L’approccio a 360° di Beazley nella protezione dai ransomware

Un attacco da ransomware è uno degli incidenti più costosi che un’azienda possa subire. Il fenomeno dei ransomware è in crescita e non accenna a diminuire. Il ransomware è in aumento e non mostra segni di rallentamento. Sempre schierati in prima linea, i team Beazley addetti alla gestione dei sinistri e alla gestione di incidenti cyber possiedono le conoscenze e le competenze necessarie per aiutarvi a proteggere la vostra azienda da questi attacchi. In collaborazione con i fornitori di servizi di esperti informatici KPMG, abbiamo elaborato una guida alle best practices in materia di ransomware che vi aiuterà a evitare il verificarsi di questi incidenti.

Scenario di un attacco da ransomware

1

Compromissione iniziale dell’ambiente di lavoro

- Un gruppo criminale prende di mira la vostra azienda con una campagna di phishing.
- Un malware viene inviato con successo a uno dei vostri ignari utenti tramite un allegato malevolo o un link a una pagina web inserito in una mail.

2

Installazione del malware

- L’utente apre l’allegato e il malware viene inconsapevolmente installato sul suo PC.
- All’insaputa dell’utente e dei vostri team del reparto sicurezza e IT, gli criminali hanno ormai messo piede nel vostro ambiente.
- Sfruttando la posizione così acquisita, gli hacker esplorano la vostra rete (ancora indisturbati) alla ricerca di sistemi vulnerabili e dati sensibili. In questa fase, esaminano i PC di altri utenti, ma anche eventuali server contenenti applicazioni di cruciale importanza e archivi di file.

3

Rilascio del ransomware

- Il gruppo criminale ha ormai conquistato l’accesso di cui necessitava ed è pronto a fare scattare la trappola.
- Provvede quindi a diffondere una forma di ransomware che si diffonde nella vostra rete, criptandola completamente.
- Gli aggressori riescono così a criptare una quota sostanziale del vostro patrimonio, bloccando completamente o parzialmente alcune parti della vostra attività.

4

Estorsione

- Gli aggressori chiedono X milioni di dollari per fornirvi il codice di decodifica.
- L’attacco diventa di dominio pubblico, causando danni alla reputazione dell’azienda.
- L’autorità di controllo desidera capire se vi sia stata una gestione impropria dei dati sensibili dei clienti, con conseguente rischio di sanzioni di notevole importo.

Come proteggere la propria azienda dai ransomware

Controlli minimi per evitare di essere vulnerabili

- **Installazione e costante aggiornamento di una soluzione antivirus a gestione centralizzata opportunamente configurata:** una solida soluzione antivirus rappresenta un componente basilare di qualunque programma di sicurezza.
- **Tagging dei messaggi di posta elettronica:** il tagging delle mail provenienti da mittenti esterni consente di avvisare i dipendenti in merito a messaggi che provengono da fonti esterne all'azienda.
- **Contenuto e consegna delle mail:** applicate rigorosi controlli SPF (Sender Policy Framework) su tutte le mail in entrata, verificate la validità dei rispettivi mittenti. Filtrate tutti i messaggi in entrata per rilevare eventuale contenuto malevolo, compresi gli eseguibili e i documenti con macro.
- **Add-on e configurazione di Office365:** attivate l'autenticazione a due fattori (2FA) su O365 e utilizzate la "O365 Advanced Threat Protection".
- **Macro:** disattivate l'esecuzione automatica delle macro. Se non servono alla vostra attività, l'ideale sarebbe disattivarle completamente.
- **Patching:** applicate tempestivamente le patch destinate alle vulnerabilità critiche su endpoint e server, in particolar modo sui sistemi interfacciati con l'esterno.
- **Controlli sull'utilizzo dei media:** mettete in atto controlli sull'installazione e/o sull'utilizzo di media sprovvisti di adeguata autenticazione o appositi identificatori.
- **Controlli sull'utilizzo dei medi:** mettete in atto controlli sull'installazione e/o sull'utilizzo di media sprovvisti di adeguata autenticazione o appositi identificatori.
- **Processo di risposta a incidenti ripetuti e ben definiti:** contribuisce a contenere le perdite e a ripristinare rapidamente le attività in seguito a un attacco da ransomware.
- **Sistemi di backup e database:** Assicurate il regolare svolgimento dei backup, che vengono verificati e archiviati offline in sicurezza.
- **Formazione degli utenti:** siccome la maggior parte degli attacchi è dovuta ad errori commessi dagli utenti, addestrateli a identificare le mail di phishing contenenti link o allegati malevoli. Un ottimo modo consiste nell'organizzare periodiche esercitazioni sul phishing.
- **Firewall:** utilizzate firewall di rete e firewall basati su host con regole ben ponderate, ad esempio, che non consentano connessioni in entrata di default.

