WHITE PAPER

La falla nella strategia di sicurezza aziendale su più livelli e come risolvere il problema

Akamai

Analisi riassuntiva

Le sfide che i professionisti della sicurezza IT affrontano diventano sempre più complesse di giorno in giorno. Le minacce alla sicurezza cambiano continuamente. Il volume e il tasso delle minacce mirate, come malware, ransomware, esfiltrazione dei dati basata su DNS e phishing, stanno aumentando. Inoltre, il fatto che le aziende non sono più costituite da dipendenti che lavorano per un'intera giornata lavorativa in maniera standard, nella stessa sede centrale (i dipendenti lavorano in sede e in remoto, full-time e part-time e ubicati in tutto il mondo) complica ulteriormente la sicurezza aziendale. Quando si considera che la maggior parte delle imprese estende l'accesso alla rete anche a collaboratori, partner e fornitori, la situazione diventa ancora più contorta.

Per confrontarsi con queste sfide, le principali imprese stanno scartando gli approcci tradizionali, come la sicurezza del perimetro e il principio del "fidarsi, ma verificare sempre", sapendo che non sono sufficientemente completi per affrontare i sofisticati attacchi attuali. Invece, le aziende si stanno muovendo verso un modello di sicurezza "zero trust", che elimina il concetto in base al quale tutto ciò che viene dall'interno è affidabile. Questa architettura presuppone che tutti gli utenti e tutti i dispositivi siano ugualmente inaffidabili e che i confini tra "interno" ed "esterno" siano stati annullati.

Un componente essenziale del modello "zero trust" è rappresentato dall'implementazione di una strategia LES (Layered Enterprise Security), che si basa su più livelli di difesa per la protezione dalle minacce, invece di un singolo livello di protezione. La maggior parte dei professionisti della sicurezza concorda sul fatto che nessun singolo prodotto sia in grado di offrire una resistenza al 100% contro tutte le minacce, né sia possibile ottenere una resilienza completa rispetto alle incessanti e incentivate minacce informatiche odierne. Pertanto, è consigliabile adottare una strategia LES per poter garantire una difesa approfondita.

Tuttavia, molte aziende che hanno effettuato la migrazione a una strategia LES non riescono ancora a proteggere la propria infrastruttura DNS (Domain Name System), un protocollo Internet fondamentale che non è mai stato progettato pensando alla sicurezza. La natura aperta del DNS, e specificamente del DNS ricorsivo (rDNS), la rende un obiettivo primario e relativamente facile per gli attacchi, tra cui campagne di malware ed esfiltrazione dei dati. È fondamentale che le aziende costruiscano e rafforzino la propria strategia LES per includere e difendere meglio il DNS.

In questo documento, esamineremo i particolari della sicurezza aziendale su più livelli, i motivi fondamentali per cui occorre monitorare e proteggere il DNS, nonché i vantaggi chiave della sicurezza basata sul DNS, tra cui la velocità e la facilità di implementazione.

Sicurezza aziendale su più livelli + modello "zero trust" = la miglior difesa

CHE COSA SI INTENDE ESATTAMENTE PER SICUREZZA AZIENDALE SU PIÙ LIVELLI?

Quando si esaminano i motivi per cui la sicurezza aziendale su più livelli è fondamentale, è utile pensare alla protezione di un ambiente fisico. Immaginate che vi sia una costante minaccia di intrusioni da parte di sofisticati criminali a danno di una vostra proprietà. Fareste affidamento esclusivamente su un sistema di allarme? Probabilmente no. Probabilmente, avreste a disposizione una vastissima gamma di sistemi di protezione, ad esempio un sistema di allarmi, rilevatori di movimento, cani da guardia, forse persino guardiani armati. Forse conservereste i vostri beni di maggior valore in varie casseforti di tipo avanzato e le porte di ciascuna stanza potrebbero essere dotate di complicate serrature. Fondamentalmente, andreste ad impiegare molti tipi di protezione dislocati in vari punti dell'edificio per mantenere al sicuro la vostra proprietà.

Lo stesso concetto si applica alla sicurezza IT della vostra azienda: gli esperti concordano sul fatto che l'utilizzo di vari livelli di protezione rappresenti il modo migliore per rilevare gli utenti malintenzionati e respingere gli attacchi. Dal momento che i criminali informatici tentano di scovare i punti deboli nei sistemi di sicurezza aziendali, non potete riporre tutta la vostra fiducia in una singola soluzione per la sicurezza. Inoltre, come affermato in precedenza, non esiste un'unica soluzione in grado di salvaguardare la vostra azienda da ogni forma di attacco informatico, il che rende fondamentale un approccio LES.

