CyberGrant
SECURITY MADE EASY

WHITE PAPER

Guida alla Cybersecurity:
Minacce, Settori, Regolamenti e Opportunità

Sommario

Introduzione al contesto attuale

L’ecosistema delle minacce

La cybersecurity è diventata una priorità strategica imprescindibile nel panorama digitale odierno. Nel 2025, ci troviamo di fronte a un ecosistema di minacce in continua evoluzione, caratterizzato da:

- **Superficie di attacco in espansione** - La crescente adozione dell’IoT, del cloud computing e del lavoro remoto ha portato inevitabilmente ad un ampliamento significativo della superficie di attacco delle organizzazioni.
- **Sofisticazione degli attacchi** – I threat actor utilizzano tecniche sempre più avanzate, inclusa l’intelligenza artificiale per automatizzare e personalizzare gli attacchi.
- **Incremento degli attacchi ransomware** - Gli attacchi ransomware double e triple extortion sono diventati particolarmente devastanti, con impatti sia operativi sia reputazionali.
- **Minacce alla supply chain** - Gli attacchi alla supply chain rappresentano una delle tendenze più preoccupanti.
- **Carenza di competenze** – La mancanza di personale qualificato in cybersecurity, con milioni di posizioni vacanti a livello globale, permane come problema.

Dati di cybersecurity aggiornati al 2024

12.732

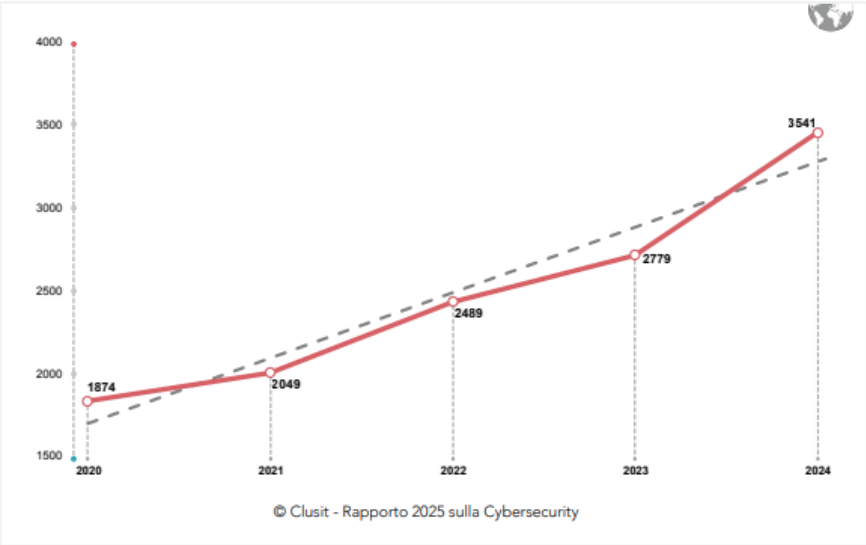
incidenti di sicurezza in 4 anni

Secondo i dati più recenti, scaturiti dal report IBM Data breach cost 2024, il costo medio di una violazione dei dati ha superato i **4,5 milioni di dollari**, con tempi di identificazione e contenimento che mediamente superano i 280 giorni.

L’”ultimo rapporto CLUSIT 2025 (Associazione Nazionale Italiana di Cybersecurity) rivela che, tra gennaio 2020 e dicembre 2024 si sono **verificati a livello globale 12.732 incidenti di sicurezza** di pubblico dominio, suddivisi come segue.

+27%

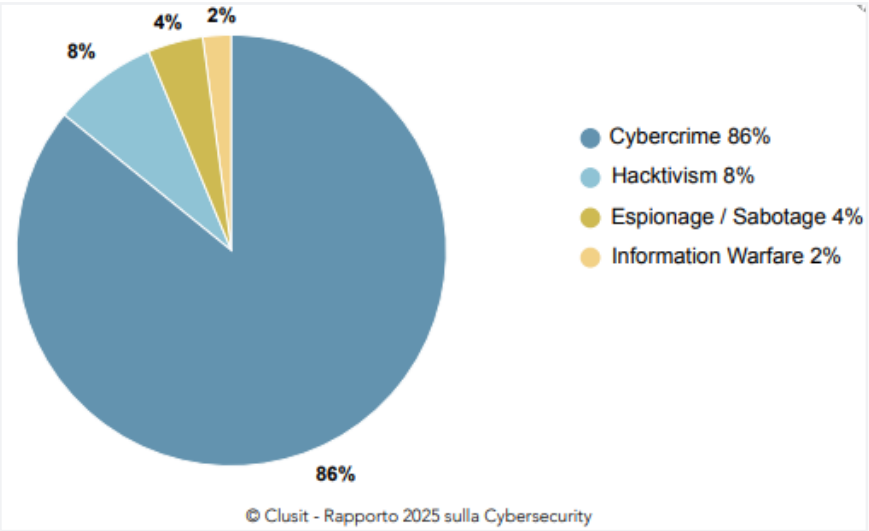
Nel 2024 si sono registrati **3.541 incidenti di sicurezza**, il numero più alto mai rilevato, con un **incremento del 27%** rispetto ai 2.779 del 2023.



