Analisi intersettoriale: pattern emergenti



L’analisi intersettoriale rivela pattern comuni che trascendono i confini industriali:

Convergenza delle minacce

Tutti i settori stanno sperimentando una convergenza delle minacce, dove attacchi tradizionalmente mirati a specifiche industrie si stanno diffondendo orizzontalmente. Gli attacchi supply chain, in particolare, dimostrano come una compromissione in un settore possa avere effetti a cascata su molteplici industrie. L’attacco Kaseya del 2021 ha colpito simultaneamente MSP, supermercati, servizi IT e istituzioni educative, evidenziando l’interconnessione dell’ecosistema digitale moderno.

Professionalizzazione degli attacchi

Tra i settori si osserva una crescente professionalizzazione degli attacchi, con cybercriminali che sviluppano expertise specifiche per industrie target. Questa specializzazione si manifesta nella comprensione approfondita dei processi operativi, delle vulnerabilità tecniche specifiche e delle dinamiche economiche di ciascun settore.

Impatti operativi critici

In tutti i settori analizzati, gli attacchi cyber stanno causando interruzioni operative significative che vanno oltre il mero danneggiamento dei dati. Nel settore sanitario, gli attacchi possono compromettere direttamente la cura dei

pazienti; nel manifatturiero, possono interrompere le catene di produzione globali; nelle telecomunicazioni, possono compromettere le comunicazioni nazionali.

Impatto macroeconomico e tendenze finanziarie

Costi diretti e proiezioni future

Il panorama economico del cybercrime presenta dimensioni che trascendono la comprensione tradizionale del crimine informatico, assumendo proporzioni macroeconomiche di portata globale. I costi mondiali del cybercrime sono stimati raggiungere i 10,5 trilioni di dollari annui entro il 2025 (fonte), sottolineando la necessità di misure di cybersecurity potenziate. Tuttavia, le proiezioni a lungo termine sono ancora più allarmanti: il costo annuale medio del cybercrime dovrebbe superare i 23 trilioni di dollari entro il 2027, in aumento dagli 8,4 trilioni di dollari del 2022 (fonte).

Queste cifre rappresentano più del PIL di molti paesi sviluppati e indicano un panorama di minacce in rapida escalation. La crescita del 15,63 trilioni di dollari entro il 2029 (fonte) evidenzia come il cybercrime stia diventando una delle forze economiche più significative del XXI secolo.

Analisi dei costi per incidente

Il costo medio globale di una violazione dati nel 2024 è di 4,88 milioni di dollari, con un aumento del 10% rispetto all’anno precedente (fonte). Tuttavia, questi dati rappresentano solo la superficie dell’iceberg economico, non considerando gli impatti a lungo termine sulla reputazione, la fiducia dei clienti e la competitività di mercato.

Le organizzazioni che utilizzano estensivamente l’AI per la sicurezza registrano costi di violazione significativamente inferiori, evidenziando come gli investimenti in tecnologie

avanzate possano tradursi in risparmi economici sostanziali (fonte). Le organizzazioni che coinvolgono le forze dell'ordine risparmiano in media 1 milione di dollari nei pagamenti ransomware (fonte).

Settore assicurativo e mercato del rischio cyber

Il mercato assicurativo cyber sta sperimentando una trasformazione fondamentale in risposta all'escalation delle minacce. Nel 2022, sono state registrate 2.123 richieste di risarcimento assicurativo cyber dovute ad attacchi ransomware (fonte). Uno studio ha mostrato che il ransomware ha contribuito come causa numero uno di perdita in quasi 6.000 richieste di risarcimento assicurativo cyber, con il riscatto medio in aumento a 247.000 dollari e il costo dell'incidente a 352.000 dollari.

Il 40% delle aziende ha acquistato assicurazione cybersecurity quando si è verificato un cyberattacco su un'altra organizzazione nello stesso settore (fonte), evidenziando come la percezione del rischio si stia traducendo in decisioni di investimento concrete.

Quando si tratta di ransomware, il costo medio di una richiesta assicurativa ammonta a circa 485.000 dollari, mentre il costo medio di un attacco ransomware è stato di 1,85 milioni di dollari nel 2023 (fonte).