Una strategia di difesa approfondita consente di garantire che, nel caso di una minaccia che riuscisse a eludere un singolo meccanismo di sicurezza, altri livelli di protezione sarebbero comunque in grado di identificare e bloccare la minaccia. Jerry Shenk, esperto di sicurezza IT, spiega:

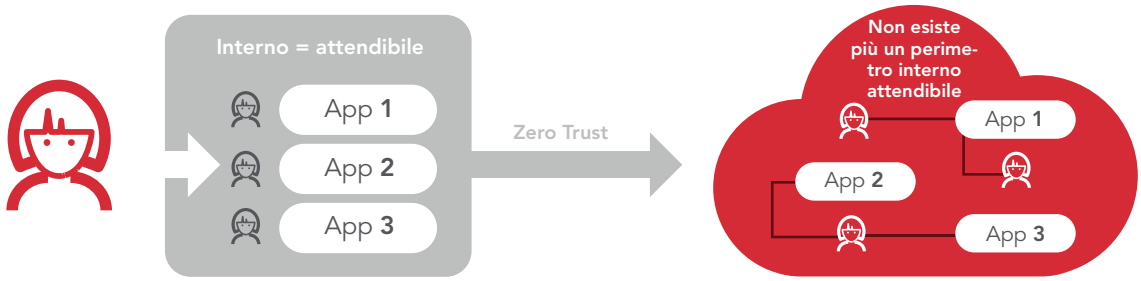
> Non esistono soluzioni adatte a tutte le situazioni e sono necessari molti processi e molte tecnologie per garantire una gestione completa dei rischi e della sicurezza… gli odierni autori degli attacchi colpiscono attraverso più livelli. Ciò significa che anche la nostra sicurezza deve essere su più livelli.[1]

Prendiamo in considerazione un normale approccio alla sicurezza IT: Software antivirus. La sua installazione su laptop e computer desktop consente certamente di proteggere un'azienda da alcuni attacchi malware. Tuttavia, il malware odierno è così avanzato che affidarsi a un singolo meccanismo di questo tipo renderà vulnerabile l'azienda alle minacce specificamente progettate per eludere l'antivirus sugli endpoint.

Con un approccio alla sicurezza su più livelli, qualsiasi falla dell'antivirus sugli endpoint nell'individuazione e nella rimozione del malware potrebbe non comportare un guasto nell'intero sistema di sicurezza. Al minimo, l'utilizzo di più tecniche di difesa rallenterà l'autore di un attacco e migliorerà i tempi di rilevamento; al massimo, la sicurezza aziendale su più livelli consentirà di sventare completamente un attacco, arrestandone l'avanzamento nei sistemi aziendali prima che si verifichino danni.

LES: una parte essenziale di un approccio "zero trust"

ANCHE SE NON SI TRATTA DI UN'IDEA NUOVA, IL MODELLO "ZERO TRUST" HA OTTENUTO UNA POPOLARITÀ SEMPRE MAGGIORE E PER UN BUON MOTIVO.



Originariamente promossa da Forrester Research, l'architettura "zero trust" si basa sull'assunto che non esiste un elemento "interno" affidabile e che tutti gli utenti e i dispositivi sono ugualmente inaffidabili. Questa struttura di sicurezza ritiene che tutti gli utenti e i dispositivi che potrebbero venire in contatto con la vostra rete sono ostili e potenzialmente compromessi e vi impone sempre l'autenticazione e l'autorizzazione. Invece di "fidarsi, verificando sempre", la regola seguita è quella del modello "zero trust". Inoltre, più numerosi sono i livelli di sicurezza di cui disponete, più efficace sarà il vostro modello di sicurezza "zero trust".

> I CIO devono passare a un approccio alla sicurezza "zero trust", che sia incentrato sui dati e sull'identità e che, dal nostro punto di vista, rappresenta il solo approccio alla sicurezza in grado di funzionare.[2]

Nel suo rapporto Zero Trust Security: A CIO's Guide To Defending Their Business From Cyberattacks, Forrester Research afferma che tutte le aziende devono "lavorare sul presupposto che tutto il traffico rappresenti una minaccia finché non siano state eseguite le attività di autorizzazione, ispezione e protezione, indipendentemente dal fatto che l'accesso ai sistemi venga effettuato da un utente interno o esterno e che i dati si trovino nel data center o nel cloud".[3]

Se tutto il traffico deve essere considerato una minaccia, perché le aziende lasciano il DNS ricorsivo, che risolve milioni di query al giorno, completamente privo di protezione?

