SOPHOS
Cybersecurity evolved.

Come Minimizzare I Rischi Di Attacco Alla Supply Chain: Alcune Best Practice

A dicembre 2020 la notizia dell'attacco informatico a SolarWinds, società di monitoraggio degli ambienti IT, ha attirato l'attenzione pubblica sugli attacchi alla supply chain. Tuttavia questo fenomeno è tutt'altro che una novità. Infatti, i dati rivelano che quasi una vittima di ransomware su 10 (9%) sostiene che l'attacco si sia infiltrato nei sistemi mediante un fornitore di terze parti attendibile. Questi dati sono emersi da un sondaggio condotto da Sophos nel 2020 a cui hanno partecipato 5.000 responsabili IT in 26 paesi[1].

Ma che cosa sono esattamente gli attacchi alla supply chain e come si svolgono? E soprattutto, quali misure si possono adottare per proteggere la propria organizzazione dall'impatto di un attacco alla supply chain?

Le risposte a queste ed ad altre domande verrà fornita nelle prossime pagine.

1 La Vera Storia Del Ransomware 2020 - Sophos, 2020

Che cos'è un attacco alla supply chain?

Spesso le organizzazioni devono affidarsi ai servizi di un fornitore di terze parti per gestire (completamente o in parte) alcune aree funzionali specifiche, come ad esempio l'infrastruttura IT. Se da un lato autorizzare fornitori di terze parti a connettersi alla rete aziendale implica notevoli vantaggi commerciali (in quanto, ad esempio, regala tempo prezioso al personale interno), dall'altro introduce inevitabilmente un rischio per la sicurezza, ovvero la vulnerabilità agli attacchi alla supply chain.

In un attacco alla supply chain, i cybercriminali non si infiltrano direttamente nei sistemi, ma sfruttano l'accesso già concesso dalle organizzazioni a fornitori di terze parti attendibili. Questa strategia li aiuta a stabilire la propria presenza in un ambiente. Una volta varcata la soglia, possono svolgere qualsiasi tipo di attività pericolosa.

Anche un solo fornitore connesso alla rete aziendale può esporre l'ambiente informatico al rischio di attacco alla supply chain. Ciononostante, in media, le organizzazioni di piccole e medie dimensioni dichiarano di concedere l'accesso ai propri sistemi ad almeno tre fornitori[2]. Proteggere i fornitori connessi è una sfida notevole per i team IT e ne aumenta il carico di lavoro. A gravare ulteriormente sulla situazione c'è anche il fatto che gli attacchi alla supply chain sono notoriamente difficili da rilevare e ancora più problematici da contrastare, in quanto possono giungere da qualsiasi punto della supply chain.

Tipi di fornitori di terze parti

Servizi professionali e fornitori di servizi IT sono due dei più comuni fornitori di terze parti in grado di connettersi alla rete di un'organizzazione.

Servizi professionali

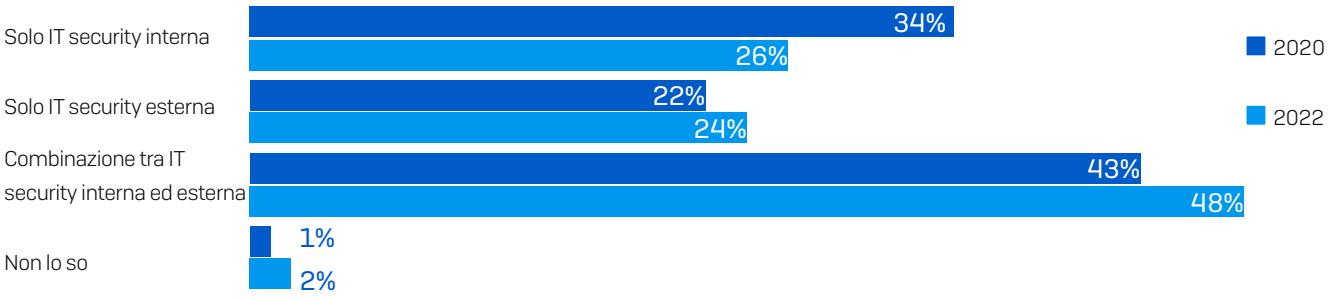
Spesso le organizzazioni si affidano ai servizi professionali per la gestione indipendente di alcune aree funzionali specifiche (o di parti delle stesse) quando non dispongono di personale interno specializzato e dotato delle competenze e conoscenze necessarie. Un esempio potrebbe essere uno studio commerciale che deve accedere (tramite software) a dati finanziari di natura sensibile, per fornire le analisi e gli approfondimenti per cui il cliente ha pagato. Come si può immaginare, un attacco informatico che riesce a violare i sistemi di un'organizzazione come questa potrebbe avere conseguenze devastanti per i suoi clienti.