Fonte immagine Rapporto Clusit 2025 – Numero incidenti noti a livello globale periodo 2020-2024

La crescita del cybercrime

Il cybercrime si conferma la principale causa degli attacchi, rappresentando l'86% del totale (+3% rispetto al 2023), tornando ai livelli record del 2021. Questa crescita evidenzia come la criminalità organizzata stia investendo sempre più nel cyberspazio, grazie alla maggiore redditività rispetto ai crimini tradizionali e ai modelli "as-a-Service", che rendono il cybercrimine accessibile anche a non esperti.



Fonte immagine Rapporto Clusit 2025 – Tipologia e distribuzione attaccanti 2024

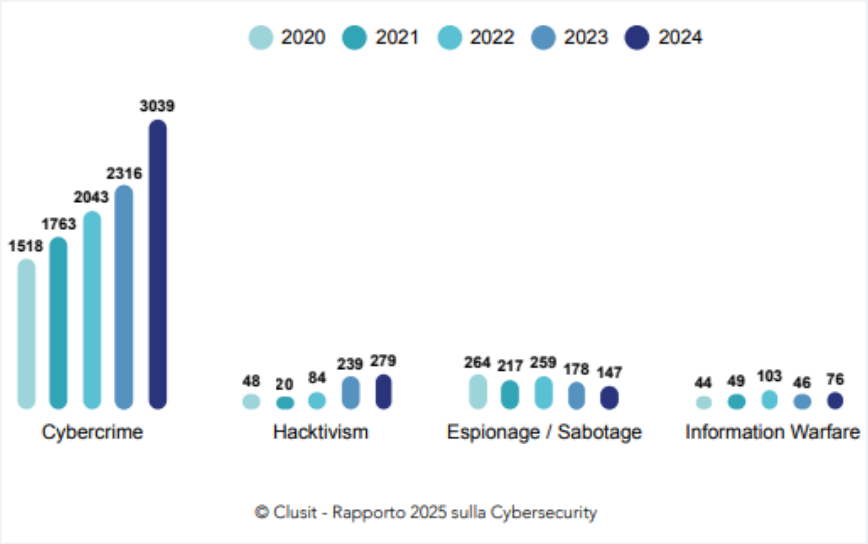
L'analisi della distribuzione degli attaccanti nel periodo 2020-2024 conferma che **il Cybercrime resta la principale causa degli incidenti di sicurezza**, con un trend di crescita costante. Nel 2024, gli attacchi motivati da finalità criminali sono aumentati del 31% rispetto all'anno precedente, consolidando un'espansione progressiva che si è mantenuta negli anni.

Altre cause di attacchi in crescita

È interessante osservare come il Cybercrime non sia l'unico attore in crescita:

- **Hacktivism** segna un aumento del 16% rispetto all'anno precedente, evidenziando un ritorno di attività su questo fronte.
- Le operazioni di **Information Warfare** registrano un incremento ancora più marcato, quasi raddoppiando rispetto all'anno precedente.

In controtendenza, gli incidenti legati a **Espionage / Sabotage sono in calo**, con una riduzione del 20%, rappresentando l'unica categoria in diminuzione nel panorama delle minacce.

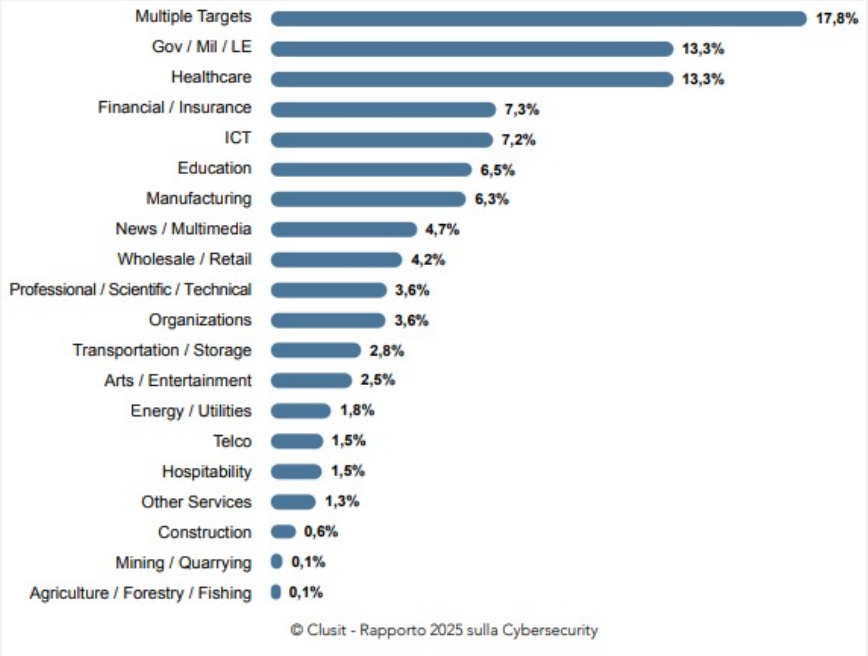


Fonte immagine Rapporto Clusit 2025 – Distribuzione attaccanti periodo 2020- 2024