Mercato delle criptovalute e monetizzazione criminale

Il mercato delle criptovalute continua a servire come principale veicolo di monetizzazione per i cybercriminali. I furti di criptovalute tramite ransomware sono aumentati del 2%, da 449,1 milioni di dollari a 459,8 milioni di dollari (fonte), evidenziando la persistente attrattiva delle valute digitali per le attività criminali.

L'analisi blockchain di Elliptic ha rivelato che 90 milioni di

dollari in pagamenti ransomware Bitcoin sono stati effettuati a DarkSide o affiliati DarkSide nell'ultimo anno, originati da 47 portafogli distinti (fonte). Secondo un rilascio DarkTracer di 2.226 organizzazioni vittima dal maggio 2019, 99 organizzazioni sono state infettate con il malware DarkSide, suggerendo che circa il 47% delle vittime ha pagato un riscatto e che il pagamento medio è stato di 1,9 milioni di dollari.

Investimenti in cybersecurity e ROI

Il mercato globale dell'AI cybersecurity dovrebbe crescere da 22,4 miliardi di dollari nel 2023 a 60,6 miliardi di dollari entro il 2028, riflettendo un tasso di crescita annuale composto del 21,9% (fonte). Questa crescita esplosiva evidenzia come le organizzazioni stiano riconoscendo il valore strategico degli investimenti in tecnologie di sicurezza avanzate.

Il 15,1% delle organizzazioni pianifica di aumentare la spesa per la sicurezza delle informazioni nel 2025 secondo Gartner (fonte). Questo incremento degli investimenti riflette una maturazione nella comprensione del rischio cyber come fattore critico di business.

Impatti settoriali specifici

Settore manifatturiero

MKS Instruments, un fornitore dell'industria dei semiconduttori, ha riportato un impatto negativo di 200 milioni di dollari sui suoi ricavi a causa di un attacco ransomware (fonte). Questo caso illustra come singoli attacchi possano avere implicazioni finanziarie enormi per aziende specifiche.

Settore sanitario

Dal 2020 al 2025, il settore sanitario spenderà 125 miliardi

di dollari per difendersi dalle violazioni (fonte). Questa cifra astronomica evidenzia come i costi di difesa stiano diventando una componente significativa dei budget sanitari globali.

Effetti macroeconomici sistemici

Interruzioni della supply chain

Le interruzioni cyber della supply chain stanno creando effetti macroeconomici che si propagano attraverso l'economia globale. L'attacco Colonial Pipeline ha causato carenze di carburante lungo la costa orientale degli Stati Uniti, con prezzi medi nazionali della benzina che sono saliti al livello più alto in oltre sei anni, raggiungendo una media di 3,04 dollari al gallone il 18 maggio (fonte).

Impatti valutari e di mercato

SolarWinds ha visto il prezzo delle sue azioni scendere significativamente all'indomani dell'attacco, affrontando scrutinio e critiche significative per il suo fallimento nel proteggere adeguatamente il processo di aggiornamento software (fonte). Questi impatti sui mercati finanziari dimostrano come gli incidenti cyber possano avere conseguenze immediate sulla valutazione del mercato.

Costi di conformità e regolamentazione

I costi di conformità stanno aumentando significativamente in risposta al inasprimento del panorama normativo. Le organizzazioni devono investire non solo in tecnologie di sicurezza, ma anche in processi, personale e audit per rispettare i requisiti normativi in evoluzione.

L'Italia ha emesso 117 multe GDPR nel 2022 (fonte), con la multa GDPR più alta mai emessa in Italia a carico di Telecom Italia (TIM) per circa 27,8 milioni di euro nel gennaio 2020 (fonte). Questi costi normativi rappresentano una componente

crescente del costo totale del rischio cyber.

Contromisure e strategie difensive

Approccio Zero Trust: ridefinizione del perimetro di sicurezza

L’architettura Zero Trust rappresenta una trasformazione paradigmatica nell’approccio alla cybersecurity, abbandonando il tradizionale modello perimetrale in favore di un principio di “never trust, always verify”. Entro il 2025, la maggior parte delle nuove implementazioni di accesso remoto si baserà su Zero Trust Network Access (ZTNA) piuttosto che su VPN tradizionali (fonte), rappresentando un ripensamento fondamentale della sicurezza aziendale.

