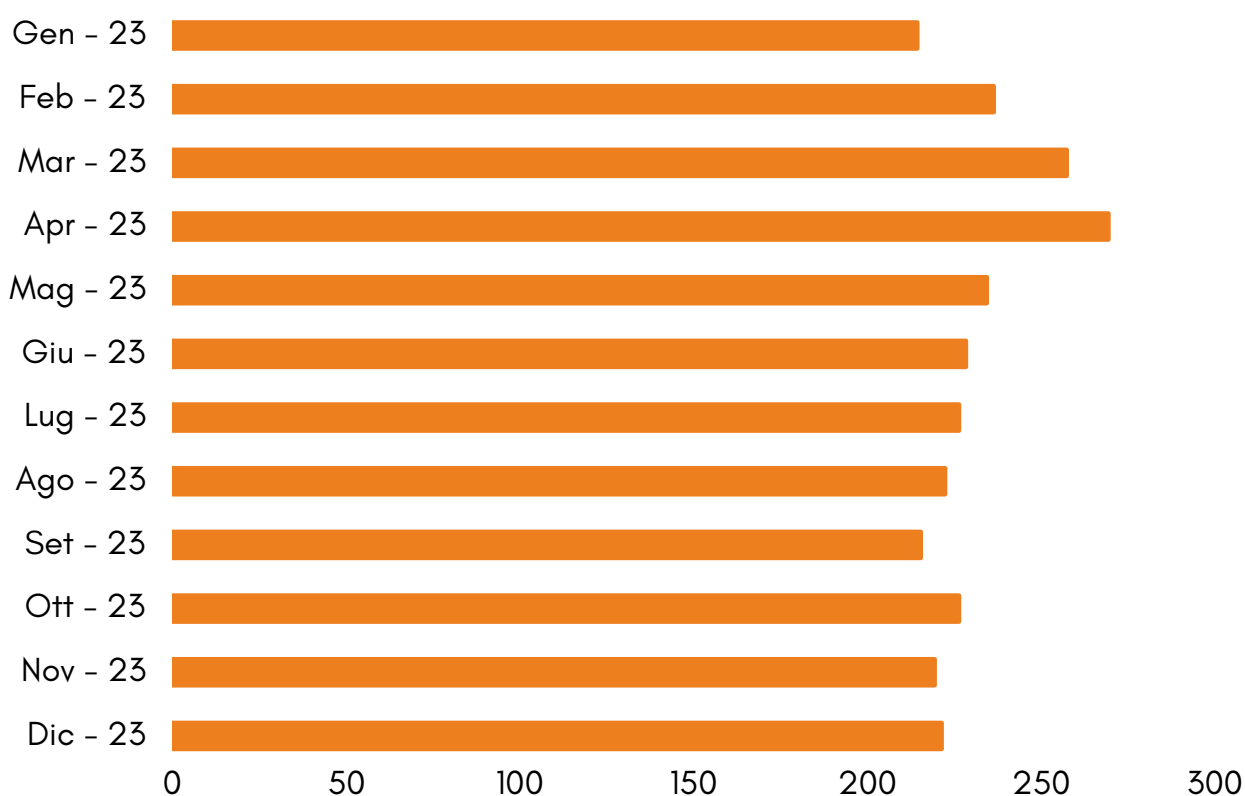


Figura 2 - Attacchi per mese a livello globale nel 2023 - Fonte: Rapporto Clusit 2024

Tuttavia, alcuni fenomeni mostrano una diminuzione piuttosto marcata, ad esempio per l'Espionage si passa dai 259 attacchi del 2022 ai 178 del 2023 mentre per l'Information Warfare dai 103 ai 46. Aumenta invece la frequenza degli attacchi dovuti ad attività di Hacktivism che triplicano passando dagli 84 del 2022 ai 239 del 2023. Il grafico sottostante evidenzia la distribuzione degli attaccanti nel periodo dal 2019 al 2023.

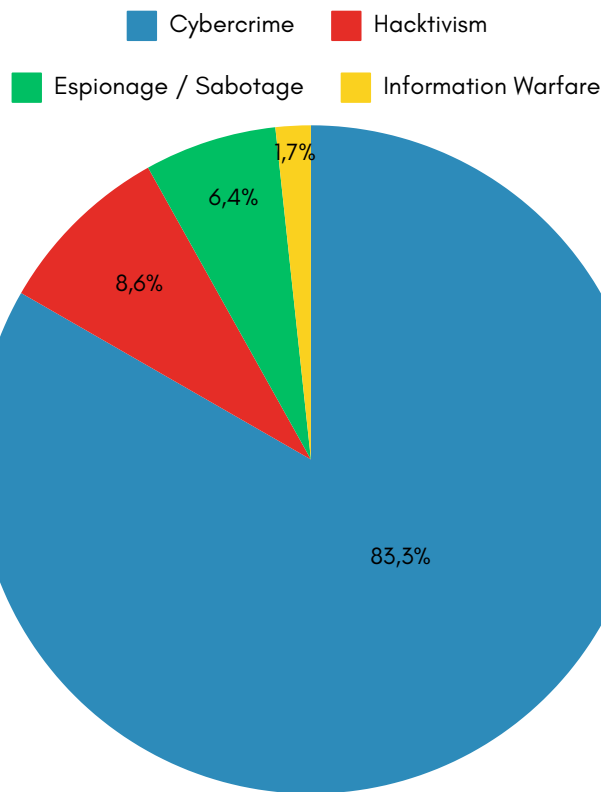



Figura 3 - La distribuzione percentuale degli attaccanti tra il 2019 e il 2023 - Fonte: Rapporto Clusit 2024



Il Cybercrime continua ad essere la **minaccia principale alla sicurezza informatica**, con una tendenza in costante crescita negli ultimi anni. Nel 2023, si è registrato un aumento del 13,4% rispetto all'anno precedente, confermando le previsioni degli analisti.

Un particolare relativo al Cybercrime è che la linea di demarcazione tra criminalità "off-line" e "on-line" si sta sempre più assottigliando, se non addirittura scomparendo. I criminali sfruttano i proventi delle loro attività illegali nel mondo reale per reinvestire nel cybercrime, creando un circolo vizioso che alimenta la crescita di questo fenomeno.

La distribuzione delle vittime degli attacchi nel nostro Paese si differenzia significativamente dal campione evidenziato su livello mondiale e si è rilevata la riduzione del 3% dell'incidenza sul totale di Multiple Target, a dispetto di un aumento nel settore Healthcare del 2% e del 3% nel comparto Financial / Insurance.

Anche i settori dell'istruzione, dell'industria manifatturiera, dei trasporti e del commercio all'ingrosso e al dettaglio hanno subito un aumento degli attacchi informatici nell'ultimo anno. Tra questi, il settore Manufacturing è quello che ha avuto la crescita più significativa, raggiungendo il suo massimo storico (dal 2% al 6% del totale degli attacchi in 5 anni). Questa tendenza evidenzia che nessun settore è immune al rischio Cyber, e che è fondamentale per tutte le aziende, indipendentemente dal settore, adottare adeguate misure di sicurezza per proteggersi.

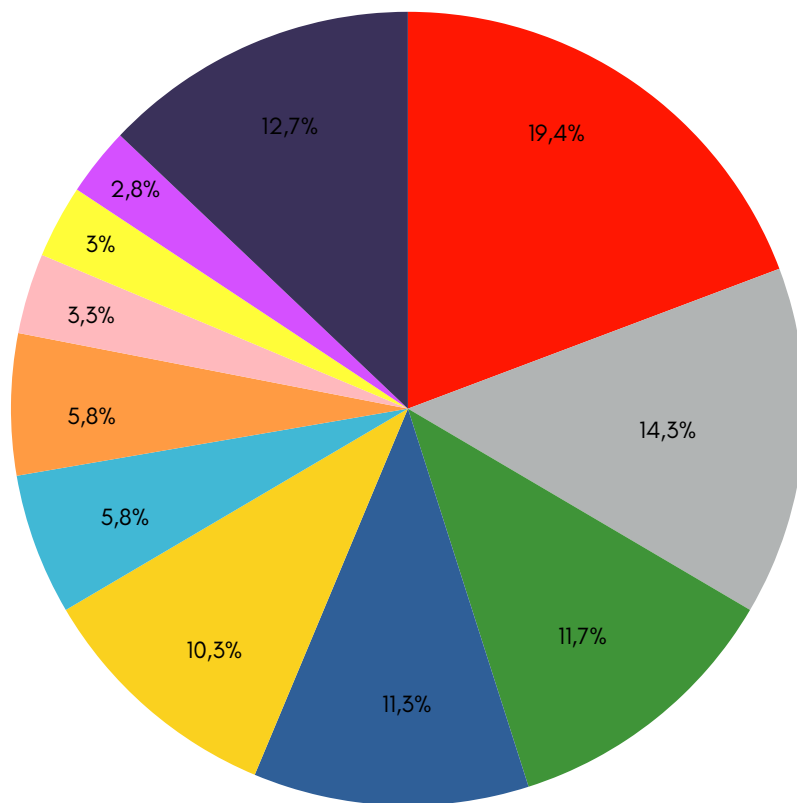
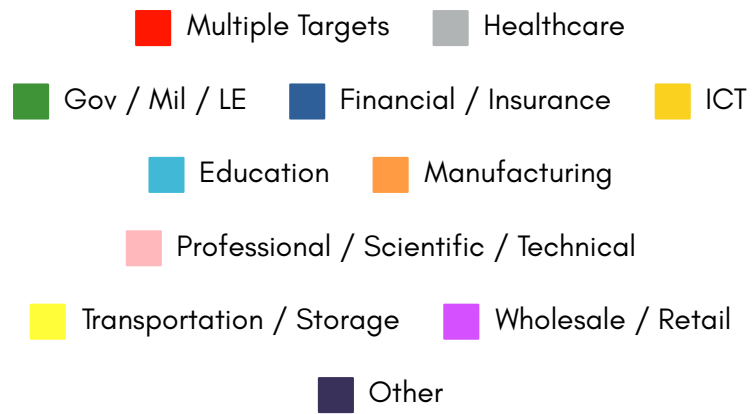



Figura 4 - Distribuzione della tipologia di vittime nel 2023 - Fonte: Rapporto Clusit 2024



L'analisi dei numeri assoluti in rapporto agli anni precedenti, ci fa capire lo scenario delle vittime in relazione alla totalità degli attacchi. Se dal grafico precedente il numero di incidenti relativi alla categoria di Multiple target è inferiore rispetto al 2022, in valore assoluto, gli attacchi sono quasi equivalenti (539 vs 540), risultando per il secondo anno consecutivo la categoria più attaccata. Al contempo, il settore governativo subisce un colpo ancora più duro, con 325 attacchi contro i 301 subiti l'anno precedente.

Nel panorama delle minacce informatiche, **gli attacchi DDoS emergono come la tecnica più diffusa**, con un incremento esponenziale dal 4% del 2022 al 36% di quest'anno. Questo dato allarmante è trainato in modo significativo dall'aumento di campagne di hacktivism, che sfruttano gli attacchi DDoS per amplificare il loro messaggio e portare all'attenzione del pubblico cause sociali e politiche.

Gli hacktivist prediligono gli attacchi DDoS per la loro capacità di interrompere i servizi online di aziende e organizzazioni. In questo modo riescono a creare disagi significativi e a richiamare l'attenzione su questioni che ritengono importanti. La violazione di un sito web tramite un attacco DDoS può rappresentare un potente strumento di denuncia e protesta, capace di sensibilizzare l'opinione pubblica e di fare pressione su governi e istituzioni.