Fornitori di servizi IT

I fornitori di servizi IT sono organizzazioni esterne a cui viene affidata la gestione dell'infrastruttura informatica e/o della cybersecurity di un'azienda. Spesso detti Managed Service Provider (MSP) o Managed Security Service Provider (MSSP), rappresentano un bersaglio molto frequente negli attacchi alla supply chain.

Sono vittime molto interessanti per i cybercriminali, poiché hanno accesso ai sistemi di molte organizzazioni diverse. Dato che si prevede che il numero di organizzazioni che delegano la gestione dell'IT security a fornitori esterni raggiungerà il 72% nel 2022[3], lo stato di sicurezza di queste terze parti è di fondamentale importanza per la propria cybersecurity.

Come viene fornita l'IT security: Ora e nel 2022



2,3 Cybersecurity: The Human Challenge - Sophos, 2020

Tipi di attacco alla supply chain

Sebbene gli attacchi alla supply chain siano diversi per quanto riguarda le modalità con cui vengono sferrati, i principi e gli obiettivi degli hacker sono spesso gli stessi: riuscire a infiltrarsi nei sistemi di un fornitore di terze parti fidato e abusare dei suoi privilegi di accesso per distribuire malware, impadronirsi di proprietà intellettuale o spiare le comunicazioni interne.

Attacchi di phishing

Uno dei più comuni vettori di attacco utilizzati per destabilizzare la supply chain sono le e-mail di phishing. I cybercriminali colpiscono i fornitori attendibili di terze parti con e-mail di phishing, per comprometterne la rete e infiltrarvisi. Questi sistemi vengono quindi sfruttati come trampolino di lancio per accedere agli ambienti informatici dei clienti.

Aggiornamenti del software compromessi

Negli attacchi alla supply chain più sofisticati, gli hacker si infiltrano nell'infrastruttura di un'azienda software o di un distributore ed inseriscono un codice dannoso nei pacchetti degli aggiornamenti del software. La terza parte distribuisce i pacchetti inviandoli ai propri clienti, ignara di averli nel frattempo infettati. Come è possibile immaginare, le conseguenze possono essere disastrose, soprattutto se l'organizzazione colpita ha un vasto numero di clienti. L'attacco a SolarWinds, avvenuto a dicembre 2020, è l'esempio perfetto.

Case study di attacco alla supply chain: SolarWinds

Verso la fine del 2020 è emerso che la supply chain della società di gestione IT SolarWinds aveva subito una violazione. La scoperta è comparsa nelle notizie di tutto il mondo, attirando l'attenzione pubblica sulla vulnerabilità della sicurezza della supply chain. Si ritiene che l'attacco abbia avuto ripercussioni su più 18.000 clienti di questa società.

