SOPHOS

La demistificazione di Zero Trust

L'era della rete aziendale e del perimetro di rete unico sta per finire. Sono sempre più numerosi gli utenti che si avvalgono del telelavoro e che svolgono le proprie mansioni lavorative sull'Internet pubblico. La crescente diffusione di app Software-as-a-Service (SaaS), piattaforme cloud e altri servizi basati sul cloud hanno eroso l'efficacia della rete quale elemento primario per la protezione delle risorse. Non possiamo più contare su un'unica rete aziendale completamente isolata e non possiamo permetterci di fidarci di tutti i sistemi situati all'interno del suo perimetro, in quanto i confini tra le reti sono ormai sfumati.

Ma ecco zero trust: una filosofia di cybersecurity incentrata su come concepire e applicare la sicurezza. Zero trust si basa sul principio "Mai fidarsi di niente, meglio controllare tutto" e indica come proteggere le risorse, indipendentemente da dove siano situate fisicamente o digitalmente, consigliando di non ritenere nessun elemento come affidabile per impostazione predefinita.

Nessun singolo vendor, prodotto o tecnologia può garantire "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.

Questo documento analizza il concetto di "zero trust", valutando i vantaggi derivati dall'implementazione di un modello zero trust e offrendo consigli pratici sulle misure che le organizzazioni devono adottare per effettuare la transizione verso questo sistema.

I tempi sono cambiati

La fiducia è diventata un concetto pericoloso nell'ambito dell'Information Technology, specialmente quando tale fiducia è implicita, ovvero quando viene fornita in maniera incondizionata o incontestata.

La creazione di un perimetro di protezione della rete aziendale esteso e isolato, unita alla tendenza a fidarsi di qualsiasi elemento all'interno di tale perimetro, si è spesso dimostrata un modello fallace. Queste aree virtuali interne, particolarmente deboli e indifese, sono un bocconcino prelibato per gli hacker. Una volta infiltratisi, spesso sono invisibili. Diffondersi all'interno della rete, accedere a sistemi importanti e altre attività sono poi un gioco da ragazzi per loro, in quanto i controlli di sicurezza più severi vengono effettuati solamente a livello perimetrale.

Che ci piaccia o meno, ormai il perimetro è stato compromesso.

Gli utenti hanno varie esigenze: vogliono lavorare in remoto, utilizzando reti non attendibili quali i Wi-Fi pubblici dei bar. Vogliono caricare i propri dati sul cloud, per potervi accedere quando ne hanno bisogno. Vogliono accedere a dati e risorse aziendali con i propri dispositivi personali. Gli utenti chiedono a gran voce un accesso senza complicazioni, in modo da poter svolgere il proprio lavoro nel momento, nel luogo e nel modo che desiderano.

L'utilizzo di app Software-as-a-Service (SaaS), piattaforme cloud e altri servizi in cloud collocano i dati all'esterno del perimetro aziendale, mentre le piattaforme cloud pubblico fanno sì che molti dispositivi o servizi un tempo limitati all'interno del perimetro aziendale vengano ora eseguiti al suo esterno. I nostri workload vengono trasferiti dovunque sia meno dispendioso elaborarli, lontano dalle reti di nostra proprietà, in aree virtuali che non possiamo controllare, né ritenere attendibili.

C'è di tutto, dappertutto. Il vecchio modello di "rete aziendale" con metodi di difesa statici non può permettere alle aziende di adottare sistemi come il cloud, senza trascurare la protezione di dati, utenti e clienti. Occorre un cambiamento di paradigma.

Ecco zero trust

Zero trust è un approccio olistico alla sicurezza che risolve i problemi derivati da queste minacce, rivoluzionando il modo di lavorare delle aziende. È un modello e una filosofia che indica come concepire e come implementare la sicurezza.

Niente e nessuno dovrebbe meritare automaticamente la nostra fiducia, sia che si trovi all'interno o all'esterno della rete aziendale, inclusa persino la rete stessa. Occorre mettere un limite alla fiducia implicita, basata sui percorsi di rete e su metodi di difesa statici quali i firewall tradizionali.