Il vostro DNS ricorsivo non protetto rappresenta un facile bersaglio per gli autori di attacchi dannosi

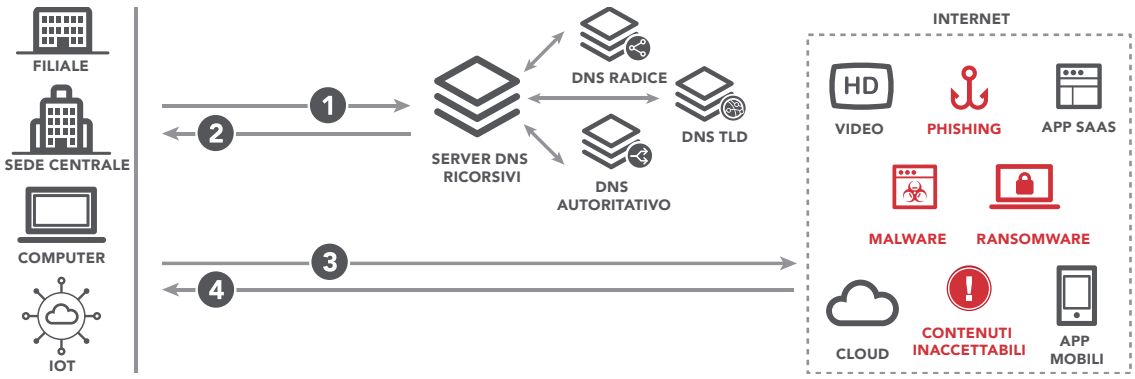
Molte organizzazioni riconoscono l'importanza di adottare un approccio alla sicurezza aziendale su più livelli e, in quanto tale, implementano più soluzioni per la sicurezza, tra cui firewall, Secure Web Gateway, sandbox, sistemi di prevenzione delle intrusioni e antivirus sugli endpoint. Eppure, gli utenti malintenzionati sono ostinati e continuano a introdursi nei sistemi aziendali sfruttando i punti deboli dei sistemi di sicurezza. Una di queste lacune è la vulnerabile "porta sul retro", rappresentata dal DNS ricorsivo.

> L'IoT (Internet of Things) è composto da miliardi di dispositivi connessi a Internet in tutto il mondo, che effettuano costantemente richieste DNS. Poiché il numero dei dispositivi IoT è in vertiginosa crescita, destinato a raggiungere la cifra di 20,4 miliardi nel 2020[4], la vostra vulnerabilità nei confronti dei criminali informatici potrà solo aumentare. Attualmente, l'80% dei dispositivi IoT non è collaudato per le vulnerabilità della sicurezza,[5] il che rende tali dispositivi l'obiettivo principale per gli utenti malintenzionati che cercano di sfruttare le falle nella sicurezza insite nel DNS.

Quali sono i motivi per cui il DNS rappresenta un obiettivo tanto attraente per gli utenti malintenzionati?

- **INTRINSECAMENTE VULNERABILE:** sebbene renda Internet veloce, efficiente e navigabile, il DNS è aperto per natura, in quanto utilizza le porte 80 e 443 non filtrate. Come illustrato in precedenza, questa esposizione è aggravata dal fatto che singoli utenti e anche aziende lo lasciano spesso senza protezione.
- **ONNIPRESENTE:** quasi tutte le azioni eseguite su Internet iniziano con una richiesta DNS che associa i nomi di dominio agli indirizzi IP. Ciò significa che, ogni volta che gli utenti aziendali o i dispositivi connessi alla rete (inclusi i dispositivi IoT) eseguono una richiesta Internet, dall'esplorazione del web all'invio di e-mail, dal retail online al cloud computing, utilizzano il DNS.
- **INCAPACE DI DISTINGUERE:** il DNS in sé non ha intelligence, pertanto risolve indiscriminatamente sia le richieste dei domini innocui che di quelli dannosi.

DNS: IL PUNTO DI PARTENZA DI OGNI RICHIESTA INTERNET



Gli utenti malintenzionati sviluppano malware specificamente concepiti per sfruttare queste qualità, nonché per eludere i livelli di sicurezza esistenti, ad esempio firewall, Secure Web Gateway, programmi antivirus e servizi di intelligence sulle minacce, che, in genere, non utilizzano il DNS come punto di controllo. Di conseguenza, l'infrastruttura DNS fornisce spesso un percorso attraverso il quale i criminali informatici possono lanciare minacce mirate contro le aziende, compresi attacchi di phishing, campagne di malware e ransomware ed esfiltrazione dei dati.

