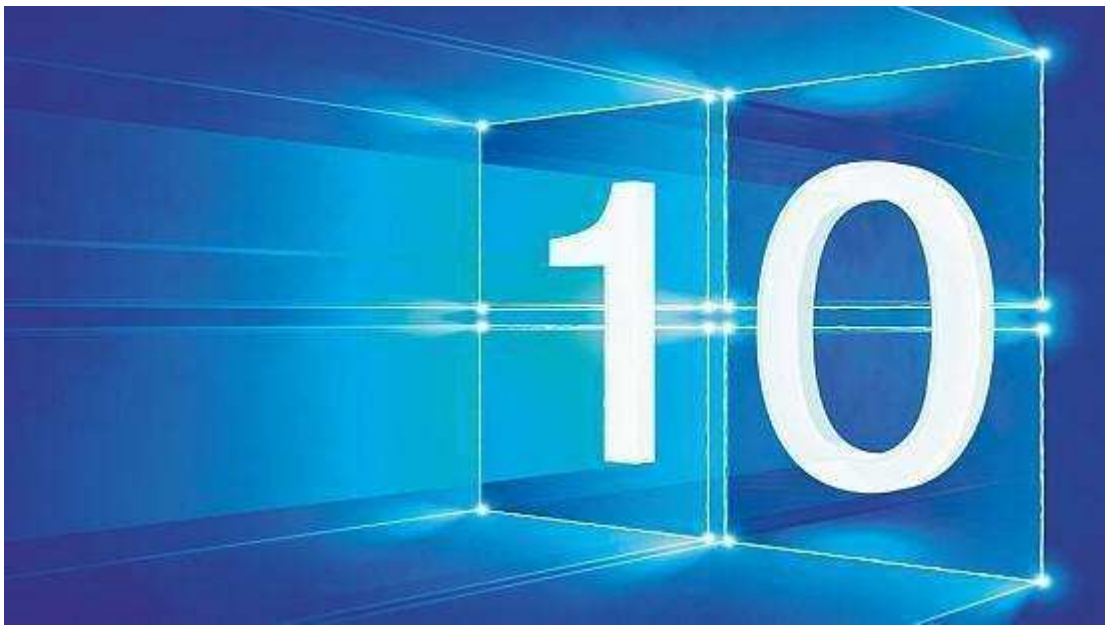
heise online

32C3: Kryptologe warnt vor dem "Botnetz" Windows 10

31.12.2015 10:52 Uhr – Stefan Krempl



Der Verschlüsselungsexperte Rüdiger Weis hat Microsofts neue "Sicherheitsanforderungen" wie verpflichtende Updates und Trusted Computing in Windows 10 verrissen. Microsoft habe "die Sache gar nicht im Griff".

Windows 10 fällt für den Berliner Kryptologen Rüdiger Weis unter die Lehrbuchdefinition für ein Botnetz, das Computer infiziert und Rechnerdienste vermietet. Die Begriffsbestimmung besage, dass "fremde Leute ohne Genehmigung auf meinem System Code ausführen können", erklärte der Professor auf dem 32. Chaos Communication Congress (**32C3 [1]**) in Hamburg. Dies treffe auf Microsoft aktuelles Betriebssystem zu, da der Nutzer darunter Updates allenfalls noch verzögern, aber nicht mehr verhindern könne.

Zum Glück gezwungen

Schon mit den Lizenzen der Testversion von Windows 10 habe Microsoft "außer dem Erstgeborenem so ziemlich alle Rechte gefordert, die man auf einem Computer vergeben kann", wetterte Weis. Wer nun Updates zumindest eventuell doch noch vermeiden wolle, müsse zunächst eine Art "Textadventure" durchlaufen. Aus Sicht Microsofts könne der Glaube: "Wir patchen besser als der Durchschnittsanwender" zwar eventuell sogar noch nachvollziehbar sein. Es sei aber "immer kritisch, wenn Leute zu ihrem Glück gezwungen werden sollen". So könne man nicht mit dem Endkunden umgehen.

Dazu komme, dass Microsoft dem Anwender die Kontrolle über die eigene Hard- und Software mit Windows 10 weitgehend entziehe, monierte der Leiter des Cryptolabs in Amsterdam. Sie **verpflichteten Rechnerhersteller auf einen Trusted-Computer-Chip [2]**, um selbst entscheiden zu können, "ob Systeme sicher sind". Der PC werde damit durch eine Set-Top-Box ersetzt, die der Kunde von dem US-Konzern "geleast" habe.

"Wir übergeben unsere ganze Sicherheit an Microsoft", warnte Weis. Es habe sich aber nicht nur in den vergangenen Jahrzehnten, sondern auch im gerade ablaufenden 2015 immer wieder herausgestellt, dass die Redmonder Sicherheit "nicht können".