Ovviamente alla fine qualche elemento deve essere ritenuto attendibile, ma con l'approccio zero trust questa fiducia viene concessa solo temporaneamente e viene determinata e rivalutata costantemente in maniera dinamica per mezzo di varie fonti di dati (molte di più di quante ne venissero utilizzate in passato). Le fonti di dati includono informazioni relative alla richiesta di accesso effettuata, all'utente, al sistema, ai requisiti di accesso e ai dati di intelligence sulle minacce. Inoltre, l'accesso a dati e/o risorse viene concesso solamente se e quando necessario, e varia a seconda della singola connessione.

Navigando tutti i giorni su Internet, sappiamo bene cosa significhi avere a che fare con reti non attendibili. I computer che si interfacciano con l'Internet pubblico vengono protetti in maniera ben diversa rispetto a quelli che si trovano all'interno del perimetro di rete tradizionale, in quanto richiedono maggiori accertamenti e più livelli di difesa per poter essere protetti dalle minacce esterne.

Il modello zero trust suggerisce di trattare tutti i dispositivi come se si interfacciassero direttamente con Internet e di creare vari microperimetri (o microsegmenti), piuttosto di un unico perimetro di rete, applicando verifiche e controlli su tutto e intorno a tutto.

I principali vantaggi di un approccio zero trust

Adottare un modello zero trust implica diversi vantaggi, per cui, per semplificarvi la vita, abbiamo selezionato alcuni di quelli principali.

Controllo dell'intero ambiente informatico

A partire dalle quattro mura dell'ufficio, fino alle piattaforme cloud utilizzate. La mancanza di controllo all'esterno del perimetro aziendale e le difficoltà presentate dagli utenti remoti appartengono ormai al passato.

Modalità di gestione e protezione identiche per tutti gli utenti

Evitando di suddividere gli elementi tra interni o esterni rispetto al perimetro aziendale, è possibile utilizzare lo stesso approccio per tutti gli utenti. Questo semplifica la sicurezza informatica, garantendo allo stesso tempo un trattamento identico per tutti i dispositivi e gli utenti.

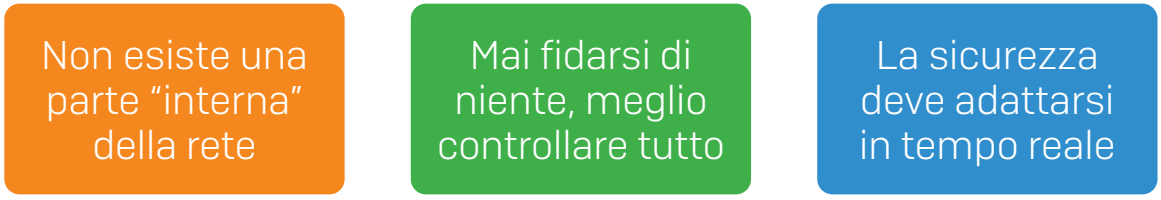
Garanzia di sicurezza anche in mancanza di piena proprietà o pieno controllo sull'infrastruttura utilizzata

Utilizzando identità, posizione, stato di integrità dei dispositivi, autenticazione a fattori multipli e tecniche di overlay per il monitoraggio e l'analisi, è ancora possibile mantenere una sicurezza efficace su qualsiasi tipo di ambiente, piattaforma o servizio.

Riduzione drastica dei movimenti del malware e degli hacker

Invece di essere liberi di girare una volta infiltratisi nella rete, gli autori degli attacchi hanno a disposizione solamente una frazione minima dei sistemi a cui può accedere l'utente compromesso. Continuando a ritenere non più attendibile l'utente autenticato, è possibile implementare verifiche tra i vari sistemi, limitando ulteriormente la libertà di diffusione del malware.

Un riepilogo del modello zero trust



Zero trust è un concetto molto esteso, se ne parla molto e la discussione è in costante evoluzione. Sostanzialmente i concetti principali di zero trust si possono riassumere in pochi ma chiari concetti di base, che è bene tenere presente durante il passaggio a questo modello.

Non esiste una parte "interna" della rete

Si immagini di gestire il proprio business da una posizione non attendibile, come ad esempio il Wi-Fi pubblico di un bar, e di aver connesso direttamente i dispositivi alla rete più pericolosa in assoluto: l'Internet pubblico. Se questa fosse la situazione reale, si sarebbe costretti ad applicare la sicurezza in modo tale da non dipendere solamente dalla protezione del tradizionale perimetro di rete aziendale.

