

Mit Siemens in den Cyberkrieg gegen Iran

USA und Israel benutzten bei „Stuxnet“-Angriffe heimlich auch Wissen des Konzerns

VON FRIEDEMANN DIEDERICH

Die USA und Israel haben bei ihrem offenbar erfolgreichen Cyber-Angriff auf die iranischen Nuklearanlagen im Oktober vorigen Jahres auch das Wissen von Experten des deutschen Konzerns Siemens benutzt, die allerdings von dem geplanten Coup nichts wussten. Dazu wurden jetzt brisante Details enthüllt.

WASHINGTON – Den Verdacht gab es bereits. Doch die Details, die von der *New York Times* gestern ausführlich veröffentlicht wurden, lassen kaum noch Zweifel an dem bisher wohl spektakulärsten Coup moderner Cyber-Kriegsführung: Dass die USA und Israel erfolgreich mit dem sogenannten „Stuxnet“-Wurm die iranische Nuklearanlage Natans attackiert und dabei vermutlich bis zu 1000 Uran-Zentrifugen so schwer beschädigt haben, dass sie derzeit nicht benutzbar sind.

In eine Falle gelockt

Erstmals wurde jetzt auch bekannt, dass sich dabei die USA offenbar des Wissens und der Kooperation von nichtsahnenden Siemens-Computerexperten bedienten. Dass es ausgerechnet Techniker des Elektronikgiganten waren, die zu diesem Erfolg im Kampf des Westens gegen die atomaren Ambitionen Teherans beigetragen haben, dürfte in der Konzernzentrale des deutschen Weltunternehmens nicht gerade helle Freude auslösen. Denn so wie es die *New York*

Times schildert, wurden die Rechner-Fachleute von Siemens im Jahr 2008 bei einem Kooperationsprogramm des „Idaho National Laboratory“ – das dem US-Energieministerium untersteht und sich vor allem mit Nuklearanlagen befasst – offenbar in eine raffinierte Falle gelockt: Die Zusammenarbeit sollte offiziell das Ziel haben, weltweit den Schutz von Industrieanlagen vor Cyber-Angriffen zu verbessern, und umfasste dabei auch die Computer-Steuermechanismen, die Siemens an seine zahlreichen Industriekunden geliefert hatte.

Zu diesen zählt auch der Iran. Doch die bei dem Projekt gefundenen Informationen über Verwundbarkeiten, in einem 62-Seiten-Protokoll festgehalten, fanden dann – so stellt es die US-Zeitung dar – den Weg zu den kooperierenden Geheimdiensten in den USA und Israel. Was man in München offenbar als peinlich empfindet: Ein ursprünglicher Hinweis auf die Studie sei kürzlich von der Siemens-Webseite gelöscht worden, berichtet die *New York Times*.

Vor allem in Jerusalem sah man das ungeheure Potenzial dieser Analyse, auf deren Grundlage dann der „Stuxnet“-Wurm entwickelt worden sei. Israelische Techniker bauten dazu, so heißt es, in der Negev-Wüste sogar die iranischen Zentrifugen originalgetreu nach, um die schädliche Software für die geplante Attacke zu optimieren.

Der erstmals im Juni letzten Jahres aufgetauchte Wurm ist ein speziell auf Siemens-Systeme ausgerichteter „Schädling“, der dem Angreifer im

Erfolgsfall erlaubt, die Kontrolle über Industrieanlagen zu übernehmen. „Um das zu schaffen, muss man die Maschinen genau kennen“, zitiert die *New York Times* einen US-Experten, „und der Wurm war deshalb effektiv, weil Israel ihn zuvor ausprobiert hat.“

Bei dem gelungenen Angriff steigerte „Stuxnet“ dann die Drehzahlen der iranischen Zentrifugen in einen kritischen Bereich. Dies wiederum soll zu einer Beschädigung und einem langfristigen Ausfall eines Teils der Anlage geführt haben.

Von Bush in Auftrag gegeben

Von staatlichen Stellen in den USA und Israel gibt es bisher keine offizielle Bestätigung für die massive Attacke, die Berichten zufolge als Teil der neuen Cyber-Kriegsführung Washingtons noch vom früheren Präsidenten George W. Bush in Auftrag gegeben wurde. Barack Obama habe dieses Programm dann noch ausgeweitet.

Gary Samore, ein Berater Obamas für den Kampf gegen Massen-Vernichtungswaffen, hatte kürzlich erklärt: „Ich bin froh, von den Zentrifugen-Problemen des Iran zu hören. Und wir und unsere Verbündeten tun alles, um es noch komplizierter zu machen.“ Der scheidende Chef des israelischen Geheimdienstes Mossad, Meir Dagan, sagte ebenfalls vor wenigen Tagen vor der Knesset, Iran habe nun „technische Probleme“, die den Bau einer Atombombe bis 2015 hinauszögern könnten.