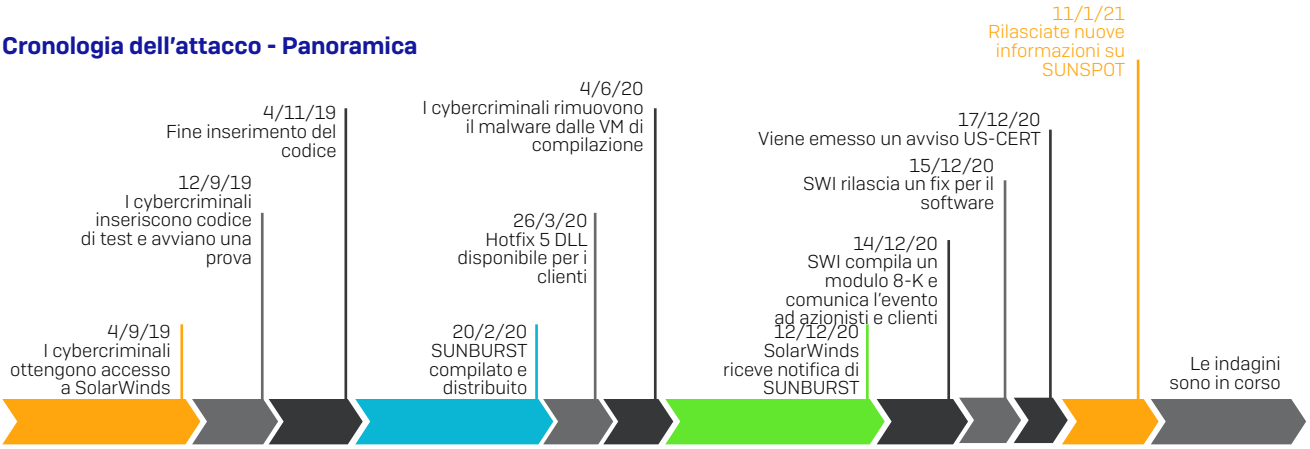
È importante sottolineare che al momento della pubblicazione di questo documento (aprile 2021) le indagini sull'attacco a SolarWinds sono ancora in corso e che pertanto potrebbero emergere nuovi sviluppi.

Come ci sono riusciti i cybercrimnali?

In sintesi, gli hacker sono riusciti a inserire un codice dannoso in Orion, la piattaforma di monitoraggio e gestione utilizzata da SolarWinds. Il codice malevolo è poi stato inconsapevolmente inviato ai clienti con un aggiornamento standard del software. Stando a quanto riferito, questi aggiornamenti sono stati installati da circa 18.000 clienti (incluse molte imprese presenti nella classifica Fortune 500 e diversi enti governativi statunitensi), che sono rimasti esposti ai rischi di attacco.

Un dato preoccupante è che SolarWinds sospettava già la presenza di attività criminali a settembre 2019, come possiamo osservare qui di seguito nella cronologia. Questo suggerisce che si trattava di una strategia calcolata da parte dei cybercriminali, che hanno esercitato estrema cautela, cercando di non dare nell'occhio durante il loro attacco di intrusione. L'analisi approfondita condotta da Sophos su come il malware Sunburst sia riuscito a eludere i sistemi di difesa è disponibile qui.

Cronologia dell'attacco - Panoramica



Tutti gli eventi, le date e gli orari sono soggetti a modifica, in attesa che vengano completate le indagini

SolarWinds - https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

Qual è stato l'impatto dell'attacco?

Il successo dell'attacco, che è stato denominato Sunburst, ha permesso agli hacker di accedere a sistemi informatici aziendali e governativi. Ha già causato il furto di quantità ancora da calcolare di dati, suscitando inoltre il timore che gli hacker abbiano utilizzato questo attacco come punto di partenza per inserire nelle reti aziendali altre backdoor ancora non individuate.

Più di ogni altra cosa, la portata globale dell'attacco ha evidenziato che molte organizzazioni sono completamente impreparate a difendersi da un attacco alla supply chain.

Pacchetti di poisoning

Un tipo di attacco alla supply chain meno comune, ma che prevediamo sarà più frequente in futuro, si basa su pacchetti che abbiamo denominato "pacchetti di poisoning". Parallelamente alla maggiore diffusione del cloud, di docker e di metodologie di sviluppo agile, cresce anche l'utilizzo di componenti pronti per l'uso che aiutano a velocizzare il ciclo di vita di sviluppo. I cybercriminali hanno cominciato a manomettere alcuni elementi comuni quali container, librerie e altre risorse, nella speranza che vengano inclusi nel prodotto finale.

Linee guida per proteggersi dagli attacchi alla supply chain

Data la complessità e la natura degli attacchi alla supply chain, le tecnologie da sole non sono in grado di prevenirli. Queste linee guida vanno invece intese come uno strumento utile per ridurre il rischio associato a un attacco alla supply chain.

