Cyber-furto di dati, sotto attacco i distretti manifatturieri del Nord

Focus 2023. Incursioni ransomware a +27%: il picco a Milano e Roma ma diffuse nelle regioni settentrionali
Il 74% delle azioni sulle Pmi. Poche denunce per evitare il danno reputazionale. Il piano Acn per le imprese

Pagina a cura di
Ivan Cimmarusti

Le piccole e medie imprese italiane restano poco inclini a denunciare gli attacchi *ransomware*, cioè «l'esfiltrazione» a scopo riscatto dei dati personali dei clienti. Anzi, troppo spesso preferiscono silenziare il cyber furto, accettando un'estorsione piuttosto che rendere nota l'aggressione hacker col rischio del danno reputazionale.

Dati alla mano il fenomeno rappresenta un'emergenza. Secondo l'Agenzia per la cybersicurezza nazionale, organismo diretto dal prefetto Bruno Frattasi e dalla vice direttrice Nunzia Ciardi, nell'ultimo anno gli attacchi *ransomware* sono aumentati del 27 per cento. In particolare, si è registrato un incremento nelle aree geografiche più produttive del Paese. Eppure, si tratta di un dato sottostimato. Ma andiamo con ordine.

La distribuzione degli attacchi

Nella grande maggioranza dei casi (84%), le vittime del *ransomware* appartengono al settore privato.

Per quanto attiene alla dimensione aziendale dei soggetti privati colpiti, l'Agenzia calcola che circa il 23,1% degli eventi *ransomware* ha interessato grandi imprese, mentre in oltre il 74% dei casi sono state coinvolte piccole (46,3%) e medie (30,6%) realtà produttive.

Secondo la classificazione delle vittime in base ai settori economici, emerge come quello manifatturiero sia stato il più colpito, in continuità con il 2022, seguito — nel 2023 — dalla vendita al dettaglio e dai settori sanitario e tecnologico. Sempre tra i privati, risultano incursioni verso società di servizi finanziari, energetici, delle telecomunicazioni, costruzioni, fornitura di acqua potabile e farmaceutico.

Dal punto di vista geografico (si veda il grafico), le zone maggiormente interessate dal fenomeno del *ransomware* corrispondono a quelle con realtà produttive più importanti. Il maggior numero è concentrato tra Roma e Milano, ma in generale i target sono soprattutto nei distretti industriali del Nord. L'Agenzia conferma che «ciò è determinato dalla maggior presenza, in tali zone, di imprese operanti nel manifatturiero».

Un dato sottostimato

Nel 2023 si parla di 165 azioni *ransomware*, cui vanno aggiunte quelle trattate dalla Polizia postale, che superano le 210 (tra il 2021 e il 2023 circa mille azioni complessivamente tra i due organismi). Dati che, secondo gli osservatori, sono decisamente sottostimati.

Nella relazione annuale dell'Agenzia, presentata mercoledì scorso a Palazzo Chigi, infatti, è specificato come «il dato rappresenti solo una parte del numero complessivo di attacchi *ransomware* effettivamente avvenuto». Il problema è che le imprese che subiscono l'incursione entro 72 ore dovrebbero comunicare al Garante della privacy la sottrazione dei dati personali dei clienti «a meno che», recita l'articolo 33.1 del Regolamento generale sulla protezione dei dati (Gdpr), «sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche». Tuttavia, quando si parla di *ransomware*, questo rischio è certo, tanto che i nominativi dei clienti finiscono regolarmente in vendita nei market del *dark web*. Con la comunicazione al Garante dell'avvenuto attacco cyber, si diceva, l'impresa dovrà dare pubblicità dell'attacco, rischiando concretamente di incorrere sia in un danno reputazionale sia in una sanzione. Per questo troppo spesso si preferisce pagare il riscatto, finendo — inconsapevolmente — nelle *black list* dei soggetti "pagatori" che periodicamente subiscono incursioni. Un errore, secondo i vademecum della Polizia postale diretta da Ivano Gabrielli, in quanto in questo modo si finisce per incentivare un business illecito che, nel 2022, ha toccato, a livello globale, quota 1,1 miliardi di dollari di riscatti.

Un ulteriore problema per le piccole e medie imprese italiane è legato allo scarso *know-how* tecnologico e di infrastrutture interne, fattori determinanti per bloccare gli assalti cyber, ormai compiuti con sistemi di Intelligenza artificiale.