Ci saranno sempre e comunque reti aziendali "attendibili" per i sistemi interni e per gestire l'amministrazione, ma l'obiettivo è fare in modo che gli utenti ordinari non possano accedere a queste reti. A tal fine, occorre utilizzare proxy per le applicazioni e altre tecnologie, allo scopo di ridurre drasticamente la superficie di attacco.

Mai fidarsi di niente, meglio controllare tutto

Occorre presumere che, in ogni momento, ci siano hacker in agguato sia all'interno che all'esterno della rete, sempre pronti a sferrare attacchi. Nessun utente o dispositivo va ritenuto automaticamente attendibile ed è necessario richiederne sempre l'autenticazione, prima ancora di valutarne l'idoneità a connettersi alla rete. Immaginando di trovarsi sotto attacco costante e proveniente da tutte le direzioni, si è costretti a implementare un sistema di autenticazione e autorizzazione solido ed efficace, stratificando i livelli di protezione e monitorando e analizzando continuamente gli eventi in tutti gli ambienti.

La sicurezza deve adattarsi in tempo reale

Le policy di sicurezza applicate per raggiungere gli obiettivi del modello zero trust devono essere dinamiche e devono modificarsi automaticamente in base all'analisi di quante più fonti di dati possibile, provenienti da un vasto numero di tecnologie diverse. Una policy statica come "QUESTO UTENTE su QUESTO DISPOSITIVO può accedere a QUESTO ELEMENTO" non fornisce una protezione adeguata, se il dispositivo in questione viene compromesso mentre l'utente risulta attivo su di esso. Se tuttavia viene tenuto in considerazione anche lo stato di integrità del dispositivo (in base, ad esempio, all'identificazione di comportamenti malevoli), la policy può utilizzarlo per adattarsi dinamicamente alla situazione senza bisogno di alcun intervento da parte di un amministratore.

Da tempo questo concetto è parte integrante della strategia e della filosofia di cybersecurity di Sophos. Prende il nome di Synchronized Security: un sistema in cui i nostri prodotti condividono reciprocamente le informazioni in loro possesso. Questo ci permette di applicare policy adattive e dinamiche, utilizzando tutte le informazioni disponibili per fare in modo che una policy non rimanga mai statica e che pertanto non sia facile da eludere.

Gran parte di tutto questo è semplicemente l'applicazione di adeguate politiche e best practice sulla sicurezza. Chiunque si sia preparato adeguatamente per il GDPR avrà già svolto la maggior parte di queste attività.

I principi dell'approccio zero trust

Mai fidarsi di niente. Mai e poi mai. Perché quando non ci si fida di niente, si è costretti a ricorrere a opportune misure di sicurezza ogniqualvolta vi sia un rischio.

Verificare tutto. Non bisogna presumere che a un elemento basti superare un controllo per essere degno di fiducia. Le credenziali di accesso non rendono un utente attendibile. Significano solamente che quell'utente ha delle credenziali. E le credenziali possono finire nelle mani sbagliate.

Tutto questo può essere riassunto in quattro semplici principi che è bene tenere in considerazione.

Verificare sempre l'identità

Occorre un'unica fonte autorevole per la verifica dell'identità. Tale fonte deve essere utilizzata per ogni Single Sign-On (SSO). Tutti gli ambiti del sistema devono essere accessibili solo tramite autenticazione a due fattori (Multi-Factor Authentication, MFA). Indipendentemente da dove si trovi l'utente e dalla risorsa a cui desidera accedere, occorre convalidarne le credenziali, verificarne il secondo (o terzo) fattore di autenticazione e richiederne spesso la riautenticazione.

In caso di furto delle credenziali o hijack dei sistemi, la MFA e la riautenticazione possono bloccare rapidamente un hacker.

Applicare sempre controlli

Applicare controlli e verifiche ovunque necessario, adottando e implementando il principio dell'assegnazione di meno privilegi possibile: gli utenti devono avere accesso solamente al minimo indispensabile per svolgere il proprio lavoro. Se un sistema di risorse umane viene utilizzato solamente da dipendenti situati in Germania, allora l'accesso deve essere concesso solamente a quei dipendenti. Nessun altro deve potervi accedere, anche se si ritiene che il rischio sia minimo.

