ABEDIN TAHERKENAREH / DPA

Atomanlage im iranischen Buschehr
Wer sind die Angreifer, was ist das Ziel?

COMPUTERSICHERHEIT

Mord ohne Leiche

Ein neuartiger Computerschädling gibt Rätsel auf: Er ist raffiniert, professionell und diskret. Wurde er verwendet, um das iranische Atomprogramm zu stören?

Sabotage, Spionage, Säbelrasseln – oder gar Krieg? Ein winziges Stück Software, kleiner als ein MP3-Song, lässt Sicherheitsexperten in aller Welt rätseln. „Stuxnet“ heißt der digitale Schädling, der sich gezielt in Steuersysteme der Firma Siemens einnistet. Im Jahr 2009 tummelte er sich schon im Netz. Im Sommer 2010 tauchte ein neues, noch tückischeres Update auf.

So weit, so normal. Sekunde für Sekunde hagelt ein Sturm bösartiger Software auf jeden Server ein, der mit dem Internet verbunden ist; Millionen Schadprogramme sind bekannt.

Doch diesmal scheint vieles anders. „Der digitale Erstschlag ist erfolgt“, trompetete die „FAZ“; „Krieg im Cyberspace“ und „Neue Viren, so gefährlich wie Panzer“ lauteten andere Schlagzeilen.

Noch allerdings ist völlig unklar: Wer sind die Opfer, wer die Angreifer, was ist der Schaden – und was das Ziel? Noch gleicht Stuxnet einem Mord ohne Leiche.

Der Mann, der den größten Wirbel um den Virus ausgelöst hat, hält sich müde an seiner Kaffeetasse fest: Ralph Langner steht auf dem Flur im Hilton Rockville, einem schmucklosen Bettenkasten in einem Vorort von Washington. Drinnen debattieren rund hundert Experten, es geht um denkbare Computerangriffe auf Fabriken, Stromnetze oder Kläranlagen. „Control Systems Cyber Security Conference“ heißt die Veranstaltung.

„Ich habe seit zwei Wochen kaum geschlafen“, sagt Langner. Der Grund: Auf seiner Website brüstet er sich, Stuxnet sei „der Hack des Jahrzehnts“, und er habe das Rätsel darum „weitgehend gelöst“: Iranische Atomanlagen seien womöglich das Ziel der Attacke gewesen.

Seitdem kommt Langner nicht mehr zur Ruhe: Fernsehsender, Zeitungen – alle wollen Beweise. Und sie wollen wissen, was es bedeutet für die internationalen Beziehungen. Aber Langner wimmelt ab: „Was soll ich dazu sagen? Ich verstehe doch gar nichts von Geopolitik.“

Er arbeitet im Hamburger Stadtteil Volksdorf, von dort aus berät er Firmen, wie sie sich vor Hackerangriffen schützen können. Seit seinem Vortrag über die mögliche Iran-Connection bemüht er sich nun, bei diesem Thema zurückzurudern: „Ich sage ja nicht, dass es so gewesen sein muss. Es ist nur ein plausibles Szenario.“

Tatsächlich gibt es bislang keine Beweise, sondern nur Indizien. Stuxnet, darin sind sich alle einig, ist anders als die meisten Schadprogramme: Der Schädling ist ungewöhnlich raffiniert komponiert. Er zeugt von viel Insiderkenntnis und nutzt geklaute Sicherheitszertifikate.

Auch in Deutschland seien Anlagen infiziert worden, wenn auch ohne größere Schäden, heißt es beim Bundesamt für Sicherheit in der Informationstechnik (BSI). „Damit entsteht eine neue Bedrohungslage“, sagt Stefan Ritter, Leiter des Computer Emergency Response Teams beim BSI. Bisher habe es sich bei Angriffen auf Industrieanlagen stets nur um theoretische Szenarien gehandelt.

MANUEL BALCE CENETA / AP

NSA-Chef Alexander
Der Hype kam nicht ungelegen

Es seien gleich mehrere Eigenschaften, die Stuxnet so ungewöhnlich machten, erklärt Liam O’Murchu, Virenspezialist bei der Antivirensoftware-Firma Symantec:

- Das Programm ist so aufwendig, dass über fünf Spezialisten ein halbes Jahr daran gearbeitet haben dürften.
- Stuxnet macht sich gleich vier unentdeckte Sicherheitslücken zunutze. Das Wissen um solche „Zero Day Exploits“ kann auf dem Schwarzmarkt sechsstellige Euro-Beträge kosten.
- Die Infektion erfolgt wohl mit Hilfe von USB-Sticks, die per Hand in die Computer vor Ort eingesteckt werden. Dieser altmodische Angriffsweg empfiehlt sich bei Anlagen, die aus Vorsicht keine Verbindung zum Internet haben.
- Von den Infektionen waren nicht reiche Länder, sondern anfangs besonders Indien, später zu rund 60 Prozent Iran betroffen. In iranischen Atomanlagen werden Siemens-Systeme vermutet.
- Stuxnet befällt nicht massenhaft und wahllos irgendwelche Rechner wie etwa der „I Love You“-Virus. Pro USB-Stick war der neue Schädling ursprünglich auf drei Infektionen beschränkt – vermutlich, um weniger aufzufallen.

Diese Eigenschaften machen Stuxnet zum idealen Spekulationsobjekt für Verschwörungstheoretiker. Denn wer wenn nicht der Mossad oder der amerikanische Geheimdienst NSA sollte eine solche Software schreiben können?

Denkbar wäre aber auch, dass es nicht zuletzt ums Geld geht. Der Erfolg der Sicherheitsbranche hängt schließlich maßgeblich von der gefühlten Bedrohung ab. Und derzeit laufen in den USA Beratungen zum Thema Computersicherheit. Am vergangenen Donnerstag forderte Keith Alexander, Chef der NSA und des neuen Cyber Command, vor dem zuständigen Ausschuss des US-Repräsentantenhauses den Aufbau eines sicheren Datennetzes für Kraftwerke und andere kritische Infrastrukturen. Der zeitgleiche Hype um den „Erstschlag“ kam den Militärs dabei vermutlich nicht ungelegen.

Der Berliner Sicherheitsspezialist Sandro Gaycken, dessen Buch mit dem Titel „Cyberwar“ im Dezember erscheinen wird, bringt noch eine andere Überlegung ins Spiel: „Vielleicht sollte Stuxnet einfach nur Überlegenheit demonstrieren – so ähnlich wie bei der Mondlandung oder den Wasserstoffbombentests.“

MARCEL ROSENBACH, GREGOR PETER SCHMITZ, HILMAR SCHMUNDT