

Chiudere il gap di protezione tra la rete e le applicazioni

Panoramica

Di fronte alla crescente maturità dei sistemi di difesa a livello di rete, gli autori degli attacchi sempre più spesso rivolgono la loro attenzione al livello applicazioni e alle corrispondenti applicazioni aziendali rese disponibili. Allo stesso tempo, le organizzazioni fanno sempre più affidamento su applicazioni Web, in particolare per soddisfare le esigenze del nuovo modello di impresa estesa, ovvero del crescente numero di utenti distribuiti. Questi vanno dai dipendenti dell'organizzazione (come collaboratori esterni e personale sul campo) a un'ampia varietà di partner (come outsourcer e componenti della supply chain), fino ai clienti, visti il successo e la continua crescita dell'e-commerce. Di fatto, con un aumento del 26% da un anno all'altro, l'e-commerce attualmente rappresenta il 2% di tutto il fatturato retail e molto probabilmente supererà il 10% entro la fine del decennio.

L'intersezione di queste varie tendenze indica chiaramente l'esigenza di implementare efficienti misure di protezione per le applicazioni Web. Non è sorprendente che il firewall per le applicazioni Web stia emergendo come un componente principale di queste misure di protezione. Tuttavia, anche se questa tecnologia è stata disponibile per diversi anni, fino a poco tempo fa la sua diffusione è stata relativamente lenta. Di conseguenza, non è molto chiaro quali siano le soluzioni più all'avanguardia dal punto di vista delle tecnologie e quali siano le best practice da seguire per l'implementazione. Lo scopo di questo documento è cercare di fare luce su questi problemi di grande importanza.

Nello specifico, le domande che verranno affrontate includono:

- Quando un firewall per le applicazioni Web può essere considerato appropriato?
- Quali sono i criteri più significativi per la scelta di un prodotto di questo tipo?
- Come dovrebbero essere implementati i firewall per le applicazioni Web?

Problema

Le statistiche relative alle vulnerabilità delle applicazioni Web offrono un buon esempio della crescente portata del problema:

- Dal primo trimestre del 2004 al primo trimestre del 2005 il numero di vulnerabilità specifiche delle applicazioni che sono state identificate è aumentato del 20% (SANS Institute).
- Oltre il 50% di tutte le nuove vulnerabilità identificate su base settimanale è attribuito ad applicazioni Web (SANS @RISK, "The Consensus Security Vulnerability Alert").
- Più dell'80% di tutto il malware diffuso nell'ultimo anno è basato sullo sfruttamento di vulnerabilità a livello di applicazioni (stima effettuata a partire da varie fonti).

Di fatto, la "cacofonia" dei dati e delle relative proiezioni sta iniziando in certo qual modo a stordire. Le informazioni sono anche difficili da assimilare perché nella maggior parte dei casi è molto complicato stabilire il grado di precisione dei loro presunti risultati. Nonostante questo, l'uniformità delle statistiche pubblicate è sufficiente per supportare un paio di conclusioni generali. In particolare, risulta sempre più chiaro: (1) che le applicazioni hanno la loro parte di punti deboli e (2) che le misure di sicurezza attualmente implementate non sono in grado di impedire in modo efficace lo sfruttamento di tali vulnerabilità.

La prima di queste conclusioni è piuttosto intuitiva e non merita ulteriori discussioni. Alla seconda, invece, è necessario dedicare particolare attenzione, soprattutto alla luce del fatto che numerosi produttori sostengono che i loro precedenti prodotti per la sicurezza delle reti ora forniscono anche protezione a livello di applicazioni. Per essere chiari, queste affermazioni non sono imprecise, ma un po' fuorvianti.

In senso stretto, i prodotti come firewall di rete e sistemi per la prevenzione delle intrusioni forniscono una protezione a livello di applicazioni, in genere imponendo un utilizzo conforme agli standard dei vari protocolli associati al livello applicazioni del modello di riferimento OSI (ad esempio, HTTP per il Web, SMTP per la posta elettronica, FTP per il trasferimento di file). Tuttavia, questo livello di funzionalità è di gran lunga insufficiente per prevenire i tipi di attacchi illustrati nel presente documento. Ad esempio, fa molto poco per proteggere il codice o la logica delle applicazioni di supporto (come server Web, sistemi di gestione dei database e server di directory) o delle applicazioni aziendali (come sistemi ERP, CRM o di online banking) che utilizzano effettivamente questi protocolli e servizi "a livello di applicazioni".