> “Dal momento che una vasta percentuale di situazioni pericolose inizia con le interazioni dell'utente, è necessario osservare e orientare le difese di rete per contrastare rapidamente le attività di attacco che hanno origine a livello dell'utente.[6]”

È chiaro che, al fine di ottenere un approccio alla sicurezza su più livelli in grado di raggiungere l'obiettivo del modello "zero trust", dovete monitorare e controllare in modo proattivo il vostro DNS. Se viene lasciato senza controllo, prima o poi uno dei milioni di richieste effettuate quotidianamente su Internet dalla vostra rete si risolverà in un download dannoso. I potenziali scenari sono scoraggianti:

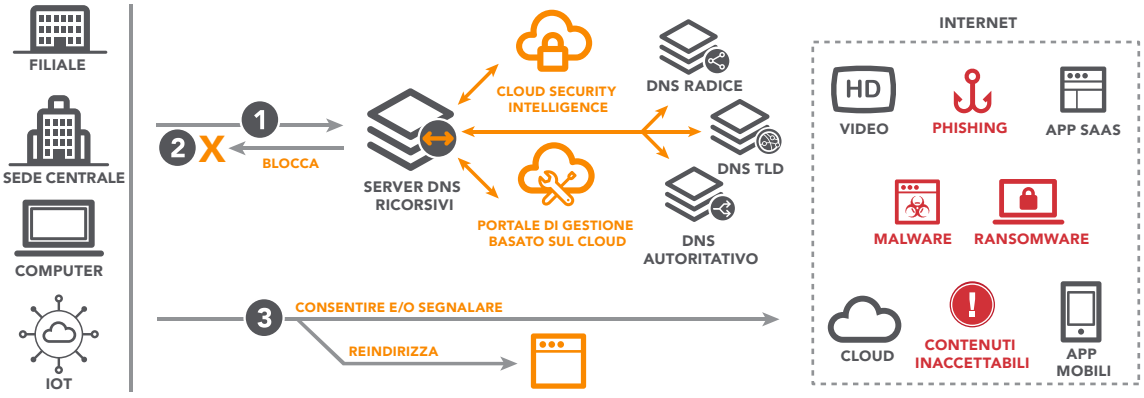
- **UN DISPOSITIVO COMPROMESSO** può diventare rapidamente la porta di accesso per infezioni con diffusione in tutta l'azienda, in grado di generare rallentamenti o interruzioni del funzionamento della rete, fenomeni di spionaggio sulle attività aziendali, furto di informazioni, eliminazione di dati e file, trasformazione dei dispositivi in "computer zombie" che ospitano contenuti illegali, vengono utilizzati per il crypto-mining, vengono coinvolti in attacchi DDoS e molto altro.
- **LA MAGGIOR PARTE DEI MALWARE** invierà una richiesta al proprio server CnC (Command and Control) dalla vostra rete per ottenere ulteriori istruzioni. Considerata la natura aperta e non filtrata del traffico DNS, queste comunicazioni dannose passeranno inosservate, scavalcando tutti i sistemi di sicurezza a livello di rete.
- **ATTRAVERSO IL DNS,** gli utenti malintenzionati posso esfiltrare i record finanziari, i numeri di previdenza sociale, le informazioni sulle carte di credito, la proprietà intellettuale e altri dati sensibili. I pacchetti di dati vengono crittografati, compressi, suddivisi e quindi trasmessi all'esterno della rete.

In che modo una soluzione per la sicurezza basata sul DNS vi aiuta a proteggere la vostra azienda

Dunque, in che modo esattamente rafforzate la vostra sicurezza aziendale, con uno sguardo rivolto al miglioramento della protezione rispetto alle lacune nella sicurezza che presenta il DNS? Attivate il DNS nella vostra linea di difesa iniziale.

Le organizzazioni IT utilizzano soluzioni per la sicurezza basate sul DNS di terze parti, che si comportano come un server DNS ricorsivo aziendale, esaminando ogni richiesta DNS per determinare se stia eseguendo la query di un dominio sicuro o dannoso. Queste soluzioni possono trasformare il DNS in un punto di controllo e in una risorsa di sicurezza preziosa, in grado di proteggere in modo proattivo la vostra rete.

UTILIZZO DI UNA SOLUZIONE PER LA SICUREZZA BASATA SUL DNS



I resolver DNS eseguono una funzione fondamentale, ossia prendono un nome di dominio leggibile e trovano il corrispondente indirizzo IP del server in cui è ubicata la risorsa. Il resolver troverà l'indirizzo IP nella cache o utilizzerà un server DNS ricorsivo per la ricerca attraverso una gerarchia di server dei nomi DNS e di server DNS autoritativi. Attraverso l'utilizzo di una soluzione per la sicurezza basata sul DNS, la vostra organizzazione non risolverà più queste richieste DNS in maniera indiscriminata.