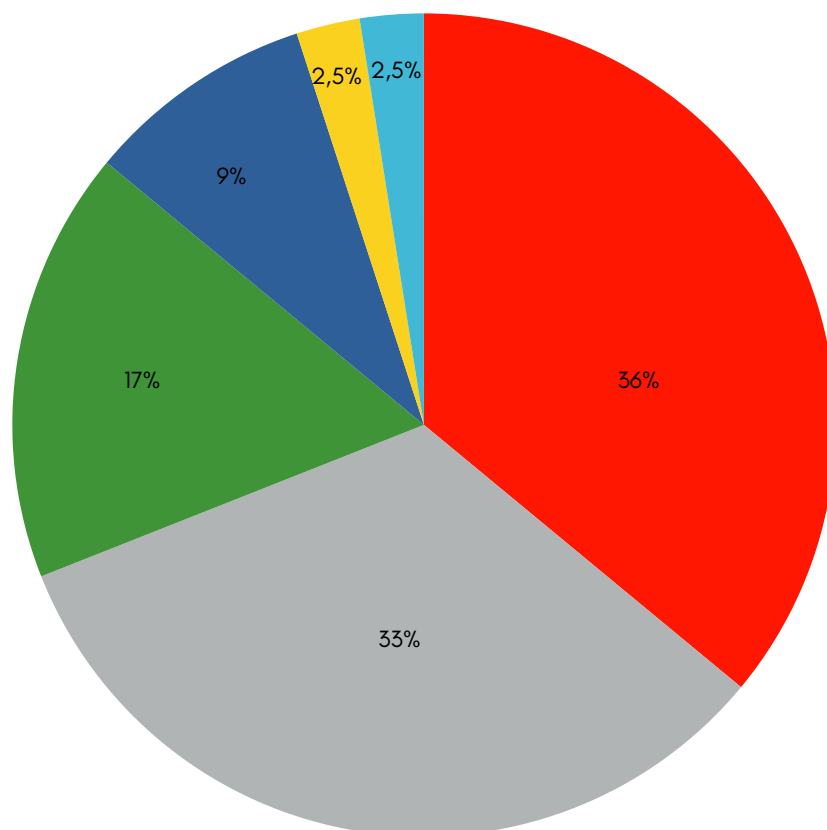


Figura 5 - Tecniche di attacco in Italia nel 2023 - Fonte: Rapporto Clusit 2024

Degna di nota la percentuale degli attacchi con i Malware, in seconda posizione, che passa dal 53% al 33%, sebbene gli incidenti siano cresciuti in valore assoluto. Il Phishing è aumentato leggermente dall'8% al 9%, rimangono stabili le Vulnerabilities ed entrano nelle statistiche i Web Attack.

VISIONE ITALIA: IL CASO FASTWEB


Questa sezione illustra la situazione del cybercrime in Italia, offrendo un'analisi approfondita dei fenomeni e delle tendenze più significative, riportando di seguito l'esempio Fastweb come case study.

Sul fronte degli attacchi DDoS (Distributed Denial of Service) nel 2023, sono stati rilevati circa 2300 eventi significativi e circa 13.000 anomalie riconducibili a possibili attacchi alla rete di Fastweb. Si è registrato un incremento deciso degli eventi DDoS ad alto impatto, con un aumento del 32% rispetto all'anno precedente, mentre le anomalie a basso impatto sono diminuite del 40%. I settori più colpiti sono Finance/Insurance e Pubblica Amministrazione che insieme costituiscono oltre il 55% dei casi.

Il settore del Gambling ha registrato un aumento significativo, passando dal 2% del 2022 a quasi il 12% nel 2023. Inoltre, il numero di server e dispositivi privi di livelli minimi di protezione è in costante diminuzione, con un calo dell'8% tra il 2022 e il 2023. Il numero di malware e botnet ha registrato una flessione del 3% rispetto al 2022, con una riduzione del numero delle famiglie di software malevoli del 29%.

Tra le minacce, Adload rappresenta il 27% delle rilevazioni totali, un adware malevolo che si diffonde tramite link.

L'utilizzo di URL malevoli rimane, infatti, il principale metodo per veicolare attacchi con il 90% dei casi, mentre le campagne fraudolente che utilizzano tattiche di social engineering sono in aumento del 13%.



L'integrazione dell'Intelligenza Artificiale negli strumenti di riconoscimento e difesa delle minacce ha migliorato la capacità di raccogliere informazioni sugli attori degli attacchi cyber, con un aumento significativo di nuove minacce individuali nel 2023.

Nell'ambito del phishing, l'Intelligenza Artificiale generativa consente ai criminali informatici di creare attacchi sempre più credibili e pericolosi, generando contenuti testuali accurati che evitano errori ortografici o di traduzione, rendendo gli attacchi più difficili da rilevare.

Le rilevazioni di Fastweb nel 2023 evidenziano un aumento della consapevolezza e della resilienza delle aziende e della pubblica amministrazione in materia di sicurezza cibernetica. Questo si traduce in una maggiore adozione di soluzioni di protezione per contrastare un panorama di attacchi sempre più sofisticati. L'evoluzione del panorama cyber conferma la centralità e l'importanza di adottare sistemi di sicurezza completi e avanzati per proteggere gli asset strategici e le persone, garantendo l'operatività aziendale.

A seguire alcuni approfondimenti sui fenomeni rilevati.

Malware e botnet

Nel 2023, il numero di infezioni malware e di attacchi botnet contro i server e i dispositivi di Fastweb hanno mostrato una diminuzione del 2,5% rispetto all'anno precedente. Nonostante ciò, il numero totale di infezioni è rimasto sostanzialmente stabile rispetto agli anni precedenti.



Dopo il picco registrato nel 2022, con 208 famiglie di malware (un aumento del 21,6% rispetto al 2021), il numero di famiglie dannose è tornato ai livelli precedenti, con 148 famiglie (-29%). Come evidenziato nel grafico sotto, nel corso del 2023 si è verificato un aumento graduale dei dispositivi infetti, a differenza del 2022, dove il numero di infezioni è diminuito dopo un picco a gennaio.

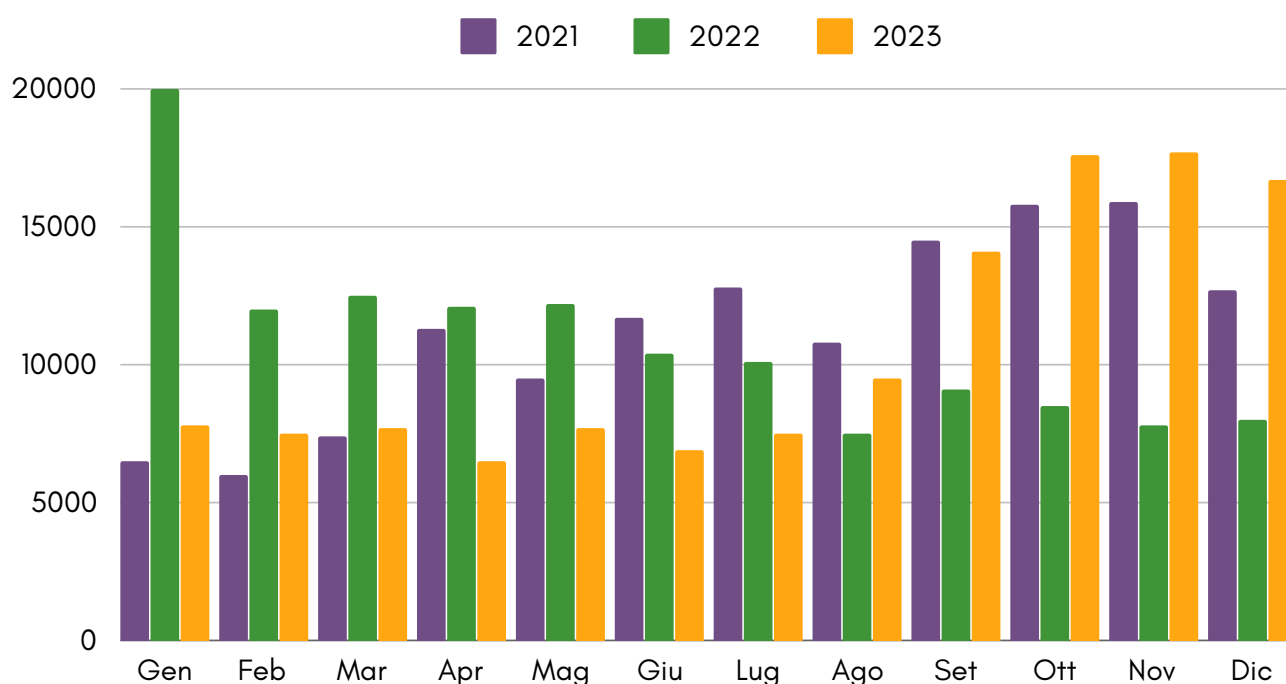



Figura 6 - Distribuzione temporale del numero di infezioni rilevate- Fonte: Rapporto Clusit 2024

Attacchi DDoS (Distributed Denial of Service)

Un attacco DoS (Denial of Service) è un tentativo di bloccare un computer, una rete o anche solo un servizio specifico. Alcuni attacchi mirano a un'applicazione o servizio particolare, come Web, SMTP, FTP, mentre altri cercano di disabilitare completamente un server.



Gli attacchi DDoS amplificano il potenziale di tali minacce, sfruttando le botnet, costituite da decine di migliaia di dispositivi (non solo computer di utenti inconsapevoli), per inviare richieste massicce verso un obiettivo specifico. Lo scopo è saturarne rapidamente la capacità rendendolo indisponibile o irraggiungibile. I danni che possono causare sono significativi per via della loro potenza e della complessità nel mitigarli tempestivamente (a meno che non si ricorra a specifici servizi di remediation).

Nel corso del 2023, sono stati individuati oltre 2.400 eventi di rilevanza significativa e 13.000 anomalie potenzialmente correlate a attacchi DDoS diretti alla rete di Fastweb. I casi gravi registrano un aumento del 32% rispetto al 2022, invertendo così il trend discendente osservato nei due anni precedenti, principalmente a causa dei notevoli cambiamenti nel panorama digitale introdotti dalla pandemia. Al contrario, le anomalie con impatto minore sono diminuite del 40% rispetto al 2022.

L'incremento nel numero di eventi rilevanti si è manifestato nella seconda metà dell'anno, soprattutto nell'ultimo trimestre, durante il quale l'impatto aggregato mensile di tutti gli attacchi DDoS rilevati e gestiti ha raggiunto livelli senza precedenti per Fastweb.

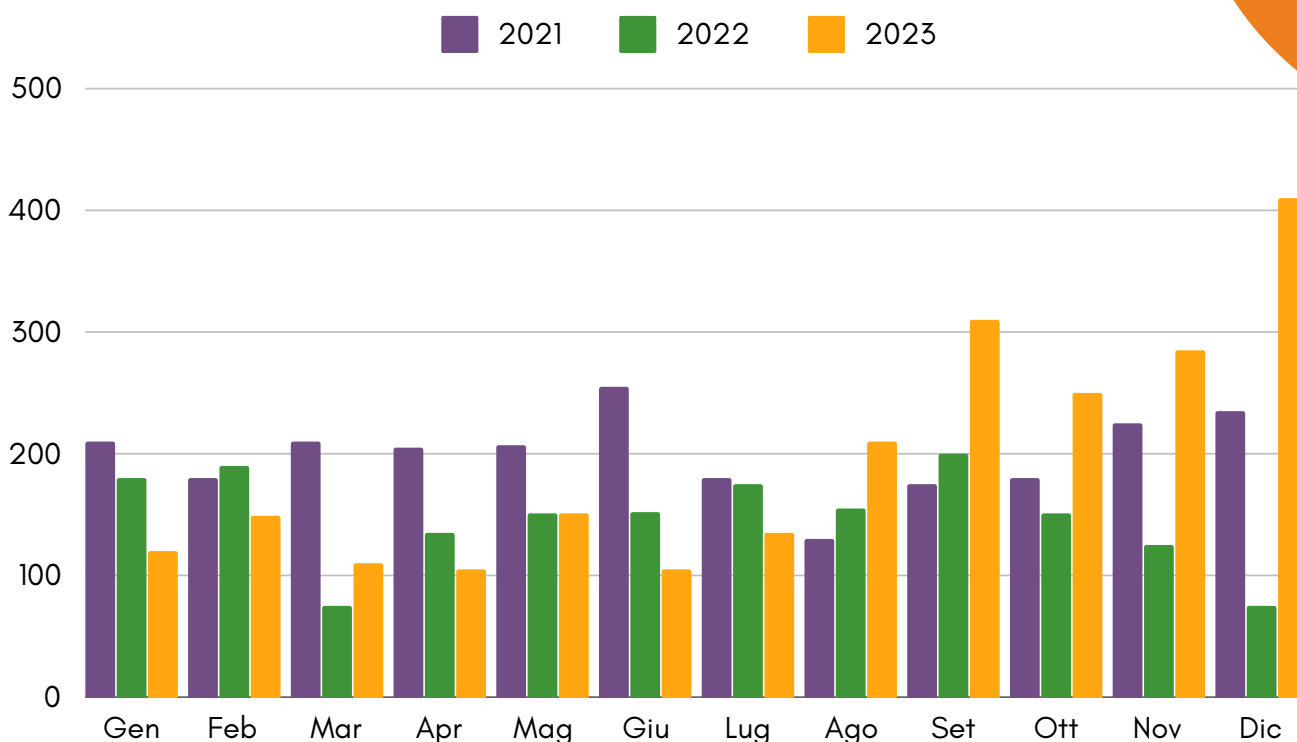


Figura 7 - Distribuzione mensile delle anomalie DDos - Fonte: Rapporto Clusit 2024

Come evidenziato nel grafico, in termini di attacchi misurati attraverso l'aggregazione mensile della banda, si osserva un aumento del 72% rispetto al 2022. Questo aumento è principalmente attribuibile all'aumento degli eventi dannosi singoli e alla maggiore disponibilità di banda dei sistemi compromessi, spesso presenti in ambienti cloud o in aree geografiche con una diffusione più ampia della banda larga.

