SOPHOS

La Protezione Endpoint e le Best Practice per Bloccare il Ransomware

Consigli pratici sulla configurazione delle soluzioni endpoint per ottenere una protezione ottimale.

Whitepaper Sophos. Ottobre 2024

Introduzione

Il ransomware è una delle minacce informatiche più pericolose, con conseguenze di vasta portata e spesso persino catastrofiche. Delle organizzazioni che hanno partecipato al nostro sondaggio "La Vera Storia Del Ransomware 2024", il 59% ha dichiarato di avere subito un attacco ransomware l'anno precedente. Nel 70% di questi casi, gli autori degli attacchi hanno crittografato i dati.

Complessivamente, il costo medio delle attività di riparazione dei danni di un attacco ransomware ha raggiunto i 2,73 milioni di $, una cifra da capogiro che rappresenta anche un aumento del 50% rispetto all'anno precedente. Inoltre, più di un terzo (34%) delle organizzazioni ha avuto bisogno di più di un mese per riprendere le normali attività in seguito a un attacco: una statistica che evidenzia la sempre maggiore complessità e gravità di questi incidenti.

I lunghi tempi necessari per la ripresa delle attività sottolineano il bisogno di un impegno di risposta più completo. Questo aumento della complessità influisce pesantemente anche sui team di sicurezza interni, con il 95% delle organizzazioni che sostiene di aver riscontrato difficoltà nello svolgere attività essenziali di Security Operations[1].

I risultati indicati sopra mettono in evidenza il bisogno impellente delle organizzazioni di potenziare le difese antiransomware e le strategie di ripresa delle attività, in quanto l'aumento dei costi, il prolungamento dei tempi di ripresa e la pressione costante sui team di sicurezza non fanno altro che confermare quanto sia pericoloso il ransomware per la continuità operativa. Una soluzione di protezione endpoint configurata correttamente costituisce uno dei metodi di difesa più efficaci contro il ransomware. Questo whitepaper si addentra nelle dinamiche degli attacchi ransomware, fornendo strategie utili per prevenirli e best practice per ottimizzare la tua protezione endpoint in modo da garantire massima sicurezza per i tuoi sistemi.

1 Il problema della mancanza di personale di cybersecurity esperto nelle PMI - Sophos

Come vengono sferrati gli attacchi ransomware

Esistono moltissimi tipi di cybercriminali, e altrettanti tipi di attacchi ransomware. Alcuni attacchi sono estremamente mirati, altri invece sfruttano opportunità fortuite. Spesso gli active adversary (detti anche cybercriminali o autori degli attacchi) sottopongono le reti a scansione, alla ricerca di punti deboli o vulnerabilità da sfruttare per infiltrarsi nel tuo ambiente. Basta riflettere sulla seguente affermazione, rilasciata da una gang di ransomware che aveva attaccato un'organizzazione canadese del settore dell'istruzione:

> *"Abbiamo trovato una vecchia vulnerabilità critica Log4j non risolta su Horizon, grazie alla quale siamo riusciti a ottenere l'accesso iniziale. Abbiamo eseguito una scansione generale, non avevamo intenzione di sferrare un attacco mirato".*

Questa citazione mette in luce anche una comune tattica sfruttata dai cybercriminali, ovvero l'exploit delle vulnerabilità a cui non sono state applicate patch, che è stata la principale causa all'origine degli attacchi ransomware nel 2024[2].

L'aumento del ransomware negli ultimi anni può essere in gran parte attribuito alla sempre maggiore diffusione del modello Ransomware-as-a-Service (RaaS). Con il RaaS, una gang di cybercriminali sviluppa un ransomware e lo "noleggia" ad altri hacker. Questo approccio rende il ransomware più accessibile a una quantità mai osservata prima di autori degli attacchi.

Una volta infiltratisi nell'ambiente della vittima, spesso gli hacker passano giorni, settimane o persino mesi a esplorare la rete, svolgendo attività di ricerca di privilegi più elevati, esfiltrazione dei dati e installazione del malware. Nel 2023, il tempo medio di permanenza degli intrusi durante gli attacchi ransomware è stato sei giorni[3]. Questo lasso di tempo permette alle vittime di identificare e bloccare gli utenti non autorizzati prima che sferrino un attacco.

