

Digitalizzazione

Criminalità informatica: ***aumento degli attacchi ransomware***

17.10.2025

A colpo d'occhio

Un'ondata di ransomware lanciata da un gruppo di hacker sta investendo la Svizzera. Le autorità federali mettono in guardia con urgenza contro questi attacchi, soprattutto perché sono in aumento quelli alle imprese.

- Oltre 200 imprese colpite dal 2023, con danni per milioni di franchi.
- Attualmente avvengono 4-5 attacchi a settimana: un triste record per la Svizzera
- Nessuna impresa è troppo piccola: i criminali informatici prendono di mira i punti deboli non protetti.

Le autorità federali mettono in guardia: attualmente un gruppo di hacker sta intensificando le proprie attività in Svizzera – le autorità registrano al momento 4-5 attacchi alla settimana. Finora circa 200 imprese svizzere sono già state vittime di questi attacchi ransomware. Il danno ammonta a diversi milioni di franchi – a livello mondiale a diverse centinaia di milioni.

Proteggetevi: nessuno è troppo piccolo o troppo grande per diventare un bersaglio

Questo avvertimento riguarda tutti noi. Gli ultimi sviluppi dimostrano chiaramente che nessuna impresa è troppo piccola per diventare un bersaglio. I criminali informatici non fanno distinzione tra grandi imprese e PMI. Cercano i punti deboli e li trovano dove mancano o sono state trascurate le misure di protezione.

Dal 2023 sono state vittime di attacchi di questo tipo oltre 200 imprese svizzere. Il ransomware non è più un fenomeno marginale. Un solo attacco può bloccare l'intera attività commerciale nel giro di poche ore. Interruzioni della produzione, perdita di dati critici per l'impresa, compromissione delle catene di fornitura: le ripercussioni vanno ben oltre il settore IT. La criminalità informatica non è quindi solo un rischio tecnologico, ma anche economico e strategico.

Responsabilità delle imprese: la preparazione è fondamentale

Per l'economia è chiaro: la prevenzione inizia all'interno dell'impresa stessa. Chi non protegge la propria infrastruttura digitale è esposto a un rischio crescente. Non occorre un reparto speciale per adottare misure fondamentali, ma è necessaria una chiara consapevolezza a livello dirigenziale.

Gli elementi essenziali della resilienza informatica sono:

- Manutenzione e aggiornamenti del sistema: gli accessi obsoleti sono uno dei punti di ingresso più frequenti.
- Piani di backup e di emergenza: salvati offline, testati e disponibili in caso di emergenza.
- Autenticazione a più fattori: un passo semplice, un grande effetto.

— Sensibilizzazione dei collaboratori: spesso l'anello più debole rimane l'uomo.

La criminalità informatica non è un problema tecnologico. È un compito dirigenziale.

Chi investe oggi nella sicurezza digitale, domani proteggerà i clienti, le catene di fornitura, la reputazione e la piazza economica svizzera nel suo complesso.

Per ulteriori informazioni sul tema dei ransomware e su come proteggersi, l'Associazione Svizzera d'Assicurazioni ha pubblicato una guida.

Ulteriori informazioni della Confederazione sono disponibili qui.

Angela Anthamatten
Responsabile supplente del dipartimento concorrenza e regolamentazione

David Stauffacher
Responsabile di progetto infrastrutture e digitale