Sicurezza informatica e cyber crime: cosa aspettarsi dal 2024



In piena continuità con i precedenti, l'anno che sta per chiudersi registra un bilancio globale poco rassicurante sul fronte degli attacchi cyber.

Oltre ai numerosi casi eclatanti con "vittime illustri" – come Federprivacy o più di recente la società PA Digitale, coinvolta nel massiccio attacco al fornitore di servizi *cloud* Walpole – volumi e portata degli incidenti informatici risultano infatti generalmente in crescita.

I dati del cybercrime

Tutti i più autorevoli rapporti di fine anno riportano dati simili circa l'aumento degli attacchi registrati negli scorsi mesi a livello mondiale. Ciò anche grazie alla diffusione del fenomeno CaaS; non a caso l'EUROPOL, nel suo *Internet Organised Crime Assessment* (IOCTA) 2023, parla di *"apex of Crime-as-a-Service"*.

Tra i settori più colpiti si confermano *Healthcare*, mondo manifatturiero (preso di mira soprattutto da attacchi rivolti alle *Supply Chain*) e Pubbliche Amministrazioni; contesti che nell'ultimo triennio hanno affrontato una digitalizzazione irrefrenabile ma non sempre accompagnata dalla piena messa in sicurezza dei sistemi informatici, né dall'adeguata formazione di dipendenti e utenti coinvolti.

Risultano poi aumentati i costi medi conseguenti a *data breach* o attacchi *ransomware*, con un'astronomica previsione di 10.5 triliardi di dollari per le perdite attese entro la fine del 2024.

Cybersecurity e Cyber Crime, trend 2024

Le analisi di settore concordano su un ulteriore aspetto: il ruolo dell'AI risulterà preponderante in qualsivoglia scenario operativo futuro.

Artificial Intelligence (AI) e Machine Learning (ML) rivoluzionano la cyber security e il cybercrime

Secondo le previsioni, nei prossimi mesi si intensificherà il ricorso all'Intelligenza Artificiale per elevare il grado di sofisticazione delle minacce basate sull'ingegneria sociale; tipicamente BEC con finalità di *phishing* (e in particolare di *spear phishing*) ma non solo.

Anche i modelli di *Machine Learning* fronteggeranno sempre più spesso il rischio di essere manipolati o ingannati mediante input malevoli, rendendo urgente irrobustirne le difese rispetto ad *"Adversarial Attacks"* dagli impatti potenzialmente devastanti.

Un fenomeno che ha avuto sempre più eco negli utili mesi – per quanto non ascrivibile alla criminalità informatica – viene dal mondo dell'arte: ultimamente, infatti, molti artisti sono ricorsi a tecniche di *Data Poisoning* per proteggere le proprie opere da furti o riutilizzi illeciti, così ostacolandone la rielaborazione (e successiva diffusione non autorizzata) tramite sistemi di AI.

Ma l'Intelligenza Artificiale gioca in prima posizione anche sul fronte difensivo, soprattutto nelle attività di *threat detection* svolte da applicazioni EDR/MDR (*Endpoint/Managed Detection and Response*) o SIEM (*Security Information and Event Management*) nonché in generale per automatizzare i processi di sicurezza, rendendoli più performanti ed efficaci.

Consapevoli di operare entro uno scenario in costante evoluzione, le organizzazioni dovranno quindi saper integrare nelle proprie strategie di cybersecurity il corretto bilanciamento tra rischi e vantaggi dell''Intelligenza Artificiale.

Deep Fake e Misinformation

Nel corso del 2024 si assumono altresì in crescita le campagne di propaganda e disinformazione online, che sempre nell'AI trovano un fattore di crescente amplificazione.

Considerato il potenziale impatto di strumenti basati su tecnologie *deepfake*, è prevedibile ciò possa esercitare effetti destabilizzanti sugli equilibri democratici sia nazionali sia internazionali; in particolare contribuendo a influenzare l'opinione pubblica tramite la diffusione di *fake news* via via più "credibili" e insidiose, un fenomeno aumentato del 1000% solo negli ultimi sei mesi.

Mobile-specific cyber threats

Il ruolo dei *deepfake* appare centrale anche per la sicurezza dei dispositivi mobili, contesto ove prosperano truffe e furti di dati che sempre più spesso utilizzano il *voice scam* come vettore di attacchi più o meno sofisticati.

La diffusione del lavoro da remoto, le pratiche BYOD e l'uso promiscuo di dispositivi privati e aziendali per comunicazioni sia personali sia professionali non aiutano certo a contingentare i rischi; in confronto agli anni precedenti, pertanto, nel 2024 le minacce rivolte al mondo *Mobile* sembrano destinate ad aumentare.

IoT Security e l'avvento dell'AI-Augmented IoT

Con oltre 207 miliardi di dispositivi connessi attesi per la

fine del prossimo anno, anche la galassia dell'*Internet of Things* rappresenterà un fronte caldo per la sicurezza.