Svolgere sempre analisi

Solo perché un utente o dispositivo si è autenticato correttamente o ha ottenuto l'accesso, non significa che debba essere ritenuto attendibile. Anche le minacce interne e i malintenzionati possono disporre di credenziali valide. È indispensabile tenere traccia di tutte le attività di rete e del sistema, analizzandole e ispezionandole regolarmente per verificare cosa avviene dopo l'autenticazione. Per svolgere questi tipi di operazione, sono emersi appositi sistemi di SIEM (security information and event management - gestione delle informazioni e degli eventi di sicurezza), EDR (endpoint detection and response - rilevamento e risposta alle minacce per endpoint) e MDR (managed detection and response - rilevamento e risposta gestiti).

Implementare sempre la protezione

Utilizzare un approccio alla cybersecurity "inside out", ovvero che parta dall'interno ma sia proiettato verso l'esterno dei sistemi. Bisogna cominciare con i dati più importanti, per poi muoversi verso l'esterno, identificando i punti vulnerabili della rete in cui i dati possono imbattersi durante la loro esistenza, dal momento della creazione fino alla loro eliminazione permanente.

Considerare soprattutto il rischio, piuttosto che la conformità o le normative. Applicare la sicurezza solo per superare i controlli di conformità o per soddisfare i requisiti normativi è pericoloso. I requisiti di conformità non tengono conto degli elementi presenti sulla rete, né dei flussi dei workload, dei sistemi o delle tecnologie. Non considerano i rischi che riguardano tutti gli elementi della rete. La considerazione del rischio e i vari modelli di minacce che vengono considerati dalla propria organizzazione, aiuta a decidere dove incrementare o ridurre le misure di sicurezza, e dove creare nuovi microsegmenti.

Come passare al modello zero trust

Cosa occorre fare per adottare il modello zero trust e usufruire di tutti i suoi vantaggi?

Definire la superficie e identificare le risorse da proteggere

Mappare i percorsi standard e quelli privilegiati

Architettare una rete zero trust

Creare policy zero trust

Monitorare e gestire i perimetri

Definire la superficie e identificare le risorse da proteggere

Prima di tutto, occorre definire la superficie che si desidera proteggere, controllare e monitorare. Quali sono tutte le risorse, i servizi, le app e i dispositivi utilizzati nella propria azienda? Avere piena visibilità su tutti gli elementi in uso sulla rete aiuta a implementare la mentalità zero trust.

Mappare i percorsi standard e quelli privilegiati

Una volta identificati tutti gli elementi, occorre mappare i percorsi standard: quali sono i flussi, i comportamenti e le relazioni tra tutto ciò che viene considerato standard e normale? Un certo gruppo di utenti può accedere a un'applicazione specifica, un dispositivo può connettersi a una rete in particolare, un servizio può collegarsi a un determinato archivio dati e così via, ma anche: quali sono i percorsi privilegiati? Un certo amministratore vorrà connettersi a una console di gestione specifica e utilizzare il Remote Desktop Protocol (RDP) per accedere a un server che ospita dati di natura sensibile, ecc. I percorsi privilegiati avranno quasi sicuramente bisogno dell'applicazione di controlli di sicurezza aggiuntivi.

Architettare una rete zero trust

Ora che sono stati identificati tutti gli elementi e le relazioni tra di essi, è possibile cominciare ad applicare la filosofia zero trust. Occorre identificare quali misure di sicurezza e controlli di accesso si desidera implementare e dove applicarli, abbinando le tecnologie più idonee alla mitigazione di rischi specifici, e così via.

Creare policy zero trust

Successivamente, occorre implementare policy zero trust che si basino sul maggior numero di fonti di dati possibile per aggiungere contesto a qualsiasi connessione o richiesta.

Monitorare e gestire i perimetri

Per ultima, ma non per questo meno importante, vi è l'esigenza di sovrapporre al tutto un monitoraggio dettagliato, che permetta di gestire i nuovi perimetri creati.

Questa è la sfida più difficile per gli amministratori. Se un tempo era possibile installare e configurare un antivirus senza mai bisogno di consultarne poi la console in futuro, con zero trust questa abitudine deve cambiare.

Occorre monitorare gli eventi che si verificano, utilizzando strumenti come EDR per identificare la causa che ha scatenato il problema e capire come abbia fatto una minaccia a infiltrarsi nell'ambiente, nonché per scoprire quali eventi si siano verificati prima di un rilevamento o dopo una potenziale violazione dei sistemi.