Cyber Index Pmi

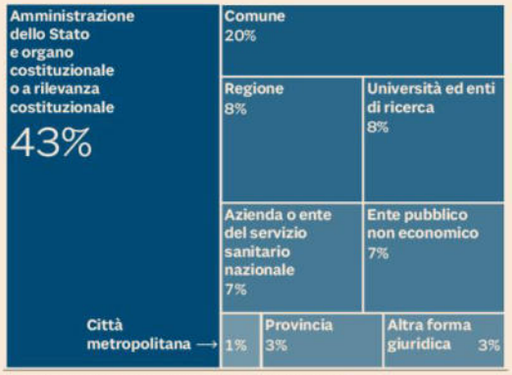
Le Pmi rappresentano un target particolarmente rilevante per l'Agenzia alla luce del numero di eventi cyber di cui sono oggetto e del livello di maturità cyber mediamente non particolarmente elevato di tali aziende. Per questo, in attuazione del protocollo d'intesa firmato nel 2022 con Confindustria e Generali Italia Spa è stato presentato il *Cyber Index Pmi*. L'obiettivo è di diffondere la conoscenza dei temi di cybersicurezza presso le Pmi e di promuovere comportamenti e strumenti contro gli attacchi.

La mappa delle aziende colpite

Fonte: Bilancio 2023 - Agenzia per la cybersicurezza nazionale

I bersagli pubblici

Distribuzione degli eventi cyber contro la Pubblica Amministrazione



Fonte: Bilancio 2023 - Agenzia per la cybersicurezza nazionale

L'intervista. Nunzia Ciardi. Vice direttrice Agenzia per la cybersicurezza nazionale

«Più cybersicurezza per la competitività di imprese e filiere»

Nunzia Ciardi. Secondo la vice direttrice dell'Acn la formazione è un fattore essenziale nel cyber

«Dico spesso che la rivoluzione tecnologica ha innescato una vera e propria rivoluzione antropologica. Il digitale, e con l'intelligenza artificiale questo sarà ancora più evidente, ha cambiato profondamente le nostre società e il nostro rapporto con la realtà. E cambiamenti così profondi richiedono un tempo di metabolizzazione e processi culturali lunghi. Uno dei compiti fondamentali dell'Agenzia per la cybersicurezza nazionale sarà proprio quello di diffondere e accelerare questa cultura e consapevolezza ad ogni livello».

Così Nunzia Ciardi, vice direttrice dell'Agenzia per la cybersicurezza nazionale, prima donna a capo della Polizia postale, nonché autrice del libro "*Con lo smartphone usa la testa*", in cui aiuta i genitori a capire cosa si può fare per difendere i più giovani.

Il mondo delle Pmi sembra poco pronto alla sfida cyber.

Abbiamo presentato pochi giorni fa l'edizione 2024 del *Cyber Index Pmi* proprio in virtù della collaborazione dell'Agenzia con Confindustria e Generali. Da un lato, digitalizzare l'attività imprenditoriale significa conferire un vantaggio competitivo alle imprese, imprescindibile per misurarsi sullo scenario globale odierno; dall'altro, la digitalizzazione comporta necessariamente una previsione in termini di cybersicurezza, la cui mancanza rende vulnerabili non soltanto l'intero sistema aziendale ma anche la filiera di appartenenza e le filiere a essa collegate. Per questo a ogni innovazione deve corrispondere una crescita degli strumenti di tutela e della consapevolezza cyber, obiettivo principale della nostra collaborazione con Confindustria.

Con l'attuazione del Pnrr, quanto è importante la prevenzione cyber in particolare negli enti locali?

È così importante che nella Strategia nazionale di Cybersicurezza la formazione e la promozione della cultura della sicurezza cibernetica sono considerati non singoli obiettivi ma fattori abilitanti senza i quali nessuno degli obiettivi può essere efficacemente realizzato.

Insomma, non bastano solo gli investimenti.

Per quanto abbondanti possano essere gli investimenti strutturali, senza una base solida di preparazione è impossibile assicurare l'obiettivo di cybersicurezza e resilienza che ci poniamo per il sistema-Paese.

Gli enti locali sono strategici.

Detengono in Italia un ruolo fondamentale per l'erogazione dei servizi al cittadino e per questo saranno tra i primi beneficiari di un'azione complessiva volta a costruire un sistema Italia consapevole e preparato in modo capillare e diffuso.

Cosa ne pensa del Ddl Cyber?

È sicuramente uno strumento preziosissimo. Va esattamente nella direzione auspicata anche grazie a una diversa configurazione dei reati che permette strumenti investigativi specifici, indispensabili per la lotta al crimine cyber. È altrettanto vero che l'evoluzione normativa deve essere accompagnata da una profonda evoluzione culturale e da una diffusione della consapevolezza necessaria a ogni livello.

Il cosiddetto fattore umano.

Chi si occupa di tutelare la cybersicurezza e la resilienza di una struttura, nulla può senza la collaborazione di tutte le risorse umane che, inevitabilmente, interagiscono con la struttura stessa. Il fattore umano può contribuire ad alimentare la forza della rete di protezione del soggetto, o, al contrario, può determinare il crollo di ogni difesa e per rendere l'uomo una risorsa e non un ostacolo nella difesa cyber, è necessario investire in programmi di *awareness* e formazione.