

Pressemitteilung

Sloth-Attacken: EfficientIP warnt vor neuer, schleichende Alternative zu DDoS-Angriffen

Security-Experte rät Unternehmen zu erhöhter Wachsamkeit bei Angriffen auf DNS-Server

Eschborn, 16. Juli 2015 – Cyber-Angriffe auf Unternehmen und sogar Regierungen sind mit Anbruch des 21. Jahrhunderts regelmäßig in den Medien vertreten. Mit den ständig neuen Formen von Hacker-Angriffen Schritt zu halten, ist dabei eine der größten Herausforderungen für Security-Experten. [EfficientIP](#), ein führender Anbieter von DDI-Lösungen (DNS, DHCP und IPAM) sieht nach der großen Bandbreite von DDoS-Angriffen eine langsamere Form als neue Bedrohung: die sogenannten Sloth-Attacken.

Behäbig statt brachial

Wer bislang Cyber-Kriminalität nicht ernst nimmt, sollte schleunigst umdenken. Eine aktuelle [Studie](#) des Telekommunikationsriesen Verizon zeigt, dass die Zahl der erfolgreichen digitalen Angriffe im Vergleich zum Vorjahr bereits um 55 Prozent gestiegen ist. Die weit verbreitete DDoS-Attacke galt hier bislang als das Brecheisen und bevorzugte Waffe im Werkzeugkoffer eines jeden Hackers. Doch in den vergangenen Monaten beobachtete EfficientIP eine neue Form der Bedrohung für DNS-Server, die auf ein weniger auffälliges Angriffsmuster setzt.

Die sogenannte Sloth-Attacke basiert auf einem langsameren Angriffstyp. Statt den Server mit Millionen von Anfragen innerhalb von Sekundenbruchteilen zu fluten, setzen Hacker nun auf die langsame aber stete Überlastung des IP-Cash-Servers. Hierzu werden Anfragen an den DNS-Server über eine langsame Domain geleitet, die diese nicht innerhalb von Millisekunden, sondern in Zeiträumen von fünf bis zehn Sekunden beantwortet. Da aber immer weitere Anfragen mithilfe eines Botnets gesendet werden, muss der DNS-Server mehr und mehr Daten verarbeiten, die jedoch nicht schnell genug beantwortet werden können. Die Folge: eine kontinuierliche Auslastung des Cash-Servers, der unter der sich nicht schnell genug klärenden Datenflut zusammenbricht. Sobald dies geschieht, sind sämtliche Online-Aktivitäten nicht mehr möglich, die Unternehmenswebseite ist für Besucher nicht länger erreichbar.

Vorbeugung von innen

Wie können Unternehmen dieser Bedrohung begegnen? Viele aktuelle Lösungen auf dem Markt sind ihr nicht gewachsen. Dies hängt damit zusammen, dass sie nur schwer aufzuspüren sind. Die Anfragen an den Server sind für sich gesehen nicht offensiv. Doch die Menge, gepaart mit der Langsamkeit in ihrer Beantwortung, zwingt die eigene Server-Infrastruktur nach und nach in die Knie. Um auf diese Angriffe reagieren zu können, ist Software erforderlich, die diese Attacken frühzeitig sichtbar macht.

EfficientIPs Lösung DNS Guardian bietet hierbei eine an sich einzigartige Herangehensweise. Sämtliche Anfragen werden innerhalb des Systems durch Guardian auf Validität geprüft. Andere DNS-Sicherheitslösungen versuchen dies von außerhalb. Doch gerade schleichende Angriffe wie die Sloth-Attacke sind erst im System erkennbar. Weisen Anfragen dort verdächtige Signaturen auf, warnt das System bereits vor möglicher Gefahr. So bleibt genug Zeit, Gegenmaßnahmen zu ergreifen. Zudem prüft DNS Guardian den Ursprung der Anfragen und isoliert diese gezielt, so dass die eigentliche Online-Präsenz des Unternehmens davon so unberührt wie möglich bleibt.

„Cyber-Angriffe, besonders auf Schwachstellen wie den DNS-Server, nahmen in den vergangenen Jahren dramatisch zu. Wichtig ist daher für uns, den Kunden ein Tool an die Hand zu geben, das sie rechtzeitig vor einer Bedrohung warnt und währenddessen dennoch ihre Online-Aktivitäten nicht beeinträchtigt“, kommentiert Ralf Geisler, Country Manager für die DACH-Region bei EfficientIP. „Wissen Unternehmen nichts über die Gefahr dieser schleichenden Angriffe, können Hacker Unternehmen immensen Schaden zufügen. Unser Ziel ist es, dies mit frühzeitiger Aufklärung zu verhindern.“

###

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 Partnernetzwerk. EfficientIP ist in den wichtigsten Branchen wie Banken, Telekomanbieter, 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. Es hebt die Verwaltung von DNS und DHCP vom Service-Level auf die Architekturebene. EfficientIP bietet eine Reihe von leistungsfähigen Hardware- und virtuelle Appliances-Lösungen wie den SOLIDserver für IP Address Management, DNS- und DHCP-Management sowie Dienstleistungen. Für weitere Informationen besuchen Sie bitte: www.efficientip.com/de.

Pressekontakt:

LEWIS PR

Mark Schüpstuhl

Tel: + 49 (0) 211 522946 0

efficient-ip@lewispr.com