Panoramica della tecnologia Intrusion Detection and Prevention

IPS di Kerio Control

Kerio Control, una soluzione per la gestione unificata delle minacce (Unified Threat Management), comprende un'architettura di analisi dei pacchetti basata su firma, conosciuta come Intrusion Detection and Prevention (IPS). Tale architettura controlla in modo trasparente le comunicazioni di rete in entrata e in uscita per identificare eventuali attività sospette. A seconda della gravità dell'attività, Kerio Control è in grado di registrare e bloccare la comunicazione. Le nuove firme vengono periodicamente aggiunte al database delle regole per prevenire le minacce emergenti.

Tale sistema è progettato per impedire connessioni non autorizzate ai server protetti da firewall, in genere originate da un Internet bot o da un hacker nel tentativo di sfruttare un servizio disponibile, ed è inoltre pensato per proteggere gli utenti della rete dal download inconsapevole di contenuti pericolosi o malware o, quanto meno, per attenuarne gli effetti in un sistema compromesso.

Protezione del server

In numerose installazioni i server si trovano dietro il firewall e solo i servizi in hosting possono ricevere connessioni. In base al tipo di servizio in hosting (ad esempio, un server SQL), il firewall potrebbe non essere in grado di controllare la conversazione reale tra client e server. Il firewall ha principalmente il compito di stabilire la connessione, senza consentire alcun altro tipo di accesso backdoor ad altri servizi disponibili sul server. Tuttavia, questo tipo di configurazione non protegge dalla potenziale minaccia di richieste o comandi che sfruttano una vulnerabilità nel software server.

Probabilmente l'episodio più noto di questo tipo di attacco si è verificato nel 2001, quando è stato sviluppato un worm per attaccare i sistemi dotati del software del server Web Microsoft IIS (Internet and Information Server). Denominato "Code Red", il worm era stato programmato per inviare una serie di comandi mediante il servizio HTTP che avrebbe causato un overflow del buffer nello spazio della memoria del software server. Ciò ha consentito all'autore dell'attacco l'introduzione e l'esecuzione di codice arbitrario sul server. Una caratteristica di questo codice consisteva nella capacità di diffondersi rapidamente interessando altri server dotati di software Microsoft IIS. Questo particolare caso si è concluso con un attacco di tipo Denial of Service nel server interessato.

Aggiunta del livello di protezione IPS

Per proteggere le applicazioni server da questo tipo di minaccia, è essenziale mantenere il software server aggiornato. I fornitori di applicazioni aggiornano periodicamente il software per correggere le eventuali vulnerabilità a livello di protezione. Tuttavia, in alcuni casi risulta impossibile aggiornare il software alla versione più recente o disporre immediatamente di una soluzione in grado di scongiurare una minaccia emergente. L'aggiunta di Intrusion Prevention System garantisce un ulteriore livello di protezione contro minacce quali il worm Code Red.

IPS si serve di un database di firme locale per identificare i tipi di attacco noti. Senza interpretare la comunicazione tra client e server, un sistema IPS è in grado di generare una firma della connessione di rete e ricercare tale firma nel database locale. Un tipo di architettura di questo genere è estremamente efficace nel combattere eventuali minacce di worm o altri attacchi al server.

Altri tipi di minacce comprendono il rilevamento delle password, noto anche come attacco di forza bruta, attacchi Distributed Denial of Service, Port scan o hijack delle sessioni. Attacchi del genere prevedono generalmente il tentativo di ottenere informazioni sul software server, ad esempio su versione e sviluppatore. Mediante tali informazioni, l'autore dell'attacco può individuare le vulnerabilità presenti nel software server e cercare di ottenere l'accesso non autorizzato al sistema o eseguire operazioni pericolose per impedire al server di funzionare correttamente. In tutti questi casi, IPS avvisa l'amministratore della presenza di attività sospette e blocca ogni comunicazione se ritenuta pericolosa per i server protetti da firewall.

