CYBER CRIME, LA TEMPESTA DOPO LA QUIETE

di BENIAMINO MUSTO

DOPO DUE ANNI DI PERDITE ELEVATE MA STABILI, IL 2023 HA VISTO UNA PREOCCUPANTE RECRUDESCENZA DI CASI DI RANSOMWARE ED ESTORSIONI INFORMATICHE, AVVERTE ALLIANZ COMMERCIAL IN UN NUOVO REPORT: LE PREVISIONI STIMANO CHE IL SOLO RANSOMWARE COSTERÀ ALLE SUE VITTIME CIRCA 265 MILIARDI DI DOLLARI ALL'ANNO ENTRO IL 2031

© anyaberkut - iStock

I miglioramenti nella sicurezza informatica e nella business continuity stanno contribuendo a combattere gli attacchi ransomware basati sulla crittografia, ma il panorama delle minacce informatiche è in continua evoluzione. Il 2023 ha visto una preoccupante recrudescenza dei ransomware e delle denunce di estorsione, con conseguente aumento di incidenti costosi, a dimostrazione che, nonostante siano stati compiuti progressi, la minaccia rappresentata dal ransomware mostra pochi segni di diminuzione.

È un quadro molto preoccupante quello che emerge dall'ultimo rapporto *Cyber security trends*, realizzato da **Allianz Commercial**. Lo studio, infatti, rileva che nel primo trimestre 2023 il numero di vittime di ransomware è aumentato fino al 143% a livello globale: in particolare, tra gennaio e febbraio di quest'anno, si è registrato il picco più elevato di casi di hacking e fuga di dati degli ultimi tre anni. E le previsioni stimano che il solo ransomware costerà alle sue vittime circa 265 miliardi di dollari all'anno entro il 2031.

AUMENTANO LE SOTTRAZIONI DI DATI

Gli hacker prendono sempre più di mira l'ambito IT e le supply chain fisiche, lanciando attacchi informatici di massa e trovando nuovi modi per estorcere denaro

alle aziende, grandi e piccole. La maggior parte degli attacchi ransomware comportano ora il furto a scopo di estorsione di dati commerciali personali o sensibili, aggiungendo ulteriori costi e complessità, nonché un maggiore potenziale di danni reputazionali. L'analisi del report su una serie di sinistri informatici di grandi dimensioni nel settore assicurativo mostra che la percentuale di casi in cui i dati vengono sottratti aumenta ogni anno: dal 40% dei casi nel 2019 a circa il 77% nel 2022, con il 2023 in procinto di superare la percentuale totale dello scorso anno.

Secondo **Scott Sayce**, global head of cyber di Allianz Commercial, "la frequenza delle denunce informatiche è aumentata nuovamente quest'anno poiché i gruppi di ransomware continuano a evolvere le loro tattiche. Sulla base dell'attività dei sinistri durante la prima metà del 2023, prevediamo di vedere un aumento annuo del numero di sinistri di circa il 25% entro la fine dell'anno".

IL GATTO CHE INSEGUE IL TOPO

Proteggere un'organizzazione dalle intrusioni, si legge nel report di Allianz Commercial, "rimane un gioco del gatto e del topo, in cui i criminali informatici hanno il vantaggio. Gli autori delle minacce stanno ora esplorando modi per automatizzare e accelerare gli attacchi, creando malware e phishing più efficaci basati sull'intelligenza artificiale", in un contesto in cui la crescita dell'Internet of Things e la capillare diffusione di dispositivi mobili connessi aprono enormi possibilità di attacchi informatici, che sembrano destinate ad aumentare nei prossimi anni.

"Prevenire un attacco informatico diventa quindi sempre più difficile e la posta in gioco è sempre più alta. Di conseguenza, le capacità di rilevamento precoce e di risposta stanno diventando sempre più importanti", si legge nel report. Un'intrusione può rapidamente degenerare e, una volta che i dati vengono crittografati e/o rubati, le conseguenze, anche in termini economici, aumentano vertiginosamente: i costi, secondo l'analisi di Allianz Commercial, possono essere fino a 1.000 volte superiori rispetto a quelli derivanti da un incidente non rilevato e contenuto tempestivamente. Pertanto "la capacità di rilevamento tempestivo e di risposta efficace saranno fondamentali per mitigare l'impatto degli attacchi informatici e garantire un mercato assicurativo sostenibile in futuro", si legge nel report.

L'EVOLUZIONE DEL RANSOMWARE

Lo studio di Allianz Commercial sostiene che nella prima metà del 2023 si è registrato un aumento del 50% su base annua dei casi. I cosiddetti kit Ransomware-as-a-Service (RaaS), i cui prezzi partono da soli 40 dollari, rimangono un fattore chiave nella frequenza degli attacchi. Le bande di ransomware stanno inoltre effettuando più attacchi più velocemente, con il numero medio di giorni necessari per eseguirne uno che è sceso da circa 60 giorni nel 2019 a quattro.

"Gli episodi di doppia e tripla estorsione, che utilizzano una combinazione di crittografia, esfiltrazione di dati e attacchi *Distributed denial of service* per ottenere denaro, non sono una novità, ma sono ora più diffusi". Il report osserva che l'esfiltrazione dei dati può aumentare in modo significativo il costo di una perdita o di un sinistro informatico, giacché la risoluzione di tali incidenti può richiedere più tempo, mentre le indagini legali e informatiche possono essere estremamente costose. Se i dati sono stati rubati, le aziende devono sapere esattamente quali dati sono stati esfiltrati e probabilmente dovranno avvisare i clienti, che potrebbero chiedere un risarcimento o minacciare un contenzioso.

SEMPRE PIÚ CASI DI DOMINIO PUBBLICO

Allianz inoltre osserva come, in passato, il numero di incidenti informatici divenuti di pubblico dominio fosse basso. Oggi invece gli hacker minacciano di pubblicare online i dati sottratti. L'analisi di Allianz Commercial sulle grandi perdite informatiche (superiori al milione di euro) mostra che la percentuale di casi diventati pubblici è aumentata da circa il 60% nel 2019 all'85% nel 2022, e nel 2023 questa percentuale potrebbe essere superiore. Le conseguenze finanziarie e reputazionali sono potenzialmente costose, tanto da spingere le aziende a sentirsi maggiormente sotto pressione nel cedere agli estorsori. Secondo il report, il numero di aziende che pagano un riscatto è aumentato di anno in anno, passando da appena il 10% nel 2019 al 54% nel 2022, sempre sulla base dell'analisi delle sole perdite ingenti (superiori al milione di euro).

Come tuttavia osserva Allianz Commercial, "il pagamento di un riscatto per i dati sottratti non risolve necessariamente il problema. L'azienda potrebbe ancora dover affrontare cause legali da parte di terzi per la violazione dei dati, soprattutto negli Stati Uniti". L'analisi su oltre 3.000 sinistri informatici negli ultimi cinque anni mostra che la manipolazione esterna dei sistemi è la causa di oltre l'80% di tutti gli incidenti. Gli autori delle minacce stanno ora esplorando modi per utilizzare l'intelligenza artificiale per automatizzare e accelerare gli attacchi, creando malware, phishing e simulazioni vocali più efficaci: in particolare, Allianz Commercial ha registrato un numero crescente di incidenti causati dalla scarsa sicurezza informatica dei dispositivi mobili connessi.