

Anzeige

NZZ Online

Dienstag, 16. November 2010, 23:55:43 Uhr, NZZ Online

Nachrichten > International

16. November 2010, 16:24, NZZ Online

Eine Software als Undercover-Agent

Stuxnet-Virus gezielt zur Sabotage in Irans Atomanlagen programmiert



Das Stuxnet-Virus hat auch Computer im iranischen Atomkraftwerk von Bushehr befallen. (Bild: Reuters)

Neueste Untersuchungen haben gezeigt, dass der Stuxnet-Computervirus so programmiert worden war, dass er gezielt zentrale Einrichtungen der iranischen Uran-Anreicherungsanlagen beschädigen konnte.

bbu. Wozu wurde Stuxnet programmiert? Und von wem? Diese Frage stellte sich, als vor knapp zwei Monaten die Meldung die Runde machte, das iranische Nuklearprogramm sei durch ein Computervirus namens Stuxnet attackiert worden. Neue Forschungen der auf Internet-Sicherheit spezialisierten Firma Symantec sollen jetzt ergeben haben, dass der Stuxnet-Virus tatsächlich nichts anderes als eine Art Cyber-Bombe ist, die gezielt für die Sabotage von Atomanlagen in Iran entwickelt worden war.

Störungen in Irans Atomanlagen

Seit dem Sommer war es nach verschiedenen Angaben in Einrichtungen des iranischen Nuklearprogramms zu einer Reihe von Problemen und Zwischenfällen gekommen, sodass Analytiker im Westen bereits eine Verzögerung im Atomprogramm Teherans für möglich hielten. Iran hatte Ende September dann bestätigt, dass eine sogenannte Cyber-Attacke durch den Computer-Schädling Stuxnet verübt worden sei. Die Regierung in Teheran spielte die Wirkung aber herunter.

Wie die Nachrichtenagentur Reuters am Dienstag berichtete, hätten die Software-Experten von Symantec jetzt herausgefunden, dass Stuxnet gezielt ganz bestimmte Antriebsmotoren der Uran-Zentrifugen, welche in Iran zur Anreicherung des nuklearen Brennstoffs verwendet werden, beeinflusste. Die Software-Steuerung dieser Motoren würden die Frequenz, mit der diese Zentrifugen rotierten, kontrollieren. Stuxnet schädige genau diese Motorsteuerung und sabotiere damit das gesamte System der Urananreicherung.

Dabei attackiert der Virus nach den neuesten Erkenntnissen nur solche Teile der Anlagen, welche mit Frequenzen zwischen 807 und 1210 Herz arbeiten. Dies sind sehr hohe Geschwindigkeiten, die nur bei ganz bestimmten Anwendungen überhaupt vorkommen – zum Beispiel bei Gaszentrifugen von Urananreicherungsanlagen.

Hinweise auf Cyber-Krieg

«Wir haben die entscheidenden Bruchstücke des Puzzles zusammengefügt» meinte nun ein Vertreter von Symantec dazu. Wegen der komplexen Programmierung des Virus war früh schon der Verdacht aufgetaucht, dieser sei nicht von privaten Auftraggebern, sondern von staatlichen Stellen entwickelt worden, welche über das dazu nötige Know-How und entsprechend qualifiziertes Personal verfügten. Diese These dürfte nun noch einiges plausibler erscheinen. Verdächtig wurden insbesondere westliche Geheimdienste und Israel, das sich vor allem vor einem nuklearen Iran zu fürchten hat.

► **Internet:** Partisanen im Cyberspace [http://www.nzz.ch/nachrichten/startseite/partisanen_im_cyberspace_1.7761855.html]

Link: http://www.nzz.ch/nachrichten/international/partisanen_im_cyberspace_1.7761855.html

► **Iran:** Spekulationen um Viren-Attacke [http://www.nzz.ch/nachrichten/panorama/irans_atomprogramm_moegliches_ziel_1.7679299.html]

Link: http://www.nzz.ch/nachrichten/international/irans_atomprogramm_moegliches_ziel_1.7679299.html

Diesen Artikel finden Sie auf NZZ Online unter:

http://www.nzz.ch/nachrichten/international/ein_virus_als_undercover-agent_1.8400645.html

Copyright © Neue Zürcher Zeitung AG

Alle Rechte vorbehalten. Vervielfältigung oder Wiederveröffentlichung zu gewerblichen oder anderen Zwecken ohne vorherige ausdrückliche Erlaubnis von NZZ Online ist nicht gestattet.