Il crescente impiego di ogni tipo di *device* in settori "sensibili" come la sanità impone di mettere al centro la tutela dei dati personali. Da monitorare i pericoli – ma anche le scommesse – legati all'avvento dell'*AI-Augmented IoT* (AIoT).

L'AIoT combina infatti l'Intelligenza Artificiale con l'Internet delle Cose, innalzando i livelli di autonomia ed efficienza dei dispositivi IoT: nel contesto della cybersecurity, consente un'analisi proattiva delle minacce velocizzando la rilevazione di *pattern* anomali e la prevenzione di intrusioni in *real-time*, incrementando così la resilienza dei sistemi. Questa tecnologia permette anche una gestione della sicurezza più adattiva e intelligente, riducendo gli errori umani e migliorando l'efficacia delle misure protettive. Tuttavia l'AIoT richiede protocolli avanzati per la protezione dei dati, in modo da evitare perdite di informazioni sensibili e mitigare i numerosi rischi legati alla privacy.

L'IoT sospinge inoltre la diffusione di strumenti come i *digital twins*, che hanno già dimostrato la propria efficacia in chiave di *cybersecurity*, anche in settori finora inesplorati. Questi modelli digitali avanzati offrono la possibilità di simulare scenari di attacco e valutare vulnerabilità in ambienti virtuali, migliorando la resilienza e l'efficacia delle risposte agli incidenti di sicurezza in ambienti IoT sempre più complessi.

Cybercrime-as-a-Service (CaaS)

Un ulteriore fronte di rischio è legato all'evoluzione in atto nel mercato nero del *cyber crime*, caratterizzato da un'offerta di servizi che spazia dalla compravendita di dati esfiltrati tramite *ransomware* alla vasta disponibilità di "pacchetti" per

la conduzione di attacchi su larga scala.

Rispetto al fenomeno CaaS/XaaS, gli esperti evidenziano come l'accesso sempre più facilitato al mondo del *cybercrime* comporti un significativo ampliamento nella platea dei potenziali attaccanti, che ormai non devono disporre di particolari competenze per poter accedere ai facili guadagni garantiti dal crimine informatico.

Ransomware 2.0

La maggiore innovazione e redditività legata al fenomeno *ransomware*, insieme al ruolo in espansione degli attori statali che vi ricorrono per fini bellici o di spionaggio, conferma come tale minaccia vada ancora considerata un'assoluta priorità di sicurezza.

Si nota che i gruppi più organizzati tendono in modo crescente a monetizzare i dati rubati non solo tramite la "classica" estorsione in danno delle organizzazioni-target ma anche rivendendoli a terzi per utilizzi malevoli futuri, in uno schema criminale che è stato definito *Ransomware 2.0*.

Questo nuovo schema incorpora tattiche aggiuntive e più aggressive, portando la cyber minaccia a un livello superiore di sofisticazione e pericolosità. Mentre nel "classico" *ransomware* ci si limita a criptare i dati della vittima e chiedere un riscatto per la decrittazione, il *Ransomware 2.0* mantiene infatti l'estrazione dei dati facendola seguire da una doppia estorsione, in cui gli attaccanti non solo chiedono un pagamento per decrittare i dati ma anche per non divulgarli, così raddoppiando la pressione esercitata sulla vittima.

Si assiste inoltre alla nascita di servizi di *Ransomware-as-a-Service* (RaaS) offerti in mercati *underground* che permettono anche a cybercriminali meno esperti di lanciare attacchi avanzati; e alla generale evoluzione di questa tipologia di

malware, oggi sempre più polimorfica (ovvero capace di cambiare il proprio codice o la propria firma digitale) e accompagnata da tecniche di attacco sempre più sofisticate come il *phishing*, l'*exploit* di vulnerabilità di rete o il *brute force*, attraverso le quali accedere ai sistemi target.

A causa della sua natura evasiva e mutevole, che lo rende difficile da rilevare con i metodi tradizionali, il *ransomware* polimorfo richiede soluzioni di sicurezza informatica avanzate.

Cyber Warfare: La Nuova Frontiera dei Conflitti Digitali e la Sfida dell'AI

Nello scenario di rischio vanno incluse anche le attività di *Cyber Warfare* legate all'instabilità geopolitica in diverse parti del pianeta e le conseguenti minacce verso obiettivi istituzionali o infrastrutture critiche, che possono determinare impatti di sicurezza estremamente gravi.

Si nota un aumento della sofisticazione dei cyber attacchi *State-sponsored*, che include un uso intensivo di AI e *machine learning* e vede il crescente ruolo dei *deepfake* nelle operazioni di disinformazione: ciò sta portando al paradosso di una cybersecurity che si ritrova a "**combattere l'AI con l'AI**", generando un ciclo di sfida e risposta sempre più complesso. Questo paradigma crea una vera corsa agli armamenti digitali, dove difensori e aggressori evolvono continuamente le loro strategie.