1. Passare da un'attitudine reattiva a un approccio proattivo alla cybersecurity

Il caso di SolarWinds è stato un campanello di allarme per molte organizzazioni in tutto il mondo. Quando l'attacco diventa visibile, spesso è ormai troppo tardi: nel momento in cui un criminale rilascia il payload, è possibile che abbia già prelevato illecitamente dati critici e in molti casi che si sia infiltrato nella rete diversi giorni prima. Occorre adottare una nuova attitudine mentale: partire dal presupposto che i sistemi sono sempre compromessi e cercare proattivamente di individuare le minacce prima che sia troppo tardi. Esistono tecnologie e servizi in grado di supportare questo approccio e ne parleremo in maniera approfondita in un'altra sezione di questo documento.

2. Monitorare i primi indicatori di compromissione dei sistemi

Nelle indagini condotte dal team Sophos Managed Threat Response (MTR), spiccano due indicatori iniziali di compromissione: il primo è l'utilizzo di credenziali per l'accesso remoto e per le mansioni amministrative fuori orario ufficio, mentre il secondo è l'utilizzo improprio di strumenti di amministrazione del sistema per sorvegliare la rete e prelevare illecitamente dati.

L'utilizzo di account legittimi e di strumenti di proprietà dell'organizzazione per ottenere e mantenere la persistenza viene spesso definito Living Off the Land (LOL). Il rilevamento di questi comportamenti richiede particolare attenzione e abilità. Tuttavia, sono facili da riconoscere per l'occhio esperto di un analista di security operations qualificato, che è in grado di segnalare l'attacco prima che causi danni irreparabili. Consigliamo di investire in tecnologie e corsi di formazione per i dipendenti che li muniscano delle competenze necessarie per rilevare internamente questi indicatori di rischio. Una valida alternativa è quella di affidarsi ad un fornitore di servizi di Managed Detection and Response (MDR) che agisca per conto dell'organizzazione.

3. Eseguire controlli di qualità per la supply chain

Potrebbe sembrare ovvio, ma dedicare del tempo alla compilazione di un elenco di tutte le organizzazioni con cui si è connessi può essere di importanza inestimabile. Probabilmente sono più numerose di quanto si immagini. Questo accorgimento aiuta a identificare rapidamente gli anelli più deboli della catena (ad esempio le organizzazioni più esposte al cybercrimine) ed a intraprendere azioni correttive per attenuare i rischi associati. Alcuni esempi di fornitori di terze parti a cui si può essere connessi sono i seguenti:

- **Fornitori di servizi IT**
  - MSP/MSSP
  - Provider di servizi cloud
- **Servizi professionali**
  - Finanza
  - Settore legale
  - Sicurezza
  - Imprese di pulizie
- **Fornitori**
  - Materiali
  - Servizi
  - Manodopera
  - Logistica

Una volta mappate le organizzazioni a cui si è connessi, è possibile valutare il tipo di accesso alla rete di cui usufruiscono ed a quali informazioni possono accedere con le proprie credenziali. Se gli elementi esposti non sono ridotti al minimo, è il momento di bloccare alcuni accessi e limitarli esclusivamente alle informazioni indispensabili. Si consiglia di cominciare con i fornitori di servizi il cui accesso è meno essenziale, per poi proseguire con gli altri.

4. Valutare lo stato di sicurezza di fornitori e partner commerciali

Ci sono vari modi per effettuare una valutazione, ma un approccio comune per i principali fornitori di servizi, operatori di servizi cloud ed elaboratori di pagamenti è stabilire a quali tipi di certificazioni e controlli sono soggetti.

Per esempio, un elaboratore di pagamenti dovrà rispettare la conformità allo standard PCI DSS. Se è soggetto a PCI DSS di livello 1 o 2, si consiglia di richiederne il Rapporto Di Conformità (Report on Compliance, RoC) emesso dal rispettivo QSA/ISA. I RoC devono essere controllati ogni trimestre, per verificare che soddisfino i requisiti necessari.