Per riassumere questo punto, le organizzazioni sono chiaramente a rischio a causa della presenza di numerose vulnerabilità specifiche delle applicazioni, della prevalenza degli attacchi ad esse associati e dell'incapacità di controllarli da parte delle misure di sicurezza attualmente implementate.

Che dire delle utilità di scansione delle vulnerabilità delle applicazioni Web? Proprio come i loro equivalenti di rete, le utilità di scansione delle vulnerabilità delle applicazioni sono utili strumenti complementari. Quanto meno, possono aiutare ad aumentare la consapevolezza del livello dei problemi di protezione delle applicazioni che un'organizzazione deve affrontare. Naturalmente, oltre a soddisfare questa esigenza di base, possono essere utilizzate per facilitare l'identificazione e l'eliminazione di un'ampia gamma di vulnerabilità. Tuttavia, è importante riconoscere che questi strumenti non saranno mai in grado di rilevare tutti i punti deboli e che di conseguenza le azioni correttive non saranno incluse nella soluzione. Inoltre, per alcune vulnerabilità la correzione potrebbe perfino non essere possibile o praticabile. Pertanto, anche se estremamente utile, un'utilità di scansione delle vulnerabilità delle applicazioni Web non deve essere considerata un sostituto di un firewall per le applicazioni Web, che di fatto è in grado di fornire protezione anche per le vulnerabilità non ancora scoperte o non risolvibili.

Soluzione

Una risposta adeguata: il firewall per le applicazioni Web

L'efficacia dei firewall per le applicazioni Web inizia dove quella delle tradizionali misure di sicurezza si ferma. Di fatto, è la capacità di tenere conto del codice e della logica delle applicazioni aziendali e di supporto che rende un firewall per applicazioni Web un dispositivo di controllo adeguato e complementare quando si tratta di aumentare la sicurezza delle applicazioni (almeno per il tipo di applicazioni oggi più diffuse: quelle Web).

Proprio come i firewall tradizionali, è opportuno che i firewall per applicazioni Web includano firme e altri meccanismi per prevenire gli attacchi noti. Tuttavia, questi modelli di protezione negativi non sono mai sufficientemente efficaci, poiché dipendono dall'attività (essenzialmente impossibile) di identificazione di tutto ciò che può andare male in una sessione di un'applicazione. Il risultato è un significativo carico di lavoro per la manutenzione e al tempo stesso una protezione molto scarsa dalle minacce "Day Zero".

Molto più efficace e pratico, e in ogni caso altamente complementare, è l'utilizzo di un modello di protezione positivo. Questo implica l'identificazione dell'universo finito delle interazioni consentite con un'applicazione e la negazione di tutte le attività che ricadono al di fuori di questo ambito. In questo caso, l'efficacia dipende dalla completezza e dal livello di dettaglio con cui vengono enumerate le interazioni consentite, il che praticamente dipende dalla capacità di eseguire questa operazione in modo automatico, o almeno con una modesta quantità di lavoro amministrativo. Queste sono quindi le caratteristiche a cui prestare maggiore attenzione quando un'organizzazione sceglie una soluzione firewall per le applicazioni Web, ovvero quanto è approfondita, accurata e automatizzata la generazione del modello di criteri.

È anche importante tenere presente che ogni applicazione da proteggere richiede uno specifico modello di criteri. Inoltre, il grado di profondità, precisione e automazione è influenzato dalle diverse tecnologie e dagli elementi di architettura utilizzati con le varie applicazioni. Ad esempio, non tutti i firewall per applicazioni Web sono in grado di tenere conto di codice JavaScript incorporato nel client o della generazione di contenuti dinamici sul server.

Di seguito sono riepilogate le principali funzionalità di protezione e gestione da valutare durante la scelta di un firewall per le applicazioni Web.

Protezione

- I filtri per gli attacchi (modello negativo) impediscono gli attacchi generalizzati (come i worm).
- Un modello di protezione positivo è focalizzato sulla prevenzione degli attacchi mirati, inclusi in via esemplificativa quelli basati su cross-site scripting, SQL injection, forceful browsing, cookie poisoning e input non validi. Idealmente, il firewall dovrebbe essere in grado di tenere conto di (a) codice/contenuti dinamici al livello sia client che server di un'applicazione, (b) stato e contesto della sessione dell'utente e (c) flussi di traffico bidirezionali.
- La protezione dei contenuti blocca la diffusione di dati riservati/sensibili, come numeri di carta di credito, informazioni sanitarie e numeri di previdenza sociale.
- Il mascheramento impedisce che informazioni potenzialmente utili sui sistemi (come tipo e stato di sistemi operativi e server Web o messaggi di errore dettagliati dei componenti) vengano esposte a utenti esterni. Collegati a questo sono l'utilizzo di un'architettura di proxy inverso e la capacità di mascherare i dati effettivi decrittando le sessioni in ingresso per l'ispezione ed eventualmente crittografandole di nuovo prima di inoltrarle ai server Web appropriati.

