Tre consigli per le best practice che consentono di evitare il ransomware

Il numero di attacchi ransomware si è moltiplicato esponenzialmente negli ultimi anni, causando infezioni in milioni di computer e costando alle aziende milioni di dollari. Descriviamo tre best practice che ogni organizzazione, a prescindere dalle dimensioni, dovrebbe implementare.

1. CONOSCENZA E CONSAPEVOLEZZA

Purtroppo, dovete essere consapevoli che il vostro maggiore vettore di attacco è anche l'anello più debole del sistema. Molti dei vostri dipendenti non hanno mai sentito parlare del phishing o di attacchi man-in-the-middle e gli hacker lo sanno bene. È fondamentale istruire i dipendenti sui più comuni metodi di attacco e sui modi per evitarli, ad esempio:

- **Mai fare clic sui collegamenti presenti nei messaggi e-mail.** Digitare o copiare l'indirizzo in un browser per evitare di aprire inconsapevolmente un collegamento contraffatto che porta a un sito web dannoso.
- **Essere molto cauti nell'aprire gli allegati e-mail.** Questo è un tipico metodo di attacco ransomware.
- **Quando si visita un sito web, fare molta attenzione all'URL.** I siti dannosi più diffusi includono URL con indirizzi IP all' inizio o pagine apparentemente sicure che non utilizzano HTTPS.
- **Gli indirizzi e-mail di spoofing sono un altro metodo per acquisire informazioni sensibili.** Non inviare mai informazioni personali via e-mail. Il nostro consiglio è fare lo forzo di alzare la cornetta e chiamare.
- **Non condividere mai le password con altri utenti via e-mail.** Le organizzazioni legittime non richiedono mai credenziali via e-mail.

2. BACKUP. BACKUP. BACKUP.

Anche se la prevenzione di minacce e attacchi è sempre il metodo di difesa ideale, dovreste aver sempre pronto un piano B. Nel malaugurato caso in cui un attacco di malware avanzato, e nello specifico un attacco di ransomware, dovesse assumere il controllo del vostro sistema, l'esecuzione regolare di backup può darvi la tranquillità mentale di sapere che i vostri dati possono essere recuperati. Ecco alcuni consigli per eseguire il backup delle informazioni:

- **Privilegiare i backup offline.** Il ransomware moderno è in grado di trovare e crittografare le informazioni archiviate in rete.
- **Semplificare i backup il più possibile.** Creare un percorso condiviso globale dove archiviare tutte le informazioni più importanti e sfruttare le partizioni dei dischi, se possibile.
- **Automatizzare i backup quando possibile.** Non si deve rischiare che un errore umano impedisca l'esecuzione del backup.

3. DIFESA PROFONDA

Gli attacchi di ransomware tentano di sfruttare tutti i vettori di attacco possibili. Più livelli di sicurezza sono presenti, più possibilità ci sono di bloccare un attacco che un altro livello si è lasciato sfuggire. Questo tipo di attacchi sa trasformarsi in qualcosa di unico, riuscendo ad eludere i tradizionali metodi di rilevamento basati su firme. Ecco alcuni livelli di sicurezza fondamentali che un'organizzazione dovrebbe sempre implementare:

- **Proteggere la rete.** Il ransomware sfrutta la rete non solo per collegarsi a un server dannoso e ottenere la chiave di crittografia, ma anche per diffondere l'attacco in tutta l'organizzazione.
- **Usare la sandbox di rete per "fare brillare" le minacce zero-day.** Una sandbox di rete è un ottimo strumento per aprire un file di malware sconosciuto senza mettere a repentaglio la sicurezza dei propri dispositivi.
- **Assicurarsi la visibilità sui dispositivi endpoint.** Gli attacchi di ransomware partono spesso dai dispositivi endpoint. Assicurarsi la visibilità sull'attività degli eventi su questi dispositivi consente di rilevare e rispondere alle minacce prima che il danno venga realmente fatto.
- **Mettere in relazione la rete e gli endpoint.** Correlare i dati sugli eventi provenienti dalla rete e dagli endpoint consente di effettuare una valutazione completa del panorama delle minacce.

