SBA Research Presseaussendung
Wien, 17.7.2015

Sicherheitsrisiko bei verschlüsselten Internetverbindungen

Tausende Server in Österreich von RC4-Lücke betroffen

- Forscher decken erneut Sicherheitsrisiko bei Verschlüsselungsmethode RC4 auf
- Angriff ermöglicht wesentlich rascheres Knacken von HTTPS-Webverbindungen als bisher angenommen
- Experten von SBA Research warnen: Starke Verbreitung in Österreich macht RC4-Lücke zur realen Gefahr

Diese Nachricht sorgte für hohe Wellen in Expertenkreisen. Belgische Forscher haben erneut eine Sicherheitslücke bei RC4 entdeckt. Diese Methode zur Verschlüsselung von Webverbindungen (z.B. HTTPS) war in der Vergangenheit schon öfters in die Kritik von Experten geraten. Aufgrund eines erhöhten Sicherheitsrisikos sollte es nach den Empfehlungen der Internet Engineering Task Force (IETF) gar nicht mehr verwendet werden. Dennoch zählt RC4 nach wie vor zu den am weitesten verbreiteten Verschlüsselungsmethoden.

SBA Research: „RC4 nicht mehr verwenden!"

Nun wurde erstmals gezeigt, dass das nachträgliche Knacken durch einen Hackerangriff wesentlich schneller durchgeführt werden kann als bisher angenommen - in 75 statt bisher 2000 Stunden. "Auch wenn so ein Angriff nicht sehr einfach durchzuführen ist, besteht aufgrund der nach wie vor starken Verbreitung von RC4 eine reale Gefahr. In Österreich sind tausende Server betroffen", warnt Martin Mulazzani, Senior Researcher bei SBA Research, und bringt es auf den Punkt: „RC4 soll nicht mehr verwendet werden!"

Die Forscher von SBA Research können nicht nur helfen, die Sicherheitslücke zu schließen, sondern haben in den letzten Wochen auch Daten zur aktuellen RC4-Verbreitung erhoben. So wurden ca. 2 Millionen TLS-Konfigurationen weltweit gescannt und ein erstaunliches Ergebnis erzielt: Noch 1,3 Millionen bzw. 61,7 % der untersuchten Konfigurationen erlauben RC4. 350.000 Servern (16%) bevorzugen RC4 sogar vor sicheren Verschlüsselungen.

Server lassen sich unter https://www.ssllabs.com/ssltest/ testen und Empfehlungen zur Deaktivierung von RC4 finden Sie unter www.bettercrypto.org oder https://tools.ietf.org/html/rfc7525.

Weitere Informationen:

- Meldung von SBA Research mit Links zu den Forschungsarbeiten: https://www.sba-research.org/2015/07/16/rc4-in-https-verbreitung/

Rückfragehinweis:
SBA Research
Martin Mulazzani
Email: mmulazzani@sba-research.org
Web: http://www.sba-research.org/