STORMSHIELD

INTRUSIONSSCHUTZ (IPS)

Funktionsumfang

IT-SICHERHEIT

Die Nutzung des Internets entwickelt sich in rasantem Tempo weiter. Noch vor kurzem beschränkte sich der Datenverkehr auf den Austausch von Multimediainhalten. Inzwischen geht es um das Hosting gewaltiger Mengen von Anwendungsdaten und interaktiven Inhalten.

Datentransaktionen werden immer komplexer, und der Einsatz einer einfachen Firewall reicht nicht mehr aus, um Bedrohungen aus dem Datenverkehr erfolgreich zu blocken. Die modernen Bedrohungen werden immer komplizierter und sind inzwischen speziell dafür ausgelegt, traditionelle Schutzmechanismen wie Signaturdatenbanken gezielt zu umgehen.

Für eine erfolgreiche Erkennung und Blockierung dieser Bedrohungen bedarf es neuester Sicherheitstechnologien, die anormalen Verhaltensmuster identifizieren können.

Intrusionsschutz (IPS)

Die meisten Angriffe nutzen Webseiten oder zugelassene Dienste wie E-Mail, Instant Messaging oder IP-Telefonie. Nun verfügt jede dieser Anwendungen über ein eigenes Kommunikationsprotokoll.

Diese Protokolle müssen sorgfältig analysiert werden, damit die Angriffe ohne Beeinträchtigung des täglichen Geschäfts des Unternehmens abgewehrt werden können. Wesentliche Kriterien bei der Bewertung von Intrusionsschutztechnologien sind die Wirksamkeit der Überprüfung und die Qualität der Erkennung von Gefährdungen.

Für eine optimale Wirksamkeit sollte der Intrusionsschutz in andere Technologien integriert werden. Die Einbindung in eine Firewall-Anwendung, die Identifizierung von Benutzern oder auch die Analyse von Schwachstellen kann die Wirksamkeit des Intrusionsschutzes zusätzlich erhöhen. Das IPS-System bildet somit das Herzstück einer multifunktionalen Firewall, die an den Segmentierungspunkten des Netzwerkes installiert ist. Sie kann auch im Transparentmodus ausgeführt werden, wenn die vorhandene Netzwerkinfrastruktur unverändert bleiben soll.

Das IPS-System von Stormshield ist das Ergebnis aus 10 Jahren Forschung. Es kombiniert verschiedene Technologien zur Analyse von Verhaltensmustern und Protokollen und ermöglicht dadurch die Erkennung und Blockierung der meisten Angriffe noch vor deren Veröffentichung (Zero-Day-Schutz).

Die Signaturlisten des IPS-Systems von Stormshield Network Security werden automatisch aktualisiert. Das Sicherheitsteam von Stormshield nimmt in die Listen täglich viele neue Signaturen auf. Stormshield Network Security sorgt mit seinen hocheffizienten Schutztechnologien dafür, dass jede neue Sicherheitslücke umgehend geschlossen wird.

Die marktführende Effizienz des IPS-Systems spiegelt sich in den Leistungsdaten aller Produkte von Stormshield Network Security wider. Durch die Kombination der verschiedenen Stormshield Network Security-Technologien finden Sie für jede Art von Angriff den geeigneten Schutz. Somit sind Sie nicht mehr allein von der Signaturdatenbank abhängig.

Dies garantiert Ihnen ein Höchstmaß an Sicherheit für alle Anforderungen. Standardmäßig sind alle Stormshield Network Security-Anwendungen mit der IPS-Funktion ausgestattet. Abhängig von der Art des Datenflusses wird im Sinne des maximalen Sicherheitsniveaus automatisch das am besten geeignete Konfigurationsprofil ausgewählt.

Der Intrusionsschutz, der innerhalb des gleichen Betriebssystems wie Stormshield Network Security entwickelt wurde, analysiert diese verschiedenen Datenflüsse in Echtzeit. Dank dieser engen Integration wird jedes kostspielige Kopieren oder Übertragen von Daten innerhalb der Anwendung überflüssig. Diese leistungsoptimierte Architektur ist besonders effizient bei sehr hohen Datenübertragungsraten oder wenn Latenzzeiten vermieden werden sollen (z. B. bei VoIP-Anwendungen).

Zero-Day-Schutz

Mit dem Zero-Day-Schutz ist Ihr Unternehmen jederzeit gegen mögliche Angriffe gewappnet. Der Schutz ist auch dann aktiv, wenn Sicherheitslücken bereits vor der Veröffentlichung der Schwachstellen ausgenutzt werden. Der Zero-Day-Schutz zielt immer auf ein anormales Verhaltensmuster ab. Die Schutzmechanismen werden häufig aktualisiert, damit neue Bedrohungen stets effektiv erkannt werden.

IT-Sicherheit gilt als ein Wettlauf gegen die Zeit, bei dem der Angreifer dem Verteidiger häufig einen Schritt voraus ist. Bestimmte Angriffe, auch Zero-Day-Exploits genannt, verbreiten sich bereits vor ihrer Veröffentlichung. Hacker nutzen diese Schwachstellen, noch bevor die Softwareunternehmen oder die Öffentlichkeit davon in Kenntnis gesetzt werden.