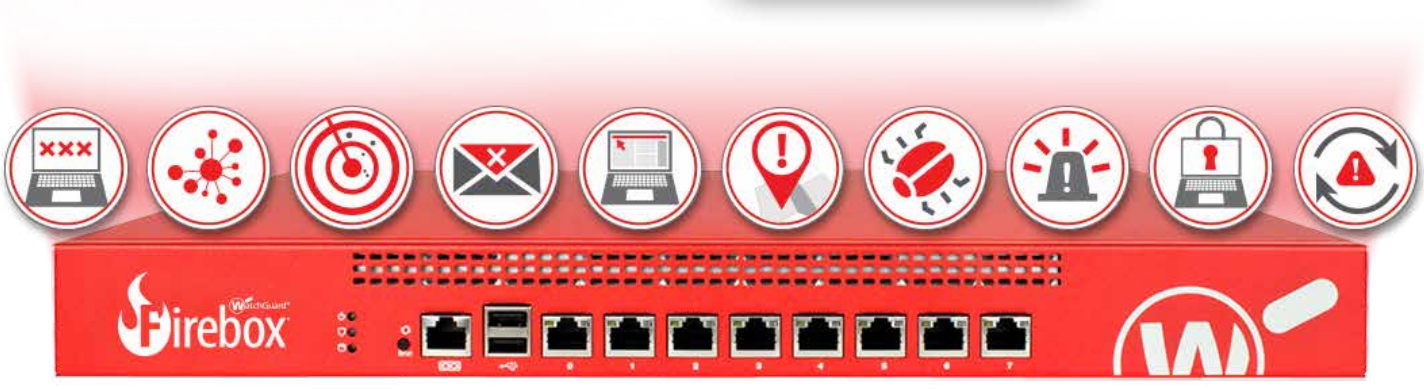
WatchGuard

CONSIGLI PER LE BEST PRACTICE

Con WatchGuard Total Security Suite, le organizzazioni di tutte le dimensioni ora possono difendersi dalle minacce di malware avanzato, come gli attacchi di ransomware. Total Security Suite è il primo servizio UTM (gestione unificata delle minacce) che consente alle organizzazioni di tutte le dimensioni non solo di rilevare e rispondere agli attacchi di ransomware, ma anche di prevenirli. Combinando strumenti come WebBlocker, APT Blocker e Host Ransomware Prevention, WatchGuard offre la serie più completa di servizi di sicurezza a disposizione oggi sul mercato.

Singolarmente, ognuna di queste soluzioni garantisce la protezione contro una delle fasi di un attacco di ransomware. WebBlocker impedisce automaticamente agli utenti di accedere ai siti noti dannosi, ma consente al contempo di filtrare gli URL per bloccare siti rischiosi e inappropriati. Con APT Blocker, gli utenti hanno a disposizione una collaudata sandbox di rete che consente di rilevare minacce sospette, "farle brillare" in un ambiente virtuale e bloccare l'esecuzione dell'attacco sulla rete. Host Ransomware Prevention sfrutta l'analisi comportamentale per rilevare nello specifico gli attacchi di ransomware e riuscire a prevenirli prima che i file vengano crittografati.

Prodotto	Supporto	TOTAL SECURITY	Basic Security
Intrusion Prevention Service (IPS)		✓	✓
App Control		✓	✓
WebBlocker		✓	✓
spamBlocker		✓	✓
Gateway Antivirus		✓	✓
Reputation Enabled Defense (RED)		✓	✓
Network Discovery		✓	✓
APT Blocker		✓	
Data Loss Protection (DLP)		✓	
Dimension Command		✓	
Threat Detection & Response		✓	
Supporto	Standard (24x7)	**Gold (24x7)**	Standard (24x7)



WatchGuard fornisce una serie completa di soluzioni per la sicurezza di rete avanzata che consente di proteggere le organizzazioni e i relativi dati, dipendenti e clienti.

- Appliance di protezione della rete
- Visibilità sulle minacce per la rete
- Servizi Total Security
- Access point wireless sicuri

Ulteriori informazioni su www.watchguard.com