Menschengemachte Schwachstellen auf der Hack.lu 2012

Die achte Sicherheitskonferenz „Hack.lu" in Luxemburg stand in diesem Jahr unter dem Motto „It can only be attributable to human error" und zitiert damit HAL aus dem Film „2001: A Space Odyssey". Entsprechend behandelten viele Vorträge „menschengemachte Schwachstellen" und ihre Beseitigung.

In ihrem Vortrag „A critical analysis of Dropbox software security" fassten Nicolas Ruff (news0ft) und Florian Ledoux (Mysterie) die bislang publik gewordenen Sicherheitsprobleme des verbreiteten Datensynchronisierungsdienstes zusammen und präsentierten ihre eigenen Analysen der Client-Software: Zur Verschlüsselung der Kommunikation würde eine veraltete und als unsicher geltende OpenSSL-Version eingesetzt. Aufgrund mangelnder Zertifikatsüberprüfungen sei zudem ein Spoofing bei über das LAN synchronisierten Dropbox-Clients möglich.

Gleich zwei Vorträge beschäftigten sich mit Android-Security. Atul Alex Cherian (Aodrulez) stellte die betriebssystemeigenen Sicherheitsmechanismen vor und zeigte die Schwachpunkte der Sandbox-Implementierung. Kevin Allix und Quentin Jerome legten den Schwerpunkt in ihrem Beitrag auf die forensische Analyse von Android-Malware. Für das konkurrierende iOS zeigte Mathieu Renard (Sogeti) bekannte Sicherheitsprobleme bei Anwendungen und Backup von iOS-Geräten. Dazu gehört, wie man die Erkennung von „gejailbreakten" Devices durch Mobile-Device-Management-Produkte umgehen kann.

Auch die Vorstellung neuer Tools kam nicht zu kurz. So veranschaulichte Patrice Auffret die Vorzüge des gerade in Version 1.0 erschienenen OS-Fingerprinting-Frameworks SinFP3 gegenüber der in Nmap eingebauten Betriebssystemerkennung. Im Gegensatz zu Nmap benötigt das neue Werkzeug meist nur ein einziges TCP-SYN-Paket, um ein Betriebssystem zuverlässig zu ermitteln. Victor Julien und Eric Leblond stellten mit Suricata außerdem eine performantere Alternative zu Snort vor, die Deep Package Inspection bietet. In weiteren Beiträgen berichteten Sicherheitsexperten, wie sie E-Book-Reader hackten, die Firmware der in mobilen Endgeräten eingesetzten Broadcom-WiFi-Chipsätze modifizierten oder mit eingebettetem Shellcode Excel-Sheets in Angriffswerkzeuge umfunktionieren konnten.

Für Penetrationstester informativ erwies sich ein Workshop von Eireann Leverett (IOActive) mit dem Titel „SHODAN: Global Logfile of Insecurity". Die Suchmaschine SHODAN sammelt im Gegensatz zu herkömmlichen Suchmaschinen technische Daten wie Serverbanner, SSL Ciphers oder Sessioninformationen – ein durchaus zweischneidiges Schwert, wie ernsthafte Angriffe auf der Basis der damit gefundenen Informationen in den letzten Jahren zeigten.

Michael Clemens (ur)