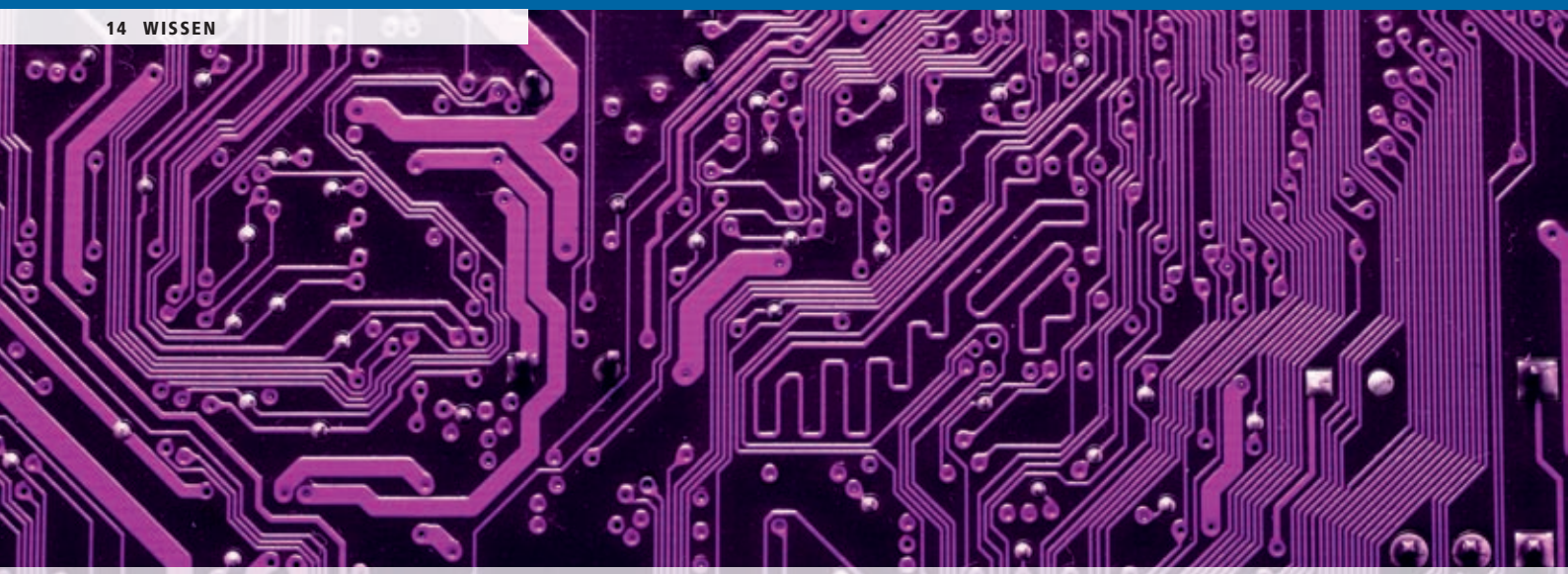

Stuxnet erinnert an Verletzlichkeit von Energiesystemen

Die Virenattacken durch den Computerwurm Stuxnet unter anderem auf Rechner des Atomkraftwerks Buschehr im Iran haben gezeigt, wie verletzlich Informationsanlagen moderner Infrastrukturen sind. Auch moderne Stromnetze und ganze Energiesysteme könnten von künftigen ähnlichen Hackerangriffen betroffen sein.

Stuxnet ist ein völlig neuartiges Computervirus. Im Gegensatz zu herkömmlichen Viren zielt es nicht nur auf digitale Systeme wie PC oder Server, sondern hat letztlich ein physisches System im Visier. «Der Computerwurm zielt auf kritische Infrastrukturen, indem er in Überwachungs- und Steuerungskonzepte technischer Prozesse eingreift», sagt ETH-Informatik-Professor Srdjan Capkun. Die Folge: Nicht nur ein Computerprogramm kann bei einem solchen Hackerangriff zu Schaden kommen, sondern auch die damit gesteuerten Anlagen. «Er ist das erste Computervirus, das verheerende Schäden in der realen Welt verursachen kann. Das Gefährliche an diesem Wurm: Hacker können damit ganze Fabriken und Kraftwerke manipulieren», schreibt auch die Computersicherheitsfirma Symantec auf ihrer Internetseite.