2 La Vera Storia del Ransomware 2024 - Sophos
3 La Quiete Prima della Tempesta? Sophos Active Adversary Report per la Prima Metà del 2024 - Sophos

Un tipico attacco ransomware può svolgersi come segue:

È importante tenere presente che i cybercriminali hanno una strategia ben precisa, ovvero attaccare le organizzazioni a orari in cui è meno probabile che vengano individuati. Spesso gli attacchi ransomware si verificano di venerdì o sabato, per approfittare di un monitoraggio informatico potenzialmente limitato durante il fine settimana.

Dalle analisi degli esperti di incident response del team Sophos X-Ops è emerso che il 43% degli attacchi ransomware nel 2023 ha avuto luogo proprio in quei giorni; inoltre, il 91% degli incidenti ha avuto inizio fuori orario ufficio (08:00-18:00, dal lunedì al venerdì) nel fuso orario della vittima, sfruttando gli archi di tempo con minore attività potenziale di rilevamento e risposta[4].

Remote ransomware

Il Report sulla difesa digitale Microsoft 2023 indica che ora circa il 60% degli attacchi ransomware coordinati da menti umane sfrutta la crittografia non autorizzata eseguita da remoto. Detta anche "remote ransomware", la crittografia non autorizzata eseguita da remoto si verifica quando un endpoint compromesso viene utilizzato per crittografare dati su altri dispositivi all'interno della stessa rete.

Uno dei principali fattori alla base della sempre maggiore diffusione di questo approccio è la sua scalabilità: un singolo endpoint non gestito o privo di protezione adeguata può esporre l'intera organizzazione al rischio di crittografia malevola da remoto, anche se sugli altri dispositivi sono installate soluzioni di sicurezza avanzate.

Le organizzazioni devono essere consce della minaccia del remote ransomware, visto che non tutte le soluzioni di sicurezza endpoint sono in grado di difendere i sistemi da questi attacchi.

4 Blocco degli Active Adversary: Lezioni Apprese dagli Esperti di Cybersecurity - Sophos

RDP: Remote Desktop Protocol o "Ransomware Distribuito con questo Protocollo"?

Remote Desktop Protocol (RDP) è stato coinvolto nel 90% degli attacchi informatici analizzati dal team Sophos Incident Response nel 2023, una statistica in aumento rispetto all'83% dell'anno precedente[5].

RDP e gli strumenti di condivisione del desktop come Virtual Network Computing (VNC) vengono utilizzati per gestire i sistemi da remoto. Tuttavia, se non vengono applicate le dovute misure protettive, possono essere sfruttati dai criminali del ransomware per svolgere attività quali: ottenere privilegi più elevati, appropriarsi delle credenziali, muoversi lateralmente, installare backdoor, creare account fasulli ed eludere il rilevamento.

È pertanto fondamentale impedire agli active adversary di utilizzare RDP per accesso esterno, accesso interno e movimenti laterali. Anche se le organizzazioni hanno fatto passi da gigante nel garantire che RDP non rimanga esposto esternamente, gli hacker continuano a usarlo in maniera diffusa per spostarsi lateralmente all'interno di un'organizzazione.

5 La Quiete Prima della Tempesta? Sophos Active Adversary Report per la Prima Metà del 2024 - Sophos

Best practice IT per proteggersi dal ransomware

Per difendersi dal ransomware e da altre minacce, avere a disposizione le soluzioni di sicurezza più moderne non basta. È essenziale anche applicare valide regole di buona prassi di IT security, che includano corsi di formazione regolari per i dipendenti. Sebbene quello che segue non sia un elenco completo, il nostro consiglio è attenersi a queste best practice.

1. Applicare le patch presto, spesso e volentieri

Sapevi che...

Anche se tutti gli attacchi ransomware comportano conseguenze negative, quelli causati da vulnerabilità a cui non sono state applicate patch si rivelano particolarmente devastanti. Le organizzazioni colpite da attacchi che hanno inizio in questo modo si trovano ad affrontare tempi più lunghi di ripresa delle normali attività e costi di riparazione dei danni 4 volte superiori rispetto a quelli degli attacchi causati da credenziali compromesse.