Servizi critici esposti su Internet

La rilevazione del 2023 indica che ci sono circa 38.000 server e dispositivi che espongono protocolli a rischio su Internet, registrando una diminuzione dell'8% rispetto al 2022, in cui ne erano stati rilevati oltre 41.000. Questa tendenza discendente si è mantenuta costante negli ultimi anni, con una diminuzione del 9% nel 2022, del 16% nel 2021 e del 18% nel 2020.

Questa diminuzione costante riflette una maggiore attenzione e consapevolezza delle aziende riguardo alla sicurezza, con un conseguente innalzamento delle misure di difesa di base e una maggiore attenzione ai servizi esposti, proteggendo quelli critici e implementando politiche per difendere gli utenti, anche in modalità di lavoro remoto come lo smartworking. L'aumento degli eventi di sicurezza e la diminuzione delle infezioni sottolineano una tendenza positiva per la cybersicurezza che sta diventando sempre più centrale nelle agende aziendali.

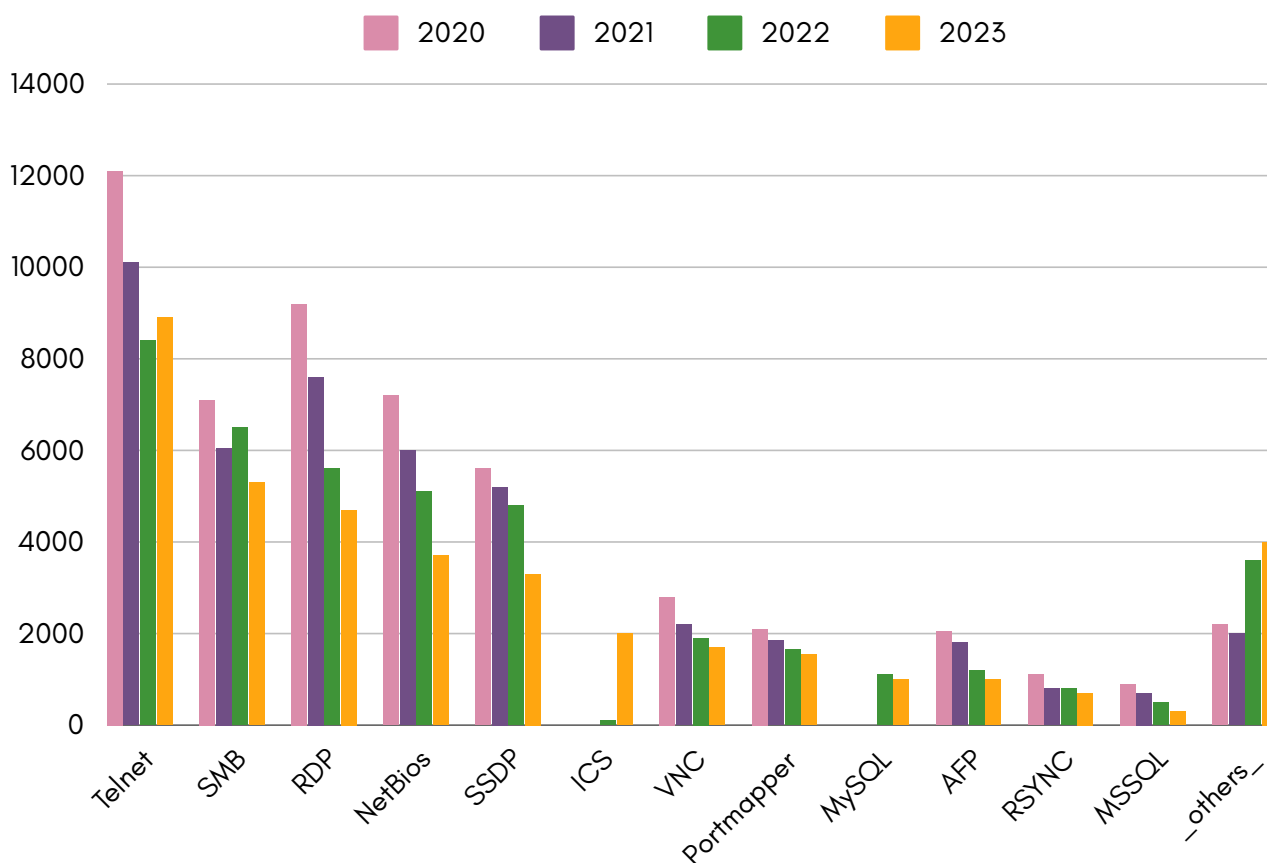


Figura 8 - Servizi critici esposti su Internet (Dati Fastweb relativi agli anni 2019 - 2023) - Fonte: Rapporto Clusit 2024

Blocklist

Nel 2023, le blocklist hanno registrato un calo significativo del 51% rispetto al 2022, con oltre 1.600 IP inseriti almeno una volta. I motivi principali per l'inserimento in queste liste includono l'invio massivo di e-mail non autorizzate, la presenza di segni tipici dello spam nelle comunicazioni e l'infezione da virus che genera attività dannose. Questo calo è in netto contrasto con la tendenza del 2022, che aveva visto circa 3.400 azioni di blocklisting.

Nonostante ciò, il numero generale di infezioni da malware è rimasto stabile, con un lieve calo del 2,5% rispetto all'anno precedente. Questo fenomeno suggerisce che i malware stiano diventando più mirati e meno invasivi, capaci di effettuare azioni più specifiche e di evitare comportamenti "rumorosi" e diffusi.

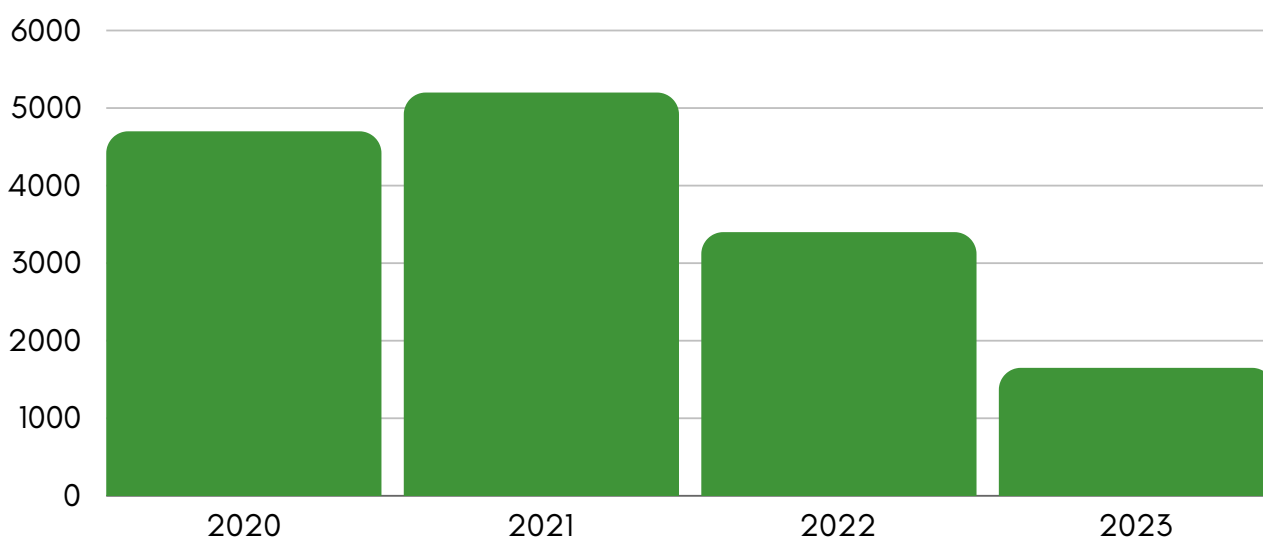


Figura 9 - Quantità di IP in Blocklist dal 2020 al 2023 - Fonte: Rapporto Clusit 2024

A livello nazionale le differenze rimangono simili a quanto visto nel 2022, con le regioni del nord Italia in testa con il 55% delle infezioni totali.

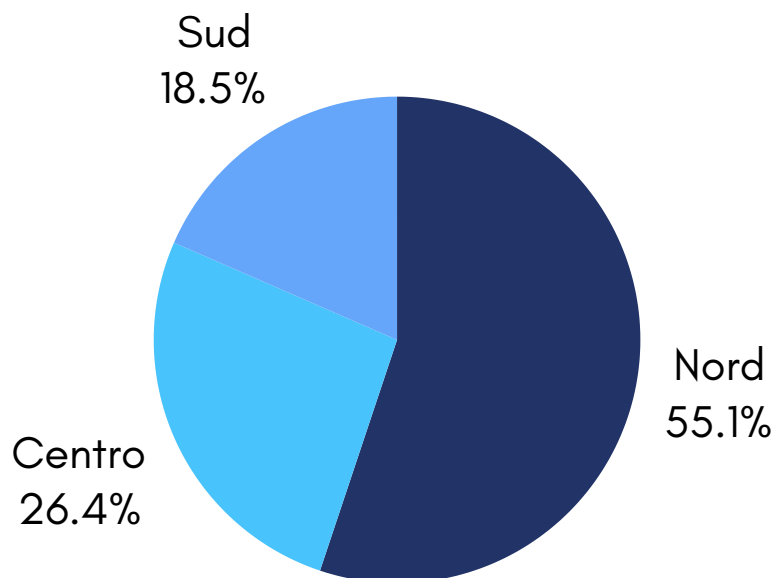


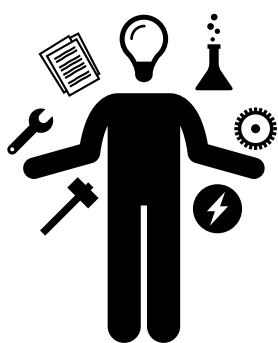
Figura 10 - Distribuzione geografica dei server in blacklist (Dati Fastweb relativi all'anno 2023) - Fonte: Rapporto Clusit 2024

SKILL SHORTAGE NELLA CYBERSECURITY: SFIDE E OPPORTUNITÀ

Nel 2024, la carenza di competenze nel settore della sicurezza informatica sarà ancora tema centrale in Italia. **Il 75% delle aziende ha serie difficoltà ad assumere risorse qualificate** per il settore della cybersecurity e il 50% fatica persino a trovare un singolo candidato per le posizioni necessarie richieste. La carenza di competenze pratiche e operative rappresenta un problema diffuso in Italia, con il sistema accademico che fornisce ancora solo conoscenze teoriche in materia di cybersecurity. Le competenze maggiormente richieste in Italia riguardano la gestione dei sistemi di sicurezza informatica, l'identificazione e la mitigazione delle vulnerabilità dei sistemi, la comprensione delle tecniche di attacco e la capacità di implementare misure di sicurezza adeguate. La spesa per la cybersecurity in Italia è in costante aumento, con una stima che prevede di raggiungere i 1.825,5 milioni di euro nel 2023. Per mitigare gli effetti della carenza di competenze, le aziende possono adottare un approccio proattivo alla cybersecurity, **investendo in programmi di formazione** e riconversione per i propri dipendenti e collaborando con fornitori di servizi gestiti e di sicurezza gestita (MSP/MSSP). Inoltre, i professionisti della cybersecurity dovranno sviluppare competenze trasversali, come la comunicazione interpersonale, la gestione delle relazioni interpersonali e le capacità di problem-solving.

