Hacker der neuen Generation

CYBER-ATTACKEN Es drängt sich die Vermutung auf, dass zunehmend kriminelle Organisationen gefährliche Schadprogramme verbreiten.

Das Stuxnet-Schadprogramm gegen Industrieanlagen wird nicht der letzte Angriff auf Computer gewesen sein. Aus dem Internet kommen Viren und „Trojanische Pferde“, die es auf vertrauliche Informationen abgesehen haben, oder, wie im Fall von Stuxnet, den Betrieb (iranischer Atomkraftwerke) stören sollen. Angriffe führen zu Arbeitsausfällen mit begrenzten Auswirkungen – die sich aber summieren – bis hin zu größeren Einzelschäden, etwa, wenn Firmenideen an Konkurrenten übermittelt oder erhebliche Summen vom Bankkonto abgebucht werden. Die Komplexität mancher Schadsoftware legt nahe, dass nicht mehr ein einzelner Hacker dafür verantwortlich ist, sondern große Unternehmen, kriminelle Organisationen oder Geheimdienste.

Wie können wir uns schützen? Die erste Möglichkeit sind Virenscanner. Diese erkennen Schadprogramme aber oft nicht, wenn sie neu sind. Die zweite Möglichkeit wäre, unsere Betriebssysteme zu verbessern. Hier besteht die Schwierigkeit darin, dass wir Nutzer sie gerne nutzen, um die verschiedensten Programme aus allen möglichen Quellen laufen zu lassen, und wir uns damit weiterhin Schadprogramme holen werden. Die dritte Möglichkeit wäre, alle Kommunikation auf dem Internet fälschungssicher zu signieren, damit man die Verursacher findet. Das wäre ein Big Brother-System, und ein Angreifer würde versuchen, sich hinter einer gefälschten Identität zu verbergen. Deshalb wird es auf offenen Netzen auch in Zukunft Schadprogramme geben.

An einer weiteren, zukunftsträchtigen Idee wird derzeit in Forschung und Unternehmen gearbeitet. Sie besteht darin, Schadprogramme unter Quarantäne zu stellen, indem nicht vertrauenswürdige Daten aus dem Internet oder von USB-Sticks vom normalerweise genutzten Betriebssystem und seinen Anwendungen in verschiedenen Containern voneinander isoliert werden. Die nicht vertrauenswürdigen Daten könnten in ihren Containern angeschaut werden. Besonders sensible Informationen würden ebenfalls von den normalen Anwendungen isoliert und in einem eigenen Container abgelegt. Neue Filter können einen begrenzten Austausch zwischen den Containern ermöglichen, etwa, wenn es um reine Textdaten geht. Die Handhabung eines solchen Rechners ist zunächst komplexer, bietet aber auch neue Freiheiten: Man kann darauf ohne Sorge alles machen.

Ist die perfekte Isolation der Container überhaupt machbar? Das ist noch nicht bewiesen. Intel und AMD arbeiten daran, dass ihre Hardware die Isolierung sicherstellt. Wir vermuten, dass Angriffsstellen für professionelle Kriminelle nur vermieden werden können, wenn die Spezifikationen und Programme eines derartigen Systems auf dem Internet veröffentlicht werden, damit sie für Interessierte überprüfbar sind. Dann könnte das System, unter Kontrolle einer geeigneten Institution, etwa aus der Linux Community, so lange verbessert werden, bis es perfekt ist. Die Autoren haben am Institut für Technikfolgenabschätzung und Systemanalyse des KIT beim Bau eines Prototypen mitgewirkt, der für die Handhabung durch Laien geeignet sein soll (http://www.itas.fzk.de/deu/projekt/2005/webe05xy.htm). Wir denken, nicht vertrauenswürdige Daten unter Quarantäne zu stellen, ist der vielversprechendste Weg, Nachfolger von Stuxnet aus unseren Betriebssystemen und Firmennetzwerken fernzuhalten.

AUSSENANSICHT

ARND UND DIRK WEBER
Die Autoren arbeiten am Institut für Technikfolgenabschätzung und Systemanalyse.

➜ Die Außenansicht gibt die subjektive Meinung des Autors wieder und nicht unbedingt die der Redaktion.