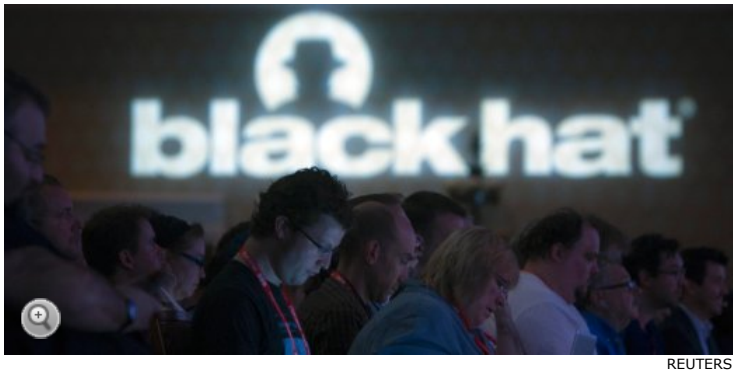
IT-Sicherheitskonferenz: Internet-Verschlüsselung unter Beschuss

Aus Las Vegas berichtet Ole Reißmann

Noch ist der Standard für sichere Datenübertragung im Web nicht geknackt worden. Doch auf der IT-Konferenz Black Hat zeigen Forscher, wie sie unter Umständen doch an Geheimnisse kommen, die damit gesichert werden - und warnen vor einer "Cryptopocalypse".

Samstag, 03.08.2013 – 07:04 Uhr



REUTERS

Teilnehmer der Black Hat 2013: Angriff auf das TLS-Protokoll

Zuerst die gute Nachricht: Noch lassen sich Internetverbindungen so verschlüsseln, dass sie sich praktisch nicht knacken lassen. Nutzer erkennen das an dem "https" in der Adresszeile des Browsers. Wenn dieses Kürzel erscheint, werden die übertragenen Daten vom TLS-Protokoll (Transport Layer Security) geschützt. Dabei wird ein öffentlicher Schlüssel genutzt, um die Daten zu verschlüsseln, und ein privater, um sie wieder lesbar zu machen. Der mathematische Aufwand, so eine asymmetrische Verschlüsselung zu knacken, ist so hoch, dass Computer dafür viele Jahren brauchen.

Doch auf der IT-Sicherheitskonferenz Black Hat haben mehrere Forscher gezeigt, wie sich das TLS-Protokoll trotz aufwendiger Verschlüsselung unter Umständen angreifen lässt. Von den versammelten Hackern wurden sie dafür gefeiert wie Rockstars. Die Beispiele zeigen, wie komplex die unverzichtbare Technik geworden ist.

- Zur Musik aus "Mission Impossible" führten Angelo Prado, Neal Harris und Yoel Gluck einen Angriff namens Breach vor. Dazu nutzten sie die Kompression von Webseiten aus. Sie schieben dem Nutzer Hunderte Anfragen an einen Webserver unter und schauen, wie sich die Größe der verschlüsselten Seite ändert. So können sie unter bestimmten Umständen Daten erraten, ohne die Verschlüsselung an sich zu knacken. Bei ihrer Präsentation konnten sie auf diese Weise einen Code innerhalb einer knappen Minute aus einer verschlüsselten Seite extrahieren. Das Department of Homeland Security warnt Website-Betreiber vor dem Problem, für dass es derzeit keine einfache Lösung gebe.

- Eine Erweiterung des TLS-Protokolls sorgt dafür, dass sich ein Webserver eine einmal eingerichtete verschlüsselte Verbindung merken kann und sie nicht jedes Mal von neuem aufbauen muss. Der in Großbritannien arbeitende Sicherheitsexperte Florent Daignière wies auf Mängel bei der technischen Umsetzung dieser sogenannten Session Tickets hin. Standardmäßig würden diese Tickets zu lange gespeichert. Er präsentierte ein Tool, mit dem er derart verschlüsselte Daten nachträglich entschlüsseln konnte.

Kryptografie

Computersicherheit

Hacker

Alle Themenseiten

Mehr auf SPIEGEL ONLINE

Netzwelt-Ticker: Web-Verschlüsselung, Facebook-Klage, Occupy-Tweets (14.09.2012)

Mehr im Internet

Breach

Session Tickets

gefälschte Logout-Bestätigung

Cryptopocalypse

No easy way to stop BREACH from plucking secrets from HTTPS pages, feds say

- Ben Smyth und Alfredo Pironti haben einen Angriff entwickelt, bei dem sie sich in die Verbindung zwischen Nutzer und Server einklinken, etwa über ein manipuliertes W-Lan. Meldet sich ein Nutzer von einem TLS-gesicherten Webdienst wie Hotmail oder Gmail ab, leiten sie den Logout-Befehl nicht an den Server weiter, schicken dem Nutzer aber eine gefälschte Logout-Bestätigung. Bekommen sie danach Zugriff auf den Computer des Opfers, können sie den Webdienst wieder aufrufen und weiternutzen. Die beiden Forscher vom französischen Institut National de Recherche en Informatique et en Automatique wollen so auch Helios-Wahlcomputer hereingelegt haben.

Die gezeigten Angriffe zielen auf konkrete Umsetzungen der Verschlüsselung, nicht auf das Prinzip als solches. Was aber, wenn in der Mathematik ein Durchbruch erzielt wird - und die asymmetrische Verschlüsselung sich plötzlich in ein paar Minuten knacken lässt? Die IT-Experten Alex Stamos, Tom Ritter, Thomas Ptacek und Javed Samuel forderten die anwesenden Industrievertreter und Hacker zur Wachsamkeit auf. Sollte es künftig bessere Lösungen geben, die zum Knacken der Codes nötigen Rechenschritte abzuarbeiten, müsste sofort alles umgestellt werden - die "Cryptopocalypse".