La formazione regolare sui rischi cyber per i dipendenti IT, con investimenti mirati in materia e nelle soluzioni centralizzate e automatizzate sono fondamentali per elevare le competenze e ridurre il carico di lavoro del team di professionisti IT. La disponibilità a potenziare le conoscenze in materia di sicurezza sarà un fattore chiave per promuovere la fiducia tra CISO e la gestione della resilienza informatica approvata dal Consiglio di amministrazione sarà via via più importante.

Strategie e prospettive per mitigare il fenomeno



Recenti studi sottolineano la crescente carenza, in termini globali, di competenze nel campo della cybersecurity. Il 36% degli intervistati afferma che la **mancanza di competenze tecniche e relazionali** critiche è il **principale ostacolo** che impedisce alle organizzazioni di **raggiungere i propri obiettivi strategici di cyber-resilienza**. La carenza non si limita a compiti specifici, ma comprende anche la mancanza di creatività, giudizio umano e capacità di comunicazione sfumata, come quelle richieste per ruoli da analisti della sicurezza informatica. Il World Economic Forum (WEF) ha identificato una carenza globale di quasi 4 milioni di professionisti della sicurezza informatica. Questo divario di competenze è aggravato dai rapidi progressi tecnologici che hanno superato l'istruzione e la formazione tradizionali, portando alla necessità di un ampio set di competenze che vanno dall'analisi del traffico di rete alla gestione della sicurezza e alla valutazione dei rischi. Il report sottolinea inoltre l'importanza dell'istruzione sulla sicurezza informatica e la necessità di un suo significativo miglioramento nei prossimi due anni.

Le principali cause del divario di competenze nel campo della cybersecurity includono:

- **Rapida espansione del panorama digitale e crescente frequenza e complessità delle minacce informatiche:** serve una forza lavoro dotata di competenze e conoscenze aggiornate per contrastare queste sfide in continua evoluzione.
- **Scarsa attrattività del settore:** i migliori talenti sono richiesti in molteplici settori, creando una mancanza di offerta di personale qualificato sufficiente a soddisfare la domanda.
- **Disallineamento tra formazione e richieste del settore:** i programmi offerti agli aspiranti professionisti della cybersecurity potrebbero non sempre allinearsi con le esigenze del settore, con conseguente carenza di competenze pratiche e conoscenze adeguate tra i laureati.
- **Rapidità del cambiamento nel settore:** i curriculum educativi tradizionali potrebbero faticare a tenere il passo con il panorama in continua evoluzione della cybersecurity, creando un divario di competenze.
- **Dipendenza crescente dalla tecnologia:** la necessità di professionisti qualificati aumenta sempre più rapidamente a causa dei progressi tecnologici e del crescente affidamento delle organizzazioni sulla tecnologia.
- **Complessità crescente delle minacce:** il panorama delle minacce in continua evoluzione richiede professionisti esperti di cybersecurity per aiutare a risolvere e mitigare i rischi.
- **Pressione sul personale esistente:** la forza lavoro esistente combatte contro la crescente pressione e le richieste, dovendosi difendere dalle minacce informatiche che aumentano in complessità, sofisticazione e frequenza.

- **Mancanza di diversità:** la forza lavoro nel settore della cybersecurity è poco diversificata, con solo il 25% circa di donne a livello globale e una rappresentanza limitata di altri gruppi sottorappresentati.
- **Aspettative irrealistiche dei datori di lavoro:** le descrizioni dei lavori spesso richiedono lauree, molteplici certificazioni e anni di esperienza, creando aspettative irrealistiche.
- **Tagli ai costi:** i tagli di budget, i licenziamenti e il blocco delle assunzioni/promozioni svolgono un ruolo fondamentale nel divario di competenze.
- **Maggiori rischi per la sicurezza:** con una carenza di professionisti qualificati, le organizzazioni sono più vulnerabili alle minacce informatiche, poiché ci sono meno persone per monitorare, rilevare e rispondere a potenziali attacchi.
- **Risposta inadeguata alle minacce:** le organizzazioni potrebbero avere difficoltà a rispondere efficacemente alle minacce informatiche a causa della mancanza di personale qualificato, con conseguente aumento dei danni derivanti da cyberattacchi.
- **Gestione del rischio inefficace:** il divario di competenze può ostacolare la capacità di un'organizzazione di valutare e gestire i rischi informatici, portando potenzialmente a misure di sicurezza inadeguate e a una maggiore vulnerabilità.
- **Burnout tra i professionisti della sicurezza informatica:** il carico di lavoro maggiore dovuto al divario di competenze può portare al burnout tra i professionisti della sicurezza informatica esistenti, aggravando ulteriormente il problema.
- **Difficoltà nel reclutamento:** il divario di competenze rende difficile per le organizzazioni trovare e assumere professionisti della sicurezza informatica, questo porta a aumento del carico di lavoro per il personale esistente.

- **Sfide di conformità:** le organizzazioni potrebbero avere difficoltà a soddisfare i requisiti normativi e mantenere la conformità alle normative sulla protezione dei dati a causa della mancanza di personale qualificato.
- **Incapacità di stare al passo con i progressi tecnologici:** il divario di competenze in materia di cybersecurity può ostacolare la capacità di un'organizzazione di rimanere aggiornata sulle ultime tendenze tecnologiche e di cybersecurity, rendendo più difficile proteggersi dalle minacce emergenti.

Per affrontare queste conseguenze, le organizzazioni, soprattutto nell'ambito dei Financial Services, possono prendere in considerazione l'implementazione di programmi di formazione per la propria forza lavoro esistente, l'utilizzo di servizi di sicurezza e la priorità alla formazione e alla consapevolezza sulla cybersecurity.

Planetica, grazie alla sua esperienza in materia, offre percorsi di formazione per professionisti anche in ambito Cyber, erogando corsi attraverso Planetica Academy.

SPECIALE FINANZA: ANALISI DEL CYBERCRIME FINANZIARIO

Il panorama del cybercrime finanziario continua a evolversi, con gruppi internazionali ben organizzati che dominano la scena. Nel corso del 2023, il settore finanziario è stato fortemente preso di mira, specialmente in Europa, con l'Italia che ha subito circa l'8% degli attacchi, seguita da Regno Unito, Germania e Portogallo.

La frode nel settore finanziario coinvolge principalmente il furto delle credenziali d'accesso, spesso utilizzate per transazioni fraudolente. Le principali tecniche includono il **phishing** per ottenere le credenziali, l'uso di **malware** per rubare informazioni sensibili o manipolare le transazioni e il **coinvolgimento diretto degli utenti** in operazioni fraudolente.

Facciamo un ripasso delle principali tecniche utilizzate:

- *Phishing*: Tramite messaggi o siti web falsi, si inganna l'utente per ottenere le sue credenziali di accesso o altre informazioni personali, come numeri di telefono, codici fiscali o indirizzi e-mail. Successivamente, si può interagire con un finto operatore per ottenere ulteriori informazioni necessarie, come codici di autenticazione o dati del dispositivo.
- *Malware*: Si installano programmi dannosi sui dispositivi dell'utente per rubare credenziali o informazioni aggiuntive necessarie per l'autenticazione, o per manipolare transazioni finanziarie.

- *Manipolazione dell'utente*: Si convince l'utente a compiere azioni specifiche, come recarsi presso uno sportello bancario e effettuare operazioni che possono essere sfruttate dai criminali.
- *Hacking del dispositivo mobile*: Si compromettono i dispositivi mobili dell'utente, ad esempio attraverso lo scambio fraudolento della SIM o l'emulazione del software dello smartphone.

Queste tattiche, o la combinazione di tecniche, variano a seconda della tipologia di vittima, con differenze tra clienti individuali e aziendali. Sarebbe naturale pensare che con l'evoluzione delle tecniche si evolvano anche i sistemi di difesa ma dalle ultime analisi svolte, i cyber criminali, hanno ideato innovative quanto fantasiose ragioni per indurre la vittima a recarsi alla sua filiale e fare operazioni dispositive allo sportello, saltando così molti dei controlli effettuati.

In generale c'è una diminuzione degli attacchi meramente tecnologici preferendo il coinvolgimento della vittima per completare l'attacco e rimanere "anonimi".

Nel contesto italiano, il fenomeno è particolarmente attivo, con una media di circa 3,6 nuove pagine di phishing al giorno nel 2023. Per anni si è pensato che il protocollo HTTPS fosse un badge di affidabilità oggi non è più così. Infatti, il 99,5% delle pagine di phishing utilizza questo protocollo.

In sostanza, la presenza dell'icona del lucchetto nella barra degli indirizzi del browser non garantisce più la sicurezza e l'affidabilità del sito. Questo perché i criminali informatici possono utilizzare

certificati di tipo domain validation (DV), che sono i più facili da ottenere e convalidare.

È importante prestare attenzione al tipo di certificato utilizzato: i certificati Organization Validated (OV) e Extended Validation (EV) offrono maggiori garanzie sulla legittimità del proprietario del sito web.

Per proteggersi dal phishing, è essenziale controllare non solo se il sito utilizza il protocollo HTTPS, ma anche il tipo di validazione del certificato. È consigliabile connettersi solo a siti che utilizzano certificati OV o EV. Tutti i browser forniscono un'indicazione visiva sul tipo di validazione del certificato, che può essere utile per valutare la sicurezza del sito.

Caratteristiche del phishing

Tra le caratteristiche del “nuovo” phishing emerge come le attività si concentrano nella seconda parte della settimana lavorativa (mercoledì - venerdì), mirando a sfruttare la vulnerabilità degli utenti quando gli sportelli bancari sono chiusi e gli help desk hanno orario ridotto.

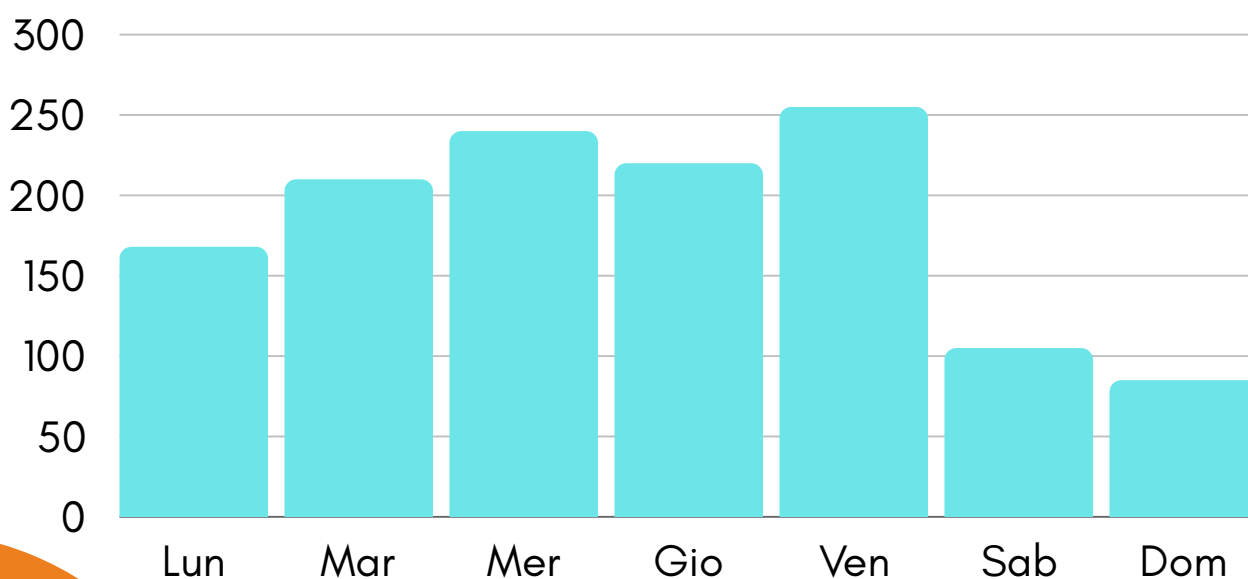


Figura 11 - Ripartizione giornaliera delle pagine di phishing - Fonte: Rapporto Clusit 2024

Il phishing nel settore finanziario italiano avviene principalmente tramite e-mail, SMS e si stanno sviluppando anche nuovi attacchi sfruttando il massivo uso di QRCode. Questi attacchi mirano principalmente a **rubare credenziali di accesso** come il codice cliente, la password, il PIN e l'OTP, insieme ad altre informazioni come il numero di telefono, il codice fiscale e l'indirizzo e-mail dell'utente. Anche informazioni apparentemente non critiche diventano utili quando combinate con altre per creare schemi di attacco su più utenti. La frode di solito avviene in più fasi, rubando gradualmente informazioni per poi usarle tutte insieme per ottenere un accesso fraudolento.