Le vulnerabilità a cui non sono state applicate patch e che sono state soggette a exploit costituiscono la root cause principale degli attacchi andati a segno nel 2024[6]. Il malware e i cybercriminali sfruttano le vulnerabilità di sicurezza presenti nelle applicazioni più comuni. Applicando tempestivamente le patch a endpoint, server, dispositivi mobili e applicazioni, ridurrai le lacune che possono essere sfruttate dai cybercriminali[7].

2. Utilizzare password complesse

Sembra banale, ma non lo è affatto: una password debole e deducibile può concedere agli hacker accesso alla tua rete in pochissimi secondi. Consigliamo di utilizzare password univoche, con almeno 12 caratteri, che includano un misto di lettere maiuscole e minuscole intervallate da segni di punteggiatura, c0m3. iN.qUe5To.e5EMP1o!

3. Abilitare l'autenticazione a fattori multipli (MFA)

L'autenticazione a fattori multipli (MFA) fornisce un ulteriore livello di sicurezza dopo il primo fattore, che di solito è una password. Abilitare l'MFA in tutti i servizi e le applicazioni che la supportano è fondamentale. I cybercriminali spesso acquistano credenziali legittime sul dark web, oppure si adoperano attivamente per ottenere credenziali valide una volta infiltratisi nel tuo ambiente.

L'MFA rappresenta un ulteriore ostacolo per gli autori degli attacchi, in quanto gli impedisce di autenticarsi come utente valido senza alcuna verifica. Infine, se supportate dalle applicazioni, consigliamo di utilizzare passkey resistenti al phishing.

4. Regolamentare l'accesso alla rete interna ed esterna

Non lasciare esposte le porte. Isola l'accesso della tua organizzazione a RDP e ad altri protocolli di gestione remota. Assicurati che gli utenti remoti utilizzino una soluzione Zero Trust Network Access (ZTNA) per accedere ad applicazioni, servizi e altre risorse dell'organizzazione.

5. Monitorare i diritti degli amministratori

Verifica costantemente i diritti locali e quelli degli amministratori di dominio. È necessario sapere esattamente chi ne sia in possesso e rimuoverli da chi non ne abbia bisogno. Non mantenere l'accesso con il ruolo di amministratore più tempo del dovuto.

6. Eseguire backup periodici dei dati, conservandoli in posti diversi, e svolgere regolarmente esercitazioni per le procedure di ripristino

Nel nostro sondaggio "La Vera Storia Del Ransomware 2024", il 68% dei responsabili IT colpiti dalla crittografia non autorizzata dei dati è riuscito a ripristinare le informazioni con l'aiuto dei backup. Esegui backup periodici dei dati e conservali in posti diversi, utilizzando l'MFA per proteggere i backup nel cloud. Svolgi esercitazioni per le procedure di ripristino dai backup, per garantire una ripresa delle attività priva di problemi. Monitora i sistemi alla ricerca di eventuali attività sospette, per proteggere i backup da potenziali minacce.

7. Rimuovere le applicazioni che non sono necessarie

Gli autori degli attacchi sfruttano applicazioni comunemente installate nei sistemi per scopi malevoli. Questo approccio, denominato "Living-Off-the-Land", complica la distinzione tra utilizzo legittimo e illegittimo. Se un utente non ha bisogno di un'applicazione per svolgere il proprio lavoro, considera attentamente se quell'applicazione debba essere installata. In caso di dubbio, meglio lasciar perdere.

8. Individuare i dispositivi non protetti all'interno della rete

I cybercriminali cercano attivamente dispositivi privi di protezione endpoint per eludere il rilevamento e stabilire indisturbati la loro presenza nel tuo ambiente. Questi dispositivi non protetti possono essere sfruttati per gli attacchi di remote ransomware.

6 La Vera Storia del Ransomware 2024 - Sophos
7 Vulnerabilità Senza Patch: Il Vettore Di Attacco Che Non Perdona - Sophos

Best practice per la protezione endpoint

Un metodo efficace per proteggere i sistemi dagli attacchi ransomware è una soluzione di Endpoint Protection, Endpoint Detection and Response (EDR) o Extended Detection and Response (XDR) che includa tecnologie di prevenzione avanzata e opzioni di threat hunting.