Übernimmt unbemerkt die Kontrolle

Stuxnet ist der erste Cyberangriff, der gezielt industrielle Steuersysteme befällt. Der Stuxnet-Wurm sucht nach Symantec-Angaben nach industriellen Steuersystemen und ändert den Code in diesen Systemen so, dass Angreifer von den Betreibern unbemerkt die Kontrolle über diese Systeme übernehmen können. Aber nicht nur die Funktionsweise des Wurms, sondern auch seine Entstehung ist einzigartig. «Die Raffinesse von Stuxnet ist in der Tat eindrücklich», erklärt Capkun. Man müsse davon ausgehen, dass dieser Wurm von einem ganzen Team programmiert worden sei, in dem sowohl Cyberexperten als auch Fachleute für den Betrieb industrieller Systeme mitgearbeitet hätten. «Aufgrund seiner hohen Komplexität und des finanziellen Aufwands sind nur wenige Gruppen in der Lage, diese Art von Bedrohung zu entwickeln», schreibt Symantec. Der Wurm besteht aus einem komplexen Computercode, dessen Entwicklung ein hohes Mass an Fachkenntnissen erfordert.

Gefahr momentan gebannt

Vorerst ist die Gefahr durch Stuxnet gebannt. Alle Antivirenfirmen bieten die nötigen Software-Updates an. Capkun geht davon aus, dass Energiesysteme und andere Infrastrukturen derzeit gut gegen Stuxnet gewappnet sind. Dies ist auch für Schweizer Kernkraftwerke der Fall: «Die nukleare Sicherheit der Schweizer Kernkraftwerke und der Schutz von Menschen und Umwelt sind gewährleistet», teilt das Eidgenössische Nuklearsicherheitsinspektorat (ENSI) mit. Dem ENSI ist das Computervirus Stuxnet seit mehreren Monaten bekannt. Die entsprechenden Spezialisten stünden mit den Betreibern der schweizerischen Kernkraftwerke sowie mit der Melde- und Analysestelle Informationssicherung MELANI in Bern in engem Kontakt. «Unsere Untersuchungen haben gezeigt, dass die nuklearen Systeme und zentralen Sicherheitssysteme vom Virus nicht betroffen sind. Auch die weiteren Systeme wie Neben- und Hilfssysteme sind nicht angegriffen worden und sind geschützt», so das ENSI.

Warnung für die Zukunft

Allgemein gesehen würden künftig die Risiken einer Infizierung steigen, gibt ETH-Informatik-Professor Capkun zu bedenken. «Dass sich das Virus anfangs über USB-Sticks verbreitete, bedeutet, dass es sogar Systeme infizieren konnte, die vom Internet getrennt gewesen sind.» Auch so genannte Smart Meters in Haushalten könnten deshalb künftig betroffen sein: Diese Geräte lesen dereinst den Stromverbrauch in Echtzeit ab und sind untereinander sowie mit einer zentralen Kommunikations- und Steuerungsinfrastruktur verbunden. «Wenn jede Person von zu Hause irgend eine Art Kommunikationsverbindung zum Versorgungsnetz hat, wird das neue Wege für Angreifer eröffnen, dieses System zu infizieren und zu untergraben», sagt Capkun. Dem Problem ist sich auch das Bundesamt für Energie bewusst. «Wir haben ein Projekt gestartet, um die Gefährlichkeit solcher Hackerangriffe in Bezug auf künftige Smart Grids zu testen», erklärt der zuständige BFE-Experte Michael Moser.

(klm)

Internet

Departement für Informatik der ETH Zürich:
www.inf.ethz.ch

Antiviren-Hersteller Symantec:
www.symantec.com/de

Eidgenössisches Nuklearsicherheitsinspektorat (ENSI):
www.ensi.ch

Forschungsprogramm Elektrizitätstechnologien und -anwendungen im BFE:
www.bfe.admin.ch/forschungelektrizitaet