Il 30% delle organizzazioni adotterà modelli Zero Trust Network Access (ZTNA) entro il 2024 secondo Gartner (fonte). Zero Trust sostituisce le VPN tradizionali fornendo accesso basato sull’identità per singola applicazione invece dell’accesso network-wide, verificando continuamente utenti, dispositivi e segnali contestuali prima di consentire le connessioni.

In Italia, il 77% delle organizzazioni ha adottato Zero Trust per motivi di sicurezza e protezione dei dati (fonte), mentre il 43% delle aziende italiane non aveva un modello Zero Trust in atto ma stava pianificando di adottarlo, e il 19% non stava pianificando di farlo.

Il mercato delle soluzioni Zero Trust Network Access è proiettato a crescere rapidamente nei prossimi anni, riflettendo l’adozione diffusa in tutte le industrie (fonte). Questo shift rappresenta un movimento fondamentale verso la microsegmentazione e l’autenticazione continua come principi di sicurezza centrali.

Intelligenza artificiale difensiva: l’automazione della sicurezza

Le organizzazioni stanno sfruttando l’AI per ridurre i tempi medi di rilevamento, risposta e recupero (MTTR), mantenendosi al passo con attaccanti avanzati (fonte). I sistemi AI difensivi possono analizzare enormi quantità di dati in tempo reale, fornendo contesto attraverso silos e identificando anomalie e potenziali violazioni prima che escalino.

Il 66% delle organizzazioni vede l’AI come il più grande game-changer per la cybersecurity quest’anno, ma solo il 37% ha salvaguardie per valutare gli strumenti AI prima dell’uso (fonte). Questo gap tra riconoscimento del valore e implementazione pratica evidenzia le sfide nell’adozione sicura dell’AI difensiva.

Le organizzazioni che utilizzano estensivamente l’AI per la sicurezza registrano costi di violazione significativamente inferiori (fonte), dimostrando il ROI tangibile degli investimenti in tecnologie AI per la cybersecurity.

Gestione avanzata delle vulnerabilità

CISA mantiene il catalogo KEV (Known Exploited Vulnerabilities) come fonte autorevole delle vulnerabilità che sono state sfruttate in natura (fonte). Le organizzazioni dovrebbero utilizzare il catalogo KEV come input per il loro framework di prioritizzazione della gestione delle vulnerabilità, rappresentando un approccio data-driven alla sicurezza proattiva.

L’implementazione di programmi di gestione delle vulnerabilità maturi include:

Scansione continua e assessment

Le organizzazioni devono implementare sistemi di scansione continua che identifichino vulnerabilità in tempo reale attraverso l’intero stack tecnologico. Questo include non solo

i sistemi tradizionali, ma anche i dispositivi IoT, i sistemi OT (Operational Technology) e l'infrastruttura cloud.

Threat intelligence integration

L'integrazione di threat intelligence nelle decisioni di patching consente alle organizzazioni di prioritizzare le vulnerabilità basandosi non solo sul CVSS score, ma anche sull'evidenza di sfruttamento attivo nel wild e sulla rilevanza per il profilo di minaccia specifico dell'organizzazione.

Automated patching e orchestrazione

L'automazione del processo di patching, quando possibile, riduce significativamente la finestra di esposizione. Questo include l'implementazione di sistemi di orchestrazione che possano coordinare il patching attraverso ambienti eterogenei mantenendo la continuità operativa.

Preparazione e risposta agli incidenti

Incident Response Planning

Meno di un quinto (19%) delle aziende britanniche ha un piano formale di risposta agli incidenti (fonte), evidenziando un gap critico nella preparazione organizzativa. Solo il 39% delle aziende britanniche ha assegnato ruoli nel caso si verifichi un incidente cyber.

