Pressemeldung

EfficientIP gibt drei Tipps zur Abschwächung von DNS-Angriffen

- DNS-Angriffe lassen sich nicht verhindern aber abmindern
- Anwender sollten DNS-Server-Software stets aktuell halten, eine Hybridlösung zum Umschalten zwischen DNS-Engines in Echtzeit implementieren und sicherstellen, dass der Server alle Anfragen stets verarbeiten kann

Eschborn, 04. August 2014 – Das Domain Name System (DNS) ist einer der wichtigsten Dienste in IP-basierten Netzwerken und ein bevorzugtes Ziel für Hacker. EfficientIP, ein führender Anbieter von DDI-Lösungen (DNS, DHCP und IPAM), erklärt, warum sich Unternehmen besser vor DNS-Angriffen schützen sollten. Der Sicherheitsexperte gibt drei zentrale Tipps, die helfen, die Risiken von DDoS-Angriffen zu minimieren und Schäden abzuschwächen.

Ein Beispiel für Angriffe auf DNS-Server 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 und alle IP-basierten Applikationen können nicht mehr genutzt werden – de facto ist das Unternehmen 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.

Einer Untersuchung von IDC zufolge sind weitere mögliche Konsequenzen der Diebstahl geistigen Eigentums (40 Prozent der angegriffenen Unternehmen), die Veröffentlichung geheimer Informationen (27 Prozent) sowie der Diebstahl von Kundendaten (11 Prozent). Kurz: Eine erfolgreiche DDoS-Attacke kann für das Unternehmen, seinen Ruf und seine Kunden

verheerende Folgen haben.

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. EfficientIP erläutert, worauf Firmen und Organisationen achten sollten:

1. Software regelmäßig aktualisieren

Anwender sollten sicherstellen, dass alle neuen Sicherheitsupdates installiert werden. BIND, die am weitesten verbreitete DNS-Engine, wird beispielsweise durchschnittlich einmal im Monat aktualisiert. Die Nutzung veralteter Software verstärkt Sicherheitsrisiken, die Angreifer ausnutzen können.

2. Verschiedene DNS-Engines nutzen

Als Best Practice hat sich bewährt, dass Unternehmen mindestens zwei DNS-Server mit unterschiedlichen Software-Engines betreiben sollten. Im normalen Betrieb kann die zweite Engine übernehmen, während die erste aktualisiert und gründlich getestet wird. Da DNS-Installationen sehr komplex sein können, ist es ratsam, eine derartige Ausweichmöglichkeit vorzuhalten, da auch ein fehlerhaftes Update ernste Folgen haben kann. Während eines Angriffs ist es noch wichtiger, über verschiedene Engines zu verfügen: Das angegriffene Unternehmen kann in Echtzeit auf die zweite Engine umschalten, die Sicherheitslücke damit ausschalten und die Attacke beenden. Besonders bei Zero-Day-Exploits ist dieses Vorgehen hilfreich, da hier keine Sicherheits-Updates verfügbar sind.

3. Vorbereitung auf DDoS-Angriffe bedenken

Das Prinzip eines DDoS-Angriffs ist einfach: Es werden mehr Anfragen an einen Server gestellt als dieser beantworten kann. Angreifer können heutzutage immer größere Angriffe fahren: 2013 fluteten 63 Prozent der DDoS-Angriffe ihre Ziel mit mehr als einer Million Anfragen pro Sekunde. Im Februar 2014 wurde sogar ein Angriff mit einem Web-Traffic von 400 Gigabyte pro Sekunde ausgeführt. Das entspricht rund 40 bis 50 Millionen Anfragen in der 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. Zudem ist die benötigte Infrastruktur viel einfacher und kostengünstiger.

David Williamson, CEO bei EfficientIP, kommentiert: “Die meisten Unternehmen haben heute schon einmal von DDoS-Attacken gehört. Sie sind aber noch immer nicht umfassend genug abgesichert. Wir raten ihnen, sich genau zu überlegen, welche Lösung sie dabei unterstützen kann, Millionen von Anfragen zu bewältigen. Unser SOLIDserver DNS Blast nimmt ihnen Sorgen und Aufwand ab.”

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