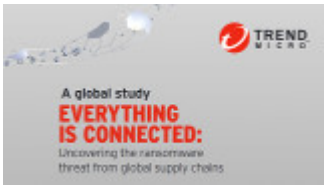
Ransomware: secondo Trend Micro il 58% delle imprese italiane ha subito almeno un attacco negli ultimi tre anni

https://www.hwupgrade.it/i/n/trendmicro_supplychain_720.JPG,



Il dato che più colpisce del nuovo report di Trend Micro è che più di un'azienda su tre sostiene di non informare i partner delle minacce. Preoccupazione per le PMI che fanno parte della supply chain di realtà più grandi e sono potenzialmente meno sicure

di Alberto Falchi pubblicata il **21 Settembre 2022**, alle **18:31** nel canale Security
Trend Micro#SEMinthecityCloud Security

Il nuovo report di **Trend Micro**, "**EVERYTHING IS CONNECTED: Uncovering the ransomware threat from global supply chains**", sottolinea come 8 responsabili IT su 10 in Italia siano preoccupati a causa dei loro partner e clienti. Il motivo è presto detto: il **57% degli intervistati dichiara di aver visto almeno un'altra azienda della propria supply chain vittima di un attacco informatico**.

La catena di approvvigionamento è insomma uno dei punti deboli per quanto riguarda la sicurezza informatica, e il fatto che il tessuto imprenditoriale del Bel Paese sia composto prevalentemente da PMI, potenzialmente più vulnerabili rispetto a realtà maggiormente strutturate, non spinge

all’ottimismo.

La supply chain è uno dei punti critici per la cybersecurity. L’analisi di Trend Micro

La ricerca di Trend Micro, realizzata da Sapio Research e basata su un campione di 2.958 IT Decision Maker in 26 Paesi (di cui 100 in Italia) si focalizza sul problema della cybersecurity della supply chain. Un’azienda, infatti, può disporre delle migliori difese possibili e dei migliori esperti, ma oggi il mondo è pesantemente interconnesso e un attacco a un cliente o partner può riflettersi anche sulle altre imprese che fanno parte della catena di approvvigionamento.

La minaccia principale è quella del ransomware, ormai rilevato in un incidente informatico su quattro. “*Il 57% delle aziende italiane ha visto almeno un’altra organizzazione all’interno della propria supply chain venire colpita da un attacco ransomware e questo mette i propri sistemi potenzialmente a rischio di compromissione*“, spiega **Alessandro Fontana**, Head of Sales di Trend Micro Italia. “*Molti però non adottano misure per migliorare la sicurezza informatica dei partner. Il primo passo per mitigare questi rischi deve essere una maggiore visibilità e controllo sulla superficie di attacco digitale che è in continua espansione*“.

Il pericolo principale è quello del **ransomware**, ormai rilevato in un incidente informatico su quattro, e in continua crescita, anche a causa dei servizi di Ransomware-as-a-Service offerti da alcuni gruppi criminali. Una vera e propria industria del crimine, che sfrutta le debolezze delle imprese.

Secondo le analisi di Trend Micro, infatti, con il crescere degli investimenti sul digitale è aumentata l'area del perimetro da difendere. Le aziende, però, non hanno investito allo stesso modo sulla cybersecurity, favorendo la produttività. E mettendo a rischio non solo se stesse, ma anche partner e clienti.

Ulteriore aspetto a destare preoccupazione è la scarsa condivisione delle informazioni: solamente il 51% delle aziende condivide i dati sugli attacchi ransomware con i propri fornitori, **inoltre il 37% dichiara di non informare i partner circa le minacce**. Il motivo, però, non è da ricercare necessariamente nel desiderio di nascondere la criticità della propria situazione: secondo Trend Micro la causa potrebbe anche essere il fatto che molte aziende non hanno informazioni da condividere. Nel senso che in alcuni casi non sanno di aver subito un incidente.

Secondo il report infatti, i tassi di rilevamento in Italia sono molto bassi: 54% per il ransomware, 44% per l'esfiltrazione di dati, 41% per l'accesso iniziale ai sistemi, 35% per l'utilizzo di strumenti come PSexec o Cobalt Strikle e il 29% per i movimenti laterali all'interno dell'infrastruttura.

Read More