Il 44% delle campagne è stata ospitata direttamente sulla piattaforma cPanel, utilizzata per gestire e amministrare siti internet e servizi di web hosting. Le campagne hanno registrato un notevole aumento nel 2023, colpendo ben 26 delle 40 istituzioni finanziarie esaminate nell'analisi Clusit. Questo approccio ha reso più veloce, conveniente e meno rischiosa la creazione di siti di phishing, risultando irresistibile per gli attaccanti e particolarmente economico.


Durante l'installazione, se l'interfaccia WebHost Manager (WHM) di cPanel non dispone di un hostname, ne viene automaticamente assegnato uno all'interno del dominio cprapid.com, generato in base all'indirizzo IP del server. Parallelamente, la Certification Authority di cPanel, genera un certificato SSL/TLS consentendo connessioni HTTPS senza generare messaggi di errore nei browser dei client. Questo rende estremamente semplice ed economico attivare autonomamente siti web di phishing senza dover fare affidamento su provider internet esterni.

Financial Malware

Secondo l'ENISA, l'Agenzia dell'Unione Europea per la Cybersecurity, i malware rappresentano una delle principali minacce cyber del 2023, subito dopo gli attacchi ransomware (che sono anch'essi malware specializzati), i DDoS e gli attacchi ai dati. In questo contesto, ci concentriamo esclusivamente sui malware finanziari utilizzati per frodi finanziarie.

L'obiettivo finale di questi malware è compiere una **frode finanziaria**, come ad esempio un bonifico dal conto della vittima, e ciò può avvenire secondo diverse modalità.





Gli attacchi sono strutturati in molteplici fasi, che includono: una tecnica di accesso iniziale per ottenere l'accesso al sistema o all'account della vittima, seguita da altre tattiche e tecniche per portare a termine la frode e, eventualmente, coprire le tracce. Dopo aver effettuato la frode, viene messa in atto la fase di monetizzazione, ovvero convertire la transazione elettronica in denaro senza lasciare tracce che possano identificare il frodatore.

In passato, c'era una chiara distinzione tra la clientela retail (i singoli individui che interagiscono con la propria banca) e la clientela corporate (le aziende). Tuttavia, questa distinzione sta diventando sempre meno evidente anno dopo anno. Nel mercato retail, l'uso dei dispositivi mobili sta crescendo rapidamente, mentre nel mercato corporate si utilizzano principalmente workstation con sistema operativo Windows. Per questo segmento, i malware finanziari rappresentano circa il 6,4% degli attacchi. È anche evidente un significativo aumento delle truffe di tipo BEC (Business E-mail Compromise), che contribuiscono al 49,7% degli attacchi.

In entrambi i casi, sia nel settore retail che corporate, il numero di frodi compiute attraverso malware sta diminuendo rispetto all'anno precedente. Questo è dovuto **all'aumento dell'efficacia dei sistemi antifrode**, all'utilizzo dell'intelligenza artificiale per individuare transazioni sospette e alla rapida analisi dei malware direttamente da parte delle istituzioni finanziarie e dei loro fornitori di sicurezza. Di conseguenza, gli sforzi dei frodatori si stanno spostando verso la manipolazione della vittima per indurla a compiere l'operazione, ad esempio convincendola a recarsi allo sportello.

Le operazioni allo sportello, infatti, poiché vengono effettuate in presenza dell'intestatario del conto, evitano molti dei controlli cui sono soggette le operazioni online remote.

Secondo le rilevazioni dell'ENISA, i dati e le valutazioni sul malware per frodi nel settore finanziario mostrano un significativo decremento nell'uso dei codici malware per compiere frodi finanziarie. Tuttavia, ciò non ha portato a una diminuzione parallela degli incidenti, ma piuttosto a una loro trasformazione.

Durante il 2023, si è osservato un notevole aumento nell'utilizzo d'InfoStealer generici che danno la possibilità ai nuovi cyber criminali di entrare nel mercato senza la necessità di competenze avanzate. I cyber criminali hanno preferito utilizzare software malevoli generici, come InfoStealers o Remote Access Tools piuttosto che malware specializzati per frodi finanziarie. Questo cambiamento segna una svolta importante, poiché **riduce il livello di competenza richiesto per condurre un attacco.**

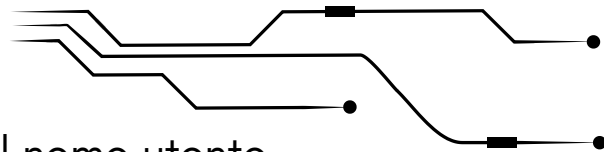
Invece, i gruppi cyber criminali stanno specializzandosi nel manipolare psicologicamente le vittime e sfruttare le vulnerabilità nei processi di autenticazione e autorizzazione delle transazioni.

Su sistemi Windows, Ursnif/Gozi, un vecchio malware bancario, è stato protagonista di molte campagne mirate agli utenti di home banking. Dal dicembre 2022, in Italia, sono state avviate campagne di e-mail dirette che hanno distribuito WailingCrab, noto anche come WikiLoader, per accedere inizialmente al computer della vittima, seguito dall'installazione di Gozi. Ursnif/Gozi è stato utilizzato per eseguire attacchi di "IBANswap", sostituendo l'IBAN del destinatario durante una transazione e dirigendo i bonifici verso conti controllati dagli aggressori.


Gozi è stato utilizzato insieme ad altri malware per infettare sia i sistemi Windows che i dispositivi Android delle vittime con Cerberus. Quest'ultimo è stato in grado di intercettare i codici inviati dalla banca attraverso SMS, inclusi i codici OTP, per verificare le transazioni bancarie, con funzionalità avanzate di anti-rilevamento e anti-analisi. Ursnif/Gozi è stato diffuso anche attraverso documenti Office con macromalevole allegati a e-mail contraffatte. Una volta infettate da Ursnif, le vittime ricevevano un messaggio a schermo che le invitava ad installare un'app di sicurezza per continuare a utilizzare i servizi bancari. In realtà, venivano reindirizzate su una falsa pagina Google Play tramite un QR code, che installava Cerberus sul dispositivo mobile. L'opzione predefinita di non consentire l'installazione di app da fonti sconosciute su dispositivi Android ha ridotto l'impatto di queste campagne. La cattura delle credenziali di accesso alle caselle di posta elettronica, sia webmail che client installati sui dispositivi, è diventata una pratica comune per i malware finanziari, usata dai gruppi criminali per lanciare attacchi di tipo BEC con un alto tasso di successo.

Furto delle credenziali

Il furto delle sole credenziali di accesso, come il nome utente e la password, non è più sufficiente per compiere un attacco contro un sistema finanziario.



La direttiva europea PSD2 ha reso obbligatorio, fin dal 2019, l'utilizzo di un ulteriore metodo di autenticazione forte del cliente



noto come SCA (Strong Customer Authentication), spesso sotto forma di OTP (One Time Password) inviata tramite SMS o generata da un'applicazione. Questo metodo, inserito in un modulo per verificare l'utente, è comunemente noto come Multi-Factor Authentication, o autenticazione a più fattori.

Tuttavia, anche la Multi-Factor Authentication è diventata bersaglio di phishing e ingegneria sociale, nonostante fosse stata ideata per prevenire il furto delle credenziali. All'utente viene richiesto d'inserire un PIN o un codice monouso in un modulo online e questo meccanismo non è immune al phishing. I cybercriminali possono creare moduli convincenti, coinvolgere falsi operatori telefonici o chat online per ottenere i fattori di autenticazione.

È evidente che la password come unico metodo di autenticazione non è più sufficiente e molti sistemi di MFA sono vulnerabili al phishing. Soluzioni come FIDO, che si basano sull'uso di dati biometrici o chiavi di sicurezza anziché password, offrono un'autenticazione più sicura. La protezione dalle frodi finanziarie è diventata sempre più complessa, con la necessità di utilizzare meccanismi di autenticazione multi-fattore resistenti al phishing. Tecnologie come FIDO/WebAuthn e l'infrastruttura a chiave pubblica (PKI) offrono soluzioni più sicure rispetto alle tradizionali password e OTP inviate via SMS.

Nel prossimo focus analizzeremo come l'intelligenza artificiale giocherà un ruolo sempre più importante sia nella cybersecurity che nelle attività criminali, e come sarà fondamentale adottare soluzioni di sicurezza agili e automatizzate per contrastare queste minacce in continua evoluzione.

STRATEGIA DI DATA SECURITY NELL'ERA DELL'IA GENERATIVA

Nell'attuale scenario digitale, marcato dall'aumento esponenziale dei dati aziendali, l'intensificazione delle minacce informatiche dovuta agli avanzamenti tecnologici (in particolare dell'Intelligenza Artificiale) e alle tensioni geopolitiche, emerge la necessità impellente di **strutturare un'adeguata strategia di cybersecurity** volta a processare e proteggere opportunamente il dato, che ha assunto il ruolo di "oro" del nuovo ordine mondiale, e la cui manipolazione può avere ripercussioni dannose non solo per questioni di sicurezza informatica ma anche di stabilità globale, soprattutto in virtù delle dimensioni sempre più importanti del fenomeno del cybercrime negli ultimi tempi.

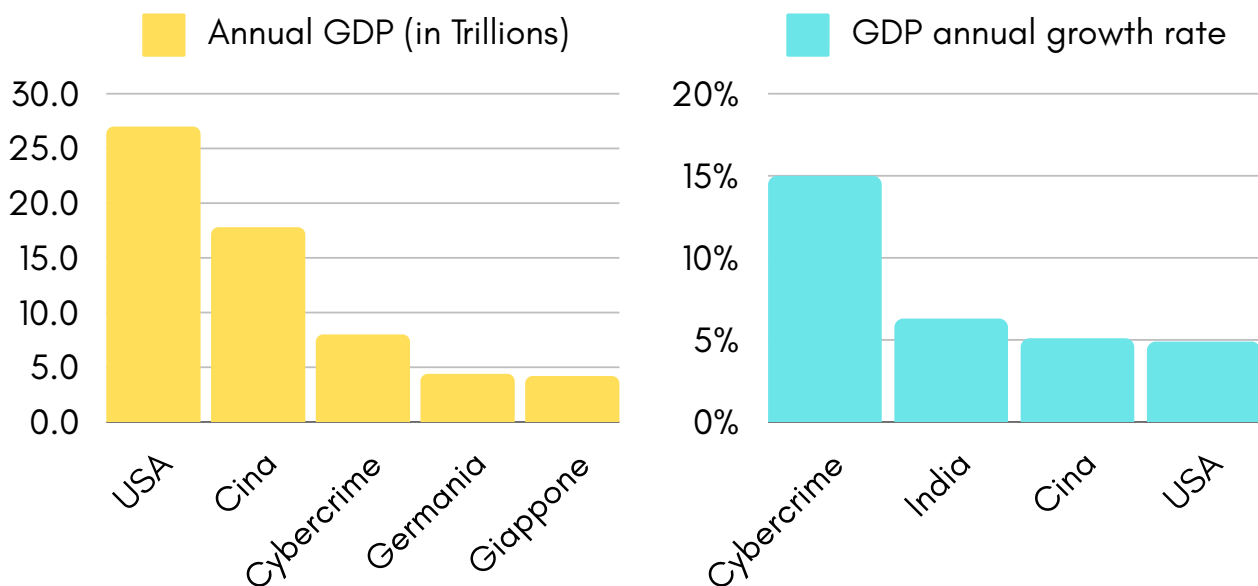


Figura 12 - Dimensioni del fenomeno cybercrime - Fonte: Microsoft Data Security Index Report

Alcuni numeri relativi a data breach o accesso non conforme ai dati, con impatti potenziali in termini di danni ai sistemi e alle attività, reputazionale perdita di informazioni:

- Secondo il recente studio Microsoft Data Security Index, nel corso dell'ultimo anno, il **74% delle organizzazioni intervistate ha subito almeno un incidente di sicurezza** che ha portato all'esposizione dei dati aziendali, con una media di 59 incidenti per organizzazione nel periodo considerato, pari a circa uno ogni sei giorni. Il 20% di questi incidenti è stato valutato come grave, con il potenziale di causare un costo annuo fino a 15 milioni di dollari;
- Il Global Data Protection Index (GDPI) 2023 di Dell Technologies rivela che il **76% delle aziende italiane ha subito almeno un'interruzione dei sistemi informatici** legata a incidenti o attacchi nel 2023, con un costo medio stimato tra 500 mila e 1 milione di dollari;
- Nel 2023, secondo il Microsoft Digital Defense Report, **il malware o ransomware rappresentano il primo elemento di rischio**, con un incremento significativo delle attività guidate da remoto (Human Operated Ransomware), l'incidenza di questo tipo di attacco è raddoppiata e nel 13% dei casi ha comportato esfiltrazione dei dati senza ricorrere alla cifratura, attraverso una copia remota dei dati dell'organizzazione, evidenziando ulteriormente quanto i dati siano asset strategici e a volte l'obiettivo finale di un attacco;
- Inoltre, relativamente ai profili delle aziende attaccate, il 70% delle organizzazioni colpite hanno meno di 500 dipendenti, con ripercussioni gravissime in termini finanziari se comparate alla dimensione organizzative.

