COMMVAULT

WHITEPAPER

Ransomware: 4 modi per proteggersi e ripartire

Le notizie escono ogni giorno - gli attacchi ransomware sono ormai un aspetto costante della vita informatica. A peggiorare le cose, gli affari per questi criminali vanno benissimo, al punto che stanno sviluppando minacce sempre più sofisticate. Questo significa organizzazioni che perdono l'accesso ai loro dati, mettendo potenzialmente a rischio il loro intero business. Queste aziende protette in modo non adeguato sono spesso costrette a pagare un riscatto - con la "speranza" che i loro dati vengano effettivamente rilasciati - o a tentare un recupero ad hoc senza garanzia di ripristino affidabile. Per mantenere l'accesso ai vostri dati più importanti, ecco quattro best practice da considerare per proteggervi e ripartire con fiducia dagli attacchi ransomware.

4 modi per proteggersi e riprendersi dagli attacchi ransomware

Implementare una strategia di sicurezza multilivello – che comprenda anti-malware, firewall personale, crittografia dei file, software di data loss prevention (DLP) e altro ancora - è fondamentale per proteggere gli endpoint e le infrastrutture dalle crescenti minacce informatiche. Tuttavia, anche se tutti questi meccanismi di protezione sono attivi, resta comunque una modesta possibilità di violazione, ed è per questo che il backup dei dati è fondamentale!

"Fare copie regolari dei file su un dispositivo separato è l'unico modo efficace per minimizzare i danni in caso di attacco informatico. Un backup affidabile permette alle persone di tornare a utilizzare il proprio computer, con tutti i file intatti, nel più breve tempo possibile" (25 words max)

The Threat Report, Myths In Cybersecurity That People Needs To Forget, 2019

Per proteggere dal ransomware anche gli ambienti aziendali che fanno un uso intensivo dei dati, abbiamo stilato le seguenti best practice:

1 Dotarsi di un information security program efficace

Se per la vostra organizzazione la sicurezza delle informazioni è una novità, o se avete implementato solo parzialmente un vostro piano di information security, considerate di intraprendere i seguenti step per mettere in atto un programma di protezione efficace.

Tabella 1: Elementi di un programma di sicurezza efficace

Misure	Integrazioni
Sapere dove sono conservati i dati critici	Ambienti complessi comportano difficoltà nel comprendere dove si trovino i propri dati: • Data Center • Strutture remote • Cloud • Service Provider • Endpoint

Misure	Integrazioni
Adottare sistemi di inventory	• Sapere quali sistemi gestiscono i dati critici: archiviazione, elaborazione e trasmissione • Comprendere il data flow • Determinare quali sistemi presentano il maggior rischio per le vostre operazioni
Valutare il rischio	Inclusi registri elettronici, supporti fisici e la disponibilità di sistemi, servizi o dispositivi chiave
Applicare i controlli di sicurezza	Selezionare, applicare e gestire i controlli di sicurezza in base al rischio
Monitorare l'efficacia	Prepararsi a una continua evoluzione delle minacce: • Valutare proattivamente l'efficacia della strategia di risk-based information security su cui si basano i controlli di sicurezza applicati e la corretta implementazione delle tecnologie di protezione • Applicare azioni correttive, di remediation e gli insegnamenti appresi
Fomare gli utenti	• Assicurarsi che i dipendenti siano istruiti su come comportarsi quando ricevono e-mail da mittenti sconosciuti con allegati o link sospetti (vedi appendice per le azioni consigliate).

2 Proteggere i dati con best practice tecnologiche

Considerato il crescente numero di minacce e attacchi sempre più sofisticati, le aziende hanno bisogno di comprendere chiaramente il rapporto di costo tra gli investimenti in sicurezza informatica e la formazione dei dipendenti da un lato, e la perdita di accesso ai dati critici e il conseguente impatto su business e reputazione dall'altro.

55% **degli intervistati dichiara che il rilevamento di minacce avanzate (nascoste, sconosciute ed emergenti) è una delle principali sfide per i loro centri operativi di sicurezza[1].**

La sicurezza di rete è una prima linea di difesa valida dagli attacchi ransomware. Implementando efficaci best practice tecnologiche, le organizzazioni possono proteggere ulteriormente i loro dati e infrastruttura IT. La tabella 2 delinea le principali strategie tecnologiche utili a eliminare il potenziale di rischio da attacchi ransomware.

Tabella 2: Best practice tecnologiche

Misure	Integrazioni
Rilevare e prevenire	Impiegare una soluzione di sicurezza poliedrica: • Mantenere sistemi e software aggiornati con le relative patch • Difendersi dalle minacce basate su file (antivirus tradizionale), con protezione di download e browser, tecnologie euristiche, firewall e un sistema di punteggio di reputazione dei file proveniente dalla community
Utilizzare gruppi di certificazione esterni (computer emergency response team)	• Possono spesso identificare un problema prima che il virus colpisca le aziende • Possono fornire raccomandazioni su azioni immediate per il filtering manuale (le aziende software possono richiedere ore o giorni per rilasciare una patch)
Identificare e fermare l'infezione	Definire una policy completa di prevenzione e prontezza di ripristino che: • Includa politiche di endpoint e network protection, oltre a prodotti di protezione, come antivirus, antispyware e soluzioni di tipo firewall; • Limiti l'esecuzione di programmi non approvati sulle workstation; • Limiti le capacità di scrittura degli utenti in modo che, anche in caso di download di un'applicazione ransomware, questa non sia in grado di crittografare file oltre a quelli specifici dell'utente; • Includa documenti elettronici, supporti fisici e la disponibilità di sistemi, servizi o dispositivi critici.
Mantenere un'immagine "ideale" dei sistemi e delle configurazioni	Un elemento fondamentale delle policy di data management: • Clonare facilmente il sistema infetto con un master