Vittime di attacchi nel 2024

L'analisi delle vittime nel 2024 mostra che quasi la metà degli incidenti di sicurezza (44%) ha colpito le prime tre categorie della classifica: **Multiple Targets (18%), Gov / Mil / LE (13%)** e **Healthcare (13%).**

Mentre gli attacchi indiscriminati di tipo "**pesca a strascico**" rimangono **una delle strategie preferite** dal cybercrime—grazie alla loro elevata intensità e all'alto numero di successi—gli altri due settori risultano particolarmente vulnerabili per il loro ruolo strategico e la sensibilità dei dati trattati, rendendoli bersagli privilegiati per attacchi mirati.

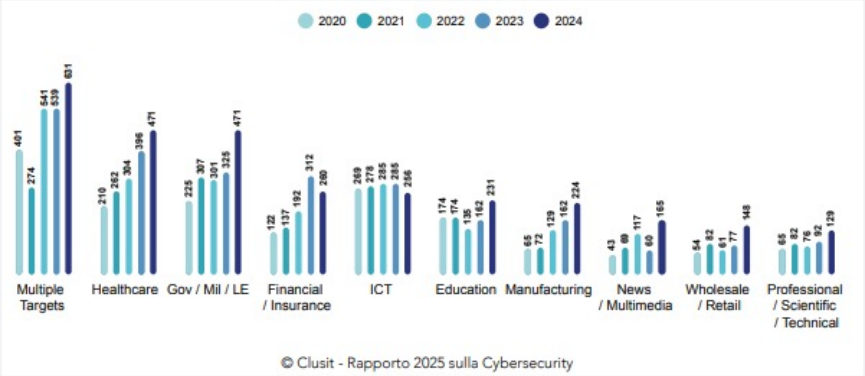


Fonte immagine Rapporto Clusit 2025 – Distribuzione attaccanti periodo 2020- 2024

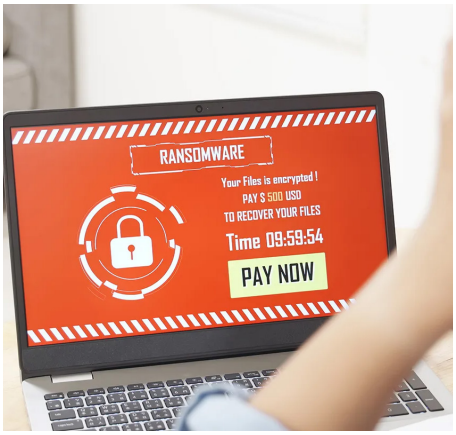
Questi dati confermano la tendenza del cybercrime a colpire con maggiore intensità settori strategici e ad alto valore informativo.

Il confronto con gli anni precedenti evidenzia una crescita costante degli attacchi nei tre principali settori colpiti:

- **Gov / Mil / LE** registra un aumento significativo del **45% rispetto al 2023**.
- **Healthcare** subisce un incremento del **18,9%**.
- **Multiple Targets** cresce di poco più del **17%**.



Fonte immagine Rapporto Clusit 2025 – Top ten vittime periodo 2020-2024



Questi numeri confermano una tendenza preoccupante: il cybercrime sta ampliando il proprio raggio d'azione, prendendo di mira settori sempre più diversificati.

L'immagine evidenzia un calo degli attacchi nel settore **Financial/Insurance**, che, dopo una crescita costante dal 2019 al 2023, registra una **riduzione del 16%** rispetto all'anno precedente. Questo calo potrebbe derivare da due fattori principali: da un lato, l'impatto delle nuove normative sulla resilienza operativa digitale, come il **Regolamento DORA** in Europa; dall'altro, un cambiamento nelle strategie del cybercrime, che sempre più spesso punta a **economie di scala**, attaccando trasversalmente più settori o prendendo di mira vittime con minori capacità di difesa.

Anche il **settore ICT** è tra i pochi a registrare una flessione, con un calo del 10% dopo due anni di stabilità. In questo caso, il miglioramento sembra legato a un **rafforzamento progressivo delle difese**, con risultati tangibili sulla riduzione degli incidenti.