“Le organizzazioni continueranno a vedere un'impennata di attacchi informatici e violazioni di dati, con conseguente esplosione di azioni legali e controversie collettive che potrebbero influenzare negativamente i CISO. Ciò riguarderà le grandi aziende ma anche le organizzazioni più piccole saranno colpite e probabilmente pagheranno milioni di euro per soddisfare gli azionisti e le persone che hanno subito la violazione. L'aumento delle class action per violazione dei dati è davvero preoccupante. Si è registrato un aumento di due volte dal 2022 al 2023. Inoltre, i risultati di un recente sondaggio mostrano che il 62% dei CISO è preoccupato per la propria responsabilità personale quando si tratta di violazioni.”

DERYCK MITCHELSON Field CISO EMEA,
Dal Security report di Check Point Software Technologies

Tutto ciò ribadisce il ruolo cruciale della cybersecurity, con un focus a 360° sul dato, che coinvolga la sua produzione, condivisione, conservazione, protezione e l'uso che se ne fa.

La tutela dei dati rappresenta infatti **un impegno prioritario per le organizzazioni**, le quali devono necessariamente riconoscere i potenziali rischi e rispettare le normative al fine di garantire la sicurezza delle informazioni e il rispetto dei diritti delle persone coinvolte.

Per conseguire questo obiettivo, è indispensabile adottare adeguate strategie:

- tecniche, tra cui la pseudonimizzazione, la crittografia, l'implementazione di misure di sicurezza informatica, la formazione del personale, l'analisi degli impatti,

- a designazione di un responsabile per la protezione dei dati, la notifica delle violazioni, la collaborazione con le autorità competenti e il coinvolgimento attivo degli interessati;
- organizzative: integrando i principi di protezione del dato adottando un approccio by design, inserendoli come elemento fondamentale anziché come un'opzione aggiuntiva, e definendo una strategia che coinvolga unitamente tutte le varie figure professionali che detengono competenze e responsabilità nella protezione dei dati e nella sicurezza informatica.

In questo contesto viene sottolineata l'importanza delle **regolamentazioni internazionali** volte a tutelare la sicurezza dei dati come il GDPR, la Convenzione di Budapest, l'European Data Strategy e il Digital Operational Resilience Act (DORA) che stabiliscono standard e obblighi per la protezione e la gestione dei dati, promuovendo al contempo la cooperazione internazionale contro i reati informatici.

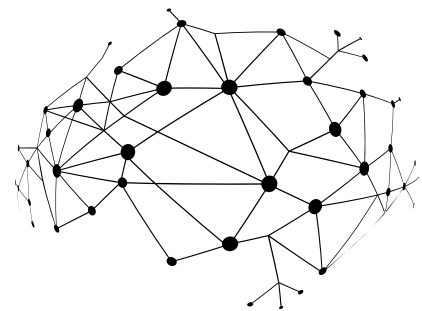


A queste si aggiungono:

- normative locali come le linee guida dall'Agenzia per l'Italia Digitale per assicurare la protezione dei dati personali degli utenti che consultano i siti e i servizi online della pubblica amministrazione (es. linee guida del Garante della Privacy e l'informativa sul trattamento dei dati personali);
- regolamentazioni legate all'utilizzo degli strumenti basati sull'Intelligenza Artificiale, ad esempio il recente AI Act.

A tal proposito, **un ruolo cruciale sarà svolto dall'IA** che, se da un lato rappresenta un'ulteriore arma per i cybercriminali che potrebbero utilizzare i modelli generativi per generare varianti di malware in grado di eludere le tradizionali soluzioni di sicurezza, dall'altro offre invece strumenti avanzati per la classificazione e la protezione dei dati, il monitoraggio delle minacce e la gestione dei rischi.

L'IA generativa, in particolare, promette di rivoluzionare l'interazione con i dati, migliorando la produttività e facilitando l'accesso all'innovazione digitale.



Ad esempio, molte grandi organizzazioni di software stanno creando strumenti che consentono di automatizzare il processo volto a garantire che i dati siano classificati e contrassegnati in linea con le politiche organizzative.

Negli ultimi decenni, l'IA ha avuto un impatto significativo nel mondo digitale. Soprattutto di recente c'è stata una diffusione esponenziale, grazie alla democratizzazione delle tecnologie, resa possibile dall'introduzione del trattamento del linguaggio naturale, rendendo l'IA più accessibile e facile da usare per un vasto pubblico.

Questo cambiamento ha trasformato radicalmente il nostro modo di interagire con le tecnologie digitali apportando miglioramenti tangibili: recenti studi rivelano che il **78% delle aziende ha utilizzato o prevede di utilizzare nel breve-medio periodo l'IA generativa** e si prevede che il settore ICT sarà il principale comparto (assieme a quello finanziario) a trarne benefici.

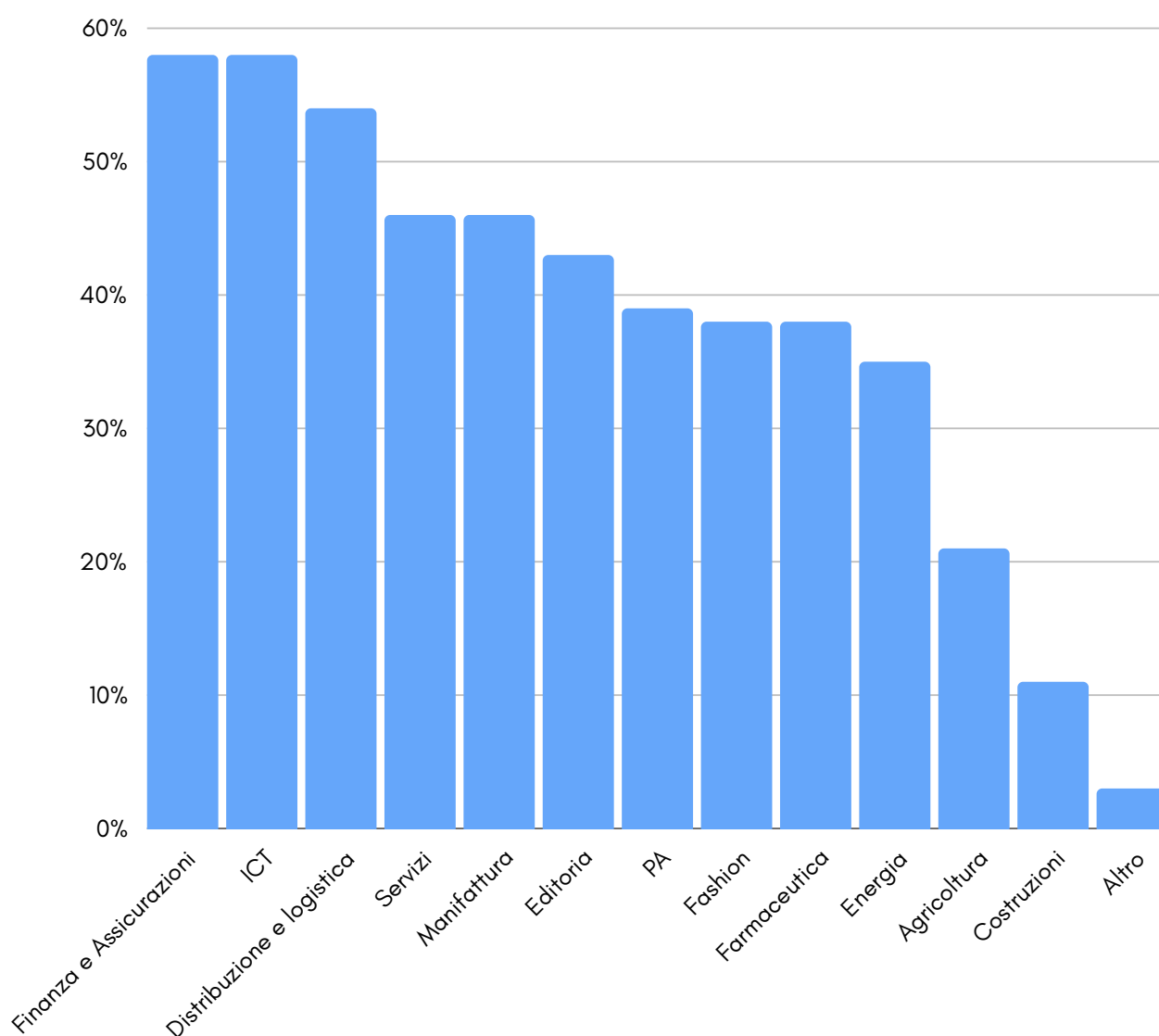


Figura 13 - Risposte alla domanda "Quali sono i settori economici in cui si osserveranno i principali benefici per il Sistema Paese e per il Made in Italy?" - Fonte: rielaborazione The European House - Ambrosetti

Inoltre, la richiesta di competenze IA/ML sta crescendo agli occhi del professionista medio della cybersecurity, posizionandosi al quinto posto tra quelle richieste, mentre nello stesso studio del 2022 non figurava nemmeno tra le prime dieci. Nei prossimi anni, questa competenza potrebbe subire un'ulteriore impennata nella domanda, in quanto l'IA varia e influenza vari aspetti delle minacce e della difesa della cybersecurity.

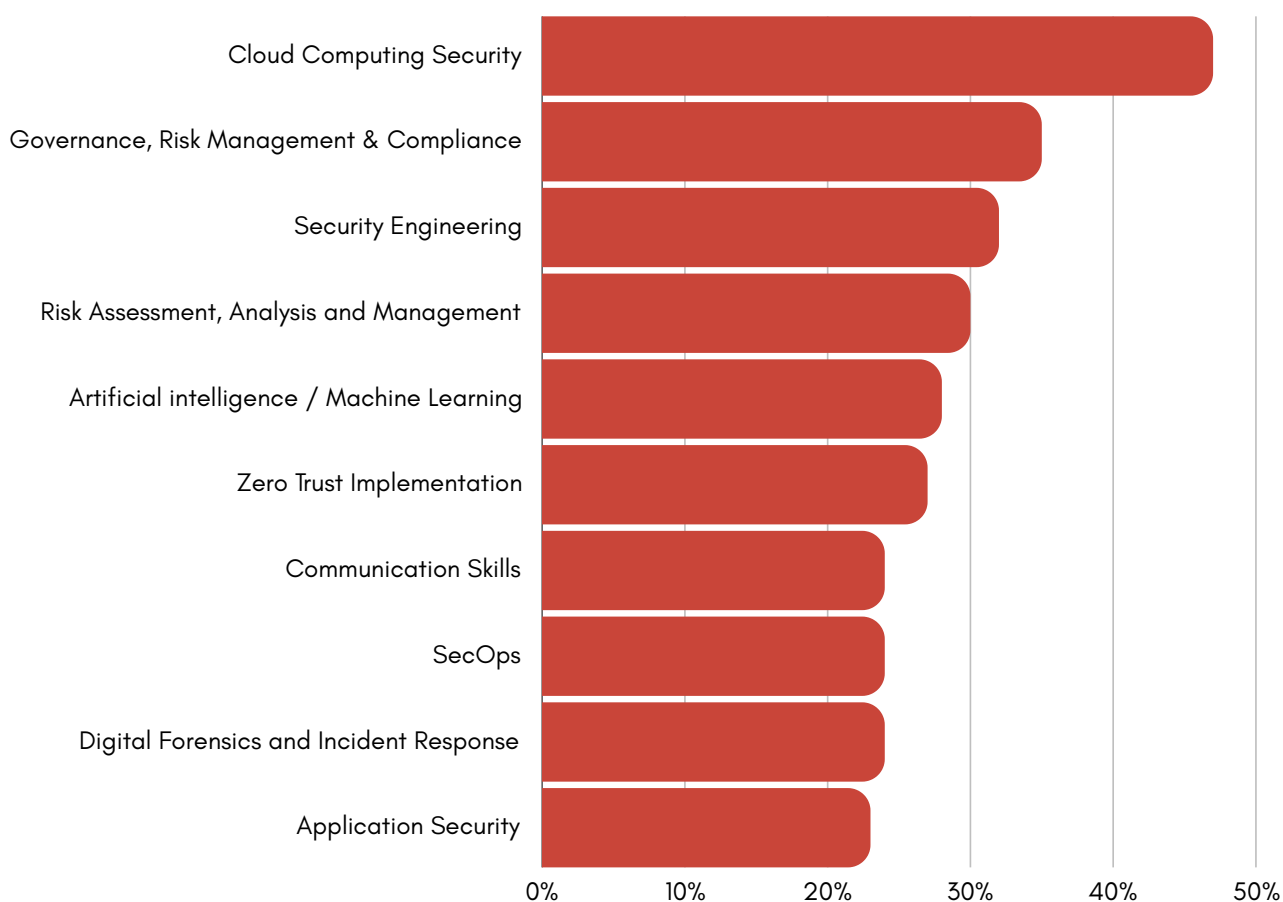



Figura 14 - Risposte alla domanda "Quali di queste competenze ritenete siano più richieste per i professionisti della sicurezza che desiderano avanzare in carriera?" - Fonte: Report ISC2 Cybersecurity Workforce Study