1 Domain Tools: The 2019 Threat Hunting Report

Misure	Integrazioni
Mantenere una strategia di backup completa	Prepararsi a minacce in costante evoluzione: • Valutare proattivamente l'efficacia di una strategia di protezione basata sul rischio, i controlli di sicurezza applicati e la corretta implementazione delle relative tecnologie • Applicare azioni correttive, di remediation e gli insegnamenti appresi
Educare gli utenti	Assicurarsi che i dipendenti siano istruiti su come comportarsi quando ricevono e-mail da mittenti sconosciuti con allegati o link sospetti

3 Implementare una solida strategia di backup

È importante comprendere che un evento ransomware è quasi sempre un'azione progressiva. Si svolge nel corso del tempo e può rimanere in background mentre apprende il comportamento delle vostre abitudini di backup. Per questo è importante mantenere una copia persistente dei dati in posizioni diverse, come parte della vostra strategia di preparazione al ripristino e delle procedure di disaster recovery.

Le aziende che si affidano solo al backup sotto forma di snapshot corrono un rischio maggiore. Se lo snapshot o l'altro elemento viene replicato, anche la fonte viene corrotta – poiché segue la replica. Avere una versione dei dati preservata da punti di recupero precedenti e collocata in una posizione protetta è un must.

Tabella 3: Best practice di data protection

Step	Azioni
Adottare processi di backup e DR	• Implementare e mantenere una strategia di backup 3-2-1 (3 copie dei vostri dati, 2 diversi tipi di supporti e 1 copia fuori sede) • Richiamare direttamente una copia di backup e non le versioni archiviate sullo stesso sistema • Avere copie di backup esterne dei dati oltre ai semplici snapshot mantenuti sul sistema di origine

Disporre di una libreria cloud è un'altra alternativa per un'adeguata conservazione esterna. Poiché il backup cloud non è visibile all'account del sistema operativo dell'amministratore locale, sarebbe necessario un ulteriore livello di sofisticatezza per accedere alle credenziali dell'utente cloud. Se nessuno ama il nastro, per alcune aziende è comunque un'alternativa valida, in quanto è la stessa natura online del disco o del cloud che li espone a un rischio costante.

4 Educare i dipendenti a proteggere l'endpoint

Infine, è essenziale formare chi utilizza i dati sulle buone abitudini di sicurezza per mantenere le aziende protette, in particolare ricordando loro di usare sempre il buon senso. Come descritto di seguito, preparate i vostri utenti a seguire queste best practice.

Tabella 4: Best practice per dipendenti ed endpoint

Step	Azioni
Abituare gli utenti a implementare le migliori pratiche di sicurezza	• Applicare una password policy • Assicurarsi che i programmi e gli utenti usino il livello più basso di privilegi necessari per completare un'attività • Disattivare AutoPlay • Disattivare la condivisione dei file se non necessaria • Disattivare e rimuovere i servizi non necessari • Se una minaccia sfrutta uno o più servizi di rete, disabilitare o bloccarne l'accesso fino all'applicazione di una patch • Mantenere sempre aggiornati i livelli di patch • Non aprire gli allegati a meno che non siano attesi • Se il Bluetooth non è richiesto per i dispositivi mobili, dovrebbe essere disattivato Far riferimento a Symantec, security Best Practice recommendations, 2018 per tutti i dettagli.

Step	Azioni
Implementare best practice di endpoint protection	• Utilizzare un firewall • Configurare il server di posta elettronica per bloccare o rimuovere le e-mail che contengono file allegati che sono comunemente usati per diffondere le minacce • Isolare rapidamente i computer compromessi per evitare che le minacce si diffondano ulteriormente • Distribuire plugin di URL-reputation che visualizzano la reputazione dei siti web dalle ricerche • Limitare il software alle applicazioni approvate dall'azienda ed evitare di scaricare programmi da siti di file sharing. Effettuare il download di software solo dai siti web di fornitori affidabili • Implementare l'autenticazione in due fasi su qualsiasi sito web o app quando disponibile • Assicurarsi che gli utenti abbiano password diverse per ogni account di posta elettronica, applicazioni e login, specialmente per siti e servizi legati al lavoro

Conclusioni

Proteggere le informazioni aziendali critiche è certamente una necessità per ogni organizzazione, e salvaguardarle dagli attacchi ransomware dovrebbe essere una priorità assoluta. Quindi, tutelate i dati tenendo in massima considerazione sicurezza, tecnologia, backup e best practice dei dipendenti. In questo modo i vostri dati saranno al sicuro e la continuità del vostro business sarà garantita al meglio, mitigando al contempo il rischio di ransomware.