Un'altra certificazione molto comune per la verifica dei controlli è SOC 2/2+/3 per i fornitori di servizi cloud. I controlli SOC valutano i controlli di sicurezza e le attenuazioni secondo cinque Trust Service Principle (principi di attendibilità dei servizi): privacy, sicurezza, disponibilità, integrità dell'elaborazione e riservatezza.

Proprio come avviene per la propria sicurezza, un'elevata quantità di controlli non offre garanzie complete, ma sicuramente può indicare che il fornitore ha un'attitudine estremamente seria verso la sicurezza e la conformità alle normative. Si potrebbe anche considerare di richiedere report che includano test di penetrazione, conformità agli standard GDPR o frequenza di casi passati di falle di sicurezza o violazione dei dati.

5. Esaminare continuamente l'integrità delle proprie IT Security Operation

Anche se conoscere lo stato di sicurezza dei fornitori è essenziale per proteggersi dagli attacchi alla supply chain, è importante non trascurare anche l'integrità della propria cybersecurity. Molte organizzazioni tralasciano questo aspetto perché non sanno da dove cominciare o perché non si ritengono abbastanza importanti per essere considerate un bersaglio. Le buone prassi di cybersecurity potrebbero essere il fattore determinante tra un disagio minore ed una violazione dei dati catastrofica.

Abilitare l'autenticazione a più fattori (MFA)

Il metodo più comune impiegato dagli attacchi alla supply chain per mietere vittime tra le organizzazioni è l'utilizzo di credenziali di accesso rubate, ma autorizzate. Spesso ai fornitori di servizi vengono concesse credenziali con gli stessi diritti e privilegi dei dipendenti aziendali.

Questo significa che non devono accedere con l'autenticazione a più fattori, per cui i cybercriminali possono sfruttare sia le credenziali acquisite illecitamente con gli attacchi di phishing, sia le credenziali riutilizzate in maniera non autorizzata dal personale. Poiché molte organizzazioni adottano il Single Sign-On (SSO), queste credenziali possono essere usate impropriamente per accedere a qualsiasi sistema che non sia strettamente necessario per svolgere operazioni specifiche. La conseguenza è un maggiore rischio di attività pericolose, sia per mano di personale interno che esterno.

Verificare l'accesso dei fornitori ed i privilegi delle applicazioni

Un altro errore molto comune è fornire accesso illimitato a VPN, RDP o altre tecnologie di accesso remoto a terze parti per la gestione delle soluzioni. Per "illimitato", intendiamo l'accesso all'intera rete, invece di segmentare e applicare protezione avanzata a tutti gli strumenti di accesso remoto che non sono strettamente necessari.

Tutti gli strumenti con connessioni esterne devono richiedere autenticazione a fattori multipli. Inoltre, devono essere limitati a singoli host o sistemi. Laddove sia desiderabile disporre di un livello superiore di accesso, si consiglia di utilizzare "jump

host" per limitare i rischi e per incrementare le opportunità di logging e monitoraggio.

Anche autorizzare per impostazione predefinita tutte le applicazioni firmate con il certificato software di un vendor specifico espone le organizzazioni agli attacchi alla supply chain. Abbiamo frequentemente osservato casi di furto di certificati che sono poi stati impiegati illecitamente per firmare malware. Gli strumenti di sicurezza devono ispezionare tutti gli elementi possibili.

Monitorare proattivamente i bollettini di sicurezza dei fornitori

Occorre monitorare tutti i bollettini di sicurezza dei fornitori per poter applicare rapidamente patch e attenuazioni quando vengono scoperte nuove vulnerabilità. Si consiglia inoltre di tenere d'occhio le news per scoprire se i propri fornitori sono stati coinvolti in un attacco. Se dovessero trovarsi alle prese con un incidente attivo grave, inviare notifiche a tutte le organizzazioni con cui sono connessi potrebbe non rientrare tra le loro priorità. Essere a conoscenza di eventuali incidenti permette di isolare l'accesso e avviare indagini adeguate per scoprire se ci siano state ripercussioni sulla propria organizzazione.