Gescheiterte Qualitätskontrolle

Microsoft plage sich nach wie vor mit "Krypto-Zombies" in Form etwa von "veralteten Algorithmen wie SHA-1" herum, führte der Experte aus. Bei einem der jüngsten Versuche, den einschlägigen Code

"rauszuschmeißen", habe die Firma nur die "Dual-Boot-Einstellung für Linux zerschossen" und zugleich die Datenschutz-Einstellungen der Nutzer ruiniert. Dabei handle es sich "einfach um handwerkliche Katastrophen", mit denen selbst Verschwörungstheorien nicht mehr hinhauten.

Noch bedenklicher sei aber etwa im Herbst das Unterfangen Microsofts gewesen, ein überaus **dubioses Update für Windows 7 [3]** unter die Nutzergemeinde zu bringen, meinte Weis. Die mitgelieferten URLs für weitere Informationen wie hckSLpGtvi.PguhWDz.fuV01.gov seien derart kryptisch gewesen, dass er selbst bei deren Wiedergabe in seinem Latex-Textverarbeitungsprogramm eine Warnung erhalte.

Für den Forscher ist damit klar: "Da hat kein menschliches Wesen reingeguckt, nicht mal ein elektronisches". Jegliche Art von Qualitätskontrolle sei so gescheitert. Eine ernstzunehmende Erklärung sei Microsoft bis zum Tage schuldig geblieben. Weis suchte dies mit einem geflügelten Wort von Bundesinnenminister Thomas de Maizière (CDU) zu deuten: "Ein Teil der Antworten würde die Bevölkerung verunsichern."

"Traumchip für die NSA"

Dass Microsoft neben einem "Trusted Platform"-Modul (TPM) auch unterschriebene Bootloader verlange, bedrohe "das ganze Entwicklungssystem für freie Software". Jede Änderung müsse nämlich künftig von dem Konzern genehmigt werden. Dies sei völlig inakzeptabel: ein Booten mit einer elektronischen Fußfessel von Microsofts Gnaden dürfe es nicht geben.

Weis verschärfte zugleich seine **Kritik an der Secure-Boot-Funktion und Trusted Computing [4]** allgemein. Das TPM sei ein "Traumchip für die NSA", gab er zu bedenken. Wenn der Schlüssel dafür außerhalb von einer staatlichen Stelle erzeugt werde, existiere damit quasi ein "Generalschlüssel für alle Systeme in einem Land". Die Hardware könne man angesichts derart weit klaffender Hintertüren dann nur noch einschmelzen. Noch größere Sorgen bereite ihm, dass bei der jüngst von Juniper offenbarten Schwachstelle offenbar jemand die NSA-Backdoor weggeworfen und eine eigene eingebaut habe.

"Wir brauchen eine internationale Kontrolle des TPM-Herstellungsprozesses", forderte Weis. Zertifizierungs-Boot-Codes müssten offen gelegt, der gesamte Ansatz kartellrechtlich überprüft werden, da fast die ganze Computerhardware jenseits der Apple-Welt auf Windows angepasst werde. Lob hatte der Skeptiker nur für Microsofts Schritt parat, gemeinsam mit T-Systems eine "**deutsche Cloud [5]**" anzubieten. Dies bringe zumindest für Firmen mehr Rechtssicherheit und sollte auch für Privatanwender stärker geöffnet werden. Die mache schon das **Urteil des Europäischen Gerichtshofs [6]** zu "sicheren Datenhäfen" nötig. (**jk [7]**)

URL dieses Artikels:
http://www.heise.de/newsticker/meldung/32C3-Kryptologe-warnt-vor-dem-Botnetz-Windows-10-3057063.html

Links in diesem Artikel:

[1] http://www.heise.de/thema/32C3
[2] http://www.heise.de/newsticker/meldung/Windows-10-Neue-Geraete-nur-mit-UEFI-Secure-Boot-und-TPM-2582371.html
[3] http://www.heise.de/newsticker/meldung/Microsoft-verteilt-dubioses-Update-an-Windows-7-Nutzer-2835515.html
[4] http://www.heise.de/newsticker/meldung/31C3-Warnung-vor-Secure-Boot-und-Trusted-Computing-2507013.html
[5] http://www.heise.de/ct/ausgabe/2015-26-Microsoft-und-T-Systems-kreieren-eine-deutsche-Cloud-3016600.html
[6] http://www.heise.de/newsticker/meldung/Datenschutz-bei-Facebook-Co-EuGH-erklaert-Safe-Harbor-fuer-ungueltig-2838025.html
[7] mailto:jk@ct.de

1720142

Copyright © 2016 Heise Medien