heise Security

Experten zu Überwachungstechnik: "Exploits radikal verbieten" UPDATE

16.12.2015 19:51 Uhr – Stefan Krempl

(Bild: dpa, Karl-Josef Hildenbrand/Symbol)

Je sicherer ein IT-Produkt sei, desto schwerer sei es, in dieses einzudringen und Nutzer zu überwachen, erklärten Sachverständige bei einem Fachgespräch im Bundestag. Ausnutzbare Schwachstellen dürften nicht mehr gehandelt werden.

Experten waren sich bei einem **Fachgespräch [1]** am Mittwoch im Bundestag einig, dass der Einsatz von Überwachungstechnik strenger kontrolliert und reguliert werden müsse. Einen Königsweg dahin kennen auch die Experten nicht. Einige Ansätze kristallisierten sich aber heraus, wie das Problem der "menschenrechtsverachtenden Technologie" angegangen werden könnte.

Exploits sind Cybercrime

Michael Waidner vom Fraunhofer-Institut für Sichere Informationstechnologie (SIT) empfahl, bei der Cybersicherheit allgemein anzusetzen. "Je sicherer ein Produkt ist, desto schwerer ist es auch, in dieses einzudringen und Nutzer zu überwachen", betonte er. Schwachstellen sollten daher bestenfalls "von Anfang an vermieden" oder die Forschung befähigt werden, einschlägige Fehler möglichst schnell zu finden: "Die Good Guys müssen schneller sein als die Bad Guys." Einen Handel mit ausnutzbaren Schwachstellen dürfe es zudem nicht mehr geben: Der Wissenschaftler plädierte dafür, "Exploits radikal als Cybercrime zu verbieten". **[Update 18.12.2015:** Waidner betont gegenüber heise online, seine Äußerung bezüglich eines Exploit-Verbots sei im Kontext der Exportkontrolle zu verstehen und auf den Handel mit Exploits bezogen.**]**

Weiter sprach sich Waidner dafür aus, die Listen kritischer Exportgüter ständig anzupassen. Ein allgemeines Verbot von Spyware und vergleichbarer Techniken sei aber nicht zu rechtfertigen, da es legitime Einsatzzwecke dafür gebe. Gleichzeitig forderte der Forscher, dass Verschlüsselungssoftware und Programme zum Erkennen von Schwachstellen dagegen frei exportierbar sein müssten. Die Sicherheit des Einzelnen habe dabei im Vordergrund zu stehen insbesondere gegenüber staatlicher Interessen an Massenüberwachung. Sicherheitsbehörden könnten trotzdem noch die "Implementierung von Kryptographie angreifen" oder Kommunikation "an den Quellen" überwachen.

Exportkontrolle

Ben Wagner, Direktor der Forschungsstelle Internet und Menschenrechte an der Europa-Universität Viadrina in Frankfurt an der Oder, sprach sich ebenfalls für eine stärkere Exportkontrolle für Überwachungstechnik aus. Dafür müsse zunächst das **Wassenaar-Abkommen [2]** weiterentwickelt werden. Mit unverbindlichen Maßnahmen der Unternehmensethik komme man in diesem Bereich, der vor allem hierzulande viel zu undurchsichtig sei nicht weit weiter. Er brachte auch eine bessere "Endverbrauchskontrolle" ins Spiel, räumte aber ein, dass eine solche gerade im Ausland nur schwer zu leisten sei.

Einblicke in die Branche gab Christian Mihr von Reporter ohne Grenzen. Aus Deutschland heraus seien etwa 15 Firmen weltweit mit Trojanern aktiv, darunter Trovicor in München oder FinFisher (Gamma International). Es gebe sogar Hinweise auf **Hermes-Bürgschaften [3]** der Bundesregierung zur Versicherung deutscher Exporte nach Syrien vor Ausbruch des Kriegs.

Beliebt bei Regimes

Autoritäre Staaten liebten das Internet dank der Kontrolltechniken inzwischen, ergänzte Sandro Gaycken von der European School of Management and Technology (ESMT). Das Netz sei dort kein Werkzeug mehr für Demokratisierung. Auch Verschlüsselung und Anonymisierung hälfen wenig, wenn sie laienhaft eingesetzt würden. Letztlich seien das Internet und Smartphones "selbst die Verräter", da die damit hinterlassenen elektronischen Spuren mithilfe von Big-Data-Analysen zu "vollständigen Profilen" zusammengesetzt werden könnten. US-Firmen wie Palantir und Blue Coat, die teils aus der Geheimdienstecke kämen, seien hier führend. Cisco und andere Konzerne versuchten zudem inzwischen genauso mitzuspielen wie asiatische Hersteller.

Ähnlich wie Waidner warb Gaycken dafür, "fertige Exploits" in die Exportkontrolle über Wassenaar mit einzubeziehen. Beide Forscher liebäugelten auch damit, Techniken fürs digitale Rechtekontrollmanagement (DRM) oder Wasserzeichen einzusetzen, um Hürden zu errichten, dass sich

Überwachungstechnik einfach weiterverbreitet. Ein Allheilmittel stelle dies freilich nicht dar. (**vbr [4]**)

URL dieses Artikels:
http://www.heise.de/security/meldung/Experten-zu-Ueberwachungstechnik-Exploits-radikal-verbieten-3045606.html

Links in diesem Artikel:
[1] http://www.bundestag.de/dokumente/textarchiv/2015/kw51-pa-digitale-agenda/398958
[2] http://www.heise.de/security/meldung/Hacking-Team-Was-ist-schon-Wassenaar-2764292.html
[3] https://de.wikipedia.org/wiki/Hermesdeckungen
[4] mailto:vbr@ct.de