Alcuni dei **vantaggi potenziali che può apportare l'IA e ML** all'interno di una strategia di cybersecurity che comprenda la difesa del dato come uno degli obiettivi primari, sia in termini di analisi e pianificazione, che in termini di operatività e reportistica, comprendono:

- l'elaborazione di enormi quantità di dati in tempo reale offrendo una visibilità estesa degli ambienti e identificando per tempo comportamenti anomali, anticipando i rischi prima che si verifichino danni irreparabili, migliorando così la sicurezza informatica e la conformità alle normative sulla privacy;
- l'individuazione, classificazione e protezione automatica dei dati sensibili, come proprietà intellettuale e segreti commerciali, per apprendere dagli insights e prendere decisioni informate;
- gli algoritmi di machine learning possono essere utilizzati per valutare il livello di rischio associato a una determinata condizione e adattare le politiche di sicurezza di conseguenza, apportando diversi benefici, in particolare una risposta rapida e flessibile alle minacce emergenti e un'ottimizzazione delle risorse;
- la NIS2 e altre normative richiedono una produzione di reportistica migliorata, sfruttando le potenzialità dell'IA generativa.



Tuttavia, l'aumento dell'uso dell'IA richiede necessariamente un miglioramento della sicurezza dei dati per consentirne un utilizzo responsabile e prevenire i rischi derivanti da un uso sbagliato. In tal senso è necessaria una governance strutturata e integrata, bilanciando gli innumerevoli vantaggi derivanti dal suo utilizzo con la privacy e la sicurezza dei dati.

Nonostante i rischi intrinseci legati alla manipolazione di dati riservati infatti, il **potenziale dell'IA generativa nell'individuare e prevenire violazioni della sicurezza è vitale.**

L'IA sta infatti rivoluzionando la sicurezza informatica, identificando, analizzando e neutralizzando minacce più rapidamente dei metodi tradizionali. Utilizzando algoritmi avanzati e il machine learning, l'IA adatta costantemente le sue strategie di difesa, diventando un alleato necessario contro la criminalità informatica.

In conclusione, nella progettazione e nell'attuazione di una strategia di cybersecurity che assicuri la corretta protezione dei dati, diventa fondamentale concentrarsi su 3 aspetti:

- adottare una solida strategia di governance e sicurezza dei dati per prevenire abusi e garantire la conformità normativa, soprattutto considerando l'attuale contesto geopolitico e l'introduzione di nuove tecnologie;
- identificare un numero limitato di partner affidabili che assicurino una copertura completa di tutti gli ambiti e dei servizi forniti dall'organizzazione;

- utilizzare responsabilmente tecnologie IA, soprattutto quelle generative, che possono accelerare gli investimenti in sicurezza informatica e semplificare la gestione dei complessi ambienti aziendali, migliorando l'efficienza complessiva della cybersecurity.

Una strategia di cybersecurity deve quindi integrare una visione che includa la convergenza tra le diverse figure professionali coinvolte, l'acquisizione di competenze specifiche in materia, l'adozione di soluzioni tecnologiche innovative e un approccio metodico alla gestione dei dati, considerando i rischi e le opportunità che l'utilizzo di IA comporta. Ciò richiede un **equilibrio tra l'implementazione delle innovazioni tecnologiche** e una rigorosa **governance dei dati** per assicurare che l'evoluzione digitale avvenga in modo responsabile e nel pieno rispetto della privacy e della sicurezza.

La sfida per le organizzazioni è di navigare in questo complesso panorama attuale, adottando politiche e misure che garantiscano una protezione dati robusta e resiliente, salvaguardando il futuro digitale e mantenendo la fiducia nel tessuto stesso della nostra società interconnessa, con particolare attenzione alla multidimensionalità dei sistemi informatici che tratteremo nel prossimo focus.


SICUREZZA IBRIDA

Nel mondo digitale odierno, le minacce informatiche stanno diventando sempre più sofisticate e pericolose. Le organizzazioni di tutte le dimensioni sono a rischio di attacchi informatici, che possono causare gravi danni finanziari, reputazionali e interruzione delle attività. Per contrastare queste minacce in continua crescita, è necessario un **approccio alla sicurezza informatica che combini misure di sicurezza tradizionali e moderne.**



La sicurezza ibrida è un approccio che utilizza una combinazione di soluzioni di sicurezza on-premise e basate su cloud, nonché solide pratiche di sicurezza e consapevolezza tra i dipendenti. Questo approccio consente alle organizzazioni di proteggere i propri dati e i sistemi da una vasta gamma di minacce, tra cui malware, phishing, ransomware e attacchi informatici.

Per implementare in modo efficace un approccio di sicurezza ibrido, ci sono diversi componenti chiave da considerare. Il primo componente è il controllo degli accessi, che implica l'implementazione di controlli rigorosi per limitare l'accesso ai dati e ai sistemi agli utenti e ai dispositivi autorizzati. Questa pratica viene implementata attraverso metodi come il controllo degli accessi basato sui ruoli (RBAC - Role-based access control), le liste di controllo degli accessi (ACL - Access-Control List) e le soluzioni di gestione delle identità e degli accessi (IAM- Identity and Access Management).



Un altro componente importante è la protezione dei dati, che prevede la salvaguardia dei dati sensibili sia in loco che nel cloud utilizzando crittografia, controlli di accesso e monitoraggio. È cruciale scegliere fornitori di cloud affidabili con un solido track record in materia di sicurezza.

La consapevolezza e la formazione dei dipendenti sulla sicurezza informatica sono anch'esse componenti cruciali. Questo implica educare i dipendenti sui rischi informatici e su come rimanere al sicuro online, fornendo sessioni di formazione regolari e aggiornamenti sulle ultime minacce e su come evitarle, e incoraggiando i dipendenti a segnalare qualsiasi attività sospetta e a prendere provvedimenti per proteggere i propri dispositivi personali e aziendali.

L'utilizzo di tecnologie emergenti come l'intelligenza artificiale (IA), il machine learning (ML) e l'automazione può migliorare anche la sicurezza informatica. Queste tecnologie possono essere utilizzate per rilevare e rispondere alle minacce in modo più rapido e preciso, nonché per automatizzare attività di sicurezza manuali.

Implementare misure robuste per prevenire, rispondere e gestire le violazioni dei dati è un altro componente importante. Questo include la pianificazione della risposta agli incidenti, l'analisi forense e la notifica ai clienti.

La **sicurezza ibrida** rappresenta, quindi, un vero e proprio scudo per le aziende, **combinando la protezione collaudata delle soluzioni on-premise con l'agilità e l'innovazione del cloud.**

Come funziona la sicurezza ibrida?

Immaginiamo la sicurezza ibrida come una fortezza inespugnabile, composta da diverse linee di difesa che lavorano in sinergia:

Identità

Nell'ambiente di lavoro ibrido, è fondamentale per le aziende essere in grado di verificare l'identità di chiunque tenti di accedere alle risorse di rete e alle informazioni. Si può sostenere che si tratti della prima linea di difesa dal punto di vista della sicurezza.

Dispositivi

Ci sono due aspetti a questo. In primo luogo, ci sono i dispositivi che i dipendenti utilizzano per accedere alla rete aziendale. Questi possono essere sia ufficiali che personali. In secondo luogo, ci sono altri dispositivi all'interno dell'infrastruttura, come telecamere di sicurezza e stampanti intelligenti, che sono tutti collegati alla rete. Le aziende hanno bisogno di capacità per verificare questi dispositivi e proteggerli dall'essere accessibili da attori malintenzionati.

Rete

Nel modo di lavorare di oggi, la rete si trova al centro di un approccio globale alla sicurezza, poiché persone, dispositivi, dati e applicazioni si spostano tutti attraverso di essa. Proteggere la rete da attori malintenzionati, minacce interne e rischi di terze parti è fondamentale per la sopravvivenza dell'azienda.

Applicazione

Mentre le aziende spostano alcune o tutte le loro operazioni nel cloud, stanno anche sperimentando un cambiamento nel modo in cui gestiscono e distribuiscono le applicazioni.

Dall'containerizzazione alle architetture serverless e ai microservizi, proteggere i carichi di lavoro delle applicazioni è fondamentale nel paesaggio digitale odierno. Gli attacchi contro queste piattaforme e servizi possono portare a violazioni di dati sensibili, perdita di produttività e danni irreparabili alla reputazione di un'organizzazione.

Dati

Spesso descritti come "nuova valuta", i dati sono emersi come uno dei beni più preziosi per le aziende. È fondamentale per le organizzazioni proteggere i dati dall'accesso non autorizzato, dall'uso, dalla divulgazione, dall'interruzione, dalla modifica o dalla distruzione. Con l'aumento della quantità di informazioni sensibili che vengono archiviate e condivise elettronicamente, le capacità e le misure di sicurezza robuste sono fondamentali per raggiungere questa protezione.

Tecnologie utilizzate per garantire sicurezza nel lavoro ibrido

Le tecnologie qui elencate sono molteplici ed essenziali per garantire la sicurezza nel lavoro ibrido. Possiamo quindi individuare:

- Componenti hardware e software per una migliore protezione degli endpoint, come HP Wolf Security, che include tecnologie modulari che possono rafforzare la sicurezza a diversi livelli integrandosi nell'hardware o estendendo la protezione attraverso il software.
- Tecnologie per la localizzazione di computer smarriti o rubati e per la cancellazione remota dei dati, come HP Protect and Trace.
- Stampanti intelligenti con intelligenza integrata che svolgono un ruolo attivo nella protezione delle informazioni.
- Strumenti di collaborazione basati su cloud, come la condivisione di desktop, la videoconferenza e l'archiviazione, che consentono alle persone di lavorare efficacemente da qualsiasi luogo.
- Una connessione di rete sicura e affidabile che consente a tutti i membri del team di lavorare e collaborare in sicurezza da qualsiasi luogo.
- Tecnologia che permette una visione completa dell'ambiente IT per ottimizzare l'esperienza utente e migliorare la gestione IT.
- Dispositivi intelligenti che possono prevenire lo stress delle riunioni video e migliorare l'equilibrio tra lavoro e vita e i rapporti con i colleghi.
- Strumenti analitici che possono migliorare l'equilibrio tra lavoro e vita e creare relazioni più strette con i colleghi.
- Tecnologie che possono inviare avvisi automatici quando le sale riunioni superano la capacità o implementare controlli senza contatto per le riunioni.

I benefici concreti della sicurezza ibrida

Adottare un approccio ibrido alla sicurezza non è solo un dovere per stare al passo con le minacce, ma offre anche numerosi vantaggi concreti:

- **Protezione completa:** la combinazione di soluzioni on-premise e basate su cloud garantisce una copertura a 360 gradi contro ogni tipo di minaccia informatica.
- **Scalabilità senza limiti:** con il cloud, la sicurezza può essere scalata facilmente per adattarsi alle esigenze aziendali in continua evoluzione, senza dover investire in infrastrutture costose.
- **Ottimizzazione dei costi:** le soluzioni basate su cloud spesso sono più convenienti di quelle tradizionali, permettendo di risparmiare denaro senza compromettere la sicurezza.
- **Agilità e velocità:** le minacce informatiche non aspettano, e la sicurezza ibrida consente di implementare e aggiornare le protezioni in tempo reale, sempre al passo con le ultime insidie.