Per quanto riguarda gli altri settori, la crescita degli attacchi si mantiene su livelli elevati, con **incrementi intorno al 40% o superiori**:

- **Education: +43%**
- **Manufacturing: +38%**
- **Professional / Scientific / Technical: +40%**

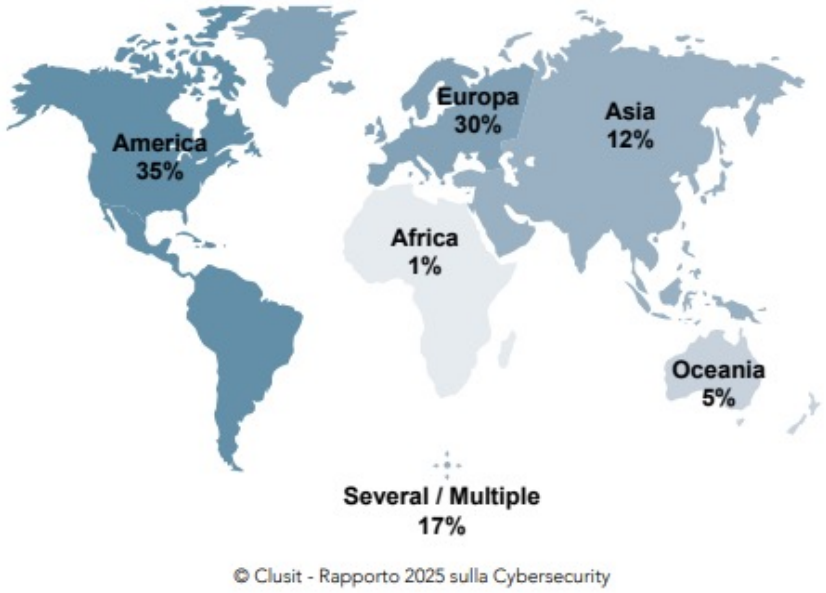
Particolarmente allarmanti sono i dati di due settori:

- **News / Multimedia: +175%**, che, dopo un anno di relativa assenza, torna tra i più colpiti (per approfondimenti, si veda "Il caso News/Multimedia").
- **Wholesale / Retail: +92%,** guadagnando una posizione rispetto al 2023.

Distribuzione delle vittime a livello globale

La **distribuzione geografica delle vittime nel 2024** mostra che oltre i **due terzi degli incidenti (65%)** si sono verificati tra **America ed Europa**. Questo dato riflette l'impatto delle normative sulla divulgazione degli incidenti informatici, in vigore da più tempo in questi territori, favorendo una maggiore trasparenza nella segnalazione.

In **Europa, oltre al GDPR**, che ha incentivato la disclosure dei Data Breach, si sono rafforzati gli obblighi di notifica degli incidenti grazie a normative come il **Regolamento DORA, le Direttive NIS 1 e 2, il PSNC in Italia** e norme equivalenti negli altri paesi UE.



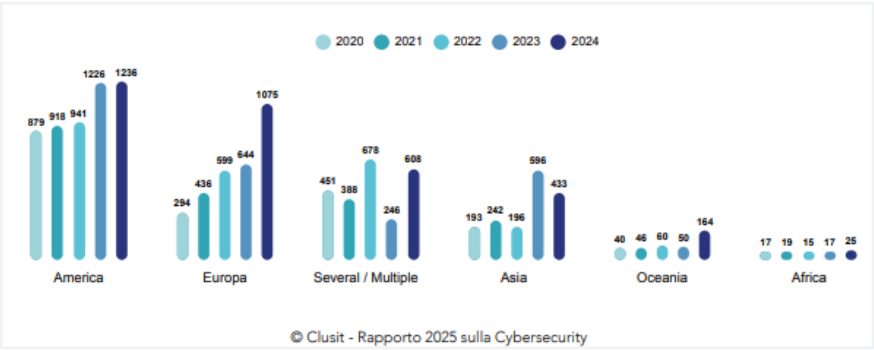
Fonte immagine Rapporto Clusit 2025 –Geografia delle vittime 2024

L'effetto è evidente:

- Negli **Stati Uniti**, il numero di attacchi noti rimane relativamente stabile.
- In **Europa**, invece, dopo anni di crescita graduale, **nel 2024 si registra un picco significativo (+67%).**

Altre tendenze degne di nota:

- Gli attacchi verso **località multiple** tornano a crescere, invertendo il calo osservato nel 2023.
- Per la prima volta, si registra un **boom di attacchi in Oceania (+228%)**, dovuto sia a un aumento dell'attenzione da parte degli **threat actors**, sia all'introduzione di nuove normative in materia di cybersecurity, simili a quanto avvenuto in Europa.



Fonte immagine Rapporto Clusit 2025 –Geografia delle vittime periodo 2020-2024

Principali minacce e problematiche

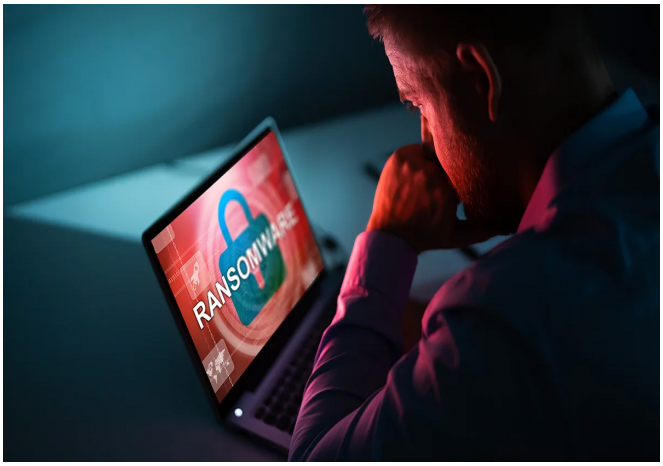
Di seguito una descrizione delle principali minacce e problematiche di cybersecurity che le aziende si trovano oggi ad affrontare.