Gestione

- Una generazione approfondita e accurata dei criteri è necessaria per aumentare al massimo la capacità di bloccare gli attacchi reali, riducendo al tempo stesso la probabilità di bloccare sessioni legittime. Strumentale per il conseguimento di questo obiettivo è l'impiego di più tecniche di "rilevamento". Ad esempio, il "crawling" offline dell'applicazione, il monitoraggio (conoscenza) online delle interazioni e l'individuazione delle modifiche (aggiornamenti) alla base di codice sarebbero una potente combinazione di capacità, che consentirebbe una comprensione più approfondita e completa dell'applicazione rispetto a ciascuno di questi metodi preso singolarmente.
- Un editor grafico per i criteri rende più semplice per l'operatore conoscere e ottimizzare le regole generate automaticamente. Inoltre, livelli di protezione predefiniti corrispondenti a diversi gradi di sicurezza e livelli di dettaglio del modello di criteri sono utili per trovare il giusto equilibrio tra protezione, potenziali falsi positivi e carico di lavoro per l'operatore.
- La capacità dei sistemi virtuali e l'amministrazione in base ai ruoli consentono di partizionare efficacemente le istanze logiche del firewall per applicazioni Web e le funzioni di gestione correlate, per supportare la protezione di più applicazioni da una sola istanza fisica del prodotto.

Per tutti i suoi vantaggi, il firewall per applicazioni Web rappresenta una "risposta adeguata". In altre parole, è focalizzato sul superamento delle limitazioni delle misure di sicurezza tradizionali per quanto riguarda la protezione delle applicazioni Web. Tuttavia, quanto è efficace la protezione se le applicazioni protette non sono disponibili o funzionano tanto lentamente da sembrarlo? Il punto è che la protezione delle applicazioni di fatto fa parte del problema più ampio e articolato della fornitura delle applicazioni. Di conseguenza, una risposta ottimale dovrebbe risolvere contemporaneamente tutti e tre gli aspetti che compongono il problema, ovvero assicurare non solo la protezione delle applicazioni, ma anche la loro disponibilità e le prestazioni.

Alla ricerca di una risposta ottimale

Una volta definita l'esigenza di protezione delle applicazioni e la necessità di alcune delle sue funzionalità principali, è necessario identificare il punto migliore e le modalità in cui implementarle. Idealmente, questo dovrebbe essere fatto in modo tale da ridurre al minimo l'impatto sugli investimenti effettuati per l'infrastruttura esistente e il carico di lavoro di gestione risultante.

Non tutte le opzioni sono uguali

Una prima opzione è combinare funzionalità di protezione delle applicazioni direttamente nei dispositivi dell'infrastruttura di rete esistente, ad esempio i router che operano come gateway iniziali da Internet all'ambiente di elaborazione dell'organizzazione. Anche se sembrano i più adatti essendo il primo punto di ingresso, per gli altri aspetti questi dispositivi sono i meno appropriati per tale compito. Fondamentalmente, sono progettati per gestire pacchetti, determinandone rapidamente alcune caratteristiche di base e decidendo dove inviarli. In genere non dispongono di capacità di elaborazione o di intelligenza a livello di applicazioni. Né, in molti casi, rappresentano una buona posizione per il processo di decrittazione del traffico, che richiede un utilizzo intensivo delle risorse. Per il supporto di tutte queste funzioni, in definitiva renderebbe necessaria una completa riprogettazione del dispositivo di rete, cosa che comunque andrebbe a discapito della sua funzione principale: il routing.