Gli errori di configurazione negli strumenti di sicurezza sono considerati il principale rischio di cybersecurity per le organizzazioni[8]. Senza una configurazione adeguata, le impostazioni dei criteri, le esclusioni e altri fattori possono mettere in pericolo il tuo profilo di sicurezza. Assicurati di configurare correttamente la tua protezione endpoint, per garantire massimi livelli di sicurezza.

Per ottenere questi risultati, ti consigliamo di seguire sette best practice per proteggere i tuoi dispositivi endpoint dal ransomware:

1. Attivare tutti i criteri e le funzionalità consigliati

Sembra scontato, ma è un metodo infallibile per ottenere la massima protezione dalla tua soluzione di endpoint security.

Lo scopo dei criteri e delle impostazioni è bloccare minacce specifiche; verificare regolarmente che tutte le opzioni di sicurezza siano state attivate ti aiuta ad avere la certezza che i tuoi endpoint sono protetti sia dal ransomware attualmente in circolazione che da quello emergente. Assicurati che le tecnologie basate sul comportamento e le funzionalità che rilevano le tecniche di attacco fileless siano tutte attivate. Inoltre, consigliamo anche di:

A) Abilitare il Blocco rimozione

Questa funzionalità impedisce la modifica o la rimozione non autorizzata del software di protezione endpoint. Una delle prime azioni svolte dagli hacker dopo essersi infiltrati in un sistema è proprio cercare di disattivare o rimuovere la protezione endpoint.

B) Abilitare i log dei sistemi di analisi forense (preferibilmente salvandoli nel cloud)

Se si subisce un attacco di compromissione, occorre sapere cosa è successo per impedire che accada di nuovo. Tuttavia, spesso i cybercriminali formattano i log di sistema per nascondere le proprie tracce, rimuovendo così importanti indizi che sarebbero stati utili per comprendere le dinamiche dell'attacco. Potresti anche perdere l'accesso al tuo dispositivo. Avere a disposizione un record delle attività salvato nel cloud ti permetterà di recuperare comunque le informazioni critiche.

C) Assicurarsi di abilitare gli aggiornamenti dei contenuti e del prodotto per la protezione endpoint

Per tenere il passo con un panorama delle minacce in continua evoluzione e per difenderti dalle minacce emergenti, è di vitale importanza aggiornare regolarmente i prodotti con dati recenti. Nel tempo, disattivare gli aggiornamenti del prodotto e dei contenuti diminuisce l'efficacia della protezione.

2. Verificare regolarmente le esclusioni

Le esclusioni fanno in modo che directory e tipi di file attendibili non vengano sottoposti a scansioni antimalware. A volte, vengono utilizzate per ridurre i ritardi del sistema e minimizzare il rischio di avvisi di sicurezza con falsi positivi.

Con il passare del tempo, un elenco sempre più lungo di esclusioni crea lacune di sicurezza che possono essere sfruttate dagli hacker. Si crea così un maggiore rischio di intrusioni di malware che riescono a infiltrarsi nelle directory escluse (magari dopo essere stati trasferiti in maniera non intenzionale da un utente) e raggiungono il proprio obiettivo.

Verifica regolarmente l'elenco di esclusioni nelle impostazioni dei criteri e rimuovine il più possibile. Se ci sono esclusioni che non possono essere rimosse, accertati che siano estremamente specifiche. Per esempio, invece di escludere la directory o l'unità di un database, escludi file specifici utilizzandone il percorso completo. In questo modo impedirai al malware di eludere i tuoi controlli di sicurezza ed eseguirsi in quella cartella.

3. Attivare l'MFA nella console di sicurezza

Questo accorgimento garantisce accesso sicuro alla piattaforma con la quale gestisci la tua protezione endpoint e altri controlli di sicurezza. Impedirai così ai cybercriminali di modificare intenzionalmente le tue impostazioni o di disattivare/rimuovere la protezione, entrambi scenari che potrebbero lasciare i tuoi endpoint e server esposti agli attacchi.

