

«Wir befinden uns in der Vorbereitung zum Cyber-Krieg»

Sibylle Katja Bossart
Donnerstag, 23. September 2010, 14:54 Uhr

Der Computervirus Stuxnet soll das iranische Atomkraftwerk Bushehr infiziert haben. Der Wurm wurde laut Experten von professionellen Gruppen geschaffen, um das Leitsystem der Anlage zu beschädigen. IT-Spezialist Ivan Bütler hat für «tagesschau.sf.tv» Fragen zu Spionage und Attacken mit Computersoftware beantwortet.



Artikel bewerten

★ ★ ★ ★ ★

Artikel teilen

-  Facebook
-  Twitter
-  E-Mail
-  Share

 Gefällt mir 1

Die vernetzte Welt: Ein Tummelfeld für Hacker und Spione und gefährlich wie ein Minenfeld. *colourbox / symbolbild*

Es gibt zwei Arten von Computerviren: Die eine, wie zum Beispiel der Wurm «I love you», soll Rechner auf der ganzen Welt befallen, die andere Art von Viren wird gezielt für Industriespionage entwickelt. Zur letzteren Art zählt Stuxnet.

«Solche Würmer dringen in Leitsysteme von Wasserkraftwerken oder Atomanlagen ein und attackieren sie», sagt Ivan Bütler. Der Trojaner wird von diesen Leitsystemen übers Internet geholt. Bei solchen Trojanern sind keine Heimprogrammierer, sondern kriminelle Gruppierungen am Werk, gibt Bütler zu bedenken.



«Wir sind hochgradig verwundbar.»

Ivan Bütler, CEO von [Compass Security AG](#)

Wer bemerkt denn einen solchen Trojaner im System eines Kraftwerks und wie? Meistens falle dem Systemadministrator auf, dass im betroffenen Computersystem etwas nicht stimme, so Bütler. Die elektronische Wanze kann durchaus erst 2-3 Jahre nach der eigentlichen Verseuchung bemerkt werden.

Trojaner wie Stuxnet seien aber nichts Neues, betont der Computerspezialist. «Das Problem ist seit acht Jahren bekannt und es gibt mehrere Fälle, die in den Medien keine Beachtung gefunden haben», äussert sich Ivan Bütler. «Wir sind hochgradig verwundbar.»

Der Virus Stuxnet

Berichte über den Computervirus Stuxnet sind derzeit in diversen Medien zu finden. Stuxnet wurde im Juni 2010 erstmals von IT-Sicherheitsexperten auf den Computern von Iranern entdeckt. Zu diesem Zeitpunkt hatte sich der Trojaner bereits in den Ländern Pakistan, Indonesien, Indien, aber auch in Europa und den USA verbreitet.

Die Experten waren verblüfft über die komplexe Struktur des Virus. Der Trojaner schaffte es, gleich vier Schwachstellen im Microsoft-Betriebssystem Windows auszunutzen.

Laut Medienberichten und Experten sind momentan weltweit gegen 50'000 Anlagen mit Stuxnet infiziert, richten dort aber keinen Schaden an. Der Trojaner scheint gezielt für die iranische Atomanlage Bushehr programmiert worden zu sein. Stuxnet und der angeblich gezielte Angriff auf Bushehr wurde auch vergangenen Dienstag an einer vertraulichen Konferenz von IT-Sicherheitsexperten nahe Washington analysiert.

Spezialisten könnten in 99 Prozent aller Systeme der Welt einbrechen, Staaten hätten es so einfach wie nie, per Computervirus Wirtschaftsspionage zu betreiben, ergänzt Bütler. Er spricht denn auch von Vorbereitungen zum «Cyber-Krieg».

Angriffe von innen

Die Ursache ist laut dem Spezialisten die weltweite Vernetzung. «Es fängt damit an, dass wir am Arbeitsplatz Internetseiten lesen sowie Mails empfangen und verschicken können», illustriert er. Eine gefährdete Zone sind auch die Intranetze von Firmen. Ist der Wurm dort einmal drin, kann er sich ungehindert verbreiten und zurück zu seinem Urheber im Internet kommunizieren.

Ein Grund dafür ist, dass Schutzvorkehrungen wie Firewalls Angriffe nur von aussen abwehren. Gegen Attacken von innen, wie im Fall des Intranets, sind sie aber machtlos.

Sicherheitsrisiko USB-Stick

Grosse Sicherheitslecks sind gemäss Ivan Bütler USB-Sticks. Bütler veranschaulicht die Gefahr am Beispiel der Personalberatung einer Firma. Schicke jemand Bewerbungsunterlagen per USB-Stick, könne dadurch auch ein Trojaner ungehindert ins System eindringen.

Und wie schützt man sich vor der Gefahr durch USB-Sticks? «Indem man keine mehr zulässt, sie zumindest freischaltet oder eine Trennung der Netze konzipiert», antwortet Bütler. Gerade in Abteilungen, die häufig ungefragt Dokumente zugeschickt bekommen - wie eben eine Personalabteilung - sei dies aber eine ungeliebte Massnahme.

Es falle dadurch natürlich eine Unmenge von Papier, das heisst Mehrarbeit, an, sagt Bütler. «Wir Menschen sind jedoch in den seltensten Fällen bereit, Einschränkungen hinzunehmen.» Es wolle natürlich auch niemand auf das Internet verzichten.

Eine weitere Schutzmassnahme sei, das Internet in einer sicheren Zone laufen zu lassen. Es gebe Organisationen, die das Internet in einer sogenannten High Secure Zone laufen lassen. Der Virus kann auch dort eingeschleust werden, doch sein Wirkungskreis ist eingeschränkt. Wer genau solches High-Secure-Internet nutzt, ist Bütler nicht zu entlocken.

Terror aus dem Computer

Das Netz könnte sich in Zukunft noch stärker als Mittel für Terroranschläge erweisen. Ivan Bütler nennt ein Beispiel dafür: «Das Leben hängt von sauberem Wasser ab; nun programmiert jemand eine Schleusenöffnung und verseucht Wasser.»

Der Computer-Spezialist glaubt, dass sich die Staaten bei den Cyber-Waffen im Aufrüstungsprozess befinden. Die Möglichkeiten seien da. «Es stellt sich nur die Frage: Wer hat die kriminelle Energie, das Internet dafür zu nutzen», so Bütler.