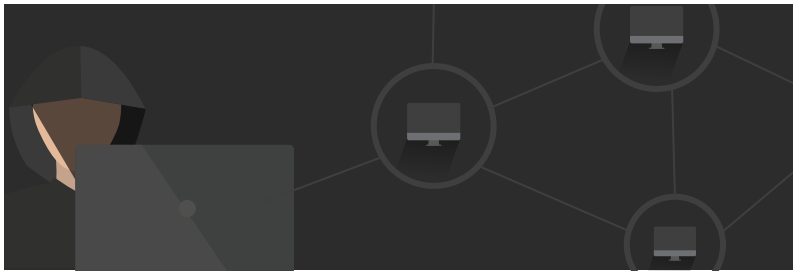
La soluzione per la sicurezza basata sul DNS agirà come server DNS aziendale, controllando i nomi di dominio rispetto a un'intelligence per le minacce aggiornata e completa, prima di risolvere l'indirizzo IP. È fondamentale comprendere che la vostra soluzione per la sicurezza a livello di DNS è efficace solo nella misura in cui lo è l'intelligence per le minacce.

Pertanto, i dati dannosi di alta qualità non elaborati della vostra soluzione devono essere integrati tramite un costante lavoro di valutazione, ricerca e convalida da parte di esperti di sicurezza dedicati. Questa intelligence deve essere aumentata tramite feed esterni da partner della sicurezza, nonché da dati pubblici, quali informazioni WHOIS e dei registrar. Il set di dati combinati deve essere analizzato mediante avanzate operazioni di analisi comportamentali offline in tempo reale e algoritmi proprietari a rotazione.

L'intelligence sulle minacce su cui si fonda la vostra soluzione per la sicurezza basata sul DNS deve essere in grado di:

- **FORNIRE** intelligence focalizzata sulle minacce correnti e pertinenti, in opposizione alla copertura del dominio.
- **ATTINGERE** a un ampio e completo volume di traffico DNS e IP, in modo da essere in grado di identificare rapidamente le tendenze delle minacce globali e rilevare le minacce prima che diventino attive su larga scala.
- **DISTINGUERE** tra domini dedicati, creati specificamente per un uso dannoso, e domini legittimi che sono stati compromessi.
- **FORNIRE** un tasso molto basso di avvisi di sicurezza falsi positivi, in modo che il vostro team addetto alla sicurezza non perda tempo ed energie nella loro ricerca.

La vostra soluzione per la sicurezza basata sul DNS deve monitorare e analizzare costantemente i registri DNS in tempo reale, controllandoli rispetto a questo robusto set di dati, e deve quindi identificare rapidamente le anomalie. Le richieste sospette, singolari e superflue verranno segnalate e bloccate (prendete, ad esempio, una singola stampante che effettua improvvisamente migliaia di richieste rDNS o il laptop di un dipendente che rilascia centinaia di query alle 3:00 del mattino), riducendo l'impatto di un problema o di un'intrusione prima che arrechi danni alla rete aziendale.



L'intelligence, il monitoraggio e il filtraggio forniti da una soluzione per la sicurezza basata sul DNS non sono attività che un'organizzazione può svolgere in maniera efficace per proprio conto. Ciò è dovuto a esigenze di volume e visibilità. Un dispositivo esegue migliaia e migliaia di query DNS ricorsive al giorno, un quantitativo che va moltiplicato per ciascun utente e dispositivo. Il volume spesso impedisce l'inserimento di un registro DNS in un sistema SIEM (Security Information and Event Management). L'esportazione di registri e la riduzione dei dati provenienti da più fonti per visualizzare il traffico DNS in aggregato rappresentano attività onerose, mentre l'esplorazione di questi dati per identificare le richieste anomale è incredibilmente dispendiosa in termini di tempo.

Anche se risolvete questi problemi di aggregazione e allocate le risorse necessarie per monitorare e analizzare costantemente i registri DNS, è molto improbabile che riusciate a identificare e mitigare un'intrusione perché ricaverete informazioni superflue. Le dimensioni del campione della vostra azienda sono troppo limitate per identificare tendenze e minacce su Internet. Maggiore è la quantità di traffico e intelligence a cui si ha accesso, più facile diventa individuare il traffico DNS irregolare. È necessario comprendere i modelli e le tendenze globali per identificare in modo coerente ed efficiente le minacce.

Le migliori soluzioni per la sicurezza basate sul DNS possono essere implementate e configurate in meno di 30 minuti, sono basate sul cloud al 100% e consentono di aumentare istantaneamente la protezione senza complessità o hardware né interruzioni per gli utenti. La vostra misura di sicurezza DNS deve consentire di amministrare quasi istantaneamente le policy e gli aggiornamenti di sicurezza da qualsiasi ubicazione per proteggere tutte le posizioni. Deve inoltre consentire l'applicazione rapida e uniforme della conformità e della policy di utilizzo (AUP), bloccando l'accesso a categorie di contenuti e domini inappropriati o discutibili. Le soluzioni migliori consentono di applicare le misure di sicurezza e le policy AUP quando i laptop vengono utilizzati al di fuori della rete aziendale e quando la rete VPN di un laptop non è attiva.

