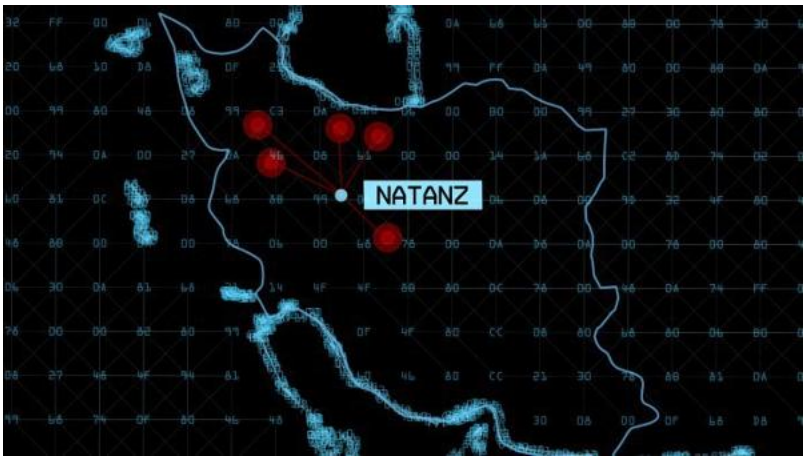
Stuxnet angeblich Teil eines größeren Angriffs auf kritische Infrastruktur des Iran

16.02.2016 16:44 Uhr – Martin Holland **vorlesen**



Ziel des Angriffs war unter anderem die iranische Atomanlage in Natanz (Bild: Zero Days)

Dass die USA und Israel hinter Stuxnet steckten, um Irans Atomprogramm zu stören, gilt mittlerweile als gesichert. Ein neuer Dokumentarfilm behauptet nun, dass der Cyber-Wurm Teil eines viel größeren Programms war, das den ganzen Iran lahmlegen sollte.

Die Cyber-Waffe Stuxnet war lediglich Teil eines viel umfangreicheren Programms, das einen umfangreichen Cyberangriff der USA auf den Iran vorbereiten sollte. Zu diesem Schluss kommt zumindest der neue Film "Zero Days" der bekannten Dokumentarfilm-Regisseurs Alex Gibney ("Taxi to the Dark Side", "Going Clear"), **berichtet *Buzzfeed*** [http://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma#.qb6ZdbeVA] einen Tag vor dessen **Premiere auf der Berlinale** [https://www.berlinale.de/de/programm/berlinale_programm/datenblatt.php?film_id=201608480#tab=filmStills] . Demnach war Stuxnet Teil des Programms "Nitro Zeus". In dessen Rahmen hätten sich die USA elektronischen Zugang zu verschiedensten kritischen Infrastrukturen des Iran verschafft, um die gegebenenfalls in kürzester Zeit lahmlegen zu können.

Komplexe Angriffsvorbereitung

Unter Berufung auf mehrere Quellen aus US-Geheimdiensten und dem US-Militär behauptet der Film demnach, dass in den USA Hunderte Personen an der Operation beteiligt waren. Insgesamt seien "Hunderte Millionen US-Dollar" ausgegeben worden, iranische Infrastruktur auf ein Kommando hin "unterbrechen, beeinträchtigen und zerstören" zu können. Dafür sei hunderttausendfach Code in iranische Anlagen eingeschleust und dann regelmäßig überprüft worden, um sicherzustellen, dass er im Fall des Befehls zum Angriff auch funktioniert.

Bedenken habe es vor allem im US-Außenministerium gegeben, das sich um die Souveränität des iranischen Cyberspace und mögliche Auswirkungen auf die Zivilbevölkerung gesorgt habe. Gleichzeitig hätten Quellen des Dokumentarfilmers auch das Ausmaß der Operation als gefährlich bezeichnet. Einige Planer hätten "keine Ahnung" gehabt, was im Fall eines Angriffs tatsächlich passieren würde. Wenn man beispielsweise nur einen Teil des Stromnetzes deaktiviere, könne in der Folge trotzdem die Elektrizität im ganzen Land ausfallen.

Der Wurm Stuxnet selbst sei im Rahmen des Programms entwickelt worden, zitiert *Buzzfeed* weiter. Die Partner aus Israel hätten dabei geholfen und ungehinderten Zugang zu dessen Quelltext gehabt. Als die USA 2009 aus Angst vor einer Entdeckung die Cyber-Waffe zurückzuziehen begannen, habe Israel eine modifizierte Version eingeschleust. Die habe sich viel einfacher ausgebreitet und schließlich Hunderttausende Computer in mehr als 115 Ländern infiziert. Diese Version sei auch die, die dann entdeckt und analysiert worden war. Diese für den Film zusammengetragenen Details decken sich anscheinend mit den Erkenntnissen, die

der deutsche IT-Experte Ralph Langner durch **die Analyse von Stuxnet gesammelt** [http://www.heise.de/security/meldung/Das-Stuxnet-Duo-Boesartige-Geschwister-2053847.html] hatte. Er war bereits von zwei unterschiedlichen Versionen ausgegangen.

Gefährliches Vorbild für die Welt

Stuxnet war **im Herbst 2010 von Sicherheitsforschern entdeckt** [http://www.heise.de/security/meldung/Iran-bestaetigt-Cyber-Angriff-durch-Stuxnet-Update-1096365.html] worden. Rasch war klar geworden, dass es der Schädling vor allem auf das iranische Atomprogramm abgesehen hatte. Er beschädigte die Zentrifugen, wobei die erste Version deutlich heimtückischer vorgegangen war, um den Angriff zu verschleiern. Langner fand die erste – offenbar von den US-Amerikanern stammende – Version beeindruckender. Seitdem wurde Stuxnet auch immer wieder bei Debatten um eine Kriegsordnung im Cyberspace angeführt. Der Ex-NSA-Chef Michael Hayden warnt dazu nun in "Zero Days": "Wenn wir hinausgehen und so etwas machen, versteht das der große Teil der Welt als neuer Standard, den sie nachahmen darf." (**mho** [mailto:mho@heise.de])

Kommentare lesen (80 Beiträge)
[http://www.heise.de/forum/heise-Security/News-Kommentare/Stuxnet-angeblich-Teil-eines-groesseren-Angriffs-auf-kritische-Infrastruktur-des-Iran/forum-254947/comment/]

Forum bei heise online: **Sicherheit** [http://www.heise.de/forum/heise-online/Internet/Sicherheit/forum-43110/comment/]

http://heise.de/-3104957 [http://heise.de/-3104957]

Drucken [http://www.heise.de/security/meldung/Stuxnet-angeblich-Teil-eines-groesseren-Angriffs-auf-kritische-Infrastruktur-des-Iran-3104957.html?view=print]

Mehr zum Thema **Computerwurm** [http://www.heise.de/thema/Computerwurm] **Stuxnet** [http://www.heise.de/thema/Stuxnet] **Cyberwar** [http://www.heise.de/thema/Cyberwar]