SECURITY LAB
sicurezza on line

Rimozione Ransomware Aziendale: Guida Completa per PMI

Il **ransomware aziendale** è oggi una delle principali minacce per le Piccole e Medie Imprese. Sempre più PMI vengono colpite da attacchi informatici che bloccano file, gestionali, server e backup, causando fermo operativo e perdite economiche significative.

In questa guida scoprirai **come funziona un attacco ransomware**, cosa fare immediatamente e come proteggere la tua azienda in modo efficace.

Cos'è un Ransomware e perché colpisce le PMI

Il ransomware è un malware che:

- Cifra i file aziendali
- Blocca l'accesso ai sistemi
- Richiede un riscatto (spesso in criptovaluta)
- In molti casi esfiltra i dati (ricatto doppio)

Tra i ransomware più diffusi a livello globale troviamo:

- WannaCry
- LockBit
- Conti

Le PMI sono bersagli privilegiati perché spesso:

- Non hanno un reparto IT strutturato
- Utilizzano RDP o VPN poco protette
- Non adottano backup offline
- Non applicano aggiornamenti regolari

Come capire se sei vittima di un ransomware

I segnali tipici di infezione sono:

- File con estensioni strane o non apribili
- Comparsa di una richiesta di riscatto
- Server o PC estremamente lenti
- Accesso negato a cartelle condivise
- Antivirus disattivato automaticamente

Se noti uno di questi sintomi, **non ignorarli**.

Cosa fare immediatamente in caso di attacco

1. Isola i dispositivi infetti

- Scollega il PC o server dalla rete
- Disattiva Wi-Fi e VPN
- Non spegnere immediatamente i sistemi senza analisi

L'obiettivo è evitare la propagazione in rete.

---

2. Non pagare il riscatto

Pagare non garantisce:

- Recupero dei dati
- Eliminazione del malware
- Non pubblicazione dei file rubati

Inoltre finanzia attività criminali.

---

3. Verifica i backup

Un backup sicuro deve essere:

- Non sempre connesso alla rete
- Non modificabile (immutabile)
- Testato periodicamente

Se il backup è stato cifrato, la situazione è più critica.

Come avviene la rimozione del ransomware in azienda

La rimozione professionale prevede:

✔ **Analisi tecnica dell'attacco**

- Individuazione del punto di ingresso (phishing, RDP, vulnerabilità)

- Verifica di eventuale furto dati
- Controllo account amministrativi

✔ **Bonifica completa**

- Reinstallazione dei sistemi compromessi
- Reset password aziendali
- Chiusura delle vulnerabilità sfruttate

✔ **Ripristino sicuro dei dati**

- Ripristino solo dopo completa eradicazione
- Test in ambiente isolato
- Monitoraggio post-intervento

Ransomware e GDPR: obblighi per le PMI

Se l'attacco ha coinvolto dati personali (clienti, dipendenti, fornitori), può configurarsi un data breach ai sensi del:

- Regolamento Generale sulla Protezione dei Dati

In tal caso potrebbe essere necessario:

- Notificare l'autorità competente entro 72 ore
- Informare gli interessati
- Documentare l'incidente

Ignorare questo aspetto può comportare sanzioni.

Quanto costa un attacco ransomware a una PMI?

I costi non si limitano al riscatto:

- Fermo produzione
- Perdita clienti
- Danno reputazionale
- Ripristino infrastruttura
- Possibili sanzioni GDPR

Spesso il danno reale supera di gran lunga la richiesta iniziale degli attaccanti.

SECURITY LAB
sicurezza on line

Come prevenire il ransomware in azienda

Le misure fondamentali per una PMI sono:

🔐 **Backup 3-2-1**

3 copie dei dati, 2 supporti diversi, 1 offline.

🔐 **Autenticazione MFA**

Protegge accessi VPN, email e pannelli amministrativi.

🔐 **Aggiornamenti costanti**

Molti attacchi sfruttano vulnerabilità già note.

🔐 **Firewall e protezione avanzata**

Bloccare tentativi di accesso non autorizzati.

🔐 **Formazione del personale**

Il phishing è ancora il principale vettore di attacco.

Domande Frequenti (FAQ)

Un antivirus basta contro il ransomware?

No. Serve un approccio multilivello con backup sicuro e controllo accessi.

Si possono recuperare i file senza backup?

Solo in rari casi esistono tool pubblici di decrittazione. Non è garantito.

Quanto tempo serve per il ripristino?

Dipende dall'estensione dell'attacco e dalla qualità dei backup.

Conclusione
La rimozione del ransomware aziendale è un processo delicato che richiede competenze tecniche, analisi strutturata e attenzione agli aspetti legali.

Per le PMI, la vera protezione non è reagire all'attacco, ma costruire un'infrastruttura resiliente prima che accada.

https://securitylab.services