8 Il problema della mancanza di personale di cybersecurity esperto nelle PMI - Sophos

4. Attenersi alle best practice e preservare l'integrità dei sistemi informatici
La valutazione regolare dell'integrità dei sistemi informatici garantisce che computer e software possano eseguirsi ai massimi livelli di efficienza. In questo modo potrai ridurre il rischio di cybersecurity e risparmiare tempo prezioso nella risoluzione di eventuali incidenti futuri.

Implementare un programma volto a garantire l'integrità dei sistemi informatici è di vitale importanza per la protezione contro attacchi ransomware e altre minacce di cybersecurity. Alcuni esempi potrebbero essere: fare in modo che RDP si esegua solo dove è indispensabile e dove è previsto, verificare regolarmente la presenza di problemi di configurazione, monitorare la performance dei dispositivi e rimuovere eventuali programmi indesiderati o inutili. Una verifica dello stato di integrità dei sistemi informatici potrebbe mettere in luce la necessità di aggiornare applicazioni software. Inoltre, è un metodo infallibile per garantire il backup regolare dei dati.

5. Individuare proattivamente gli active adversary presenti nel tuo ambiente
Nell'attuale panorama delle minacce, i cybercriminali sono più astuti che mai: spesso sfruttano strumenti legittimi e credenziali prelevate illecitamente per eludere il rilevamento. L'individuazione proattiva di minacce avanzate e active adversary è fondamentale per identificare e bloccare questi attacchi di tipo "Living-Off-the-Land". Una volta rilevata la loro presenza, devi anche essere in grado di intraprendere azioni adeguate per bloccarli rapidamente.

Tecnologie come Endpoint Detection and Response (EDR) ed Extended Detection and Response (XDR) offrono al tuo team di sicurezza interno capacità di threat hunting, indagine e neutralizzazione delle minacce. Tuttavia, poiché spesso gli hacker sferrano i loro attacchi fuori orario ufficio, il tuo team di sicurezza potrebbe non essere disponibile per bloccarli. Molte organizzazioni fanno fatica a proteggere i sistemi dagli attacchi ransomware 24 ore su 24, ed è proprio per questo che i servizi di Managed Detection and Response (MDR) sono in molti casi fondamentali.

Tecnologie di sicurezza a più livelli, per una protezione efficace contro il ransomware

Il detto "prevenire è meglio che curare" ci insegna che risolvere un problema sul nascere è più facile che rimediare ai danni in un secondo momento. Per la protezione della tua organizzazione contro il ransomware, puoi adottare un approccio all'IT security a livelli multipli, che prevede l'interazione di più tecnologie per potenziare le difese e la visibilità. Le organizzazioni possono cominciare con la protezione endpoint, per poi aggiungere ulteriori livelli secondo necessità, incrementando la protezione e la visibilità nel tempo.

Alcuni esempi possono essere:

- **Un firewall** per identificare e bloccare il traffico di rete sospetto e impedire alle minacce di infiltrarsi nel tuo ambiente. Un firewall offre visibilità sul traffico di rete in entrata e in uscita dalla tua organizzazione. Non è in grado di analizzare il traffico di rete all'interno del tuo ambiente.
- **Un prodotto di Network Detection and Response (NDR)** può rilevare i dispositivi non protetti e identificare gli intrusi che si spostano lateralmente nella tua rete. NDR offre visibilità sul traffico di rete interno che non può essere analizzato dal firewall.
- **Una piattaforma XDR** offre capacità di threat hunting, indagine e neutralizzazione delle minacce. Inoltre, può integrarsi nelle tue altre soluzioni di IT security, per garantire visibilità su tutti i controlli di sicurezza, da un'unica piattaforma.
- **Un servizio MDR** offre threat hunting e monitoraggio 24/7 a cura di esperti specializzati nel rilevamento e nella risposta agli attacchi informatici, prevenendo incidenti impossibili da fermare con il solo uso delle tecnologie. Il tuo servizio MDR deve offrire opzioni di incident response a 360 gradi in grado di bloccare, contenere e rimuovere completamente gli active adversary senza alcun costo aggiuntivo. Un servizio MDR deve potersi integrare con gli strumenti di cybersecurity che già usi, per garantire visibilità totale sul tuo intero ambiente. L'MDR offre i più alti livelli di protezione contro attacchi ransomware avanzati e coordinati da menti umane.
- **Una soluzione di gestione della superficie di attacco esterna (External Attack Surface Management, EASM) o gestione delle vulnerabilità** può essere utilizzata per identificare e assegnare priorità alle vulnerabilità. Sarai così in grado di identificare le patch mancanti e di applicarle prima che possano essere sfruttate dai cybercriminali.

