

Pressemeldung

Im Kopf des Hackers: EfficientIP erläutert, wie Cyberkriminelle vorgehen

Hacker suchen nach hohem Schadenspotenzial und schwachen Sicherheitsvorkehrungen

Eschborn, 01. September 2014 – Erfolgreiche Hacks können Websites lahmlegen, Datendiebstahl ermöglichen und in der Folge großen Schaden für Image und Umsatz des betroffenen Unternehmens nach sich ziehen. Diese bleiben oft mit einer substantiellen Frage zurück: Warum wurden wir Opfer von Hacker-Angriffen? [EfficientIP](#), ein führender Anbieter von DDI-Lösungen (DNS, DHCP und IPAM), beleuchtet die Vorgehensweise von Cyberkriminellen, ihre Ziele sowie Möglichkeiten, sich gegen die gefürchteten DDoS-Attacken zu verteidigen.

Ziel: Einflussnahme und Macht demonstrieren

Häufig geht es Hackern, vor allem „Haktivisten“, um Einfluss. Sehr öffentlichkeitswirksam kündigte beispielsweise die Hacker-Gruppe Anonymous im Vorfeld der Fußball-WM in Brasilien an, die Server von Sponsoren wie Adidas, Emirates oder Coca-Cola anzugreifen. Letztlich hielt sich der tatsächlich verursachte Schaden in Grenzen und beeinträchtigte nicht den Ablauf des Turniers. Trotzdem nutzten die Hacker die Aufmerksamkeit der Welt, um auf ihre Ziele hinzuweisen. Häufig ist auch der Diebstahl sensibler Daten Ziel der Angreifer. Anfang August 2014 wurde publik, dass russische Hacker laut der US-Sicherheitsfirma Hold Security 1,2 Milliarden Login-Kombinationen und über 500 Millionen E-Mail-Adressen erbeutet haben. Angeblich fischten die Angreifer bei 420.000 Websites Nutzerdaten ab. Allein die Größenordnung macht deutlich, wie gefährlich Angreifer im Internet sein können. Um den verursachten Schaden zu maximieren beziehungsweise möglichst viele Daten zu erbeuten, wählen Hacker oft Ziele aus, die aufgrund ihres Geschäftsmodells umfangreiche Datenmengen

vorhalten: E-Commerce-Seiten mit großen Webshops, Banken, Behörden oder Internet Service Provider. Letztere können sogar als Multiplikator dienen, wenn über sie ein Zugriff auf etliche Tausend Websites von Unternehmen und Privatleuten erfolgt.

Hackerwerkzeug DDoS: Die virtuelle Brechstange

Ein weit verbreiteter Angriffstyp ist die Distributed Denial of Service-Attacke (DDoS), bei der Hacker den Unternehmensserver mit Millionen von Anfragen pro Sekunde fluten. Bricht der Server unter der Last zusammen, ist die Website des Unternehmens nicht mehr erreichbar. Sämtliche IP-basierten Applikationen können nicht mehr genutzt werden – de facto ist das Unternehmen dann nicht mehr geschäftsfähig. Außerdem entstehen durch den überlasteten DNS-Server Sicherheitslücken, die ein Angreifer nutzen kann, um den DNS-Cache zu beeinflussen. So lässt sich beispielsweise der Web-Traffic von der Unternehmenswebsite auf eine betrügerische Seite umleiten.

Vorsicht statt Nachsicht: Vorbereitung auf DDoS-Angriffe

Das Prinzip eines DDoS-Angriffs ist einfach: Es werden mehr Anfragen an einen Server gestellt als dieser beantworten kann. Angreifer können heutzutage dabei immer größere Angriffe fahren: 2013 fluteten 63 Prozent der DDoS-Angriffe ihre Ziel mit mehr als einer Million Anfragen pro Sekunde. Da selbst die leistungsfähigsten herkömmlichen DNS-Server nicht mehr als 300.000 Anfragen bearbeiten können, benötigen Unternehmen zum Schutz dutzende redundante Server sowie zusätzliche Komponenten wie Load Balancer – eine hochkomplexe und teure IT-Infrastruktur. Als Alternative hat EfficientIP jüngst den SOLIDserver DNS Blast vorgestellt, der 17 Millionen Anfragen pro Sekunde verarbeiten kann. Durch die hohe Leistungsfähigkeit werden nur wenige Geräte benötigt, um selbst große Angriffe praktisch ohne Folgen ins Leere laufen zu lassen.

„Die wohl wichtigste Erkenntnis aus den Angriffen der vergangenen Jahre ist, dass Hacker immer professioneller vorgehen und oft hervorragend ausgestattet sind. Sie sind in der Lage, Sicherheitslösungen zu erkennen und deren Wirksamkeit zu beurteilen. So können sie ihre ‚Instrumente‘ mit hoher

Effektivität einsetzen, erklärt David Williamson, CEO bei EfficientIP. „Da Unternehmen häufig nicht um diese Risiken wissen, investieren nur wenige ausreichend in spezialisierte DNS-Sicherheitslösungen. Dadurch werden DNS-Server zum schwächsten Glied der gesamten IT-Infrastruktur und setzen sich Gefahren aus, die sie mit einer Sicherheitssoftware wie dem SOLIDserver DNS Blast abwenden könnten.“

Mehr Informationen zu EfficientIP und SOLIDserver DNS Blast:

www.efficientip.com

###

Über EfficientIP

EfficientIP ist ein internationaler Software-Hersteller für DDI-Lösungen (DNS, DHCP und IPAM - IP Address Management). Das Unternehmen vertreibt seine Produkte über ein weltweit agierendes Partner-Netzwerk. EfficientIP ist in den wichtigsten Branchen wie Banken, Telekom-Anbieter, Industrie, Dienstleistungen und Behörden tätig. Als einer der führenden Anbieter im Markt nutzen Hunderte der anspruchsvollsten Unternehmen die EfficientIP-Lösungen. Dazu gehören Unternehmen wie Vodafone, EADS, BskyB, Crédit Agricole, STMicroelectronics und T-Mobile.

EfficientIP hat das fortgeschrittene SmartArchitecture-Konzept entwickelt. Dadurch wird die Verwaltung von DNS und DHCP vom Service-Level auf die Architektur-Ebene gehoben. EfficientIP bietet eine Reihe von leistungsfähigen Hardware- und virtuelle Appliances-Lösungen wie den SOLIDserver für IP Address Management, DNS- und DHCP-Management und Dienstleistungen. Für weitere Informationen, besuchen Sie bitte: www.efficientip.com/de.

Pressekontakt:

LEWIS PR

Shushila Pandya

Tel: + 49 (0) 211 522946 0

efficient-ip@lewispr.com