Telpress
Sezione:BANCHE FINANZA VIGILANZA
la Repubblica
AFFARI&FINANZA
Dir. Resp.:Maurizio Molinari
Tiratura: 400.000 Diffusione: n.d. Lettori: n.d.
Rassegna del: 28/06/21
Edizione del:28/06/21
Estratto da pag.:48
Foglio:1/1

LE POLIZZE INFORMATICHE

Crimini informatici, come ridurre i costi di indennizzo

BRAD SLINGERLEND*

Fiducia zero è l'atteggiamento verso gli hacker che cercano documenti su quanto sia assicurata una società contro il ransomware

L'anno scorso abbiamo dovuto affrontare un'altra epidemia: l'aumento degli attacchi informatici. "I criminali informatici stanno usando sempre più spesso disruptive malware contro le infrastrutture sensibili e le istituzioni sanitarie, a causa del potenziale di alto impatto e beneficio finanziario," ha detto l'Interpol ad agosto dell'anno scorso. Un attacco informatico contro SolarWinds a dicembre ha compromesso 100 aziende come Microsoft e Intel, insieme a una dozzina di agenzie governative statunitensi tra cui il Tesoro e i dipartimenti della Difesa, della Giustizia e dell'Energia, secondo l'amministratore delegato della società con sede in Texas, Sudhakar Ramakrishna. Il vaccino si chiama Fiducia Zero. Uno dei motivi per cui le organizzazioni del settore pubblico e privato si stanno concentrando sulla fiducia zero è l'aumento dei costi di indennizzo contro gli attacchi ransomware, che sono quadruplicati nel 2020 a 348 milioni di dollari, anche grazie alle criptovalute, secondo il Wall Street Journal.

Una tecnica utilizzata dagli hacker è quella di cercare un documento che dettagli quanto sia assicurata una società contro il ransomware, il che permette loro di impostare le loro richieste al limite della politica in modo da evitare di danneggiare gli utili della società vittima. Axa è stata colpita da un attacco ransomware poco dopo aver detto che non avrebbe più sottoscritto l'assicurazione ransomware in Francia, mentre il fornitore di assicurazioni informatiche CNA ha pagato 40 milioni di dollari per recuperare i suoi dati dagli hacker che cercavano di ottenere una lista di aziende con copertura ransomware. Tali premi assicurativi potrebbero essere meglio spesi per le protezioni basate sul cloud, che potrebbero a loro volta consentire ad alcuni dei 150-200 miliardi di dollari spesi annualmente per la sicurezza IT aziendale di essere reindirizzati in modo migliore.

Con le istituzioni pubbliche e private che adottano sempre più spesso la fiducia zero, sembra che la modernizzazione della cybersecurity stia acquistando slancio. Un'architettura a fiducia zero che sfrutta le partnership Api-enabled tra accesso (Okta), governance (SailPoint), accesso privilegiato (CyberArk), sicurezza degli endpoint (CrowdStrike), sicurezza della posta elettronica (Proofpoint) e Cloudflare, si dimostrerebbe molto più resistente di firewall obsoleti o altre "barriere" intorno ai server le cui vulnerabilità sono ormai chiare. Senza alcun segno che gli attacchi diminuiranno, le organizzazioni devono assumere che i loro dati non sono sicuri e dare la priorità alla costruzione di un'architettura di autenticazione a più fattori che presuppone che le minacce siano reali.

– *co-fondatore e investitore di NZS Capital LLC, partner di Jupiter AM

1 Il crimine cyber è una delle più grandi minacce alla sicurezza della navigazione e le compagnie cercano di difendersi con prodotti assicurativi ad hoc

1

1 Anche Microsoft è stata coinvolta nell'attacco a SolarWinds


L'assalto dei pirati viaggia sulla rete