Sophos protegge dal ransomware

Sophos Endpoint adotta un approccio alla sicurezza a 360 gradi e incentrato sulla prevenzione, per bloccare le minacce senza fare affidamento su un'unica tecnica. Blocca un'ampia gamma di attacchi, sfruttando tecnologie sofisticate quali:

- **Protezione antiransomware impenetrabile**, che difende i sistemi dagli attacchi ransomware locali e remoti, nuove varianti incluse. Blocca in tempo reale la crittografia non autorizzata e ripristina automaticamente allo stato pre-attacco i file crittografati in maniera illecita, riducendo al minimo l'impatto commerciale dell'incidente.
- **Tecnologie antiexploit**, per proteggere i sistemi dagli attacchi fileless e dagli exploit zero-day, bloccando le tecniche utilizzate dai cybercriminali in ogni fase della catena di attacco.
- **Protezione adattiva contro gli attacchi**, che offre una difesa dinamica e innovativa, in grado di modellarsi in tempo reale per rispondere agli active adversary e agli attacchi coordinati da menti umane. L'abilitazione dinamica di difese potenziate impedisce ai cybercriminali di intraprendere ulteriori azioni, poiché limita la superficie di attacco e blocca i tentativi di intrusione.

Sophos Endpoint è facile da configurare e da gestire. Basta installarla, ed è subito pronta all'azione! Le tecnologie di sicurezza consigliate sono abilitate di default, per cui avrai immediatamente il massimo livello di protezione, senza bisogno di modificare le impostazioni. Se richiesto, è disponibile anche un controllo più granulare.

Sophos Endpoint viene gestita da **Sophos Central**, la piattaforma di cybersecurity più attendibile a livello internazionale. Questa potente soluzione di gestione della cybersecurity basata sul cloud riunisce in un'unica piattaforma tutte le soluzioni di sicurezza next-gen di Sophos, e implementa l'MFA per l'accesso.

I clienti Sophos gestiscono la protezione endpoint da Sophos Central e possono usufruire della funzionalità "Verifica integrità account", che identifica eventuali deviazioni del profilo di sicurezza in criteri ed esclusioni, nonché altri errori di configurazione ad alto rischio, per permettere agli amministratori di correggere i problemi con un semplice clic.

Sophos XDR - Threat hunting proattivo e strumenti di monitoraggio dell'integrità informatica

Sophos XDR è una piattaforma unificata di rilevamento e risposta alle minacce, basata sull'approccio incentrato sulla protezione di Sophos Endpoint. Permette di rilevare, analizzare e rispondere rapidamente alle minacce multifase su tutti i principali vettori di attacco.

Grazie alla completa integrazione nella piattaforma Sophos XDR, le tecnologie Sophos agiscono in perfetta sincronia per garantire i migliori risultati di sicurezza possibili. Oltretutto, puoi ottenere un maggiore ritorno sull'investimento nei tuoi prodotti attuali di cybersecurity, grazie alle integrazioni subito pronte per l'uso con un ampio ecosistema di soluzioni di terze parti, incluse opzioni per endpoint, firewall, rete, e-mail, identità, produttività, sicurezza per il cloud, e backup e ripristino.

Sophos XDR offre strumenti e funzionalità progettati per incrementare l'efficienza degli analisti di sicurezza e dei team informatici.

- I rilevamenti con priorità stabilite dall'IA su tutte le principali superfici di attacco aiutano a identificare le attività sospette che richiedono attenzione immediata.
- Rilevamenti e casi vengono automaticamente mappati alle Tattiche MITRE ATT&CK, per permetterti di identificare facilmente eventuali lacune di sicurezza nei tuoi sistemi di difesa.
- Azioni automatizzate e accelerate come l'interruzione dei processi, il ripristino dei file crittografati dal ransomware e la segregazione della rete isolano rapidamente le minacce e ti aiutano a risparmiare tempo prezioso. Le opzioni di IA generativa focalizzata sui risultati permettono agli analisti di sicurezza di neutralizzare più rapidamente gli avversari, incrementando l'efficienza degli analisti e permettendo alle aziende di prendere decisioni corrette.