In conclusione, la sicurezza ibrida è alla base di una strategia di Data Protection efficace soprattutto considerando che il numero degli attacchi in cloud continuano a crescere, approfondiremo questo tema nell'ultimo focus di questo report.

CLOUD ADOPTION E CLOUD-NATIVE APPLICATION PROTECTION PLATFORM

Le minacce alla sicurezza del cloud continuano a crescere e gli attacchi non accennano a rallentare. Recenti studi rivelano che **gli attacchi mirati alle infrastrutture cloud sono aumentati del 75%** nel 2023, mentre i gruppi criminali specializzati in attacchi esclusivamente cloud sono cresciuti del 110%.

Questi avversari, definiti "cloud-conscious", diventano sempre più sofisticati e rapidi nell'esplorare e sfruttare le vulnerabilità della sicurezza cloud. In media, impiegano solo 62 minuti per entrare nei sistemi e muoversi all'interno delle reti compromesse, con il tempo di breakout più rapido registrato in soli 7 minuti.



La difesa efficace contro queste minacce dipende dalla capacità dei team di sicurezza di raccogliere, correlare e analizzare i dati attraverso ambienti distribuiti, che includono soluzioni on-premise, ibride e multi-cloud. La sfida è individuare e mitigare le vulnerabilità prima che gli avversari possano sfruttarle. Tuttavia, gli approcci convenzionali di sicurezza falliscono nel fornire una visibilità e un controllo granulari necessari per gestire i rischi associati agli ambienti cloud, in particolare per quanto riguarda i microservizi.

Le configurazioni ibride, che distribuiscono componenti tra più ambienti cloud e sistemi on-premise, introducono complessità che allunga i tempi di risposta e sovraccarica a livello operativo i team di sicurezza.

L'adozione di molteplici soluzioni di monitoraggio e protezione e la creazione di silos di sicurezza aprono a lacune di copertura e visibilità, rendendo difficile la rilevazione e la mitigazione delle minacce in modo tempestivo. Di conseguenza, i tempi di identificazione e risposta alle minacce si allungano, generando uno svantaggio per i difensori e facilitando il compito degli attaccanti.

Per contrastare l'evoluzione e il volume dei moderni attacchi cloud, **è necessario un approccio più agile e intelligente alla sicurezza**. Implementare soluzioni native per il cloud, progettate per ambienti dinamici, è essenziale. Queste soluzioni dovrebbero fornire ai difensori una visibilità continua e informazioni approfondite sulle tecniche degli avversari, consentendo una maggiore rapidità e agilità.

Una piattaforma di protezione delle applicazioni cloud-native unisce diverse funzionalità di sicurezza in una soluzione unica, incentrata sull'identificazione e la prioritizzazione dei rischi in tutto l'ambiente cloud.




Una CNAPP, acronimo di Cloud-Native Application Protection Platform, è una **piattaforma** progettata per **offrire protezione completa alle applicazioni sviluppate secondo il modello cloud-native**.

Queste applicazioni sono tipicamente distribuite su infrastrutture cloud, utilizzano microservizi, contenitori come Docker e orchestrazione attraverso sistemi come Kubernetes.

La CNAPP combina varie funzionalità di sicurezza necessarie per proteggere queste applicazioni moderne attraverso tutto il loro ciclo di vita, dallo sviluppo alla produzione. Ecco alcune delle funzioni principali:

- Scansione delle vulnerabilità: identifica le vulnerabilità nel codice sorgente delle applicazioni, nelle immagini dei container e nelle configurazioni delle infrastrutture cloud.
- Gestione della configurazione di sicurezza: aiuta a garantire che le configurazioni di rete, di sistema operativo e di applicazioni siano conformi agli standard di sicurezza.
- Rilevamento e risposta alle minacce: monitora le attività delle applicazioni in esecuzione e le infrastrutture per rilevare comportamenti anomali o potenzialmente dannosi, intervenendo in caso di attacchi.
- Gestione degli accessi e delle identità: controlla chi ha accesso a quali risorse e con quali permessi, per garantire che solo gli utenti autorizzati possano accedere ai dati e alle risorse sensibili.
- Compliance e audit: supporta il rispetto di normative e standard di settore attraverso la raccolta e la gestione di log e la generazione di report per audit interni o esterni.
- Protezione dei dati: include tecnologie per la crittografia dei dati a riposo e in transito, oltre a funzionalità di prevenzione della perdita dei dati (DLP).
- Più in generale, per un approccio efficace alla sicurezza del cloud, è necessario considerare 5 aspetti fondamentali che permettono di contrastare gli attacchi, anche i più sofisticati, e di proteggere le infrastrutture cloud:

- **Visibilità del 100%:** assicura una copertura completa in ambienti multi-cloud e ibridi per eliminare i punti ciechi e prevenire gli attacchi.
- **Threat Intelligence Integrata:** offre informazioni affidabili e tempestive sulle minacce per comprendere e anticipare gli attacchi, identificare i comportamenti degli avversari e correlare le tattiche, tecniche e procedure (TTP).
- **Strumenti Consolidati e Integrati:** riduce la complessità unendo vari strumenti di sicurezza in un unico framework. Questo consolidamento aiuta a ottimizzare la gestione delle minacce e la compliance, migliorando la risposta agli incidenti.
- **Automazione su Scala Cloud:** sfrutta l'automazione per accelerare la rilevazione e la risposta alle minacce, riducendo il carico di lavoro manuale e gli errori umani, e implementa controlli di sicurezza automatizzati nel ciclo di sviluppo delle applicazioni.
- **Esperienza e Competenza Cross tra Cloud e Security:** promuove una profonda conoscenza del cloud e delle best practice di sicurezza, essenziale per la progettazione e l'implementazione di strategie di sicurezza efficaci. Include la formazione continua e il supporto di partner esterni per colmare eventuali lacune di competenza.



In conclusione, un efficace approccio alla sicurezza in cloud dovrebbe integrare sia tecnologie basate su agent che soluzioni senza agent, garantendo così una copertura completa sia per endpoint tradizionali che per ambienti ibridi e multi-cloud. Questa combinazione in un'unica piattaforma unificata permette alle organizzazioni di avere una **visibilità totale sui diversi ambienti**, facilitando l'**identificazione e la correzione rapide di vulnerabilità** ed **errori** di configurazione.

L'efficienza operativa si ottiene attraverso pratiche sicure che coprono l'intero ciclo di sviluppo fino alla fase di runtime, con piattaforme che includono funzionalità native come la scalabilità e aggiornamenti continui per supportare lo sviluppo dinamico delle applicazioni e tenere il passo con l'evoluzione rapida delle minacce.

Adottare una strategia CNAPP completa può migliorare notevolmente il livello di sicurezza complessivo di un'organizzazione, semplificando i flussi di lavoro di sicurezza, la condivisione delle conoscenze e le attività collaborative. La decisione di investire in questa strategia dipende dalla valutazione del business case specifico dell'organizzazione, con l'obiettivo di massimizzare il valore dell'investimento e l'efficienza operativa.

CONCLUSIONI: UN IMPEGNO CONDIVISO PER UN FUTURO DIGITALE SICURO

La minaccia informatica si erge come una sfida in continua evoluzione, che richiede un impegno costante e condiviso da parte di individui, organizzazioni e governi. La crescente sofisticazione degli attacchi, l'aumento del 65% dei casi nel 2023 rispetto ai quattro anni precedenti, e la carenza di competenze specializzate nel settore, sottolineano la necessità di un'azione collettiva per rafforzare la sicurezza cibernetica a tutti i livelli.

Investire nella formazione di professionisti qualificati è fondamentale per colmare il divario di competenze e costruire una forza lavoro preparata ad affrontare le sfide future. Allo stesso tempo, le organizzazioni devono adottare strategie di sicurezza robuste che includano misure tecniche e formative adeguate, sfruttando il potenziale offerto dall'intelligenza artificiale e dal machine learning per migliorare la protezione dei dati e la gestione delle minacce.

L'utilizzo responsabile dell'IA nella cybersecurity è imprescindibile. Garantire una governance strutturata e integrata di queste tecnologie è fondamentale per bilanciare i loro vantaggi con la tutela della privacy e la sicurezza dei dati, prevenendo i rischi derivanti da un uso improprio.

Allo stesso modo, l'awareness dei dipendenti sulla cybersecurity rimane fondamentale per proteggere le aziende da minacce digitali. Educare i dipendenti sulle pratiche sicure online e offline riduce il rischio di attacchi informatici. Programmi di formazione regolari e simulazioni di phishing possono aumentare la consapevolezza dei dipendenti sui potenziali rischi. Coinvolgere attivamente i dipendenti nella sicurezza informatica, promuove una cultura aziendale consapevole e protetta.

Planetica, tramite i corsi della propria Academy, rappresenta una valida opzione per contribuire alla formazione di professionisti qualificati, con competenze e conoscenze approfondite in ambito Cyber.

La collaborazione globale e un approccio multidisciplinare che integri competenze umane e tecnologie avanzate sono elementi chiave per costruire un futuro digitale più sicuro e resiliente. Solo attraverso un impegno condiviso e un'azione collettiva sarà possibile affrontare le sfide sempre più complesse poste dalle minacce informatiche e costruire un mondo digitale più sicuro per tutti.

BIBLIOGRAFIA / SITOGRAFIA

- **Rapporto Clusit 2024 sulla sicurezza ICT in Italia - Security summit;**
- **Global Threat Report 2024 di CrowdStrike;**
- **<https://www.zscaler.it/resources/security-terms-glossary/what-is-cloud-native-application-protection-platform-cnapp>;**
- **https://www.trendmicro.com/it_it/what-is/cloud-native/cnapp.html;**
- **Report ISC2 Cybersecurity Workforce Study, 2023 “How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce”;**
- **IA 4 Italy: impatti e prospettive dell’Intelligenza Artificiale generativa per l’Italia e il made in Italy - The European House - Ambrosetti;**
- **<https://www.automazione.news/rapporto-clusit-2024-in-italia-cyber-attacchi-65-ma-e-solo-punta-dell'iceberg/>;**
- **<https://www.ilsole24ore.com/art/italia-impreparata-attacchi-cyber-2024-timori-infrastrutture-critiche-AFTuukFC>;**
- **<https://www.cybersecurity360.it/news/attacchi-cyber-nei-dati-clusit-uno-scenario-fosco-nel-2023-piu-12-per-cento/>;**

- <https://www.csoonline.com/article/2074581/the-cybersecurity-skills-shortage-a-ciso-perspective.html>;
- <https://channels.theinnovationgroup.it/cybersecurity/il-fenomeno-del-cyber-security-skill-shortage-in-italia-e-nel-contesto-internazionale/>;
- <https://www.cybersecurity360.it/news/cyber-security-le-tendenze-degli-scenari-2024-dove-e-cruciale-garantire-la-cyber-resilience/>;
- <https://www.cybersecurity360.it/news/competenze-qualificate-introvabili-i-consigli-per-le-aziende-europee/>;
- WEF_Global_Cybersecurity_Outlook_2024.
- <https://vervoe.com/cyber-security-skills-gap/>;
- IBM Security X-Force Threat Intelligence Index 2023 IBM
- <https://www.techtarget.com/searchsecurity/tip/Cybersecurity-skills-gap-Why-it-exists-and-how-to-address-it>;
- IBM Security X-Force Threat Intelligence Index 2023 IBM Security
- <https://cybermagazine.com/articles/cybersecurity-skills-gap-leaving-businesses-vulnerable>;
- <https://www.stationx.net/cyber-security-skills-gap/>;

CONTATTI



Matteo M. Marzan
matteo.marzan@planetica.it



Andrea Rivetti
andrea.rivetti@planetica.it

Team di lavoro



Riccardo Mandioli



Marco Nunzi



Alessandro Croce



Giovanni Mastrippolito

Per maggiori informazioni:

Tel: +39 02 82785 740 | E-mail: segreteria@planetica.it | Indirizzo: Via Crocefisso 5, Milano



Visita il nostro sito web per ricevere il
report completo



www.planetica.it