Ransomware e attacchi di estorsione

I gruppi ransomware hanno evoluto le loro tattiche verso modelli multi-estorsione, che prevedono:

- **Crittografia dei dati**
- **Esfiltrazione e minaccia** di pubblicazione
- **Attacchi DDoS** come forma di pressione aggiuntiva
- **Contatto diretto** con clienti, partner e media dell'organizzazione colpita

Inoltre, gruppi come Lockbit, ALPHV/BlackCat e Conti hanno sviluppato sofisticati modelli RaaS (Ransomware-as-a-Service) che rendono questi attacchi accessibili anche a criminali con limitate competenze tecniche.



Advanced Persistent Threats (APT)

Gli attacchi APT, spesso sponsorizzati da stati nazionali, mirano a obiettivi strategici attraverso:

- Operazioni di **cyber-spionaggio**
- **Sabotaggio** di infrastrutture critiche
- **Furto di proprietà intellettuale**
- **Interferenza politica**

Tali attacchi sono caratterizzati da lunghi periodi di latenza all'interno dei sistemi compromessi e da tecniche di esfiltrazione altamente sofisticate.

Vulnerabilità della supply chain

Gli attacchi alla supply chain compromettono componenti software o hardware ancora prima della loro installazione presso l'utente finale. Esempi significativi includono:

- Compromissione di librerie open source
- Manipolazione di aggiornamenti software
- Inserimento di backdoor in componenti hardware
- Compromissione di servizi cloud e SaaS

Phishing e social engineering avanzato

Le tecniche di phishing si sono evolute con:

- Phishing mirato (spear phishing)
- Compromissione delle e-mail aziendali (BEC – Business E-mail compromise)
- Uso di deepfake e voiceprinting
- Sfruttamento dell'intelligenza artificiale per creare messaggi personalizzati e convincenti

Minacce legate all'IoT e ai dispositivi connessi

La proliferazione di dispositivi IoT ha introdotto nuove vulnerabilità, ovvero:

- Dispositivi con sicurezza by-design inadeguata
- Difficoltà di aggiornamento e patch
- Uso come vettori di accesso alla rete aziendale
- Veicoli Potenziali per la creazione di botnet

Quadro normativo di cybersecurity

Di seguito una panoramica delle normative e regolamentazioni di cybersecurity a livello Europeo, Stati Uniti e Sud America.

Europa

Il quadro normativo europeo è tra i più avanzati a livello globale in termini di cybersecurity e risulta al momento così articolato:

NIS2 (Network and Information Security Directive 2) – Si tratta di una Direttiva che è stata recepita a livello Paese. Essa:

- Espande significativamente l'ambito della precedente direttiva NIS
- Impone requisiti di cybersecurity più stringenti
- Introduce sanzioni più severe per le non conformità
- Coinvolge un numero maggiore di settori, inclusi fornitori di servizi digitali

GDPR (General Data Protection Regulation) – Si tratta di un regolamento, oramai in vigore dal 2018, che:

- Costituisce riferimento globale per la protezione dei dati personali

- Prevede sanzioni fino al 4% del fatturato globale annuo
- Impone notifiche di violazione entro 72 ore
- Richiede valutazioni d'impatto sulla protezione dei dati (DPIA)

DORA (Digital Operational Resilience Act) – È un regolamento specifico del settore finanziario ed assicurativo, s che:

- Stabilisce standard per la resilienza operativa digitale
- Richiede test regolari di resilienza informatica
- Regola i rapporti con fornitori terzi di servizi IT

Cyber Resilience Act – È un regolamento che:

- Impone requisiti di cybersecurity per prodotti con componenti digitali
- Stabilisce obblighi per tutto il ciclo di vita del prodotto
- Introduce un sistema di certificazione europeo

Stati Uniti

Il quadro normativo statunitense si caratterizza per un approccio settoriale:

Normative federali

- **CMMC (Cybersecurity Maturity Model Certification)** – Si tratta di una certificazione per i fornitori del Dipartimento della Difesa. Lo scopo del framework CMMC è proteggere le informazioni governative da accessi ed esposizioni non autorizzati.
- **Federal Information Security Modernization Act (FISMA)** – È un regolamento per le agenzie federali che definisce un quadro di linee guida e standard di sicurezza per proteggere le informazioni e le operazioni governative.
- **Executive Order on Improving the Nation's Cybersecurity** - Rafforza i requisiti per le agenzie federali e i loro fornitori. In particolare, l'Ordine esecutivo mira a stabilire una strategia nazionale coesa per migliorare la sicurezza informatica tra agenzie federali, aziende private e settori delle infrastrutture critiche. Inoltre, esso disciplina una vasta gamma di questioni critiche, tra cui nuovi standard di sicurezza informatica per i contraenti federali, una migliore condivisione delle informazioni tra pubblico e privato, la promozione di tecnologie avanzate come la crittografia resistente ai quanti e l'intelligenza artificiale (IA) e l'imposizione di sanzioni agli attori informatici stranieri.

