NEUE SICHERHEITSANSÄTZE GEGEN HACKER-ATTACKEN

Die starke Zunahme von Cloud Computing und Social Media, kombiniert mit der Raffinesse von Botnets, Angriffen aus der Kategorie «Advanced Persistent Threats» (APTs) und «Distributed Denial of Service (DDoS)»-Attacken machen Unternehmen anfälliger.

→ VON ERNESTO HARTMANN

So wurde im vergangenen Jahr ein Schweizer Unternehmen Opfer des bislang grössten DDoS-Angriffs hierzulande. In Spitzenzeiten erreichte dieser Angriff eine Datenflut von bis zu 300 GBit/s. Der herkömmliche Perimeter-Schutz stösst dabei nicht selten an seine Grenzen. Mit der Wahl der richtigen Sicherheits-Technologie lassen sich auch zukünftige Anforderungen erfüllen.

Online-Anwendungen und Web-Seiten sind die häufigsten Angriffsziele von Hackern und bergen innerhalb von Firmennetzwerken das grösste Gefahrenpotenzial. So ist es nicht erstaunlich, dass immer mehr Unternehmen und Rechenzentrumsbetreiber mit der steigenden Anzahl von Cyber-Angriffen auf Rechenzentrums-Infrastrukturen kämpfen und der leider immer professionelleren Vorgehensweise der Hacker. Naturgemäss sind auch hier die Übeltäter – wie im Sport beim Doping und dessen Bekämpfung – einen Schritt voraus. Dies widerspiegelt sich auch im diesjährigen Forschungsbericht des Ponemon-Institutes «Effizienz neuer Netzwerksicherheits-infrastrukturen». 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. Zudem äusserte sich eine Mehrheit der befragten Sicherheits-Profis dahingehend, dass die aktuellen Netzwerksicherheitstechnologien, wie Next-Generation-Firewalls und IP-Adressen basierten Reputationslösungen nur einen Teil der Cyber-Bedrohung adressieren und insbesondere bei Zero-Day-Angriffen, DDoS und SQL Injections an ihre Grenzen stossen.

Zu den Autoren

Ernesto Hartmann: Senior ICT Security Architect.

InfoGuard ist spezialisiert auf umfassende Informationssicherheits- und innovative Netzwerklösungen. Zu ihren Kompetenzen zählen massgeschneiderte Dienstleistungen nach internationalen Sicherheitsstandards sowie die Entwicklung und Implementierung technischer Sicherheits- und Netzwerklösungen.

Mehr Informationen: www.infoguard.ch

InfoGuard
and information becomes secure

SPOTLIGHT AUF DEN ANGREIFER

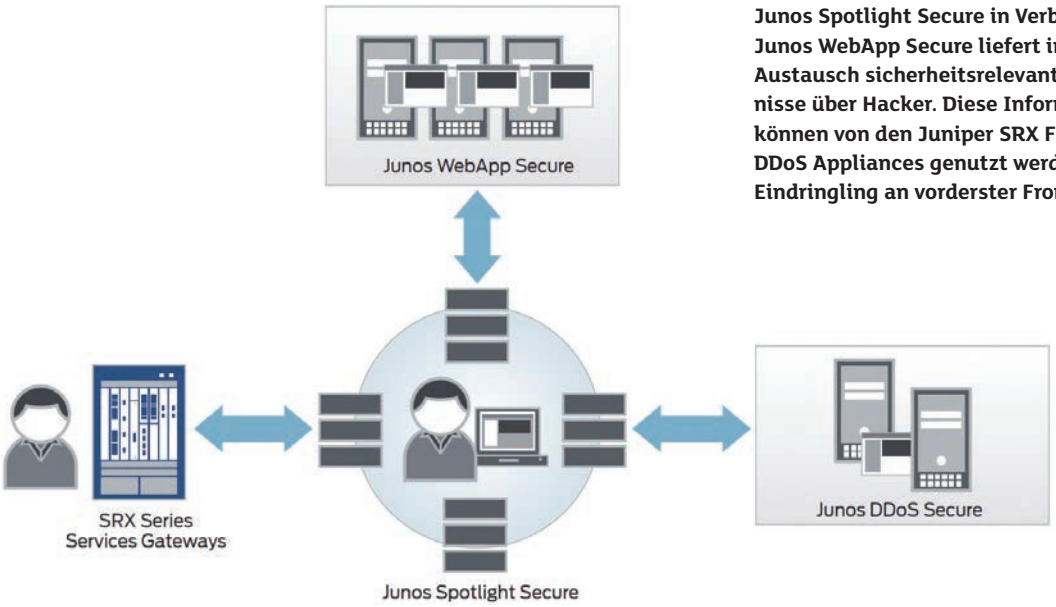
Trotz erheblicher Investitionen in Sicherheitslösungen sehen Unternehmen gerade bei den genannten DDoS- und Zero-Day-Angriffen noch immer Lücken in der IT-Sicherheit und der Wirksamkeit der eingesetzten Lösungen. Der Grund ist einfach. Traditionelle Abwehrkräfte verlassen sich mehrheitlich auf Signaturen 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, vergleichbar mit der Verwendung einer Postanschrift, um eine Person eindeutig zu identifizieren. Wie eine Postanschrift, ist auch eine IP-Adresse ein einzelnes Stück an Information. Zur endgültigen und zuverlässigen Identifikation einer Person werden aber viel mehr Attribute benötigt. Denn die meisten Internet-Benutzer befinden sich in einer einzigen Struktur oder hinter einer einzigen IP-Adresse.

Es leuchtet darum ein, dass reputationsbasierte Abwehrlösungen in so einem Fall nur marginal wirksam sind. Wenn man dann 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, welche in der Lage sind 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 grosse Rechenzentren auch gegen die heutigen Bedrohungen schützen. Diese Bedrohungen artikulieren sich in der Unterbrechung der



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.

Grosse DDoS-Attacke
auf Schweizer Firma

Eine der grössten DDoS-Attacken hatte sein Ziel in der Schweiz. Die Spamhaus-Gruppe mit Sitz in der Schweiz erstellt unter anderem Echtzeit-Blacklists von Spam-Versendern, um Internetanbietern das Herausfiltern der Urheber zu ermöglichen.
Der Web-Auftritt der Gruppe wurde am 19. März 2013 zum Ziel des bislang grössten DDoS-Massenangriffs. Die Attacke gegen Spamhaus sprengte allerdings den bislang bekannten Rahmen und das in mehrfacher Hinsicht und war zeitweise im gesamten Internet zu spüren.

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 (siehe Box). 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 Sicherheitsbeauftragte 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, das Skill-Level des Eindringlings zu ermitteln. Dabei sammelt das System wertvolle Informationen, die zum Schutz vor weiteren Angriffen genutzt werden. Dieses Vorgehen basiert auf einem aktiven und intelligenten Ansatz, das Bedrohungen eliminiert sobald sie auftauchen. Unternehmen behalten 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. ←