La difesa contro i ransomware in 5 passaggi:

come rafforzare i sistemi di difesa oltre il perimetro

SOMMARIO

La crescita e la diffusione dei ransomware 03

Il business del ransomware può costarvi caro 04

Bloccate il movimento laterale. Bloccate la diffusione dei ransomware. 05

Creazione di una strategia di difesa inviolabile 06

Che succede nella rete? 07

Creazione di una strategia di difesa dai ransomware 08

Conclusione 09

Introduzione

La crescita e la diffusione dei ransomware

Il ransomware, un tempo semplicemente un fastidioso malware usato dai malintenzionati per limitare l'accesso a file e dati tramite la crittografia, si è trasformato in un metodo di attacco di proporzioni epiche. La perdita definitiva di dati è un danno scioccante, ma oggi i criminali informatici e gli autori di attacchi governativi sono talmente sofisticati da usare i ransomware per penetrare e paralizzare aziende, enti pubblici statali e locali, infrastrutture globali e organizzazioni sanitarie e molto altro. Molti di questi gruppi offrono addirittura i propri servizi a noleggio come RaaS (Ransomware as a Service).

Nel 2031, si stima che gli attacchi ransomware si siano verificati ogni due secondi e siano costati 265 miliardi di dollari.

Cybercrime Magazine

Il business del ransomware può costarvi caro

Nel 2022, un attacco ransomware ha costretto 7-Eleven a chiudere 175 negozi perché non erano in grado di utilizzare i registratori di cassa o di accettare pagamenti. All'inizio di quell'anno, un attacco ransomware BlackCat contro una compagnia petrolifera tedesca ha colpito 233 stazioni di servizio, costringendo la Royal Dutch Shell a dover reindirizzare le spedizioni verso diversi depositi di rifornimento a causa del problema. L'attacco Colonial Pipeline è avvenuto nel maggio 2021, interrompendo le forniture di petrolio e gas lungo tutta la costa orientale degli Stati Uniti. E nel 2020, l'attacco ransomware Snake ha provocato l'arresto delle operazioni globali di Honda.

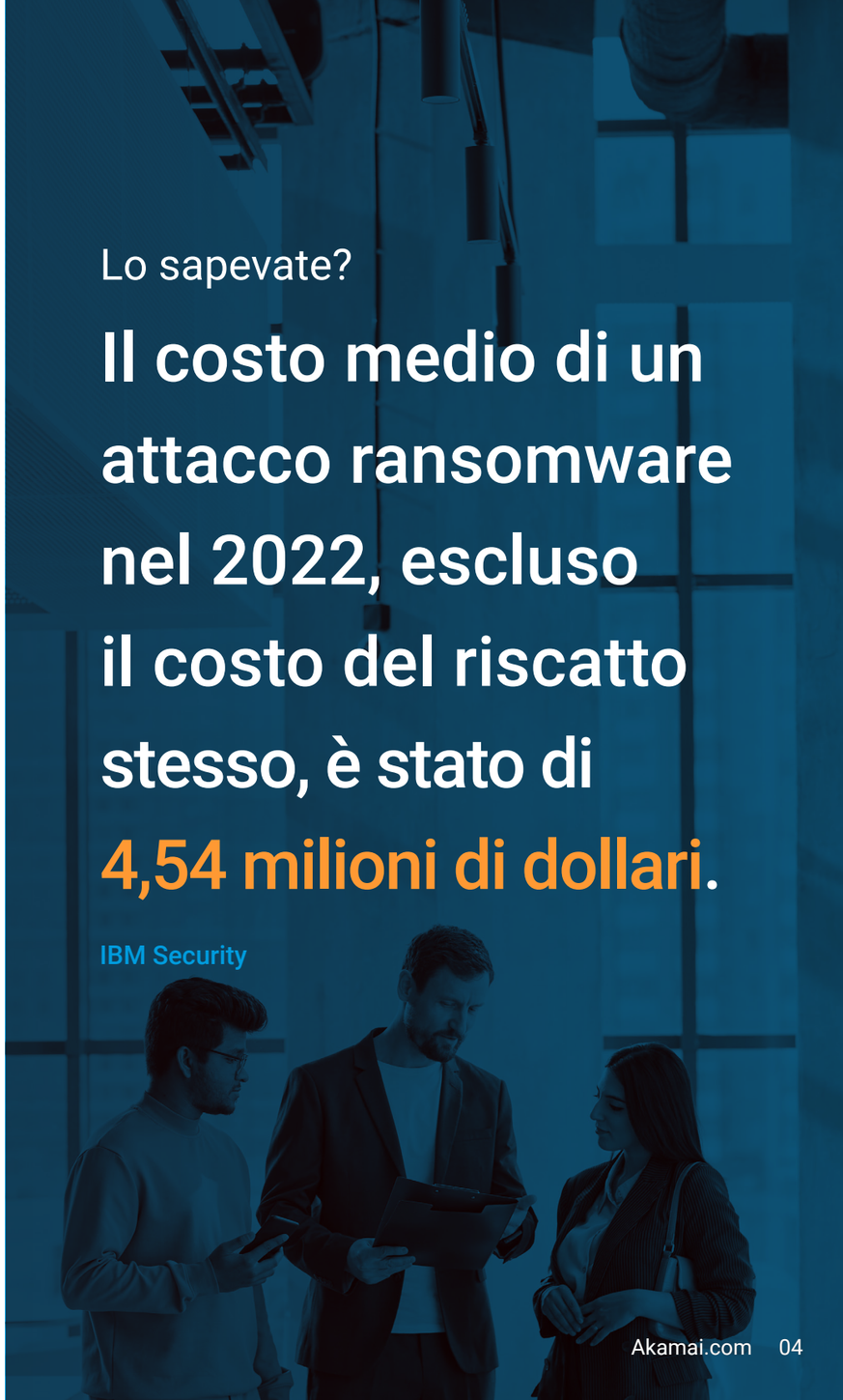
Oggi giorno, a causa di una combinazione di tecnologie obsolete, strategie di difesa deboli e incentrate esclusivamente sui perimetri e sugli endpoint, mancanza di formazione (e scarsi protocolli di sicurezza) e assenza di una soluzione nota, le organizzazioni di tutte le dimensioni sono a rischio. I criminali informatici stanno cercando di crittografare il maggior numero possibile di reti aziendali per estorcere un riscatto di migliaia o milioni di dollari.