Normative settoriali

- **HIPAA** (Health Insurance Portability and Accountability Act) per il settore sanitario.

- **Gramm-Leach-Bliley Act** per il settore finanziario.
- **CCPA (California Consumer Privacy Act) e CPRA (California Privacy Rights Act)** per la protezione dei dati personali in California.
- **Colorado Privacy Act** e Virginia Consumer Data Protection Act, iniziative statali sulla privacy dei dati.

Direttive SEC (Securities and Exchange Commission)

- Nuovi requisiti di divulgazione degli incidenti di cybersecurity per le aziende quotate.
- Obbligo di riportare incidenti materiali entro quattro giorni lavorativi.
- Richiesta di informativa dettagliata sulle strategie di gestione del rischio cyber.

America del Sud

Il panorama normativo in termini di cybersecurity è in evoluzione. Vediamo Paese per Paese a che punto siamo

Argentina

- **Ley de Protección de los Datos Personales**
- **Ley n. 26.388** – Si tratta della legge sui reati informatici e la sicurezza informatica è la legge che regola i reati informatici in Argentina. Questa legge recepisce nel Codice penale argentino i reati commessi in ambiente

Brasile:

- **LGPD (Lei Geral de Proteção de Dados)** è l'equivalente brasiliano del GDPR
- **Normativa del Banco Centrale per le istituzioni finanziarie (CMN)**, si tratta di requisiti specifici per la resilienza cyber nel settore bancario
- **Política Nacional de Cibersegurança, o "PNCiber"** -. Questa politica mira a guidare le attività di sicurezza informatica nel paese, stabilendo linee guida per proteggere le infrastrutture critiche e promuovere la cyber-resilienza.

Cile:

- **Ley 21719: Protección de datos personales**
- **Ley 21663:** Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información - Si tratta di un framework strategico per la sicurezza informatica nazionale

Colombia:

- **Ley 1581: Protección de datos personales**
- **CONPES 3854** è un documento strategico sulla cybersecurity a livello nazionale

Ecuador

- **Ley Orgánica de Protección de Datos Personales (LOPDP)**

- **Política de Ciberseguridad y la Estrategia Nacional de Ciberseguridad**

México:

- **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**
- **Ley Federal de Ciberseguridad**

Panama:

- **Ley 81 de Protección de Datos Personales**
- **Estrategia Nacional de Ciberseguridad**

Paraguay:

- **Ley n. 1682/01 -** Si tratta della legge che stabilisce le norme di base per la protezione dei dati personali.
- **Estrategia Nacional de Ciberseguridad 2024-2028**

Perú:

- **Ley N. 29733 de Protección de Datos Personale**
- **Programa de Ciberseguridad y Ciberdefensa 2025**

Uruguay:

- **Ley n. 18.331**
- **Estrategia Nacional de Ciberseguridad (ENC) 2024 - 2030**

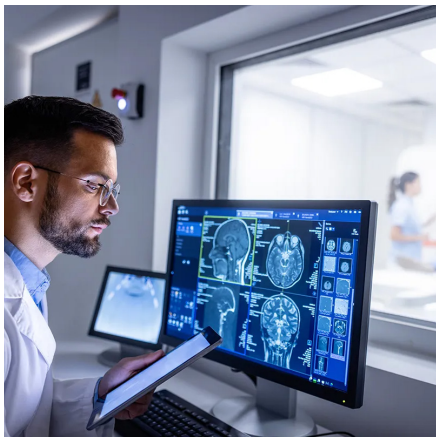
Venezuela:

- **Nessuna legge sui dati** - Non esiste una legge specifica sulla protezione dei dati personali, ma la Costituzione Nazionale e la Legge di Protezione della Privacy delle Comunicazioni offrono alcune garanzie. Inoltre, la Legge Speciale contro i Reati Informatici mira a prevenire l'uso improprio dei dati. Tuttavia, il paese deve ancora sviluppare un quadro normativo in linea con gli standard internazionali.
- **Ley Especial contra los Delitos Informáticos y el Consejo Nacional de Ciberseguridad**

Cybersecurity per settori

Di seguito un'analisi in termini di cybersecurity suddivisa in base ai settori industriali e, precisamente:

Sanità



Principali minacce

- Ransomware mirati alle strutture sanitarie
- Furto di dati sanitari sensibili
- Compromissione di dispositivi medici connessi
- Interruzione di servizi critici

Sfide specifiche

- Bilanciamento tra accessibilità dei dati e sicurezza
- Protezione di dispositivi medici legacy con limitate capacità di aggiornamento
- Interoperabilità sicura tra diversi sistemi e piattaforme
- Conformità a normative sanitarie in base alle varie latitudini (HIPAA, GDPR per dati sanitari, ecc.)

