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.