Black Hat Europe: Neugier ist kein Vergehen

Mit dem politischen Vortrag „Shelters or windmills: the struggle for power and information advantage" eröffnete Rick Falkvinge, Begründer der ursprünglichen Piratenpartei, die europäische Ausgabe der amerikanischen Sicherheitskonferenz „Black Hat" in Amsterdam.

Er stellte dar, wie die Mächtigen der Gesellschaft seit jeher versuchen, die Kontrolle über Informationen zu erhalten, und die Geschichte sich diesbezüglich ständig wiederholt. Auch in Gedenken an den im Januar verstorbenen Hacker und Aktivisten Aaron Swartz forderte er die Konferenzteilnehmer schließlich auf, neugierig zu sein: „Curiosity is not a crime. Locking up knowledge and culture however is."

Dass gerade Security Appliances oft erhebliche Sicherheitsmängel aufweisen, verdeutlichte Ben Williams von der NCC Group. Während seiner Arbeit als Penetrationstester kamen ihm sogar Gateway-Systeme unter, die sich als Zugang in das dahinterliegende Netzwerk missbrauchen ließen, oder Anti-Spam-Produkte, die nach Ausnutzung von Schwachstellen dem Versand von Spam-Mails dienten. Er musste feststellen, dass gängige Härtungsmaßnahmen meist nicht an solchen Appliances vorgenommen werden und man ihnen nicht blind vertrauen kann.

Mit „To Dock Or Not To Dock" wies Andy Davis (NCC Group) auf die Gefahren von Dockingstationen für Notebooks hin, denen man im Regelfall wenig Beachtung schenkt. Sie bieten einem Angreifer jedoch meist genug Platz, darin beispielsweise einen Raspberry Pi zu verstecken, der dann direkten Zugriff auf alle Schnittstellen des angeschlossenen Notebooks hat. Über Mobilfunk können so Bild- und Tonausgabe sowie Netzwerkverkehr mitgeschnitten werden. Sogar der Zugriff auf die im Notebook eingebaute Webcam ist möglich.

Überlistete Sandbox

Dass Sandboxing nicht zwangsweise auch Sicherheit bedeutet, zeigten Rafal Wojtczuk und Rahul Kashyap (beide Bromium Inc.) anhand populärer Produkte und Implementierungen wie Sandboxie oder den Mechanismen des Chrome Browser und Adobe Reader. Die Autoren hoben vor allem hervor, dass man Kernel-Exploits auch aus der Sandbox heraus ausnutzen könne und diese aufgrund der hohen Privilegien der vermeintlich sicheren Umgebung unweigerlich zur Rechteerweiterung führten.

Auf unterhaltsame Art riet Brad Antoniewicz den Zuhörern, bei RFID-Zugangskontrollsystemen nicht nur auf die Funkübertragung selbst, sondern auch auf die damit zusammenhängenden Geräte zu achten. Er demonstrierte, wie er mit einem Arduino den auf dem Wiegand-Protokoll basierenden Verkehr mitschneiden und anschließend wiedergeben konnte und wie schlecht es um die Sicherheit der stark verbreiteten Kontrolleinheit HID VertX V2000 samt zugehörigem Webinterface steht. Zu den Schwachstellen zählen hartcodierte und schwache *root*-Passwörter sowie GET-Requests, mit denen man Türen öffnen, schließen oder sogar dauerhaft geschlossen halten kann.

Michael Clemens (ur)