L'implementazione di piani di incident response efficaci deve includere:

- **Definizione di ruoli e responsabilità** chiari durante un incidente
- **Procedure di escalation** ben documentate e testate
- **Comunicazione delle crisi** sia interna che esterna
- **Processi di preservazione delle evidenze** per supportare

investigazioni forensi

Business Continuity e Disaster Recovery

Il 86% degli incidenti ha comportato interruzioni operative secondo il 2025 Unit 42 Global Incident Response Report (fonte), evidenziando la necessità critica di capacità di business continuity robuste.

La preparazione alla business continuity deve contemplare:

- **Backup immutabili e testati** regolarmente per garantire la capacità di ripristino
- **Sistemi ridondanti** per operazioni critiche
- **Piani di comunicazione alternativa** che non dipendano dall'infrastruttura IT primaria
- **Processi manuali di backup** per operazioni essenziali

Sicurezza della Supply Chain

Vendor Risk Management

Il 60% delle organizzazioni utilizzerà i rischi di cybersecurity come criterio chiave per valutare nuove opportunità di business entro il 2025 secondo Gartner (fonte). Questo approccio riflette una maturazione nella comprensione dei rischi sistemici della supply chain.

L'implementazione di programmi efficaci di vendor risk management include:

- **Due diligence di sicurezza** approfondita durante la selezione dei fornitori
- **Monitoraggio continuo** della postura di sicurezza dei fornitori critici
- **Clausole contrattuali** che richiedano standard di sicurezza specifici
- **Piani di contingenza** per la sostituzione rapida di fornitori compromessi

Software Supply Chain Security

Il controllo dei rischi della supply chain software è più efficace nel processo di integrazione continua e sviluppo (CI/CD), quindi la verifica accurata di partner e fornitori e il requisito di buoni controlli di sicurezza nei contratti sono modi essenziali per migliorare la sicurezza di terze parti (fonte).

Le best practice includono:

- **Software Bill of Materials (SBOM)** per tutti i componenti software
- **Firma digitale e verifica** di tutti gli artefatti software
- **Scanning di sicurezza** automatizzato nel processo CI/CD
- **Isolation e sandboxing** di componenti di terze parti

Formazione e Awareness del personale

Security Awareness Training

Il 90% di tutti gli incidenti cyber è il risultato di errore umano o comportamentale (fonte), sottolineando l'importanza critica della formazione del personale. Solo il 19% delle aziende implementa sessioni di formazione extra dopo un cyberattacco, evidenziando un'opportunità mancata per l'apprendimento organizzativo.

I programmi di formazione efficaci devono includere:

- **Training personalizzato per ruolo** che rifletta i rischi specifici di ciascuna funzione
- **Simulazioni di phishing** regolari per testare e migliorare la preparazione
- **Aggiornamenti continui** sulle nuove minacce e tecniche di attacco

- **Metriche di performance** per misurare l’efficacia del training

Insider Threat Management

Il 48% delle organizzazioni riporta che gli attacchi insider stanno diventando più frequenti nell’ultimo anno (fonte). La gestione delle minacce insider richiede un approccio equilibrato che combini controlli tecnici con sensibilità per la privacy e la cultura aziendale.

Tecnologie emergenti per la difesa

Behavioral Analytics e UEBA

L’implementazione di User and Entity Behavior Analytics (UEBA) consente alle organizzazioni di identificare attività anomale che potrebbero indicare compromise o insider threats. Questi sistemi utilizzano machine learning per stabilire baseline comportamentali e identificare deviazioni significative.

Threat Hunting proattivo

L’implementazione di capacità di threat hunting proattivo consente alle organizzazioni di identificare minacce avanzate che potrebbero evadere i controlli di sicurezza tradizionali. Questo include l’uso di threat intelligence, analisi forense e tecniche di detection avanzate.

Extended Detection and Response (XDR)

Le piattaforme XDR forniscono visibilità e capacità di risposta integrate attraverso endpoint, network, email e cloud, consentendo una detection e response più efficaci degli attacchi sofisticati che utilizzano tecniche multi-vettore.