Una seconda opzione è l'integrazione delle funzionalità di protezione necessarie direttamente nelle applicazioni. Senza dubbio, questo approccio dovrebbe essere perseguito, almeno a un certo grado. Eliminare le vulnerabilità alla radice implementando tecniche sicure di sviluppo del codice potenzialmente può avere grande efficacia. Tuttavia, vari problemi di ordine pratico rendono questo un obiettivo a lungo termine, oltre che un obiettivo che non può mai essere sufficiente, o può esserlo solo relativamente. Questi problemi includono:

- Rendere la sicurezza una priorità tra gli sviluppatori di applicazioni (sia interni che esterni), che da sempre si preoccupano solo delle funzionalità (e in qualche misura delle prestazioni), richiederà un cambiamento radicale a livello culturale, oltre a una notevole quantità di formazione.
- È molto improbabile che una maggiore protezione a livello di sviluppo possa influenzare le decine (o migliaia) di applicazioni che ogni organizzazione ha già implementato, in particolare quando le organizzazioni non dispongono dei diritti sul codice sorgente di molte di queste applicazioni.
- Gestire numerose funzionalità di protezione a livello di singola applicazione introduce problemi di complessità e scalabilità, molti dei quali possono essere ridotti sfruttando risorse centralizzate per questi servizi.

Infine, anche se gli elementi della protezione sono incorporati in ogni applicazione, come dovrebbero iniziare a essere, per aderire alle best practice sarà comunque necessaria una strategia di difesa a più livelli. In altre parole, sarà comunque consigliabile implementare un ulteriore sistema di protezione "consapevole delle applicazioni", per prevenire eventuali errori o elementi sottovalutati nel processo di sviluppo sicuro delle applicazioni.

Questo ci porta a una terza opzione per il posizionamento delle funzionalità necessarie per la protezione delle applicazioni: il firewall di rete. Questa posizione effettivamente ha dei vantaggi. La consapevolezza delle applicazioni può essere aggiunta in modo relativamente semplice, in particolare per il sottoinsieme dei prodotti firewall basati su un'architettura proxy per le applicazioni. Anche l'elaborazione SSL non rappresenta un traguardo irragionevole, in particolare se si considera il fatto che la maggior parte dei firewall già gestisce le intensive operazioni e le delicate funzioni di gestione delle chiavi associate alle VPN IPSec. Di fatto, il problema di questa opzione non ha tanto a che fare con la sua adeguatezza, quanto con la disponibilità di un'opzione ancora migliore.

Nello specifico, come accennato in precedenza, la fornitura delle applicazioni non riguarda solo la protezione, ma anche l'ottimizzazione e la garanzia della disponibilità delle applicazioni. Queste due ultime funzioni sono il dominio di quelli che nel settore vengono attualmente definiti Application Front-End (AFE). Gli AFE sono essenzialmente un'innovazione legata alla fusione dei dispositivi per il bilanciamento del carico dei server e di offload/accelerazione SSL. Senza entrare nei dettagli, incorporano un'ampia gamma di funzionalità per assicurare non solo che le sessioni delle applicazioni dispongano di un percorso praticabile tra il client e il server, ma anche che venga utilizzato il percorso ottimale (quando ne è disponibile più di uno) e che le sessioni stesse siano ottimizzate per ridurre sia la latenza che il carico per l'infrastruttura. Alcune delle tecnologie utilizzate includono: bilanciamento del carico dei server, failover con stato, compressione, caching, offload SSL e ottimizzazione di TCP.

Non a caso, gli AFE sono anche le piattaforme ideali per l'hosting delle funzionalità dei firewall per le applicazioni Web. Risiedono vicino alle applicazioni che rendono disponibili. Dispongono di una crescente consapevolezza delle applicazioni, in particolare con l'estensione delle tecniche di ottimizzazione e disponibilità nello stack. Eseguono già la decrittazione SSL, ed eventualmente la ri-crittografia, evitando che questa operazione venga effettuata altrove in modo ridondante. Inoltre, sono basati su architetture e hardware progettati per le prestazioni elevate, sia in termini di throughput che di latenza. Questa caratteristica è stata intenzionalmente omessa dal precedente elenco di criteri chiave, ma è chiaramente un'altra importante considerazione per la scelta di un firewall per le applicazioni Web. Infine, se le relative funzionalità vengono integrate correttamente, il risultato può essere un approccio unificato e semplificato alla gestione dei criteri, con caratteristiche di disponibilità, ottimizzazione e protezione, tutte gestibili contemporaneamente e "nel contesto" in base alla singola applicazione.

Senza dubbio è anche disponibile una quinta opzione. Di fatto, implementare un firewall standalone per le applicazioni Web può rivelarsi la scelta più appropriata, ad esempio se un'organizzazione ha già effettuato significativi investimenti in AFE o prodotti analoghi che non dispongono delle funzionalità associate.

