arcasafe
Born to Safe You

CHECKLIST OPERATIVA PER PMI

Ransomware alle PMI

12 verifiche nell'ordine in cui avviene un attacco:
cosa controllare, perché conta, come accorgersene

COSA TROVI DENTRO

Il ransomware non arriva con un attacco spettacolare: arriva da una mail, una credenziale debole, un accesso remoto lasciato aperto. La buona notizia è che la catena ha anelli deboli anche per chi attacca: basta spezzarne uno prima della cifratura, e l'attacco resta un incidente invece di diventare un blocco totale.

COME SI USA

Le verifiche seguono l'ordine reale degli eventi, dall'ingresso alla richiesta di riscatto. Si legge dall'alto: la prima sezione serve a capire dove hai già una difesa, le successive dicono cosa fare e come verificarlo. Ogni voce ha una riga di spiegazione con la verifica pratica: se non sai rispondere, quella è la voce da cui partire.

LE SEZIONI · 12 VERIFICHE IN TOTALE

01 Come entra

Le quattro fasi di un attacco tipico. Riconoscerle serve a capire dove hai già una difesa e dove no.

- [ ] **Ingresso: phishing o credenziale rubata**

  La maggior parte degli attacchi parte da credenziali valide, non da un exploit: chi entra sembra un utente legittimo. Verifica se gli indirizzi aziendali compaiono in una fuga di dati nota e imponi il cambio password dove serve.

- [ ] **Accesso: desktop remoto o VPN esposti su internet**

  Un accesso remoto raggiungibile da fuori è il secondo ingresso più usato. Cerca le porte di desktop remoto aperte e i portali VPN senza secondo fattore: sono visibili anche a chi scandaglia internet a tappeto.

- [ ] **Movimento laterale e furto di credenziali**

  Dall'utente compromesso si cercano account con più diritti. Se tutte le persone sono amministratori del proprio computer, questa fase dura minuti invece di giorni.

- [ ] **Cifratura e richiesta di riscatto**

  Prima di cifrare, chi attacca cancella le copie di sicurezza raggiungibili dalla rete. Se i backup stanno sullo stesso dominio, spariscono insieme al resto.

02 Dove si spezza: prima che entrino

Le tre misure che fermano la maggior parte degli ingressi. Sono anche le prime che chiedono i questionari NIS2.

- [ ] **Autenticazione a due fattori ovunque, VPN e posta comprese**

  Blocca gran parte del furto di credenziali: la password rubata da sola non basta più. Controlla che non ci siano eccezioni «temporanee» diventate permanenti, di solito su account tecnici e caselle condivise.

- [ ] **Nessun accesso remoto esposto direttamente**

  Metti desktop remoto e pannelli di amministrazione dietro VPN o accesso controllato, e chiudi il resto. Una verifica dall'esterno dice in dieci minuti cosa si vede della tua rete.

- [ ] **Filtro sulla posta e persone allenate a riconoscere le trappole**

  Il filtro ferma il grosso, le persone fermano quello che passa. Una simulazione di phishing all'anno dice come siete messi davvero, molto meglio di un corso in aula.

03 Dove si spezza: quando sono già dentro

Se l'ingresso è avvenuto, questi tre punti decidono se l'attacco resta un incidente o diventa un fermo.

- [ ] **Protezione sugli endpoint che ferma l'esecuzione**

  Un antivirus tradizionale riconosce i file già noti, un EDR riconosce i comportamenti: è quello che vede la cifratura mentre parte e la blocca.

- [ ] **Rete divisa in zone**

  Se produzione, uffici e backup stanno nella stessa rete piatta, chi entra da un punto arriva ovunque. Separare limita il danno a una zona sola e fa guadagnare le ore che servono per reagire.

- [ ] **Qualcuno che guarda gli allarmi, anche di notte**

  Gli attacchi si chiudono quasi sempre fuori orario, nei fine settimana e nelle chiusure. Il monitoraggio continuo è ciò che distingue «bloccato in un'ora» da «scoperto lunedì mattina».

04 La rete di sicurezza

Quando tutto il resto ha fallito restano queste due. Sono anche le uniche che si possono provare in anticipo.

- [ ] **Backup immutabili, staccati dalla rete e testati**

  Un backup che chi attacca può cancellare non è un backup. Immutabile significa che nessuno può modificarlo o eliminarlo prima della scadenza, nemmeno con le credenziali di amministratore. E va provato il ripristino, non solo il salvataggio.

- [ ] **Un piano di risposta con nomi e numeri di telefono**

  Nelle prime ore serve sapere chi decide, chi parla con i clienti e chi con le autorità. NIS2 chiede una prima notifica entro 24 ore dalla scoperta: senza un piano scritto non ci si arriva.

Da leggere dopo

Tre approfondimenti sul nostro sito, gratuiti e senza registrazione.

Ransomware alle PMI: come entra e come si ferma

La catena d'attacco spiegata passo per passo, con i punti in cui conviene intervenire.

https://arcasafe.eu/ransomware-pmi-catena/

SOC, SIEM, EDR: cosa fa davvero la differenza

Le tre sigle che tornano in ogni preventivo, e cosa serve davvero a un'azienda di 50 persone.

https://arcasafe.eu/soc-siem-edr-differenza-pmi-2/

Wazuh: il SIEM open source alla portata delle PMI

Come si mette in piedi un monitoraggio continuo senza il budget di una multinazionale.

https://arcasafe.eu/wazuh-siem-open-source-pmi/

Le tue note

Le voci rimaste senza risposta, e chi se ne occupa.