Rivedere la polizza assicurativa per la cybersecurity (se ne possedete una)

Infine, se si ha stipulato una polizza assicurativa per la cybersecurity, stabilire se includere i sinistri causati da terze parti e come richiedere indennizzi, se necessario. Si consiglia di consultare i propri vendor per verificare che la copertura assicurativa sia completa alla luce delle loro polizze.

Tecnologie e servizi chiave per promuovere la sicurezza

Come già discusso, proteggere i sistemi dagli attacchi alla supply chain è una questione di natura complessa. Si tratta per lo più di gestire il rischio associato a tali attacchi, per mitigarne l'impatto. Fortunatamente esistono tecnologie e servizi appositamente realizzati per supportare l'attenuazione di questo tipo di rischio.

Threat hunting

Abbiamo parlato dell'importanza di passare a un approccio proattivo alla cybersecurity per proteggere i sistemi dagli attacchi alla supply chain. Il threat hunting è una prassi fondamentale, che implica un'attitudine mentale che le organizzazioni hanno bisogno di adottare e applicare.

Endpoint Detection and Response (EDR)

Una tecnologia essenziale per promuovere la sicurezza è EDR. EDR, tipicamente integrata nelle piattaforme di protezione endpoint, offre la combinazione tra monitoraggio costante e in tempo reale, dati degli endpoint e funzionalità di risposta e analisi automatizzate. Queste opzioni permettono ai team di sicurezza di identificare rapidamente le minacce e intraprendere azioni correttive.

Sophos Intercept X Endpoint include potenti funzionalità EDR. Sophos EDR è la prima soluzione progettata sia per gli analisti di sicurezza che per gli amministratori IT: offre gli strumenti necessari per formulare domande dettagliate durante le attività di threat hunting e per incrementare l'integrità delle IT security operations. Garantisce accesso a potenti query SQL personalizzabili e subito pronte all'uso, che aiutano a reperire tutte le informazioni necessarie per prendere decisioni informate.

Inoltre, l'identificazione automatica delle minacce di Sophos EDR consente di individuare automaticamente le attività sospette, attribuire la giusta priorità agli indicatori di minaccia e cercare rapidamente potenziali minacce su endpoint e server.

Maggiori informazioni sulle funzionalità di Sophos EDR

Servizi di Managed Detection and Response (MDR)

Generalmente, per le minacce informatiche dagli effetti più devastanti, come l'attacco SolarWinds, si ha a che fare con attacchi coordinati da una mente umana. Sebbene le tecnologie, in particolar modo gli strumenti di threat hunting come EDR, svolgano un ruolo importante, devono comunque essere utilizzate da operatori esperti. Per bloccare gli attacchi coordinati da una mente umana, occorre un threat hunting con supervisione umana. I responsabili IT ne sono consapevoli, infatti nel 48% dei casi hanno in programma di integrare queste prassi nel corso dei prossimi 12 mesi[4].

4 Cybersecurity: il fattore umano - Sophos, 2020

Uno dei modi per adottare un approccio al threat hunting che preveda la supervisione umana è affidarsi ad un servizio di MDR. Il pluripremiato servizio MDR di Sophos, Sophos Managed Threat Response (MTR), non si limita semplicemente a inviare notifiche per le minacce: offre supporto concreto all'organizzazione, grazie a un team dedicato di esperti di cybersecurity disponibili 24/7, che agisce individuando proattivamente le minacce, confermandone la natura e intraprendendo le azioni necessarie per ripristinare lo stato di sicurezza dei sistemi.

Il team Sophos MTR, composto da esperti di threat hunting e risposta alle minacce:

- Intercetta e conferma proattivamente la presenza di potenziali minacce e incidenti
- Utilizza tutte le informazioni disponibili per determinare il raggio di azione e la gravità delle minacce
- Applica il giusto contesto imprenditoriale per le minacce identificate
- Avvia azioni volte a fermare, contenere e neutralizzare le minacce in remoto
- Offre consigli pratici per risolvere alla radice il problema degli incidenti ricorrenti

Maggiori informazioni su Sophos MTR

L'evoluzione verso un approccio zero trust alla cybersecurity

Precedentemente abbiamo discusso dell'importanza di esaminare regolarmente il proprio stato di sicurezza, in particolar modo mediante l'abilitazione dell'autenticazione a più fattori ed il monitoraggio costante dei privilegi di accesso e delle applicazioni. Tutto questo è possibile adottando un approccio zero trust alla cybersecurity.

