Neue Sicherheitsansätze gegen Hacker-Angriffe

Angriffe aus der Kategorie «Advanced Persistent Threats» (APTs) und Distributed Denial of Service (DDoS) Attacken machen Unternehmen anfälliger. Der herkömmliche Perimeter-Schutz stösst dabei an seine Grenzen.

Online-Anwendungen und Web-Seiten sind die häufigsten Angriffsziele von Hackern und bergen ein grösstes Gefahrenpotenzial. So ist es nicht erstaunlich, dass immer mehr Unternehmen mit der steigenden Anzahl von Cyber-Angriffen und der immer professionelleren Vorgehensweise der Hacker zu kämpfen haben. Dies widerspiegelt sich auch in einem Forschungsbericht des Ponemon Institutes «Effizienz neuer Netzwerksicherheitsinfrastrukturen». Dabei wurden web-basierte Angriffe mit 62 Prozent und Denial of Service-Attacken (60 Prozent) als die schwerwiegendsten Arten von Angriffen eingestuft. Traditionelle Web Application Firewalls stossen hier zusehends an ihre Grenzen. Denn um Angriffe erkennen zu können, sind sie von einer ganzen Sammlung an Signaturen abhängig, was sie anfällig für unbekannte (Zero-Day) Angriffe macht.

Im vergangenen Jahr wurde ein Schweizer Unternehmen Opfer des bislang grössten DDoS-Angriffs hierzulande.

Spotlight auf den Angreifer

Trotz erheblicher Investitionen in Sicherheitslösungen sehen Unternehmen gerade bei den genannten DDoS- und Zero-Day-Angriffen noch immer Lücken in der IT-Sicherheit und der Wirksamkeit der eingesetzten Lösungen. Der Grund ist einfach. Traditionelle Abwehrkräfte verlassen sich mehrheitlich auf Signaturen bekannter Angriffsmuster und IP-Adressen von bekannten Hackern. Signaturen, verwendet in Antivirus-und Intrusion Prevention-Systemen (IPS), sind aber nur wirksam bei der Erkennung bekannter Angriffe. Sie sind jedoch nicht wirksam, wenn es um die Erkennung neuer Angriffe oder zum Aufspüren von Hackern geht, wenn diese sich noch in der Aufklärungs-Phase befinden.

IP-Reputations-Datenbanken basieren auf der Vorstellung, dass alle Hacker durch ihre IP-Adressen identifiziert werden können und teilen diese Informationen über Systeme hinweg. Leider ist dies eine ineffektive Methode, denn für eine zuverlässige Identifikation einer Person werden viel mehr Attribute benötigt. Denn die meisten Internet-Benutzer befinden sich in einer einzigen Struktur oder hinter einer einzigen IP-Adresse.

Wenn man nun eine IP-Adresse blockiert, trifft dies alle Mitarbeitenden eines Unternehmens, obwohl nur eine einzelne Person eine Bedrohung darstellt. Zusätzlich ist es heute einfach die IP-Adresse zu ändern, indem man über einen anonymen Proxy ins Internet geht. Der Kampf gegen Hacker intensiviert sich und so muss der Fokus auf die aktuellen Angreifer und nicht auf die Jagd nach den gestrigen Attacken gelegt werden. Ein neuer «Spotlight» muss auf Systeme gelegt werden, welcher in der Lage ist Angreifer eindeutig zu identifizieren. Dazu werden die unterschiedlichsten Attribute, wie u.a. die verwendete Client Software. inklusive Plugins und Scripts, die History, der Name und Threat-Level des Angreifers aber natürlich auch die IP-Adresse als «Fingerprint» gesammelt und in Echtzeit über ein breites Netzwerk geteilt. Dadurch wird der Angreifer bereits in der Analysephase gestoppt, noch bevor der eigentliche Angriff erfolgt.

DDoS Attacken als Business-Case

Sicherheitslösungen der nächsten Generation müssen Unternehmen auch gegen die heutigen Bedrohungen schützen. Diese Bedrohungen artikulieren sich in der Unterbrechung der Verfügbarkeit und Hacking von Web-Anwendungen sowie dem Missbrauch von Daten. Die Zahl der Distributed Denial of Service (DDoS)-Attacken auf Internetseiten und Online-Shops hat in den vergangenen Jahren drastisch zugenommen. Heutzutage kann man Bot-Netze für wenige hundert Dollar stundenweise bei Kriminellen mieten. Dadurch lassen sich Angriffsfunktionen auf tausende von infizierten Computern verteilen. Das macht Angriffe auf Webseiten vergleichsweise einfach – zumal es sich «lohnt»: Dies widerspiegelt auch ein kürzlich veröffentlichter Bericht der Gartner-Analystin Avivah Litan. Sie berichtet, dass DDoS-Attacken auf eine neue Art genutzt werden. Während Sicherheitsbe-

