

Die unterschätzte Gefahr: HTTPS schleust Malware ins Unternehmen

07.05.2015, 19:48 | IT, New Media & Software

Pressemitteilung von: *Dell*

Frankfurt am Main, 7. Mai 2015 – Dell warnt vor Malware, die sich des HTTPS-Protokolls bedient. Auf diese Weise verschlüsselter Schadcode ist von herkömmlichen Firewalls nicht zu erkennen; erst Firewalls mit SSL-Inspektion bieten auch vor derartigen Angriffen Schutz.

In der Öffentlichkeit gilt die verschlüsselte Kommunikation über HTTPS als sicher. Banken und Online-Shops nutzen dieses Protokoll zum Austausch sensibler Daten, zum Beispiel für Zahlungsvorgänge im Netz. Gefahren werden meist nur in Verbindung mit einem fehlenden oder falschen Einsatz von HTTPS gesehen.

"Völlig außer Acht bleibt dabei, dass HTTPS selbst eine Gefahrenquelle darstellt, und zwar auch dann, wenn es richtig angewendet wurde", erklärt Florian Malecki, International Product Marketing Director Network Security bei Dell. "Gefahr droht nämlich aus einer ganz anderen Richtung: Angreifer können über HTTPS unerkannt Malware in ein Unternehmensnetz einschleusen. Das Problem ist, dass herkömmliche Firewalls nicht in der Lage sind, die mit HTTPS verschlüsselte Malware zu identifizieren, und sie ungehindert passieren lassen."

Dell hat in seinem jährlichen Sicherheitsbericht (1) festgestellt, dass 2014 der mit HTTPS gesicherte Datenverkehr um 109 Prozent gewachsen ist. Entsprechend höher ist das Risiko von Attacken, die sich solcher Verbindungen bedienen. Malware wie ZeroAccess, Poison Backdoor, BlackHole, Ransomware oder Kazy Trojan kann sich problemlos in SSL verstecken. Das daraus entstehende Risiko ist außerhalb von Expertenkreisen jedoch noch immer nur wenig bekannt.

"Die größte Herausforderung ist hier meines Erachtens, dass sich Anwender der Gefahr überhaupt nicht bewusst sind", führt Malecki aus. "Wir sprechen immer wieder mit Anwendern, die aus allen Wolken fallen, weil sie meinen, mit dem Einsatz von HTTPS auf der sicheren Seite zu sein. Natürlich ist das HTTPS-Protokoll für kritische Daten, wie sie etwa im Online-Banking anfallen, heute unverzichtbar. Aber HTTPS alleine reicht nicht: Anwender müssen die mit HTTPS entstehende Lücke durch Firewalls der nächsten Generation absichern. Nur Systeme, die in der Lage sind, eine umfassende SSL-Inspektion vorzunehmen, die also auch die verschlüsselte Kommunikation auf Malware untersuchen können, bieten Schutz."

Rund ein Sechstel der von diesen Systemen erkannten Malware nutzt bereits SSL. Das zeigt, dass diese Gefahr alles andere als nur theoretischer Natur ist.

Dell auf Twitter: <http://twitter.com/DellGmbH>

Dell Blog: www.dell.de/d2dblog

(1) <http://software.dell.com/whitepaper/dell-network-security-threat-report-2014874708>

Diese Meldung kann auch unter www.pr-com.de/dell abgerufen werden.

Portrait

Über Dell

Dell hört seinen Kunden zu und bietet innovative und zuverlässige IT-Lösungen und -Dienstleistungen, die auf Industrie-Standards basieren. Sie sind ganz auf die individuellen Anforderungen der Anwender zugeschnitten und ermöglichen es Unternehmen, erfolgreicher zu sein. Weitere Informationen unter www.dell.de und www.dell.de/d2dblog. Unter www.dell.com/conversations bietet Dell zudem die Möglichkeit zur direkten Kontaktaufnahme.

News-ID: 852670 • Views: 139 (Stand: 12.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/852670/Die-unterschaetzte-Gefahr-HTTPS-schleust-Malware-ins-Unternehmen.html>