Perché tre soluzioni per la sicurezza estremamente diffuse traggono vantaggio da un ulteriore livello di sicurezza basata sul DNS

Esaminiamo tre tecnologie di sicurezza comunemente utilizzate dalle aziende, i loro punti di forza e di debolezza, nonché le modalità con cui un livello di sicurezza basato sul DNS le integra, rafforzando nel contempo la difesa di un'azienda dagli attacchi di utenti malintenzionati.

SOLUZIONI ANTIVIRUS SUGLI ENDPOINT

Le soluzioni antivirus sugli endpoint rilevano, bloccano e rimuovono i malware dai dispositivi degli utenti finali, ad esempio laptop e computer desktop. Un motore di rilevamento esegue le scansioni delle pagine web e dei file richiesti e confronta i risultati rispetto a un elenco di firme di malware aggiornato di frequente.

Punti forti: le soluzioni antivirus sugli endpoint offrono una protezione rapida e soddisfacente da minacce note.

Punti deboli: dal momento in cui una minaccia colpisce una soluzione antivirus sugli endpoint, il software rappresenta l'ultimo livello di difesa. Se il software non ha ricevuto un aggiornamento delle firme, quel singolo dispositivo compromesso può essere sufficiente a provocare danni significativi. L'antivirus sugli endpoint offre anche protezione limitata da minacce ignote/zero day e malware senza file. Inoltre, i database della firma diventano molto grandi e possono risultare non aggiornati su molti dispositivi, in particolare sui laptop che potrebbero venire collegati raramente alla rete aziendale.

Modalità di difesa offerte da un livello di sicurezza basato sul DNS: se un dominio dannoso noto rilascia nuovo malware o una nuova variante di malware, una soluzione per la sicurezza DNS è in grado di proteggere in modo proattivo l'azienda, come risultato dell'intelligence sulle minacce in tempo reale della soluzione; non sono necessari aggiornamenti delle firme.

Se un dispositivo è già infettato da malware e viene inserito nella rete aziendale, una soluzione per la sicurezza basata sul DNS è in grado di rilevare tale dispositivo compromesso prima che possa provocare danni. Ciò dipende dal fatto che la stragrande maggioranza del malware utilizza il DNS per raggiungere il proprio server CnC. Quando il dispositivo tenta di stabilire questo contatto, viene identificato. Inoltre, poiché una soluzione per la sicurezza a livello di DNS utilizza il DNS come punto di controllo, l'elusione di tale punto di controllo attraverso la kill chain di sicurezza è improbabile.

SOLUZIONI PER FIREWALL AZIENDALE

Noti anche come firewall di prossima generazione (NGFW), questi firewall di ispezione approfondita dei pacchetti oltrepassano il blocco e l'ispezione della porta/del protocollo per aggiungere l'ispezione a livello di applicazione, la prevenzione delle intrusioni e l'intelligence al di fuori del firewall. In maniera sempre crescente, i firewall NGFW aggiungono funzioni di sandbox, protezione avanzata dalle minacce, filtraggio URL e prevenzione della perdita di dati.

Punti forti: i firewall NGFW offrono protezione da attacchi dannosi in entrata e risultano efficaci su tutte le porte e tutti i protocolli.

Punti deboli: richiedono una gestione complessa e dispendiosa in termini di tempo e, di conseguenza, possono essere facilmente configurati in modo errato, il che può creare eventuali vulnerabilità. I firewall NGFW non rappresentano soluzioni efficaci per la protezione dei laptop al di fuori della rete e la maggior parte di essi non utilizza il DNS come punto di controllo della sicurezza.

Modalità di difesa offerte da un livello di sicurezza basato sul DNS: una soluzione per la sicurezza a livello di DNS blocca le minacce nella fase iniziale, prima della connessione IP. Consente inoltre di liberare risorse IT tramite la gestione di whitelist, blacklist ed elenchi di controllo degli accessi (ACL), un processo dispendioso in termini di tempo. Mitigando più attacchi a livello del DNS, le organizzazioni riducono il numero di eventi da dover affrontare con altri sistemi di sicurezza sulla rete, rendendo il lavoro del team di sicurezza IT più gestibile.