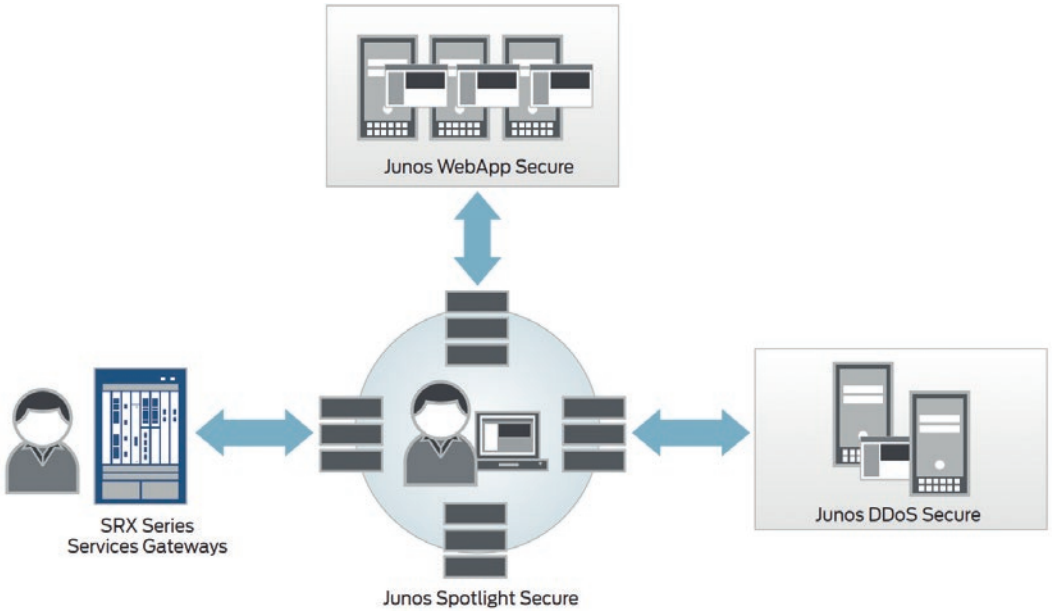

Abbildung 1: Junos Spotlight Secure in Verbindung mit Junos WebApp Secure liefert in Echtzeit den Austausch sicherheitsrelevanter Erkenntnisse über Hacker. Diese Informationen können von den Juniper SRX Firewalls und DDoS Appliances genutzt werden um den Eindringling an vorderster Front zu stoppen.

auftragte sich darauf konzentrieren, die Erreichbarkeit der Website und die betreffenden Dienste sicherzustellen. Erfolgt die eigentliche - und viel ernsthaftere Attacke im Sinne einer Erpressung! Mindestens drei Banken wurden der Analystin zufolge unter solchen Umständen um Millionenbeträge erleichtert. Deshalb ist es heutzutage für businesskritische Internet Services unerlässlich einen DDoS-Schutz vorzusehen. Dieser sorgt dafür, dass die Web-Anwendungen für legitime Nutzer online bleiben.

Mit raffinierten neuen Methoden Hacker hinters Licht führen

In einem zweiten Schritt muss eine Intrusion Deception Lösung den Hacker in Echtzeit identifizieren und sowohl auf der Anwendungsebene als auch am Netzwerk-Firewall flexible Reaktionsszenarien bieten. Ziel ist es dabei, den Hacker bereits zu erkennen, wenn er das Web Portal ausspioniert. Vergleichbar mit einem Dieb, der ums Haus schleicht, um den vermeintlich besten Ort für den Einbruch zu finden. Einmal erkannt, schützt die Lösung vertrauliche Daten, indem dem Hacker ausschliesslich unbrauchbare Informationen und fiktive Angriffsflächen offengelegt werden. Dies hält den Angreifer hin und ermöglicht es, die Skills des Eindringlings zu ermitteln. Dabei sammelt das System wertvolle Informationen, die zum Schutz vor weiteren Angriffen genutzt werden. Unternehmen behalten so die Oberhand gegenüber Hackern, ohne dabei ihren Datenverkehr einzuschränken oder signaturbasierte Verfahren zu verwenden.

Next-Generation Security

Dank der globalen Junos Spotlight Secure Hacker-Datenbank bieten die Security-Produkte von Juniper Networks einen optimalen Schutz gegen die neuen Cyber-Attacken. Die Angreifer werden durch die Junos WebApp Secure Plattform eindeutig identifiziert. Dies geschieht anhand eines Fingerabdrucks des Hackers mit über 200 einzigartigen Merkmalen. Jedes neue Profil wird sogleich global verfügbar gemacht. Verglichen mit den derzeit verfügbaren Reputations-Feeds, welche sich auf IP-Adressen verlassen, liefert Junos Spotlight Secure nicht bloss weit mehr zuverlässige Informationen über Angreifer, sondern beseitigt so auch Fehlalarme. In Kombination mit dem vollautomatisierten DDoS-Schutz für Webanwendungen entsteht ein einzigartiger Sicherheitsansatz für Attacken mit hohen Volumen, sowie gegen sogenannte «low-and-slow» Angriffe und bieten so eine breite Abwehr gegen Angreifer und Bedrohungen für Rechenzentren von innen und ausserhalb des Perimeters.

Autor: Ernesto Hartmann,
Senior ICT Security Architect,
InfoGuard AG

InfoGuard
and information becomes secure

InfoGuard AG
Lindenstrasse 10, 6340 Baar
Tel. +41 41 749 19 00, Fax +41 41 749 19 10
info@infoguard.ch
www.infoguard.ch