Collaborazione Internazionale e

risposta istituzionale

Iniziative Governative e coordinamento internazionale

La risposta istituzionale al cybercrime ha assunto una dimensione sempre più coordinata e strategica a livello internazionale. Nel gennaio 2025, il Dipartimento del Tesoro degli Stati Uniti ha sanzionato Beijing-based Integrity Technology Group Inc., citando il suo ruolo nell'abilitare le operazioni cyber del gruppo Flax Typhoon dal 2022 al 2023, particolarmente contro organizzazioni di telecomunicazioni, media e agenzie governative statunitensi (fonte).

L'esempio italiano del gennaio 2025 illustra perfettamente la dimensione geopolitica del cybercrime contemporaneo: un gruppo hacker pro-russo ha rivendicato la responsabilità di un cyberattacco contro siti web del governo italiano, inclusi ministeri, servizi pubblici e piattaforme di trasporto in città come Roma e Palermo (fonte). L'attacco è stato una risposta all'incontro della Premier Giorgia Meloni con il Presidente ucraino Volodymyr Zelenskyy, evidenziando come gli attacchi cyber siano diventati strumenti di pressione diplomatica.

Framework normativi emergenti

Cyber Resilience Act Europeo

Il Cyber Resilience Act, adottato nell'ottobre 2024 dal Consiglio Europeo, rappresenta l'ultimo sforzo politico per rendere più coerente il framework legislativo europeo esistente per la cybersecurity e per garantire che i prodotti con componenti digitali siano realizzati in modo sicuro attraverso la supply chain e il loro ciclo di vita (fonte).

CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act)

Negli Stati Uniti, il CIRCIA del 2022 rappresenta una svolta nel requisito di reporting degli incidenti cyber per le infrastrutture critiche, stabilendo tempistiche specifiche e metodologie standardizzate per la notifica degli incidenti alle autorità competenti.

Operazioni Law Enforcement coordinate

Takedown Operations

L'FBI ha chiuso 13 marketplace DDoS-for-hire nella prima metà del 2023 (fonte). Similarmente, nel luglio 2024, le autorità del Regno Unito hanno interrotto DigitalStress, un servizio illegale per lanciare attacchi DDoS.

Queste operazioni coordinate dimostrano l'efficacia della cooperazione internazionale nel contrastare l'infrastruttura criminale cyber. Il successo nel recupero di 63,7 bitcoin dal pagamento del riscatto Colonial Pipeline da parte del Dipartimento di Giustizia americano (fonte) illustra come le capacità forensi avanzate possano recuperare asset criminali anche in ecosistemi pseudonimi come le criptovalute.

Arresti e processi

L'arresto di Yaroslav Vasinskyi in Polonia nell'ottobre 2021 in connessione con l'attacco ransomware Kaseya (fonte), e la sua successiva estradizione negli Stati Uniti nel marzo 2022, rappresenta un precedente significativo per la cooperazione internazionale nell'perseguire cybercriminali transnazionali.

L'Ucraina ha giocato un ruolo particolare in questi sforzi di law enforcement, con l'arresto di membri del gruppo REvil e la collaborazione con autorità internazionali per smantellare

infrastrutture criminali.

Diplomazia Cyber e deterrenza

Dialogo bilaterale

Dopo l'attacco Kaseya del 9 luglio 2021, il Presidente Biden ha chiamato il Presidente russo Putin, dichiarando successivamente alla stampa: "Gli ho reso molto chiaro che gli Stati Uniti si aspettano che quando un'operazione ransomware proviene dal suo territorio, anche se non è sponsorizzata dallo stato, ci aspettiamo che agiscano se gli forniamo informazioni sufficienti per agire su chi sia" (fonte).

Norme internazionali

Nel 2024, l'ONU ha adottato il primo trattato globale completo alla sua convenzione sul cybercrime (fonte), rappresentando un passo significativo verso la standardizzazione delle risposte internazionali al cybercrime.

Iniziative di Capacity Building

Programma cyber dell'Ucraina

Per aiutare a proteggere l'infrastruttura critica ucraina contro gli attacchi russi, il Regno Unito ha lanciato il 'Ukraine Cyber Programme' nel 2022 (fonte). Il Regno Unito ha mobilitato un pacchetto iniziale di 6,35 milioni di sterline in risposta all'aumentata attività cyber russa immediatamente dopo l'invasione dell'Ucraina.