Si prevede che, entro il 2019, il 75% di tutto il traffico web sarà crittografato.[7] Di conseguenza, il traffico crittografato diventerà il principale metodo di distribuzione dei malware e di esecuzione degli attacchi informatici. Ispezionare

il traffico crittografato è un'operazione molto intensiva a livello del processore perché richiede alle organizzazioni di decrittografare e ispezionare il traffico SSL. Grazie all'utilizzo di una soluzione per la sicurezza basata sul DNS per il monitoraggio del traffico DNS sospetto e il blocco del traffico DNS dannoso, potete ridurre la quantità di traffico HTTPS da ispezionare, ponendo un carico minore sul firewall.

SOLUZIONI SECURE WEB GATEWAY

Un SWG (Secure Web Gateway) protegge i dispositivi connessi a Internet da infezioni e rafforza la conformità delle policy aziendali e normative. Un SWG include filtraggio degli URL, rilevamento e filtraggio di codice dannoso, nonché controlli delle applicazioni per le più diffuse applicazioni basate sul web, come la messaggistica istantanea e Skype.

Punti forti: un Secure Web Gateway funziona a livello di URL, fornendo un controllo più minuzioso. Prende in esame sia la risorsa richiesta che il payload, si integra con i sistemi di identità e consente la creazione di policy estremamente flessibili.

Punti deboli: i sistemi SWG sono complessi da gestire. I loro motori antivirus presentano le stesse limitazioni di un antivirus sugli endpoint. Un Secure Web Gateway è inoltre costoso da implementare in tutti i siti se vi servono interruzioni locali e non rappresenta la soluzione ideale per la protezione dei dispositivi al di fuori della rete. Purtroppo, i sistemi SWG non sono efficaci contro il malware che non utilizza il protocollo HTTP/HTTPS sulle porte 80/443. Inoltre, i sistemi SWG offrono una protezione limitata dalle minacce specifiche del DNS, come il traffico CnC malware, e le relative blacklist statiche sono facili da eludere tramite algoritmi di generazione dei domini (DGA) e Fast Flux.

Modalità di difesa offerte da un livello di sicurezza basato sul DNS: associato a un Secure Web Gateway, un livello di sicurezza presso il punto di controllo DNS colma una lacuna nella sicurezza. Grazie all'utilizzo di un sistema SWG basato su cloud (rispetto a un sistema NGFW in sede), una soluzione per la sicurezza DNS blocca le minacce in anticipo, prima della fase di connessione IP.

Un altro vantaggio di una soluzione per la sicurezza DNS: è basata sul cloud. Ciò significa che non sono necessari controlli in sede che devono essere monitorati continuamente dall'IT. Inoltre, whitelist, blacklist e ACL vengono gestiti automaticamente. Infine, grazie alla mitigazione di più attacchi a livello di DNS, occorre gestire un minor numero di eventi di sicurezza tramite altri sistemi di sicurezza sulla rete.

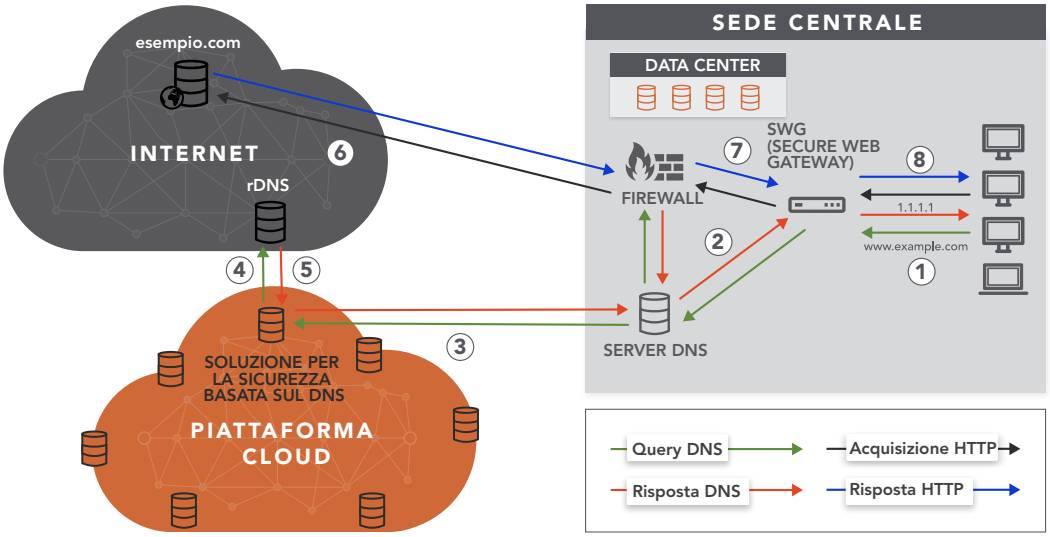
Una configurazione generica: livello di sicurezza basato sul DNS + Secure Web Gateway + firewall aziendale