Attenuazione degli effetti di trojan, worm, spyware e altri tipi di malware

Oltre allo sfruttamento dei servizi disponibili delle applicazioni vulnerabili, esistono altri modi per sfruttare un sistema operativo. Una delle strategie più comuni utilizzate dai malintenzionati consiste nell'applicare un piggyback su applicazioni software gratuite. L'utente viene indotto a installare malware attraverso l'installazione di un'altra applicazione oppure viene incoraggiato a effettuare l'accesso a un sito Web su cui è in esecuzione uno script lato client per installare il malware. Applicazioni di questo tipo non sono visibili all'utente, ma possono essere programmate per rilevare informazioni aziendali sensibili sul computer interessato. Inoltre, sono in grado di ridurre le prestazioni del computer o impedire l'esecuzione di altre applicazioni. Poiché apparentemente questi programmi risultano installati legittimamente, non vengono rilevati dal software antivirus.

L'architettura IPS consente di individuare i sistemi interessati da questo tipo di applicazioni e riconosce quando l'utente sta inavvertitamente cercando di scaricare un'applicazione non desiderata. A questo punto è in grado di intervenire interrompendo la connessione e impedendo così al file di raggiungere il computer dell'utente. Anche nell'ipotesi in cui un computer precedentemente infetto si trovi in rete, è possibile identificare e bloccare l'attività del malware installato. Pertanto, l'utilizzo dell'IPS di Kerio Control insieme al firewall e alle capacità di filtraggio dei contenuti contribuisce a impedire la diffusione di malware in rete.

Architettura

(1) Posizione. Generalmente, un sistema di individuazione delle intrusioni si trova a livello della rete che riceve la trasmissione di tutte le attività ad essa correlate. IPS **deve essere posizionato in un router gateway o un firewall**, che provvede al trasporto del traffico IP tra i diversi segmenti di rete e Internet. In quanto firewall perimetrale, Kerio Control implementa la prevenzione delle intrusioni "basata su rete". In altre parole, il traffico gestito dal firewall tra le reti protette e Internet verrà protetto dal sistema IPS di Kerio Control.

(2) Analisi dei pacchetti. Alla base della tecnologia di scansione di Kerio Control c'è un analizzatore di pacchetti basato su **Snort**. Snort è un sistema IDS/IPS open source che analizza in modo trasparente tutte le comunicazioni di rete e fornisce un framework per l'integrazione di regole personalizzate. Ulteriori informazioni sono disponibili sul sito Web www.snort.org.

(3) Database. Kerio Control applica un insieme di regole gestite nell'ambito di un progetto promosso dalla comunità sulle minacce emergenti, denominato **Emerging Threats**. Ciascuna regola è provvista di firma digitale per assicurare l'autenticità degli aggiornamenti e prevenire qualsiasi tipo di manomissione. Tali regole sono frutto di innumerevoli anni di contributi da parte dei professionisti del settore e vengono costantemente aggiornate. Ulteriori informazioni sono disponibili sul sito Web www.emergingthreats.net.

IPS di Kerio Control propone tre diversi tipi di operazione, a seconda del livello di gravità del potenziale attacco:

- Bassa gravità: (nessuna operazione)
- Media gravità: (solo registrazione)
- Alta gravità: (registrazione e rimozione)

Si tratta di impostazioni predefinite, ma le operazioni possono essere adattate in base alle esigenze dell'organizzazione. Il livello di gravità si basa su criteri stabiliti nelle regole. Le regole di eventi ad alta gravità corrispondono a una maggiore probabilità di attacco effettivo in rete. L'individuazione di attività di rete da parte di un'applicazione trojan potrebbe costituirne un esempio. Gli eventi di categoria media si definiscono sospetti e potenzialmente dannosi, ma esiste una possibilità che si tratti di attività legittime, ad esempio una connessione a una porta standard mediante un protocollo non standard. Un'attività che non causa danni immediati, come una scansione delle porte di rete, potrebbe considerarsi una minaccia di bassa gravità.

Inserimento di indirizzi IP nelle liste nere

Oltre a un database di regole provvisto di firme per il comportamento in rete, Kerio Control dispone di un database di indirizzi IP, ai quali viene negato qualsiasi tipo di accesso mediante firewall. Gli indirizzi IP inclusi nel database si ritengono l'origine di una qualche forma di attacco. In molto casi, tali indirizzi sono stati attribuiti ad aziende legittime ma sono stati in seguito utilizzati per attività illecite, ad esempio per la distribuzione di spam. Il database di indirizzi IP viene utilizzato da diverse fonti Internet e gestito da organizzazioni come Dshield e Spamhaus. Tali liste vengono archiviate in locale e aggiornate automaticamente.