In questo ambito, risultano particolarmente utili servizi quali MDR, che consentono agli esperti di cybersecurity di aiutare gli amministratori, monitorando la rete e annientando le minacce per conto loro.

Lo stack di tecnologie zero trust

Per proteggere tute le risorse e gli asset di una rete, occorrono varie tecnologie. Non esiste un unico vendor, prodotto o sistema tecnologico in grado di risolvere tutti i problemi.

Uno stack di tecnologie zero trust deve occuparsi di due aspetti principali: la gestione dell'approccio zero trust e la sicurezza e il controllo delle varie risorse e asset.

Gestione: questo aspetto è a sua volta suddiviso in tre ambiti secondari:

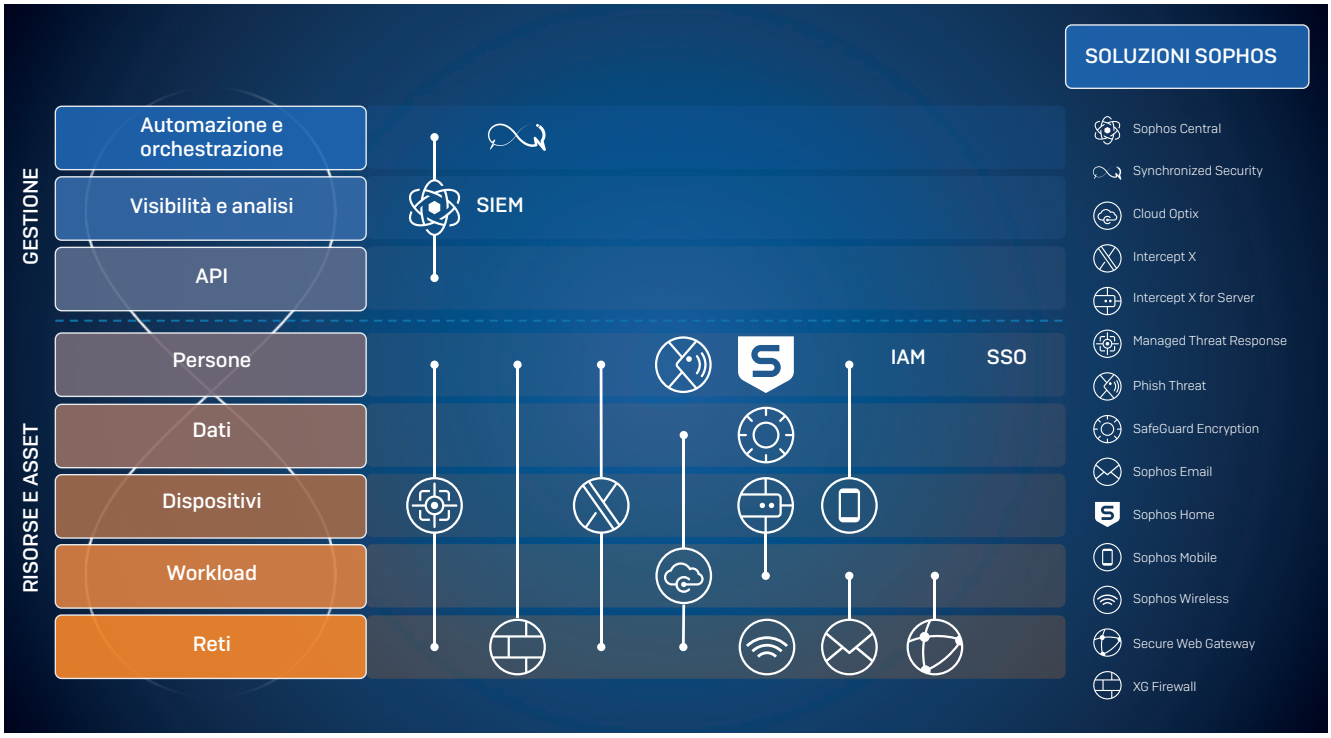
1. Automazione e orchestrazione, per la definizione di policy dinamiche, la coordinazione di tutte le varie tecnologie, e l'implementazione dell'intero sistema
2. Visibilità e analisi, per supervisionare la rete e garantire il corretto funzionamento di tutti gli elementi, nonché per identificare le minacce e i casi di violazione se o quando si dovessero verificare
3. API, per la mutua integrazione di tecnologie diverse, nonché per lo scambio reciproco di dati tra i vari sistemi

