Keine Angst vor «Modern Malware»

Gezielte, hoch spezialisierte Angriffe erfordern neue Sicherheitsdispositive

Dank der Verknüpfung von «Next Generation Firewall»-Funktionen, Code-Analysen in der «Sandbox» (Wild-Fire) sowie zeitnahen Signatur-Updates bietet Palo Alto Networks ein wirksames Dispositiv gegen Schadcode jeder Art – selbst in unbekannten Anwendungen.

Durch das Zusammenspiel der «Next Generation Firewall» von Palo Alto Networks mit Technologien wie Cloud-basierte Malware-Analyse und «Sandboxing» wird die IT- und Netzwerksicherheit entscheidend maximiert.

Im Bereich der IT-Security ist ein folgenreicher Paradigmenwechsel feststellbar. Zeichneten sich frühere Angriffe u. a. durch eine möglichst breite Streuung von Viren, Trojanern und unspezifischen Attacken auf Server und Datacenter aus, sind moderne Angriffe wesentlich gezielter. Sie dienen beispielsweise der Werkspionage oder verfolgen Ziele wie die Aushebelung von Verschlüsselungssystemen und Zertifikaten, Angriffe auf Finanz-Applikationen (z. B. E-Banking), Datenklau im grossen Stil, Attacken auf staatliche Stellen und wichtige Infrastrukturen oder Zerstörung von Industrieanlageteilen.

Das Einschleusen eines Schädlings – z. B. über Web2.0-Anwendungen und «Social Engineering»-Strategien – ist ein typischer Startpunkt für «Modern Malware». Dieser nistet sich unerkannt im Zielsystem ein und macht es verletzbar (Exploit Vulnerability). Um das kompromittierte System unter die Kontrolle des Angreifers zu bringen, veranlasst der Schadcode in der Regel den Download eines Backdoor-Programms, das seinerseits einen unerkannten Kommunikationskanal nach aussen etabliert. Dieser ermöglicht sowohl die Kommunikation mit anderen verseuchten Plattformen als auch die Remote-Steuerung des befallenen Rechners durch den Hacker. So lassen sich spielend DDoS-Attacken reiten, Passwörter abfangen, Daten entwenden, elektronische Systeme wie industrielle Steuerungen (zer)stören.

Gefahren erkennen – bevor sie wirken

Konventionelle Firewalls sind Bedrohungsformen dieser Art nicht mehr gewachsen. Denn: Die vermehrte Nutzung Web-basierter Anwendungen wie Facebook, Twitter oder Skype, die vermehrte Nutzung von Cloud- und Virtualisierungs-Technologien sowie die zunehmend mobile Arbeitsweise führen dazu, dass sich einzelne User nicht mehr klar definierten IP-Adressen zuordnen lassen. Zudem wird der Schadcode nicht zwingend als solcher erkannt und kann sein Gesicht im Laufe der Zeit verändern. Um Herausforderungen dieser Art wirksam zu begegnen, verbindet Palo Alto Networks zwei zentrale Security-Mechanismen zu einer integralen Gesamtlösung:

Kontrolle von Anwendungen, Usern und Inhalten

Mit ihren «Next Generation Firewalls» setzt Palo Alto Networks auf die Identifikation und Kontrolle von Anwendungen, Benutzern und Inhalten. Dabei werden User unabhängig von IP-Adressen und Applikationen, von Port, Protokoll, Verschlüsselung oder Verschleierungsmethoden erkannt. Ebenso lassen sich bekannte Anwendungen und die daraus entstehenden Gefährdungen einfach identifizieren, transparent darstellen und gegebenenfalls blockieren. Zudem lässt sich granular definieren, welche Anwendungen und Zugriffe für welche User und Anwendergruppen freigegeben beziehungsweise gesperrt sind.

Analyse unbekannter Dateien

Um sicherzugehen, dass auch nicht bekannte Daten «clean» sind, bietet Palo Alto Networks mit WildFire einen entsprechenden Cloud-Service an. Identifiziert das System eine unbekannte Datei, kann diese automatisch in eine virtuelle, Cloud-basierte Umgebung verlagert werden, wo sie auf Malware-Merkmale und bekannte Signaturen untersucht wird. Zudem wird der Code in einer «Sandbox» ausgeführt. Diese abgeschottete Umgebung bildet einen perfekten «Nährboden» für weitreichende Code-Analysen im sicheren Labor. Auf Basis entsprechender Erkenntnisse erstellt Palo Alto Networks neue Signaturen und übermittelt diese an die «Next Generation Firewall». Dadurch verringert sich die «Time to Protection» für registrierte Kunden markant.

Kontakt

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Telefon 056 437 60 60
info@boll.ch
www.boll.ch