Questo programma fornisce incident response per proteggere le entità del governo ucraino contro gli attacchi, oltre a protezione DDoS così che i cittadini ucraini possano ancora accedere a informazioni critiche e firewall per bloccare gli attacchi.

Pubblico-privato partnership

Joint Cyber Defense Collaborative (JCDC)

CISA ha stabilito il Joint Cyber Defense Collaborative (JCDC) per catalizzare una comunità di esperti in prima linea nella difesa cyber – dal settore pubblico e privato – per condividere insights e informazioni in tempo reale per comprendere le minacce e ridurre il rischio per la nazione (fonte).

Dal suo stabilimento, il JCDC ha guidato la risposta nazionale a una delle vulnerabilità software più estese mai scoperte, ha giocato un ruolo centrale nella campagna Shields Up di CISA per proteggere l'infrastruttura critica da potenziali cyberattacchi russi, e ha riunito più di 25 principali operatori di pipeline e partner di sistemi di controllo industriale per rafforzare le pratiche di sicurezza.

Intelligence Sharing e Threat Intelligence

Programmi di Intelligence Sharing

L'espansione di programmi come il CISA's vulnerability scanning service, che invia alert alle organizzazioni iscritte quando il servizio identifica vulnerabilità note per essere sfruttate da APT (fonte), rappresenta un evoluzione significativa nella condivisione proattiva di intelligence.

Attribution e Naming Conventions

La standardizzazione delle convention di naming per gruppi APT attraverso organizzazioni come MITRE ATT&CK, Mandiant e Microsoft ha migliorato la capacità della comunità di sicurezza di condividere intelligence actionable e coordinarsi nelle response.

Previsioni e Scenari Futuri

Evoluzione del Threat Landscape

I leader di sicurezza anticipano un panorama di minacce sempre più complesso nel 2025, con il 54% delle grandi organizzazioni che cita le sfide della supply chain come la maggiore barriera alla resilienza cyber (fonte). Questa complessità è guidata dall'interdipendenza crescente dei sistemi digitali e dalla convergenza di minacce tradizionalmente separate.

Il World Economic Forum's Global Cybersecurity Outlook 2025 rivela che quasi il 60% delle organizzazioni afferma che le questioni geopolitiche influenzano la loro strategia di cybersecurity, con CEO preoccupati per lo spionaggio cyber e il furto di proprietà intellettuale, mentre i leader cyber si concentrano sull'interruzione delle operazioni (fonte).

Intelligenza artificiale: la nuova frontiera

Il 2025 sarà probabilmente l'anno dell'AI agentica, con strumenti di AI agentica (o agenti AI) che possono prendere decisioni ed eseguire una serie di compiti complicati per conto dell'utente (fonte). Questa evoluzione trasformerà l'AI generativa da un "giocattolo divertente" in un'applicazione automatizzata con implicazioni profonde sia per l'attacco che per la difesa.

L'Hao Yang, VP di intelligenza artificiale presso Cisco-owned Splunk, spiega: "In precedenza, eravamo concentrati su assistenti AI che potevano rispondere a prompt o input da un utente. Ora stiamo guardando a strumenti di AI agentica che possono prendere decisioni e portare avanti una serie di compiti complicati per conto dell'utente" (fonte).

Minacce quantistiche: l'orizzonte

della crittografia

Forse la minaccia a lungo termine più significativa identificata per il 2025 è l'avanzamento delle capacità di quantum computing (fonte). Mentre i computer quantistici potrebbero rivoluzionare molti campi, pongono anche rischi esistenziali per i metodi crittografici attuali che proteggono l'infrastruttura digitale globale.

Le organizzazioni devono iniziare a preparare le transizioni verso algoritmi post-quantici per proteggere i dati sensibili a lungo termine. Questa transizione richiederà anni di pianificazione e implementazione graduale, rendendo essenziale iniziare i preparativi ora.