Opportunità e best practices

- Implementazione di soluzioni Zero Trust per l'accesso ai dati sanitari
- Segmentazione della rete per isolare dispositivi medici critici
- Programmi di formazione specifici per il personale sanitario
- Sviluppo di piani di continuità operativa e disaster recovery
- Adozione di blockchain per la gestione sicura delle cartelle cliniche elettroniche

Settore Finanziario

Principali minacce

- Attacchi alle infrastrutture di pagamento
- Frodi finanziarie sofisticate
- Attacchi di phishing mirati ai clienti
- Insider threat
- Attacchi DDoS a servizi finanziari online

Sfide specifiche

- Garantire la resilienza dei sistemi di pagamento
- Bilanciare innovazione (fintech) e sicurezza
- Conformità a regolamenti finanziari internazionali
- Protezione contro minacce avanzate sponsorizzate da stati

Opportunità e best practices

- Implementazione di sistemi avanzati di rilevamento frodi basati su AI
- Adozione di autenticazione multi-fattore per clienti e per dipendenti
- Sviluppo di SOC (Security Operation Center) specializzati per il settore finanziario
- Test regolari di resilienza e red teaming
- Collaborazione con autorità di regolamentazione e altre istituzioni finanziarie

Manifatturiero

Principali minacce

- Attacchi ai sistemi di controllo industriale (ICS)
- Spionaggio industriale e furto di proprietà intellettuale
- Sabotaggio delle linee produttive
- Ransomware che blocca la produzione

Sfide specifiche

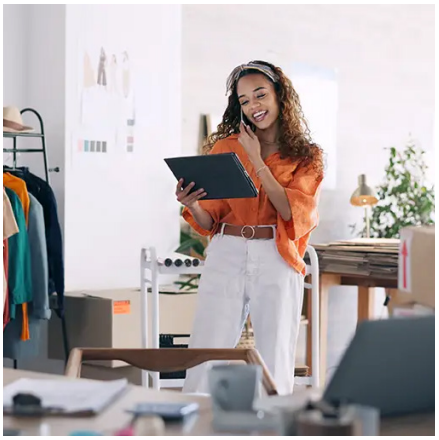
- Integrazione sicura di IT (Information Technology) e OT (Operational Technology)
- Protezione di sistemi di controllo industriale legacy
- Gestione della sicurezza in ambienti Industria 4.0
- Difesa della proprietà intellettuale

Opportunità e best practices

- Implementazione di air gap o segmentazione avanzata tra reti IT e OT
- Sviluppo di strategie di monitoraggio specifiche per ambienti ICS
- Adozione di standard come IEC 62443 per la sicurezza dei sistemi di automazione industriale

- Programmi di formazione sulla sicurezza per il personale operativo
- Implementazione di tecnologie di rilevamento anomalie in ambiente OT

Retail ed eCommerce



Principali minacce

- Attacchi ai sistemi di pagamento e skimming (i.e. riguarda il furto di dati delle carte di credito e altre informazioni sensibili dai siti web all'insaputa dei proprietari o degli utenti dei siti stessi)
- Furti di account cliente
- Frodi di identità e account takeover
- DDoS durante periodi di vendita critici

Sfide specifiche

- Protezione dei dati dei clienti e delle transazioni
- Gestione sicura di picchi di traffico stagionali
- Bilanciamento tra user experience e sicurezza
- Protezione di applicazioni multicanale (web, mobile, IoT)

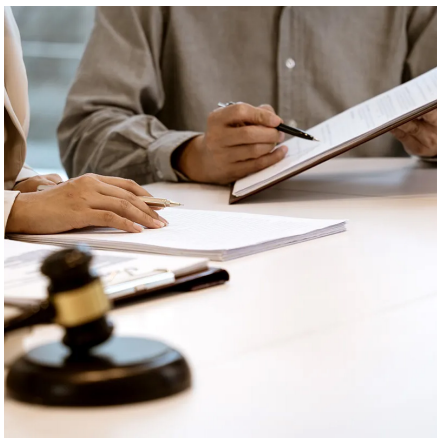
Opportunità e best practices

- Implementazione di soluzioni antifrode basate su machine learning
- Adozione di standard PCI-DSS per la protezione dei dati di pagamento
- Utilizzo di WAF (Web Application Firewall) avanzati
- Monitoraggio continuo per il rilevamento di codice malevolo sui siti di eCommerce
- Sviluppo di capacità anti-bot per combattere scraping e credential stuffing

Legale e Amministrativo (Avvocati e Commercialisti)

Principali minacce

- Furto di informazioni privilegiate e confidenziali
- Compromissione delle e-mail aziendali
- Ransomware mirati a studi professionali
- Attacchi di spear phishing contro figure chiave



Sfide specifiche

- Protezione del segreto professionale
- Sicurezza delle comunicazioni con clienti sensibili
- Conformità a regolamenti specifici per la professione
- Gestione sicura di documenti legali e finanziari sensibili

