La soluzione automatica per arrestare la diffusione di ransomware all'interno della tua organizzazione

Diciamoci la verità: anche le organizzazioni che dispongono dei migliori livelli di protezione sono vittime dei ransomware. I criminali informatici sviluppano costantemente modi nuovi e innovativi per aggirare i metodi di rilevamento tradizionali basati sulla prevenzione. Per proteggersi dai ransomware, un'organizzazione deve evolvere le proprie difese di sicurezza e introdurre un approccio a più livelli. Una volta che il ransomware ha attivato il suo carico utile (crittografia), potrebbe essere troppo tardi per una reazione da parte del sistema di sicurezza. A questo punto, l'elemento cruciale è la velocità con cui puoi fermare la criptazione illegittima fino a 10.000 file al minuto.

Un approccio a più livelli include una soluzione complementare per rilevare e fermare la criptazione illegittima una volta che è iniziata; ciò può avvenire monitorando l'attività dei file su condivisioni e cloud. Non appena la soluzione identifica l'attività di criptazione criminale in corso e il danneggiamento dei file, reagisce e isola l'utente che la sta causando.

Presentazione della soluzione di contenimento dei ransomware di Ricoh, RICOH RansomCare powered by BullWall, un livello di difesa unico e collaudato. Oltre 20 sensori di rilevamento valutano ogni modifica di file sulle condivisioni monitorate. Se vengono avviati i segnali rivelatori di ransomware (criptazione illegittima) e i file vengono attivamente crittografati su condivisioni di file e cloud monitorate, RICOH RansomCare reagisce isolando il dispositivo e l'utente compromessi per interrompere il processo di criptazione criminale. La soluzione è un elemento essenziale della vostra strategia di difesa generale, in quanto fornisce una maggiore sicurezza nella protezione dei dati aziendali.

Puoi rispondere a queste domande in caso di diffusione di un ransomware?

- Come individui quali file sono crittografati e dove si trovano?
- Come identifichi quale utente e quale dispositivo crittografano i file?
- Come si interrompe rapidamente la criptazione prima che si verifichino danni significativi?
- Quanto tempo ci vorrà per ripristinare centinaia di migliaia di file e qual è il costo totale dei tempi di inattività?
- Quanto tempo è necessario per segnalare con precisione alle autorità dei dati se migliaia di file con informazioni personali sono stati crittografati illegalmente?

RICOH
imagine. change.

Perché i ransomware non vanno sottovalutati

Ora più che mai, la "C-suite" (ad es. CIO, CISO, CFO e CEO) ha un interesse significativo nella protezione dei dati e del capitale intellettuale per proteggere le informazioni di identificazione personale, le entrate, mantenere la fedeltà dei clienti e garantire il valore per le parti interessate. Le tradizionali difese di sicurezza si concentrano sulla prevenzione dell'esecuzione dei malware, qualora gli endpoint ne fossero il bersaglio. Ma cosa succede se falliscono? I ransomware sono un'altra storia. Hanno paralizzato intere organizzazioni nonostante queste disponessero di soluzioni di sicurezza all'avanguardia. Le organizzazioni oggi dovrebbero prendere in considerazione l'implementazione di un'ulteriore linea di difesa che funga da "sistema sprinkler antincendio" in caso di fallimento delle soluzioni di sicurezza basate sulla prevenzione.

È fondamentale che le organizzazioni non si affidino esclusivamente a una risposta reattiva alle moderne minacce malware. Ogni giorno ci giungono segnalazioni di come questa strategia si sia rivelata fallimentare. La strategia di difesa del futuro deve includere la continuità aziendale e il disaster recovery, per abilitare avvisi automatici, una risposta di arresto e un ripristino rapido senza gli ingenti costi spesso associati agli attacchi ransomware.

Come funziona

La superficie di attacco da difendere è in rapida espansione e le organizzazioni di oggi hanno molteplici punti di ingresso per i malware; RICOH RansomCare offre una risposta di contenimento automatizzata 24 ore su 24, 7 giorni su 7 alla diffusione di ransomware con risposta e reportistica integrate. Non importa quale utente o quale dispositivo abbia attivato la criptazione; né importa se l'attacco è una variante di ransomware nota o sconosciuta, se la diffusione è iniziata su un endpoint, un telefono cellulare, un dispositivo IoT, tramite e-mail, USB o se il ransomware è stato distribuito da qualcuno all'interno della tua organizzazione. RICOH RansomCare esamina l'euristica di ogni file monitorato in locale o nel cloud ed al quale accede ogni utente, senza causare alcun sovraccarico di rete. Quando RICOH RansomCare rileva la criptazione in corso e il danneggiamento dei file sulle condivisioni monitorate, viene generato immediatamente un avviso e viene attivata una risposta per disabilitare e isolare il dispositivo e l'utente che criptano i dati.

RICOH RansomCare funziona anche in ambienti virtuali come server/sessioni Citrix, server/sessioni Terminal, Hyper-V, VMware e il cloud, inclusi Azure e Amazon AWS/EC2, SharePoint, Google Drive e Microsoft 365. È possibile utilizzare un'ampia gamma di metodi di isolamento personalizzabili, come l'arresto forzato, la disattivazione della VPN, la disattivazione dell'utente AD, la disattivazione dell'accesso alla rete, la revoca delle autorizzazioni cloud e molti altri. L'integrazione tramite l'API RESTful ad altre soluzioni di sicurezza fa sì che il vostro team IT possano gestire un numero sempre più alto di endpoint garantendo i massimi livelli di sicurezza.

Installazione da remoto senza problemi

RICOH RansomCare è una soluzione agentless e non è installata su endpoint, file server o NAS. Non vi è alcun impatto sulle prestazioni della rete. Il monitoraggio del comportamento dei file agentless e le tecniche di apprendimento automatico vengono implementate facilmente in quattro o sei ore e RICOH RansomCare verrà configurato in base al tuo ambiente. RICOH RansomCare offre connettori cloud per le organizzazioni che utilizzano Microsoft O365 (SharePoint, Teams, OneDrive) e Google Drive. L'integrazione completa con altre soluzioni di sicurezza come Cisco ISE e Windows Defender ATP o il sistema SIEM è disponibile tramite l'API RESTful, consentendo ai team di sicurezza di unificare la gestione della sicurezza in un mare sempre più complesso di endpoint.

- Nessuna installazione cloud
- Nessuna installazione su endpoint (agentless)
- Nessuna installazione di storage/server per file

Avvisi e integrazioni

Servizi di avviso integrati RICOH RansomCare

Notifiche via e-mail
Avvisi via SMS
"SOC" mobile
API ad altri sistemi

Interfaccia a due vie a Restful

Splunk
Cisco ISE
Windows Defender
Aruba
IBM Radar
McAfee
Symantec
TrendMicro
ForeScout
e molti altri

Test di valutazione del ransomware

Siamo in grado di eseguire un test di valutazione del ransomware nel corso del quale un simulatore di ransomware sicuro e controllato viene utilizzato per simulare la crittografia dei file zero-day e le modifiche rapide dei file. Testeremo quindi RICOH RansomCare nel tuo ambiente per dimostrare come la soluzione risponde alla criptazione dei file. Rivolgiti a un rappresentante di vendita per maggiori informazioni.

RICOH
imagine. change.