L'approccio zero trust si basa sul principio "Mai fidarsi di niente, meglio controllare tutto" e si focalizza sulla protezione delle risorse, indipendentemente da dove siano fisicamente o digitalmente situate. Nessun singolo vendor, prodotto o tecnologia può garantire la "Zero Trust". Occorrono piuttosto un completo cambiamento di mentalità e l'utilizzo di varie soluzioni diverse per modificare i paradigmi su cui basiamo la protezione delle nostre risorse. Tuttavia, un passo importante verso questo modello è l'adozione di una soluzione di tipo Zero Trust Network Access (ZTNA).

Come si può dedurre dal nome, ZTNA si basa sul principio della zero trust. Consente agli utenti di accedere in maniera sicura ai dati da qualsiasi luogo e garantisce agli amministratori la disponibilità di controlli estremamente dettagliati.

ZTNA prevede la verifica costante dell'utente, di solito mediante l'autenticazione a più fattori ed un provider di identità, per poi convalidare lo stato di integrità e conformità del dispositivo, controllando che sia registrato, aggiornato, dotato di sistemi di protezione adeguati, predisposto per la cifratura, ecc. Successivamente, le informazioni ottenute vengono utilizzate per prendere decisioni in base alle policy impostate, per determinare i livelli di accesso ed i privilegi per le applicazioni di rete più importanti. ZTNA è un'ottima alternativa alla VPN di accesso remoto, in quanto offre controlli estremamente dettagliati sugli utenti e sugli elementi a cui possono accedere: una caratteristica essenziale per la protezione dagli attacchi alla supply chain che sfruttano l'accesso ai sistemi dei fornitori di servizi.

È attualmente in corso l'Early Access Program (EAP) di Sophos ZTNA, la nostra nuova soluzione di accesso alla rete distribuita e gestita tramite cloud. La disponibilità generale è prevista per la seconda metà del 2021. Offre sicurezza per tutte le applicazioni di rete ospitate sulle reti aziendali on-premise, nel cloud pubblico o su qualsiasi sito di hosting. Protegge ogni ambito: dall'accesso tramite RDP alle condivisioni file di rete, fino ad applicazioni come Jira, Wiki, repository del codice sorgente, app di supporto e ticketing e molto di più.

Maggiori informazioni su Sophos ZTNA

Conclusione

A causa della loro complessità, è pressoché impossibile impedire che si verifichino attacchi alla supply chain. Tuttavia, seguendo le linee guida fornite in questo documento si può ridurre il rischio di cadere vittima di un attacco e impedire che un attacco abbia effetti disastrosi sul business. In sintesi occorre:

1. Passare da un'attitudine reattiva a un approccio proattivo alla cybersecurity
2. Monitorare i primi indicatori di compromissione dei sistemi
3. Eseguire controlli di qualità per la supply chain
4. Valutare lo stato di sicurezza di fornitori e partner commerciali
5. Esaminare continuamente l'integrità delle proprie IT Security Operation

Inoltre, potrebbe essere consigliabile adottare servizi e tecnologie come EDR, MTR e ZTNA per assicurare il raggiungimento dei propri obiettivi di sicurezza per la supply chain.

Il panorama delle minacce si è evoluto e il rischio che la supply chain venga compromessa è un problema per tutte le organizzazioni, sia di piccole che di grandi dimensioni. Siamo tutti nell'occhio del mirino. E ridurre al minimo il rischio di attacco ai sistemi di terze parti nella supply chain non è mai stato così essenziale.

Scoprite di più sulle soluzioni di cybersecurity e sui servizi Sophos a cura di esperti leader di settore, visitando sophos.it

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità Next-Gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di intelligenza artificiale e machine learning.

14/04/2021 (SB-NP)

SOPHOS