Sophos MDR - Managed Detection and Response 24/7

Sophos MDR è un servizio di sicurezza gestito e operativo 24/7, a cura di esperti altamente specializzati. Protegge i tuoi sistemi dalle minacce più recenti e dagli active adversary più sofisticati, agendo per conto tuo. Il servizio Sophos MDR offre la migliore protezione antiransomware in assoluto.

Con il livello di servizio Sophos MDR Complete, potrai usufruire di una incident response completa e illimitata, senza restrizioni e senza costi aggiuntivi. I nostri esperti sono in grado di intraprendere un'ampia gamma di azioni di risposta alle minacce per conto tuo, intervenendo da remoto per interrompere l'attacco, isolare il problema e rimuovere gli active adversary dai tuoi sistemi.

Analogamente a Sophos XDR, Sophos MDR raccoglie e incorpora dati di telemetria da tutti i prodotti Sophos, integrandosi con la stessa ampia gamma di prodotti di sicurezza di terze parti, per offrire maggiore visibilità e protezione nell'intero ambiente.

Sophos Incident Response Services Retainer - Un servizio di incident response sempre pronto a entrare in azione

Avere un team di incident response a cui rivolgersi per richiedere intervento immediato in caso di attacco è l'unico modo per risparmiare tempo, ridurre i costi e mitigare l'impatto di una violazione (ad es. quando gli active adversary fanno detonare il ransomware).

Sophos Incident Response Services Retainer è una subscription annuale che permette di accedere "on-demand" ai nostri Threat Hunter, subito pronti a entrare in azione nel tuo ambiente per sventare e isolare l'attacco: il nostro team rimuove completamente la presenza dei cybercriminali e ristabilisce la normale operatività, evitando lunghi tempi di attesa e molta burocrazia. La subscription include anche utilissime risorse di preparazione agli incidenti informatici, con le quali puoi migliorare il profilo di sicurezza della tua organizzazione, riducendo così il rischio di violazione.

Nota: l'acquisto di Sophos Incident Response Services Retainer non è richiesto, in presenza di una subscription per il livello di servizio Sophos MDR Complete, che include incident response a 360 gradi come componente standard.

Sophos Managed Risk - Servizio di gestione delle vulnerabilità e della superficie di attacco esterna

Le vulnerabilità a cui non sono state applicate patch sono la principale causa all'origine degli attacchi ransomware. Questo significa che è fondamentale identificare, svolgere indagini e assegnare le giuste priorità ai casi di esposizione ad alto rischio nel tuo ambiente informatico, prima che possano diventare un serio problema. Per fare tutto ciò, puoi contare su Sophos Managed Risk, basato sulla tecnologia leader di settore Tenable.

Con **Sophos Managed Risk,** i nostri analisti esperti identificano le vulnerabilità di cybersecurity e i potenziali vettori di attacco che presentano un livello più alto di rischio. Questo consente di intraprendere azioni adeguate per prevenire gli attacchi prima che possano interferire con le attività della tua azienda.

Conclusione

Il ransomware continua a evolversi e a rappresentare un fattore significativo che spinge le organizzazioni delle vittime a pagare un riscatto. Il tuo obiettivo è impedire agli active adversary di infiltrarsi nella tua organizzazione, e individuarli e rimuoverli rapidamente se dovessero riuscirci. Per raggiungere questo obiettivo, ti consigliamo di seguire le best practice di IT e protezione endpoint, di continuare a formare e sensibilizzare gli utenti, e di mantenere un occhio vigile sui tuoi ambienti per individuare l'eventuale presenza di minacce e cybercriminali. Un approccio alla cybersecurity incentrato sulla prevenzione e a più livelli, con rilevamento e risposta alle minacce 24/7, offre alla tua organizzazione le maggiori probabilità di riuscire a difendersi dal ransomware e dalle minacce più recenti.

Per esplorare come Sophos può aiutarti a ottimizzare le tue difese antiransomware, parla con un consulente o visita www.sophos.it

2024-10-01 (WP-NP)

SOPHOS