Geopolitica cyber: tensioni Crescenti

Minacce State-Sponsored

La U.S.## Settori Verticali: Analisi per Industria

Settore sanitario: target privilegiato dell'ecosistema criminale

Il settore sanitario continua a rappresentare il target più popolare per gli attacchi ransomware nel 2023 (fonte), evidenziando una vulnerabilità sistemica che ha implicazioni critiche per la sicurezza pubblica. L'Healthcare Industry Cybersecurity Report rivela che dal 2016, gli attacchi ransomware hanno causato perdite totali di 157 milioni di dollari ai fornitori sanitari negli Stati Uniti (fonte).

Le statistiche del settore sanitario presentano un quadro particolarmente preoccupante: si stima che nel 2019 gli attacchi ransomware abbiano costato all'industria sanitaria 25 miliardi di dollari. L'8% delle richieste di violazione dati nel settore sanitario è stato innescato da attacchi ransomware

(fonte), evidenziando come questa tipologia di attacco rappresenti una componente significativa del panorama delle minacce sanitarie.

Per il tredicesimo anno consecutivo, l'industria sanitaria ha riportato le violazioni dati più costose, con un costo medio di 10,93 milioni di dollari secondo IBM (fonte). Nel 2020, 560 strutture sanitarie sono state colpite da attacchi ransomware in 80 incidenti separati, mentre gli attacchi ransomware che colpiscono le organizzazioni di erogazione sanitaria sono raddoppiati dal 2016 al 2021.

I tempi e i costi di recupero nel settore sanitario variano significativamente: in media, il 64,8% dei dati sanitari è stato ripristinato dopo aver pagato il riscatto (fonte). Tuttavia, i costi di recupero sono sostanziali: 1,58 milioni di dollari per l'istruzione inferiore e 1,42 milioni di dollari per l'istruzione superiore, con processi di ripristino che possono richiedere mesi.

Settore manifatturiero: la vulnerabilità dell'automazione

Il settore manifatturiero è emerso come il più vulnerabile agli attacchi cyber, con punteggi di rischio cyber inferiori dell'11,7% rispetto alla media globale secondo Cowbell (fonte). Questa vulnerabilità è principalmente attribuibile alla dipendenza crescente dall'automazione e alla sensibilità della proprietà intellettuale che caratterizza il settore.

Le aziende manifatturiere con fatturato superiore a 50 milioni di dollari hanno probabilità 2,5 volte maggiori di subire incidenti cyber rispetto ad organizzazioni più piccole (fonte). Questa correlazione riflette sia la maggiore superficie di attacco delle grandi organizzazioni sia la loro attrattività come target per cybercriminali motivati finanziariamente.

Il settore manifatturiero è particolarmente esposto agli

attacchi alla supply chain, rappresentando uno dei 22 settori colpiti nei primi cinque mesi del 2025 secondo l'analisi Cyble (fonte). Solo i settori Mining e Real Estate sono rimasti intoccati dagli attacchi supply chain in questo periodo.

Settore educativo: l'escalation degli attacchi

Le istituzioni educative stanno affrontando un'escalation drammatica degli attacchi cyber. Secondo Cowbell, gli attacchi contro le istituzioni educative sono aumentati del 70% nell'ultimo anno (fonte), riflettendo la crescente attenzione dei cybercriminali verso infrastrutture tradizionalmente considerate "soft target".

Il report Verizon evidenzia che l'istruzione, che ha rappresentato il 30% delle violazioni dati nel 2022, ha sperimentato un aumento significativo degli attacchi ransomware, risultando in 1.241 incidenti di violazione dati (fonte). Di questi attacchi, 282 hanno confermato perdita o divulgazione di dati.

La distribuzione degli attacchi nel settore educativo mostra pattern specifici: gli attacchi all'istruzione inferiore (56%) e superiore (64%) sono aumentati, con attori di minaccia esterni che causano il 75% delle violazioni, mentre il 25% proviene da fonti interne (fonte).

Nonostante quasi la metà di coloro che sono stati attaccati abbia pagato il riscatto per recuperare i propri dati, solo il 2% ha ottenuto indietro tutti i dati, evidenziando l'inefficacia del pagamento come strategia di recupero.

Settore finanziario: sofisticazione e persistenza degli attacchi

Il settore finanziario/banking rappresenta il principale utilizzatore finale della sicurezza IT in Italia (fonte), seguito dal settore delle utility. Questa prioritizzazione riflette tanto la criticità dell'infrastruttura finanziaria

quanto la sua attrattività per gli attaccanti.