Misure di riferimento per una protezione più solida

- **Applicazione di una configurazione di base sicura:** siccome i malware si basano sulla ricerca di falle da sfruttare, una configurazione di base conforme agli standard tecnici come i benchmark CIS (Center for Internet Security) può contribuire a colmare queste lacune.
- **Filtraggio del traffico di navigazione:** gli strumenti di fi per la navigazione su internet aiutano ad evitare che gli utenti accedano a siti malevoli.
- **Uso del DNS di protezione:** contribuisce a negare l'accesso a indirizzi IP malevoli noti su internet.
- **Gestione efficace degli accessi:** i ransomware non devono diventare virali all'interno dell'azienda. Adottate dunque su scala aziendale opportune misure per l'accesso generico di utenti e sistemi. Implementate misure adeguate per l'accesso privilegiato a risorse critiche (server, endpoint, applicazioni, database, ecc.). Applicate l'autenticazione multifattoriale (MFA) ove opportuno (ad es. accesso remoto/VPN, applicazioni interfacciate con l'esterno, ecc.).
- **Controllo regolare dei backup:** riduce i tempi di inattività e la perdita di dati in caso di ripristino da backup dopo un attacco da ransomware.
- **Scollegamento dei backup dalla rete aziendale:** evita l'accesso e il criptaggio dei backup da parte di un ransomware in caso di attacco alla rete aziendale principale.
- **Conservazione in luogo separato delle credenziali di backup univoche:** impedisce agli aggressori di accedere ai dati di backup e criptarli.

Procedure che assicurano la massima protezione

- **Strumenti di EDR (Endpoint Detection and Response):** le soluzioni di EDR monitorano server, laptop, desktop e dispositivi mobili per rilevare segnali di attività malevole o insolite. Questi strumenti consentono anche una risposta quasi immediata da parte di esperti in materia di sicurezza. Se correttamente implementati e monitorati, gli strumenti di EDR rappresentano una delle migliori difese dagli attacchi da ransomware e altri tipi di malware.
- **Valutazione intelligente della posta elettronica:** detonate e valutate automaticamente gli allegati in entrata in un ambiente sandbox per determinare se sono dannosi prima della consegna all'utente.
- **Monitoraggio completo e centralizzato dei log:** la raccolta e il monitoraggio centralizzati dei log, preferibilmente tramite un sistema SIEM (Security Information and Event Management), individua le minacce che violano le difese aziendali interne.
- **Sottoscrizione di servizi esterni di threat intelligence:** offre l'accesso a servizi esterni che possono fornire informazioni dettagliate sullo sviluppo di tattiche, tecniche e procedure di attacco. Questi servizi consentono anche l'accesso a database di siti pericolosi noti, allegati di posta elettronica malevoli, ecc.
- **Criptaggio dei backup:** impedisce l'utilizzo dei dati di backup da parte degli aggressori in caso di violazione.
- **Segregazione della rete:** controlli di accesso implementati nell'ambiente di rete per limitare l'accesso e/o il flusso di traffico. Un fi wall opportunamente configurato con una serie di regole assicura che soltanto il traffico richiesto possa passare da una sezione all'altra.
- **Isolamento del web:** utilizzate una tecnologia di isolamento e contenimento del web per creare un'esperienza di navigazione in Internet sicura per i vostri utenti.
- **Permessi per le applicazioni:** permettete solo alle applicazioni di cui la vostra organizzazione si fida di girare su dispositivi.

KPMG

KPMG offre una vasta gamma di servizi destinati ad aiutare le aziende a difendersi e a reagire in presenza di attacchi da ransomware. Per approfondirne le caratteristiche, vi invitiamo a contattare:

Matthew Martindale – Partner, Cyber Security
cyber@kpmg.co.uk

beazley

BZCER034_IT_09/20