Schutzsignaturen werden nach Bekanntwerden einer neuen Bedrohung stets so schnell wie möglich erstellt und bereitgestellt. Diese Vorgehensweise hat sich als sehr effizient erwiesen, da ein Software-Bugfix nicht selten mehrere Tage oder gar Wochen auf sich warten lassen kann. Aber selbst wenn eine Schwachstelle nur kurze Zeit vorhanden ist, handelt es sich um eine reale Bedrohung. Die für IT-Sicherheit zuständigen Mitarbeiter sind permanent auf der Suche nach effizientem Zero-Day-Schutz, um die gleichnamigen Bedrohungen erfolgreich abzuwehren.

Die Intrusionsschutzfunktion von Stormshield Network Security wurde speziell für den maximalen Schutz vor Zero-Day-Angriffen konzipiert. Die Schutzmechanismen verfügen über verschiedene Technologien, die sich gegenseitig ergänzen:

- Protokollüberprüfung
- Erkennung anormaler Verhaltensmuster
- Erkennung versteckter interaktiver Verbindungen (z. B. C&C Botnet)
- Proaktive Erstellung kontextabhängiger Schutzsignaturen

Mit diesen vier Analysetypen ist Ihr Unternehmen noch vor Bekanntwerden einer Schwachstelle effizient geschützt. Die Überwachung der Protokolle bildet das Fundament des Zero-Day-Schutzes von Stormshield Network Security.

Das Sicherheitsteam von Stormshield Network Security ergänzt jedes Protokoll kontinuier-

lich durch neue Überwachungsalgorithmen und reagiert somit vorausschauend auf potenzielle Schwachstellen. So gibt es für das Sprachprotokoll SIP bereits mehrere Stufen für den Schutz gegen Identitätsbetrug und DoS-Angriffe (Denial-of-Service). Diese Analysen können bei allen Anwendungen effizient eingesetzt werden.

VoIP und CoIP

Die Nutzung der IP-Telefonie hat in den letzten Jahren deutlich zugenommen. Die inzwischen marktreife und deutlich kostengünstigere Technologie ermöglicht konvergente Sprach- und Datenübertragungen.

- Mit dem Telefonsystem können die Daten künftig über das Netz übertragen und somit die vorhandenen Ressourcen besser genutzt werden.
- Das Netz ermöglicht dabei gleichzeitig die Verwaltung des Telefonsystems und die Übertragung der Sprachdaten.

Diese Entwicklungen werden aber auch von immer mehr Angriffen begleitet, die es auf Schwachstellen in Bezug auf zwei Technologien abgesehen haben. Die Schwachstellen der IP-Netzwerke und -Sprachprotokolle können durch DoS-Angriffe sowohl auf Anwendungs- als auch auf Protokollebene ausgenutzt werden.

Identitätsbetrug und die illegale Aufzeichnung von Telefongesprächen sind Angriffsstrategien, die den boshaften Zugriff auf Daten erleichtert. Durch die Einschleusung von SQL-Code können Unbefugte an vertrauliche Daten gelangen. Ein zuverlässiges Sicherheitssystem wird daher in Zukunft für jedes Unternehmen, das seine Telefonsysteme und Netze hinreichend schützen will, unerlässlich sein.

Mit den Schutzlösungen von Stormshield Network Security garantieren wir unseren Kunden die Sicherheit ihrer Netzressourcen und insbesondere ihrer IP-Telefonsysteme. Mit den modernen Funktionen dieser Lösungen sind Unternehmen in der Lage, in Echtzeit auf neue Datenanforderungen und alle Aspekte der Sprach-Daten-Konvergenz flexibel zu reagieren.

LEISTUNGSFÄHIGKEIT EINES IP-TELEFONSYSTEMS MIT ECHTZEITÜBERTRAGUNG

Damit die Sicherheit nicht zu lasten der Leistungsfähigkeit geht, ist der Intrusionsschutz in allen Stormshield Network Security-Standardanwendungen standardmäßig aktiviert. Durch die Konfiguration und Verwaltung der Dienstgüteparameter kann zudem auf alle Latenz- und Jitterprobleme angemessen reagiert werden.

IP-TELEFONIE

Die Anfälligkeit der IP-Telefoniesysteme stellt ein hohes Sicherheitsrisiko dar. DoS-Angriffe, Remotecodeausführung oder die illegale Beschaffung sensibler Daten sind nur einige Beispiele für mögliche Schwachstellen. Die Stormshield Network Security-Lösungen verfügen über einen Risikomanagementdienst (Stormshield Network Vulnerability Manager),

der regelmäßig Berichte ausgibt, die Geräte auf Schwachstellen untersucht und geeignete Korrekturen vorschlägt. Auf dieser Grundlage können Sie Maßnahmen ergreifen und die Sicherheitsrisiken in Ihrem IP-Telefonsystem effektiv steuern. Mit nur einem Mausklick können Sie Sicherheitsrichtlinien festlegen und entsprechende Filter für die gefährdeten Geräte setzen.

ÜBER STORMSHIELD

Arkoon und Netasq, 100%ige Töchter von Airbus Defence and Space CyberSecurity, vertreiben unter der Marke Stormshield innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Arbeitsplatzgeräten (Stormshield Endpoint Security) sowie Daten (Stormshield Data Security).

STORMSHIELD

N°Cristal 09 69 32 96 29
APPEL NON SURTAXE

WWW.STORMSHIELD.EU

Netasq
Parc Scientifique Haute Borne - Parc Horizon, Bat 6, Avenue de l'Horizon 59650 Villeneuve d'Ascq