Opportunità e best practices

- Implementazione di soluzioni di crittografia end-to-end per le comunicazioni
- Adozione di DLP (Data Loss Prevention) per prevenire fughe di dati
- Formazione specifica su social engineering per professionisti
- Sviluppo di procedure di verifica avanzate per trasferimenti finanziari
- Utilizzo di spazi di lavoro virtuali sicuri per la collaborazione con clienti

Servizi di Consulenza

Principali minacce

- Furti di proprietà intellettuale
- Compromissione di credenziali di accesso a sistemi client
- Attacchi alla supply chain digitale
- Spionaggio industriale

Sfide specifiche

- Protezione delle informazioni di diversi clienti
- Sicurezza in ambienti multi-cliente
- Gestione del rischio di accesso privilegiato ai sistemi dei clienti
- Mobilità sicura dei consulenti

Opportunità e best practices

- Implementazione di solide procedure di onboarding e offboarding
- Adozione di tecnologie CASB (Cloud Access Security Broker)
- Sviluppo di framework di valutazione del rischio per ingaggi con clienti
- Implementazione di PAM (Privileged Access Management)
- Creazione di ambienti di lavoro isolati per ciascun cliente

Conclusioni e prospettive future

La sicurezza dei dati è essenziale per proteggere informazioni sensibili, garantire la conformità normativa e prevenire frodi e accessi non autorizzati. **CyberGrant Inc.** offre soluzioni avanzate per la condivisione sicura dei dati con partner e clienti, prevenendo l'esfiltrazione di informazioni critiche e garantendo un controllo totale sulla protezione e sull'integrità dei dati.

In particolare, CyberGrant Inc. propone due soluzioni principali:

FileGrant

FileGrant è una piattaforma innovativa per la **condivisione sicura di file con l'esterno**. Inoltre, FileGrant è funzionale nei settori sopra descritti in termini di:

- **Protezione dei file critici** -Ogni file è protetto da cifratura avanzata, impedendo accessi non autorizzati e garantisce altresì a conformità alle varie normative in termini di protezione dei dati e di cybersecurity. Ciò assicura l'integrità e la riservatezza dei documenti sia aziendali sia dei clienti.
- **Accessi protetti e controllo utenti** – È garantito l'accesso in base ai ruoli (Role -based Access Control – RBAC), evitando che utenti non autorizzati accedano o modifichino documenti.
- **Gestione documentale** – Favorisce la collaborazione aziendale in tempo reale, garantendo la gestione avanzata delle versioni documentali. Inoltre, previene la distribuzione non autorizzata dei documenti, oltre a limitarne l'uso anche dopo il download, attraverso un approccio equilibrato tra operatività e protezione.

RemoteGrant

RemoteGrant è una soluzione avanzata di **Data Loss Prevention** che tutela i dati sensibili su tutti i computer aziendali, inclusi quelli utilizzati al di fuori dell'organizzazione. È progettato per:

- **Blocco di ransomware e attacchi cyber** – Protegge le aziende di vari settori da ransomware, malware e attacchi zero-day. Inoltre, difende le porte di rete dagli hacker, oltre ad impedire modifiche alle porte RPD, riducendo il rischio di intrusioni nei sistemi critici attraverso gli end-point.

- **Protezione avanzata del phishing** – È in grado di monitorare la situazione in tempo reale, bloccando siti fraudolenti e tentativi di furto delle credenziali. Protegge dati aziendali, bancari, proprietà intellettuale e segreti industriali da furti e da frodi.
- **Accessi sicuri ai dati** – Garantisce che i file ogni tipo di dati sensibili siano accessibili da PC autorizzati, oltre a bloccare le copie in RDP e su USB.

RemoteGrant semplifica il percorso di compliance alle normative e direttive vigenti a varie latitudini, garantendo alle organizzazioni gli strumenti necessari per soddisfare e superare le rigorose esigenze delle leggi sulla protezione dei dati e sulla privacy. Inoltre, impedisce modifiche non autorizzate e protegge i codici sorgenti da manomissioni e furti.

Conclusione

La cybersecurity si conferma come un elemento fondamentale e strategico per qualsiasi organizzazione, indipendentemente dal settore. Le principali tendenze future includono l'adozione diffusa di approcci Zero Trust, la convergenza tra cybersecurity e resilienza operativa, l'automazione della sicurezza e una maggiore collaborazione pubblico-privato. Per affrontare efficacemente le sfide future, le organizzazioni dovrebbero adottare un approccio basato sul rischio, sviluppare una cultura della sicurezza a tutti i livelli, oltre ad implementare programmi di formazione continua e a stabilire solidi piani di risposta agli incidenti.

Partner come CyberGrant possono supportare con successo le aziende nella gestione della cybersecurity e della sicurezza dei dati, contribuendo a facilitare il percorso di compliance alle varie normative a diverse latitudini.

A cura di **Federica Maria Rita Livelli**

www.cybergrant.net