Tuttavia, in gioco c'è molto di più della redditività. Le conseguenze di un attacco ransomware possono essere deleterie: i problemi di downtime possono interrompere le attività aziendali, arrestare la produttività e compromettere i dati.

Una volta che i dati proprietari di un'azienda vengono divulgati o compromessi, l'azienda probabilmente subirà danni al brand e perderà la fedeltà dei clienti. Secondo un sondaggio del 2020, l'80% delle violazioni dei dati hanno incluso informazioni di identificazione personale dei clienti; nel 32% delle violazioni, sono state compromesse proprietà intellettuali e nel 24% delle violazioni, sono stati compromessi dati anonimizzati dei clienti, per non parlare del fatto che i criminali possono usare questi dati sensibili contro un'azienda o effettuare altre operazioni insidiose, tra cui la vendita di dati riservati.

Con la minaccia dei ransomware che si propagano rapidamente nelle reti, la protezione del solo perimetro non è più sufficiente.

Akamai



Bloccate il movimento laterale. Bloccate la diffusione dei ransomware.

Un attacco ransomware inizia con una violazione, spesso perpetrata tramite un'e-mail di phishing, una vulnerabilità nel perimetro di rete o attacchi di forza bruta che creano delle falle, distraendo, al contempo, i sistemi di difesa dall'intento effettivo dell'autore dell'attacco.

Una volta penetrato nel dispositivo o nell'applicazione, l'attacco procede con un movimento laterale attraverso la rete e più endpoint, al fine di massimizzare l'infezione e i punti di crittografia. In genere, i criminali si impossessano di un controller di dominio, compromettono le credenziali, quindi riescono ad individuare e crittografare il backup per impedire all'operatore di ripristinare i servizi bloccati.

Il movimento laterale è fondamentale per il successo di un attacco. Se il malware non riesce ad espandersi oltre il punto di approdo, è inutile, pertanto, la prevenzione dal movimento laterale è essenziale.

La vostra strategia di mitigazione degli attacchi ransomware è completa?

Mitigazione del rischio

Creazione di una strategia di difesa inviolabile

Il rilevamento e la protezione del movimento laterale si riducono a due ambiti principali: in primo luogo, **occorre ridurre il vettore di attacco iniziale**, quindi **bisogna limitare i percorsi di propagazione**.

È possibile effettuare varie operazioni, come limitare il numero dei server esposti a Internet, stare al passo con la gestione delle patch per garantire una superficie di attacco minore, adottare misure di contenimento per ridurre i percorsi di propagazione tra le applicazioni ed eseguire il backup dei dati in modo da poter tornare rapidamente online ed evitare un'ingente perdita di dati in caso di attacco.

Come rendere prioritaria la pianificazione della sicurezza in quattro mosse

La sicurezza deve essere inclusa ad un livello più ampio di strategia, pianificazione e budget in vista della preparazione di un'organizzazione al fine di incrementare la consapevolezza tra i dirigenti di livello C e i membri del consiglio di amministrazione, nonché di restare vigili sui potenziali rischi e su ciò che occorre per mitigarli.

1. Assicuratevi di includere la sicurezza informatica nel ruolo che gestisce la mitigazione del rischio complessiva della vostra organizzazione. Assicuratevi che il team dirigenziale disponga di competenze in materia di sicurezza.
2. Non dimenticate di dedicare budget e risorse alla generazione di backup e alla segmentazione della rete.
3. Create appositi piani di risposta prima del verificarsi di un disastro o un evento avverso (come un attacco ransomware). Se siete organizzati e preparati, potrete reagire in modo più rapido ed efficiente.
4. Analizzate l'impatto sulla sicurezza ad ogni operazione di integrazione, progettazione o sviluppo di nuovi prodotti e servizi. Chiedetevi: sto aprendo una nuova porta ai criminali?