Ora esaminiamo il modo in cui un'organizzazione può aderire a un modello di sicurezza aziendale su più livelli, in conformità ai concetti del modello "zero trust". Una configurazione generica implementata dalle aziende di grandi dimensioni è una soluzione per la sicurezza basata sul DNS con un Secure Web Gateway e un firewall aziendale. Ecco come funziona il flusso quando un utente effettua una richiesta di accesso a una risorsa esterna:

1. L'utente effettua una richiesta per esempio.com. La richiesta raggiunge il Secure Web Gateway.
2. Il sistema SWG controlla l'URL richiesto rispetto alla policy di filtraggio assegnata all'utente del dispositivo. Se l'URL non è consentito, la richiesta viene annullata e l'utente riceve una pagina di blocco. Se l'URL è consentito, il SWG invia la richiesta DNS al resolver DNS.
3. Il resolver DNS invia la richiesta DNS alla soluzione per la sicurezza basata sul DNS, che controlla il dominio rispetto alla policy configurata per la sede centrale. Se la richiesta è relativa a una risorsa interna, il resolver DNS risponde con l'indirizzo IP della risorsa interna.
4. Se il dominio è consentito nell'ambito della policy della soluzione per la sicurezza basata sul DNS, la richiesta viene inviata ai server DNS ricorsivi.
5. I server DNS rispondono con l'indirizzo IP del server in cui è ospitato esempio.com e l'indirizzo IP viene reinviato al dispositivo.
6. Il dispositivo effettua quindi la richiesta all'indirizzo IP della risorsa.
7. Il payload della risposta viene ricevuto dal SWG e il contenuto viene ispezionato dall'antivirus in linea.
8. La pagina web richiesta viene reinviata al dispositivo.

Di seguito, viene riportato un esempio del possibile aspetto di una configurazione aziendale.

LA SOLUZIONE PER LA SICUREZZA BASATA SUL DNS UTILIZZATA



È opportuno sottolineare che l'architettura complessiva è identica a quella precedente all'aggiunta di un livello di sicurezza al punto di gestione DNS. L'unica differenza consiste nel fatto che ora il resolver DNS è configurato per l'invio di richieste DNS di risorse esterne alla soluzione per la sicurezza DNS, il che rappresenta una modifica rapida e semplice da apportare per l'organizzazione IT.

Conclusione

La maggior parte dei professionisti IT concorderà sul fatto che è giunto il momento di adottare un modello zero trust per la sicurezza e che il solo modo per raggiungere questo obiettivo è costituito da un approccio alla sicurezza aziendale su più livelli. Poiché il DNS rappresenta un obiettivo attraente e facile da sfruttare per gli attacchi dannosi, è fondamentale utilizzare un livello di sicurezza basato sul DNS.

Le soluzioni per la sicurezza DNS di primo livello possono essere implementate in pochi minuti e offrono una protezione proattiva e continua da minacce in continua evoluzione. Integrano le soluzioni di sicurezza IT esistenti e offrono una serie di vantaggi che non solo proteggono meglio la vostra azienda dai criminali informatici, ma consentono anche di liberare risorse IT per concentrarsi su altre priorità fondamentali per l'azienda.

Per ulteriori informazioni sull'utilizzo del DNS come fondamentale punto di controllo della sicurezza, nonché sull'integrazione di una soluzione basata sul DNS con strategie di sicurezza aziendale su più livelli e di tipo "zero trust", visitate il sito www.akamai.com/etp.

FONTI

1) Jerry Shenk, *La sicurezza su più livelli: perché funziona* (SANS Institute, 2013), 2, 12.

2) Martha Bennett, *La sicurezza "zero trust": guida di un CIO alla difesa della propria azienda dagli attacchi informatici* (Forrester Research, 2017),

3) Bennett, *Sicurezza "zero trust"* 4.

4) "Gartner afferma che nel 2017 saranno in uso 8,4 miliardi di "oggetti" connessi, il 31 per cento in più rispetto al 2016", Gartner.com, 7 febbraio 2016, ultimo accesso 10 aprile 2018.

5) Ponemon Institute LLC, *White paper 2017, uno studio sulla sicurezza delle applicazioni mobili e IoT* (Arxan Technologies, 2017), 12.

6) Chase Cunningham, *Sviluppate la vostra strategia di sicurezza della forza lavoro "zero trust"* (Forrester Research, 2017), 5.

7) "NSS Labs prevede che il 75% del traffico web sarà crittografato entro il 2019", NSS Labs, 9 novembre 2016, ultimo accesso 22 marzo 2018.