Infrastruttura di servizi per le applicazioni

Che operino in modalità standalone o siano integrate in un singolo dispositivo, le funzionalità combinate offerte da AFE e firewall per le applicazioni Web possono essere definite "infrastruttura di servizi per le applicazioni". Con questa espressione intendiamo fare riferimento a un set centralizzato e completo di servizi di supporto che possono facilmente essere (ri)utilizzati per tutta la popolazione di applicazioni. Una soluzione di questo tipo essenzialmente permette a tutte le applicazioni (non solo a quelle Web) di effettuare sottoscrizioni ai servizi disponibili e che ne migliorano la condizione. Si può prevedere che nel tempo la gamma di servizi disponibili si espanderà, ad esempio per includere una maggiore copertura di protezione per le applicazioni Web, ulteriori tecniche di ottimizzazione o servizi specifici per particolari tecnologie o tipi di applicazioni, come Web service o VoIP.

Conclusioni

Complessivamente, il valore di un'infrastruttura di servizi per le applicazioni è la capacità di offrire tutti i vantaggi di applicazioni più sicure e con prestazioni superiori, in modo efficiente ed economico. I cicli di sviluppo e deployment delle applicazioni possono essere abbreviati grazie al fatto di sfruttare funzionalità di protezione esterne. L'infrastruttura complessiva di rete e dei sistemi viene notevolmente semplificata grazie al consolidamento dei servizi correlati. Inoltre, le attività di gestione operativa si riducono poiché vengono utilizzati meno dispositivi ed è disponibile un sistema integrato per le funzioni di gestione, risoluzione dei problemi e controllo dei criteri. In breve, l'implementazione di un'infrastruttura di servizi per le applicazioni rappresenta la risposta ottimale per risolvere i problemi di fornitura delle applicazioni che le organizzazioni di oggi devono affrontare. Non solo permette di superare gli attuali rischi di una protezione inadeguata delle applicazioni, ma consente anche di soddisfare i requisiti complementari relativi alla disponibilità e all'ottimizzazione delle applicazioni.



INFORMAZIONI SULL'AUTORE

Mark Bouchard, CISSP, è un consulente indipendente che si occupa di strategie di protezione delle informazioni e di gestione dei rischi. In precedenza, per quasi 10 anni ha lavorato come analista di settore, esaminando le tendenze tecnologiche e di business relative a un'ampia varietà di aspetti della protezione delle informazioni. Ha una reputazione di grande capacità di leadership e sono molto apprezzati i suoi interventi nelle aree delle architetture di protezione, progettazione di DMZ, protezione dell'accesso remoto, protezione delle reti e tecnologie correlate, come firewall, sistemi per la prevenzione delle intrusioni e VPN.

Si dedica con entusiasmo ad aiutare le organizzazioni a superare i problemi legati alla protezione delle informazioni. Durante la sua carriera, ha assistito centinaia di organizzazioni di tutto il mondo in tutti gli aspetti relativi alla sicurezza, dalle iniziative strategiche (come la creazione di piani quinquennali e delle architetture di protezione correlate) alle decisioni tattiche su giustificazione, selezione, acquisizione, implementazione e utilizzo di singole tecnologie e prodotti. Collabora inoltre regolarmente con sviluppatori e rivenditori di soluzioni per la protezione delle informazioni, per aiutarli a comprendere e soddisfare meglio le esigenze del mercato.

Informazioni su F5

F5 Networks è il leader globale nel settore dell'Application Delivery Networking. F5 offre soluzioni che rendono le applicazioni sicure, rapide e altamente disponibili, aiutando le organizzazioni a trarre il massimo vantaggio dai propri investimenti. Integrando nella rete avanzate funzionalità di gestione per ridurre il carico delle applicazioni, F5 ottimizza le applicazioni, ne aumenta la velocità e consente loro di utilizzare meno risorse. L'architettura estendibile di F5 integra in modo intelligente funzionalità di ottimizzazione, protezione delle applicazioni e della rete e caratteristiche per la disponibilità, il tutto in una singola piattaforma universale. Oltre 9000 organizzazioni e service provider di tutto il mondo si affidano a F5 per la costante operatività delle proprie applicazioni. L'azienda ha sede a Seattle, nello stato di Washington, e dispone di filiali in tutto il mondo. Per ulteriori informazioni, visitare www.f5.com.