Risorse e asset: un aspetto suddiviso a sua volta in cinque ambiti secondari:

1. Persone: utenti, amministratori, ecc. che lavorano per o con l'azienda
2. Dati: la linfa vitale di qualsiasi organizzazione, e forse anche l'asset più importante da proteggere
3. Dispositivi: server, laptop, virtual machine, ecc. che vengono utilizzati per svolgere le attività aziendali
4. Workload: servizi e app utilizzati per elaborare dati, eseguire calcoli, generare report, ecc.
5. Reti: canali di comunicazione utilizzati per flussi di dati, web, e-mail, Wi-Fi, Internet e così via

Sophos vi può aiutare, ecco come

Sebbene non sia possibile affidarsi a un solo vendor per migrare un'organizzazione verso un modello zero trust, Sophos offre una vasta gamma di tecnologie che possono aiutarvi a raggiungere questo obiettivo.



La gestione nel modello zero trust

Sophos Central, la nostra piattaforma di cybersecurity nativa del cloud, aiuta a gestire un ambiente zero trust. Agisce orchestrando tutte le nostre tecnologie da un'unica console, e permette di supervisionare tutti i sistemi da un unico punto centrale, con la disponibilità di API in grado di connettere anche tecnologie di terze parti.

È anche possibile utilizzare un SIEM per aggregare i log dei prodotti Sophos e di terzi, semplificando così la supervisione completa di tutti gli eventi. Le nostre API aiutano a estrarre le informazioni necessarie dalla nostra piattaforma Sophos Central, per integrarle nel proprio sistema SIEM.

Sophos Synchronized Security (controllata da Sophos Central) è un'altra tecnologia che svolge un ruolo essenziale. Quando è abilitata Synchronized Security, le soluzioni Sophos condividono reciprocamente le informazioni in loro possesso, per attivare una risposta automatica agli incidenti. Nel contesto di zero trust, le soluzioni sono in grado di adattarsi a qualsiasi scenario, grazie alla presenza di policy dinamiche e all'automazione di operazioni complesse quali l'isolamento dei computer e altro ancora.

Sicurezza e controllo su risorse e asset

Molti dei nostri prodotti aiutano a proteggere contemporaneamente varie risorse e asset, ma questo non significa che sia sufficiente applicare solamente una tecnologia. Ad esempio, per proteggere le persone occorre un elevato numero di tecnologie diverse, utilizzate nell'ambito di una rete strutturata secondo il concetto zero trust.

Cloud Optix offre alle organizzazioni le opzioni di analisi e visibilità ininterrotta necessarie per identificare, contrastare e prevenire le lacune di sicurezza e conformità nel cloud che mettono a rischio i sistemi. In un ambiente zero trust, Cloud Optix aiuta a proteggere dati, dispositivi, workload e reti nel contesto del cloud pubblico.

Intercept X garantisce una protezione endpoint che non ha rivali ed è in grado di bloccare un'estesa gamma di attacchi, grazie alla combinazione esclusiva tra rilevamento antimalware con deep learning, prevenzione degli exploit, individuazione dei comportamenti anomali e antiransomware. In un ambiente zero trust, Intercept X aiuta a proteggere tutte le risorse e gli asset.

Intercept X for Server è appositamente realizzata per proteggere gli ambienti server in cloud, on-premise o ibridi. In un ambiente zero trust, Intercept X for Server aiuta a proteggere dispositivi e workload.

Managed Threat Response (MTR) è una soluzione di risposta alle minacce gestita dai nostri esperti. Unisce le tecnologie di machine learning all'intelligenza umana, offrendo funzionalità di threat hunting, rilevamento e risposta alle minacce attive 24h su 24 e 7gg su 7. In un ambiente zero trust, MTR aiuta a proteggere tutte le risorse e gli asset.

Phish Threat è la nostra soluzione antiphishing dedicata. Aiuta a promuovere la consapevolezza in tema di sicurezza tra i dipendenti, offrendo corsi di formazione e una reportistica progettata per aiutare gli amministratori a valutare il livello di preparazione della propria organizzazione per contrastare le minacce di phishing. In un ambiente zero trust, Phish Threat aiuta a proteggere i dipendenti.

