

Kolumne von Michael Maercks**Stuxnet und andere Staatstrojaner**

Stuxnet heißt das Computervirus, das international für Aufregung sorgt. Doch diesmal ist nicht der heimische Computer bedroht, sondern Steuerungscomputer von Industrieanlagen. Stuxnet greift speziell eine Software von Siemens an, die zur Steuerung und Überwachung von Betriebsabläufen in großen Industrieanlagen und Kraftwerken eingesetzt wird und die auf Windows-Rechnern läuft.



Nicht Industriespionage ist das Ziel, sondern durch Manipulation von Kenndaten sollen Steuerungsprozesse manipuliert werden. Stuxnet wird deshalb als reines Sabotageprogramm eingeschätzt. Der Chaos Computer Club-Sprecher Frank Rieger spricht von einem "digitalen Erstschlag".

Das besondere an diesem Virus ist die Komplexität der Programmierung und die Art der Verbreitung. Weil Industriecomputer in der Regel keinen Zugang zum Internet haben, verbreitet sich das Virus über infizierte USB-Speichersticks. Diese Lücke im Windows-Betriebssystem soll schon seit einem Jahr bekannt sein, aber erst jetzt, nachdem Stuxnet schon tausende Computer befallen hat, hat Windows diese Lücke mit einem Sicherheits-Patch geschlossen. Es konnte von Virenschutzprogrammen nicht erkannt werden, weil digitale Signaturen anderer Hersteller verwendet wurden, die das Betriebssystem automatisch als vertrauenswürdig interpretiert hat.

Der volle Programmumfang dieses Trojaners konnte noch nicht entschlüsselt werden. Stuxnet wird nur in Anlagen mit einer spezifischen Konfiguration aktiv, er zielt auf ganz spezielle Prozesse. Infiziert sind vor allem Computer im Iran, Pakistan und Indien. Experten schließen deshalb nicht aus, dass es ein digitaler Angriff auf die iranischen Uran-Anreicherungsanlagen oder den neuen Reaktor in Bushehr ist. In diesen Anlagen soll die Steuerungssoftware von Siemens arbeiten.

Weil das Programm so komplex ist, gehen Experten davon aus, dass als Auftraggeber nur staatliche Stellen in Frage kommen. Auch Deutschland arbeitet an solchen Programmen. Das zeigte die Auseinandersetzung um den Bundestrojaner, mit dem der Verfassungsschutz die Computer ausspähen kann. Mit dem neuen Paragraphen 20k des BKA-Gesetzes ist dafür die Rechtsgrundlage geschaffen worden.

Der "Cyber-Krieg" erhält damit eine neue Dimension. Bisher dienten IT-Angriffe der Spionage oder Überwachung, der Unterbrechung der Kommunikation oder waren Bestandteil der psychologischen Kriegsführung. Jetzt zeigt sich, dass über solche Trojaner auch gezielt Sabotage mit möglicherweise katastrophalen Folgen betrieben werden kann.