Falsi positivi ed eccezioni

La tecnologia Intrusion Detection and Prevention non è infallibile. Come avviene con l'anti-spam, è normale che esista un'esigua percentuale di falsi positivi. In altre parole, è possibile scambiare una comunicazione di rete legittima per una comunicazione pericolosa perché corrisponde a firme di attività sospette. Per questo motivo, è necessario fornire un semplice metodo per individuare le opportune eccezioni del database di firme.

Come ottimizzare IPS

(1) Analisi del registro di protezione. Qualsiasi comunicazione bloccata dal motore IPS viene inserita nel registro di protezione, che contiene i dettagli di ogni evento, compreso "l'ID della regola". Se un utente segnala un problema di connessione in una particolare applicazione che si serve di un protocollo legittimo, è opportuno controllare il registro di protezione per scoprire se si tratta di un'intrusione effettiva o meno.

(2) Verifica dell'integrità dell'applicazione. Se ISP ha bloccato la comunicazione di un'applicazione, sarà necessario analizzare tale applicazione per assicurarsi che non sia compromessa e verificarne il normale comportamento.

(3) Creazione di eccezioni. Se esiste un'eccezione al database di firme, l'ID della regola ottenuto dall'evento di registro può essere aggiunto alla finestra di dialogo relativa alle firme ignorate disponibile nelle impostazioni avanzate dell'interfaccia di gestione di IPS.

Gestione degli aggiornamenti

Come accade per i virus, ogni giorno vengono identificate nuove minacce. Pertanto, è necessario provvedere periodicamente all'aggiornamento del database di firme. Il sistema IPS di Kerio Control verifica la presenza di aggiornamenti una volta al giorno, ma può anche essere impostato per farlo ogni ora.

L'ambiente della comunità emergingthreats.net offre costantemente il proprio contributo aggiungendo nuove regole o firme. Kerio provvede alla manutenzione continua delle firme e incoraggia gli amministratori a utilizzare IPS di Kerio Control per partecipare allo sforzo comune volto a identificare i nuovi attacchi e contribuire allo sviluppo di nuove regole. Ulteriori informazioni sono disponibili sul sito Web www.emergingthreats.net

Regole IPS correlate

L'approfondito controllo integrato dei pacchetti di Kerio Control apporta un ulteriore livello di difesa attraverso il controllo trasparente di protocolli specifici per assicurare che la comunicazione non violi alcuna specifica. I contenuti pericolosi che il database di firme potrebbe non riconoscere vengono filtrati. Oltre alle liste nere e ai database di firme, Kerio Control dispone di diverse funzioni automatiche in grado di potenziare le capacità di prevenzione delle intrusioni:

- Blocco peer-to-peer. Quando disattivato, il firewall controllerà la connessione ad alcune porte per identificare e bloccare l'attività di applicazioni P2P note, che contribuiscono notevolmente alla diffusione del malware.
- Blocco di dati binari illeciti nelle connessioni HTTP. Come parte del controllo dei pacchetti, il firewall impedirà l'utilizzo illecito dei dati binari nelle connessioni HTTP.
- Filtraggio della vulnerabilità GDI+JPEG. Un file immagine JPEG appositamente creato può causare un overflow del buffer in sistemi operativi Windows senza patch, consentendo l'esecuzione di codice arbitrario (MS04-028). Kerio Control identifica e blocca il trasferimento di questo specifico file mediante protocolli e-mail e Web.
- Test di laboratorio costanti per la certificazione ICSA. In conformità con la certificazione di laboratorio ICSA (International Computer Security Association), Kerio Control deve costantemente superare un certo numero di controlli di sicurezza, ad esempio per attacchi TCP SYN Flood, FTP Bounce, Man-in-the-middle e altre minacce simili.

Riepilogo

Intrusion Detection and Prevention è una tecnologia altamente sofisticata, basata su un vasto insieme di regole differenti. Ogni rete è unica, dunque una cosiddetta "intrusione" può essere soggetta a interpretazione. Il sistema IPS di Kerio Control è ideato per identificare e bloccare eventuali attacchi nel modo più efficace possibile, garantendo al contempo un livello ottimale di prestazioni di rete.

Brian Carmichael, Sales Engineer, Kerio Technologies Inc.

Pubblicato ad aprile 2010.