SafeGuard Encryption cifra i contenuti non appena vengono creati. Garantisce proattivamente la protezione dei dati, grazie alla verifica costante dell'identità degli utenti, delle applicazioni e dell'integrità della sicurezza di un dispositivo, prima di concedere l'accesso ai dati cifrati. Di conseguenza, in un ambiente zero trust, aiuta a proteggere i dati.

Secure Web Gateway aiuta a implementare la protezione avanzata del web, grazie a livelli mai raggiunti prima di sicurezza, controllo e analisi del web. In un ambiente zero trust, Secure Web Gateway aiuta a proteggere reti e workload.

Sophos Email sfrutta l'intelligenza artificiale per garantire una sicurezza delle e-mail predittiva e più intelligente. In un ambiente zero trust, Sophos Email aiuta a proteggere reti e workload.

Sophos Home è progettata per mettere in sicurezza i computer domestici, con le stesse tecnologie utilizzate in molti dei nostri prodotti destinati alle aziende. In un ambiente zero trust, Sophos Home aiuta a proteggere le persone.

Sophos Mobile è la nostra soluzione di Unified Endpoint Management (UEM) e aiuta le aziende a ridurre il tempo e l'impegno da dedicare alla gestione e alla protezione dei dispositivi mobili e degli endpoint tradizionali. In un ambiente zero trust, Sophos Mobile aiuta a proteggere dispositivi, dati e persone.

Sophos Wireless offre un modo semplice ed efficace per gestire e proteggere le reti wireless. In un ambiente zero trust, Sophos Wireless aiuta a proteggere le reti.

XG Firewall offre una protezione next-gen a 360 gradi che agisce esponendo i rischi nascosti, bloccando le minacce sconosciute e rispondendo automaticamente agli incidenti. In un ambiente zero trust, XG Firewall aiuta a proteggere tutte le risorse e gli asset.

Implementare queste tecnologie può rivelarsi molto utile durante il passaggio verso un modello zero trust. Tuttavia, come già menzionato, nessun vendor o tecnologia (Sophos inclusa) può, da solo, aiutarvi a completare la transizione verso un ambiente zero trust. Per permettere agli utenti di adoperare i servizi cloud ovunque si trovino, occorre anche una valida soluzione di gestione accesso e identità (Identity Access Management, IAM) con Single-Sign On (SSO), per applicare un'unica fonte autorevole per la verifica dell'identità su tutti i sistemi e i servizi: questo è uno degli aspetti fondamentali del modello zero trust.

Per maggiori informazioni sui nostri prodotti e servizi, e per demo immediate, visitare: www.sophos.it.

La nostra vision per la cybersecurity

Zero trust e la nostra vision per la cybersecurity, ovvero Synchronized Security, hanno molti obiettivi in comune e sono reciprocamente complementari.

Synchronized Security è la cybersecurity come sistema. Analizza, adatta e automatizza costantemente le attività informatiche più complesse, tutto monitorando dinamicamente le attività del sistema, i comportamenti degli utenti, il traffico di rete e lo stato di conformità in tempo reale. Tutte le tecnologie condividono reciprocamente le informazioni in loro possesso, per mettere a disposizione di tutti gli altri componenti del sistema capacità di analisi e visibilità di cui altrimenti non potrebbero usufruire.

Le tecnologie devono essere in grado di comunicare tra loro. Solamente abilitando questa comunicazione sarà possibile creare le necessarie policy adattive e dinamiche, nonché basate su fonti di dati multiple, per raggiungere l'obiettivo di una rete zero trust.

Conclusione

Al momento, zero trust non è altro se non una filosofia orientata sulla cybersecurity, che solo pochi sono pronti ad adottare. Tuttavia, con la costante erosione dei perimetri di rete, l'esigenza di implementare questo approccio diventerà sempre più diffusa. I cybercriminali adottano misure sempre più innovative e i sistemi di difesa fanno fatica a tenere il passo con queste evoluzioni. Il modello zero trust rappresenta un ottimo modo per minimizzare effettivamente le minacce, impostando nuovi standard per i protocolli di cybersecurity.

È ora di pensare in maniera alternativa. È giunto il momento di evolversi.

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

© Copyright 2020. Sophos Ltd. Tutti i diritti riservati.
Registrata in Inghilterra e Galles con N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito
Sophos è un marchio registrato da Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

10/03/20 WP-IT (DD)

SOPHOS