CISOs CONNECT

in collaborazione con

AimPoint Group | W2Communications

Focus Ransomware

Cosa ne pensano i CISO

Per comprendere il clamore mediatico suscitato da questo argomento, ad agosto del 2021 abbiamo chiesto il parere di oltre 250 CISO (Chief Information Security Officer) per raccogliere delle testimonianze dirette sulle loro esperienze con i ransomware, capire quali sono le preoccupazioni reali e scoprire i piani messi in atto per proteggere le aziende in futuro.

La situazione non migliora

In tutto		Aziende di medie dimensioni (da 1000 a 10.000 dipendenti)
53%	Aziende colpite almeno una volta da un attacco ransomware negli ultimi 12 mesi	66%
69%	Aziende che saranno probabilmente colpite almeno una volta da ransomware nei prossimi 12 mesi	80%

I 3 settori principali che saranno probabilmente colpiti da ransomware nei prossimi 12 mesi

Edilizia e macchinari

Vendita al dettaglio e beni di consumo durevoli

Settore manifatturiero

Il costo del riscatto NON è la preoccupazione principale

Gli effetti *più preoccupanti* dei ransomware

1. Esposizione di dati proprietari o sensibili

2. Costi di recupero/ripristino delle normali operazioni

3. Perdita di fatturato dovuta all'interruzione delle attività

Gli effetti *meno preoccupanti* dei ransomware

9. Calo della produttività dei dipendenti

10. Costi per il pagamento del riscatto

11. Costo di sanzioni normative e di mancata conformità

Riscatto sì o riscatto no?

Il pagamento del riscatto ha portato al recupero *COMPLETO* dei dati

Il pagamento del riscatto ha portato al recupero *PARZIALE* dei dati

Il pagamento del riscatto *NON* ha portato al recupero dei dati

1 su 5 ..... vittime dei ransomware che hanno subito un impatto economico pari a ..... Più di 5 Mln USD

1 su 20 ..... vittime dei ransomware che hanno subito un impatto economico pari a ..... Più di 50 Mln USD

Strategie di difesa

Le contromisure tecniche più importanti per mitigare gli attacchi ransomware

- Backup e recupero dei dati
- Piattaforme di protezione degli endpoint (EPP)
- Sicurezza delle e-mail (con rilevamento del phishing)
- Consapevolezza e formazione degli utenti

Le migliori contromisure tecniche che verranno aggiunte alle difese contro i ransomware nei prossimi 12 mesi

- Analisi del comportamento degli utenti e delle entità (UEBA)
- Segmentazione della rete/accesso zero trust
- Prevenzione da perdite/fughe di dati (DLP)

Non tutto il male vien per nuocere...

La risonanza mediatica dei ransomware e la portata del loro impatto sulle aziende sta contribuendo a catalizzare l'attenzione dei CdA sulla questione della sicurezza informatica.

Ostacoli principali **per l'ottenimento di una protezione efficace dai ransomware**

- Difficoltà nell'implementazione di strumenti/tecnologie
- Mancanza di personale qualificato per l'implementazione delle soluzioni
- Altre priorità contrastanti

Ostacoli secondari **per l'ottenimento di una protezione efficace dai ransomware**

- Difficoltà nel giustificare le relative richieste sul budget
- Mancanza di supporto del CdA

Clicca qui per scaricare il report completo >>>>

zscaler