10.03.2017 – 10:21 Uhr

Vault 7: Die Cyber-Waffen der CIA

Bochum (ots) -

- Querverweis: Bildmaterial wird über obs versandt und ist
abrufbar unter http://www.presseportal.de/pm/65324/3581551 -

Die Veröffentlichungen von vertraulichen CIA-Dokumenten auf der Enthüllungsplattform Wikileaks beleuchten deren Aktivitäten im Bereich Hacking von Hard- und Software in den Jahren 2013 bis 2016. Ziele sind unter anderem iPhones, Android-Geräte, Linux, Windows und Smart-TVs. Auch Sicherheitsanbieter sind in den Dokumenten des Auslandsnachrichtendienstes genannt. Es scheint somit kein Betriebssystem und keine Soft- und Hardware vor den Cyber-Waffen der CIA sicher zu sein. Die G DATA Sicherheitsexperten Eddy Willems und Ralf Benzmüller haben sich einen Überblick über die vorliegenden Dokumente verschafft und ordnen die aktuellen WikiLeaks-Enthüllungen in ihrem heutigen Blog-Artikel ein.

+ Breit aufgestellt

Ähnlich wie bei den Snowden-Leaks ist es nicht verwunderlich, dass Geheimdienste spionieren, sondern viel eher wie und in welchem Ausmaß sie das tun. Das ist auch bei Vault 7 der Fall. Es geht nicht nur um Sicherheitslecks bei Desktop-PCs und Servern. Demnach hat der US-Geheimdienst alle internetfähigen Geräte ins Visier genommen. Neben Smartphones mit Android und iOS, Routern und Smart-TVs werden in den Wikileaks-Dokumenten auch eigebettete Systeme aus dem IoT-Umfeld genannt. Auch Werkzeuge zum Hacken von Industriesteueranlagen und Fahrzeugen sind im CIA-Arsenal. Es gibt Tarnverfahren für die CIA-Software und Werkzeuge zum herausschmuggeln von Daten. "Man hat den Eindruck, dass jede Technologie, die eine gewisse Verbreitung im Markt hat, systematisch für einen Einsatz im Umfeld von Cyber-Spionage und Cyber-Warfare geprüft wurde", so Eddy Willems, G DATA Security Evangelist.

+ Lang gehegte Vermutung wurde bestätigt

"Es wäre blauäugig zu glauben, dass die Entwicklung von sog. Cyber-Waffen nur von amerikanischer Seite vorangetrieben wird. Unserer Einschätzung nach arbeiten alle Geheimdienste seit vielen Jahren an vergleichbaren Programmen, die auch millionenschwer ausgestattet sind", so Ralf Benzmüller, Executive Speaker der G DATA Security Labs. "Die veröffentlichten Enthüllungen bestätigen die von vielen IT-Security Experten seit langen gehegten Vermutungen. Als äußerst problematisch betrachten wir es, wenn die entwickelten E-Spionage-Programme als Cyber-Broken-Arrows in die Hände von Kriminellen und Terroristen gelangen. Die Folgen wären fatal."

Nach Einschätzung der beiden G DATA Sicherheitsexperten ist davon auszugehen, dass die entwickelten Spionageprogramme nicht in einer breit angelegten Kampagne gegen gewöhnliche Internetnutzer zum Einsatz kommen bzw. kamen, sondern eher für gezielte Angriffe gedacht sind.

Die vollständige Meldung steht Ihnen im G DATA Newsroom zur Verfügung: https://blog.gdatasoftware.com/2017/03/29561-wikileaks-vault7

Die umfassende Einordnung der beiden IT-Security Experten finden Sie im G DATA Security Blog: https://blog.gdatasoftware.com/2017/03/29561-wikileaks-vault7

Kontakt:

G DATA Software AG

Thorsten Urbanski
Leiter Unternehmenskommunikation
Phone: +49 (0) 234 - 9762 239

Christian Lueg
PR-Manager
Phone: +49 (0) 234 - 9762 160

E-Mail: presse@gdata.de
Internet: www.gdata.de

G DATA Software AG, G DATA Campus, Königsallee 178, 44799
Bochum, Deutschland