Tale scenario e il conseguente rischio di ingenti perdite economiche influiscono, naturalmente, anche sul piano delle *cyber insurance*.

Cyber Insurance: Crescita del Mercato e

Nuove Sfide imposte dalla Cyber Warfare e dall'AI

Nell'ultimo triennio – complici la situazione di incertezza globale e il citato aumento dei costi medi di un attacco – il mercato delle assicurazioni contro gli attacchi informatici è stato interessato da una crescita rapidissima.

Le attuali stime parlano di un valore globale superiore ai 7 miliardi di dollari, che nel 2024 si prevede continui a procedere senza tregua.

La *cyber warfare* e l'intelligenza artificiale stanno giocando un ruolo sempre più centrale nel settore delle assicurazioni cyber: con l'evoluzione della guerra cibernetica, le compagnie assicurative si sono trovate a dover riprogettare le proprie polizze al fine di proteggere il mercato da rischi insostenibili. Un lavoro estremamente complesso, specie considerando la difficoltà nell'attribuzione degli attacchi a uno specifico *Threat Actor* (o Stato).

L'aumento di sofisticazione e frequenza degli attacchi informatici comporta una valutazione del rischio estremamente dettagliata, con un aumento dei premi e condizioni di copertura sempre più rigide, spingendo così le aziende verso standard di sicurezza più elevati.

Diventa quindi imprescindibile lo sviluppo di strategie di prevenzione che includano la formazione dei dipendenti e l'adozione di tecnologie di sicurezza avanzate, contribuendo alla sensibilizzazione in materia e all'adozione di *security posture* più adeguate.

Cybersecurity nell'Era del 5G e dell'Edge Computing

L'impiego crescente dell'*Edge computing*, reso possibile dalla diffusione delle reti 5G, rappresenterà un'ulteriore

innovazione nel panorama cyber.

Si auspica infatti che l'elaborazione decentrata di importanti moli di dati possa velocizzare l'automazione sia dei flussi produttivi, sia dei controlli di sicurezza: ciò specialmente nel contesto della *Smart Factory* dove le tecnologie *Edge computing* facilitano la convergenza tra tecnologie IT e OT, permettendo l'applicazione di soluzioni di sicurezza maggiormente integrate ed efficaci.

Nell'ambito della cybersecurity, l'*Edge Computing* e il 5G presentano sfide uniche.

Poiché i dispositivi *edge* ampliano la superficie di attacco con i dati elaborati localmente, essi richiedono protezione anche a livello di dispositivo e di conseguenza accrescono la necessità di una sicurezza distribuita; mentre il 5G, offrendo maggiori velocità e connettività, espone a nuove vulnerabilità di rete rendendo necessaria una gestione avanzata della sicurezza dei dati in transito, in particolare attraverso la crittografia.

L'integrazione di queste tecnologie richiede, perciò, un approccio di sicurezza olistico e multi-livello.

Blockchain e Cybersecurity: Opportunità e Rischi nella Protezione dei Dati

Anche le tecnologie *blockchain* potranno rappresentare una risorsa, includendo le garanzie di riservatezza offerte dalla crittografia dei dati e una maggiore resilienza delle reti.

Oltre al mondo *Finance* – nel quale è già ampiamente diffusa – si stima pertanto che le migliori performance della *blockchain* per la cybersecurity saranno osservabili in campo di *Data Protection*.

Al contempo occorre essere consapevoli dei rischi derivanti dalla natura aperta e decentralizzata di questo strumento, che

può rendere meno semplici i controlli di sicurezza lasciando spazio a minacce mirate in particolare agli *Smart Contracts* o al furto di criptovalute (dove un singolo attacco può fruttare oltre 200 milioni di dollari, come accaduto nel settembre 2023).

Cyber Security Skills: Carenza Globale di Competenze

Un tema cruciale riguarderà infine gli investimenti necessari alla diffusione delle *Cyber Security Skills*, affinché l'esigenza di includere nella forza lavoro di ogni settore un sufficiente numero di esperti di sicurezza non sia frustrata dalla scarsa disponibilità di professionisti adeguatamente formati.

Si prevede che già oggi manchino dal mercato oltre 4 milioni di professionisti specializzati in cybersecurity a livello globale, in particolare in campo di AI/ML e *cloud security*: un numero probabilmente destinato ad aumentare nei prossimi anni.

Conclusioni

Nell'affrontare un simile scenario, molto dipenderà anche dalle scelte degli organismi regolamentari.

In attesa della Convenzione ONU sul Cybercrime (in corso di elaborazione presso le competenti sedi) e del Regolamento UE sull'intelligenza artificiale (su cui si è recentemente raggiunto un nuovo accordo, non esente da critiche quanto alle scelte operate in tema di diritti civili), resta evidente come anche nel 2024 la sfida della sicurezza informatica debba procedere nel solco della formazione e della cooperazione fra tutti gli attori in campo.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/sicurezza-informatica-e-cyber-crime-cosa-aspettarsi-dal-2024/