Checklist per il rilevamento dei ransomware

Che succede nella rete?

Per la vostra organizzazione, come per molte altre, rilevare un ransomware può risultare complicato. Purtroppo, questa difficoltà si traduce in un'inevitabile vulnerabilità della rete aziendale agli attacchi. Chi non dispone di solide capacità di rilevamento si troverà spiazzato da una richiesta di riscatto, perché a quel punto sarà ormai tardi: gran parte della rete aziendale sarà stata già crittografata.

Bisogna bloccare il ransomware nella fase precedente, mentre si sta diffondendo. Ecco ciò che vi serve:

Forte visibilità

Se non sapete cosa sta succedendo nella rete aziendale, non potrete rilevare ransomware né altre minacce informatiche indesiderate.

Policy di segmentazione

Una volta definita e chiarita ogni comunicazione, eventuali anomalie emerse verranno segnalate.

Sistema IDS e strumenti di rilevamento dei malware

Consentono di rilevare i tentativi di propagazione degli operatori di ransomware, avvalendosi di regole e firme predefinite per le vulnerabilità o gli exploit accertati oppure di un sistema di rilevamento delle anomalie più generico o automatizzato.

Strumenti per il rilevamento delle frodi

La configurazione di tattiche, honeypot o di una piattaforma distribuita per il rilevamento delle frodi, in grado di identificare movimenti laterali non autorizzati, può risultare efficace per scoprire una violazione in corso con attacchi ad alta fedeltà.

Creazione di una strategia di difesa dai ransomware

Anche in presenza dei migliori sistemi di difesa del perimetro, le violazioni sono inevitabili. Ecco perché è necessario mettere in atto una strategia di difesa in grado non solo di ridurre l'efficacia di un attacco, ma anche di arrestarne la diffusione nella rete aziendale. Affidatevi a un fornitore capace di offrire una soluzione di sicurezza completa, che rilevi le minacce nel traffico dei data center a 360 gradi e blocchi il movimento laterale.

Preparazione

Trovate una soluzione che vi consenta di identificare tutte le applicazioni e le risorse in esecuzione nel vostro ambiente IT. Questo livello di visibilità granulare vi permetterà di mappare le risorse, i dati e i backup più importanti, nonché di identificare vulnerabilità e rischi. Disponendo di un quadro completo dell'ambiente di rete, potrete rispondere e attivare rapidamente le regole appropriate durante una violazione.

Prevenzione

La soluzione adottata deve consentirvi di creare regole tali da bloccare le tecniche di propagazione dei ransomware più comuni. Con una segmentazione definita dal software, potete creare micro-parametri Zero Trust a protezione delle applicazioni, dei backup, dei file server e dei database più importanti. Inoltre, potete creare politiche di segmentazione per restringere il traffico tra utenti, applicazioni e dispositivi, bloccando, in definitiva, i tentativi di movimento laterale.

Rilevamento

Implementate una soluzione in grado di avvisarvi di qualsiasi tentativo di accesso alle applicazioni e ai backup segmentati. Questi tentativi di accesso bloccati sono indicatori di movimento laterale. Inoltre, è consigliabile integrare un sistema di rilevamento basato sulla reputazione in grado di avvisarvi della presenza di domini e processi dannosi noti. Rilevando rapidamente gli attacchi che sono riusciti a violare il perimetro, potrete ridurre al minimo i tempi di attesa e catturare i criminali prima che superino il punto di approdo.

Rimedio

L'avvio di misure automatiche di contenimento e messa in quarantena delle minacce quando viene rilevato un attacco è fondamentale. Applicate regole di isolamento tali da consentire la rapida disconnessione delle aree della rete interessate, mentre le policy di segmentazione bloccano l'accesso alle applicazioni e ai backup di sistema più importanti.

Ripristino

Infine, vi servono funzionalità di visualizzazione per il supporto di strategie di ripristino in più fasi, in cui la connettività viene gradualmente ripristinata man mano che alle diverse aree della rete viene dato il "via libera".

Conclusione

Redditività

Vi fidate della vostra strategia di difesa?

Gli attacchi ransomware non scompariranno, nel 2021, infatti, il ransomware ha colpito il 66% delle organizzazioni, un aumento del 78% rispetto al 2020 e questa percentuale non sembra diminuire. Ciò significa che il mondo continuerà ad assistere ad una frequenza di attacchi più elevata, ad un maggior numero di obiettivi di valore elevato e a richieste di riscatto più onerose, il tutto con conseguenze preoccupanti per le aziende. Ora più che mai, è necessario creare in anticipo strategie di pianificazione e mitigazione del rischio che vadano oltre un approccio incentrato solo sul perimetro.

Bloccate il movimento laterale dei ransomware nella rete. Ecco come avviene.

Per ulteriori informazioni, visitate il sito **akamai.com/guardicore**.