Il settore finanziario è stato identificato come il più targetizzato nei tentativi di phishing, con un aumento del 58,2% nel 2023 secondo Z Scaler (fonte). Questa concentrazione di attacchi riflette il valore intrinseco dei dati finanziari e l'accesso diretto alle risorse monetarie che caratterizza questo settore.

L'analisi CyberEdge rivela che le aziende di servizi finanziari sono considerate a maggior rischio di subire cyberattacchi nei prossimi 12 mesi, evidenziando una percezione di vulnerabilità elevata tra gli operatori del settore (fonte).

Pubblica amministrazione: obiettivi geopolitici

La pubblica amministrazione e i servizi educativi affrontano rischi elevati, particolarmente da attacchi ransomware (fonte). Nel marzo 2025, le agenzie governative hanno rappresentato il 47% dei target primari dei gruppi APT, seguite da organizzazioni e individui che rappresentano il 16% (fonte).

Gli attacchi contro la pubblica amministrazione spesso hanno motivazioni geopolitiche oltre che finanziarie. L'esempio dell'attacco ai siti web del governo italiano nel gennaio 2025, rivendicato da un gruppo hacker pro-russo come risposta all'incontro della Premier Meloni con il Presidente ucraino, illustra perfettamente questa dimensione geopolitica (fonte).

Settore delle telecomunicazioni: infrastruttura critica sotto assedio

Il settore delle telecomunicazioni rappresenta un target strategico privilegiato per gli attaccanti, come evidenziato dalla campagna Salt Typhoon che ha colpito almeno 8 fornitori di telecomunicazioni statuniteniti (fonte). Questo settore è particolarmente vulnerabile perché fornisce l'infrastruttura

di comunicazione critica di cui dipendono tutti gli altri settori.

Gli attacchi alle telecomunicazioni hanno spesso implicazioni che vanno oltre il danno immediato, potendo compromettere le comunicazioni nazionali e facilitare operazioni di spionaggio su larga scala. Il caso Salt Typhoon ha dimostrato come gli attaccanti possano acquisire accesso ai sistemi di intercettazione legale, compromettendo potenzialmente la sicurezza nazionale.

Analisi intersettoriale: pattern emergenti

L'analisi intersettoriale rivela pattern comuni che trascendono i confini industriali:

Convergenza delle minacce

Tutti i settori stanno sperimentando una convergenza delle minacce, dove attacchi tradizionalmente mirati a specifiche industrie si stanno diffondendo orizzontalmente. Gli attacchi supply chain, in particolare, dimostrano come una compromissione in un settore possa av# Cybercrime: Ultimi Accadimenti nel Mondo – Analisi Tecnica per Professionisti della Sicurezza Informatica

Sommario esecutivo

Il panorama del cybercrime nel 2025 si caratterizza per un'escalation senza precedenti in termini di sofisticazione, frequenza e impatto economico. I costi globali del cybercrime sono destinati a raggiungere i 10,5 trilioni di dollari annui entro il 2025, con una proiezione di crescita fino a 15,63 trilioni di dollari entro il 2029. Questa crescita esponenziale riflette non solo l'aumento numerico degli attacchi, ma anche la loro crescente complessità e l'integrazione di tecnologie emergenti come l'intelligenza

artificiale.

Fonti:

Center for Strategic and International Studies (CSIS) – Significant Cyber Incidents.

AAG IT Support – Latest Cyber Crime Statistics.

Bright Defense – Cybercrime Statistics for 2025.

SentinelOne – Key Cyber Security Statistics for 2025.

Sophos – The State of Ransomware 2025.

CrowdStrike – 2025 Global Threat Report.

FBI – Cyber Crime News and Press Releases.

Palo Alto Networks Unit 42 – Ransomware Trends 2025.

Cybersecurity and Infrastructure Security Agency (CISA).

World Economic Forum – Global Cybersecurity Outlook 2025.

Associazione Italiana per la Sicurezza Informatica (CLUSIT).

National Cybersecurity Centre (NCSC) UK.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/analisi-intersettoriale/