Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 86 (2011)
Heft: 9

Artikel: Wunderwaffe Stuxnet
Autor: [s.n.]
DOI: https://doi.org/10.5169/seals-717624

Wunderwaffe Stuxnet

Zum israelischen Stuxnet-Angriff auf die iranische Atomrüstung werden nach und nach Einzelheiten bekannt. Es bestätigt sich, dass nur ein Staat diese grossangelegte Attacke auf Persien durchführen konnte. Dass nichtstaatliche Akteure, zum Beispiel jugendliche Hacker, hinter der Operation stehen, das wird heute kategorisch ausgeschlossen. Zu kompliziert war das Vorgehen, zu gross der technisch-taktische Aufwand.

Vor gut einem Jahr, im Juni 2010, betrat Stuxnet die Bühne der Weltpolitik: ein Computervirus, das in Hochsicherheitsrechner eindrang, was vorher als unmöglich gegolten hatte.

Das Virus frass sich durch die Steuerungscomputer im iranischen Natans, wo Wissenschafter Uran anreichern. Stuxnet manipulierte die Zentrifugen bis zur Selbstzerstörung und drang so ins Herz des persischen Stromprogramms vor.

Neue Waffe

Stuxnet hat die moderne Kriegsführung um eine grundlegend neue Waffe erweitert: um den militärischen Angriff mit einem auf ein Ziel zugeschnittenen Programmcode.

In Tel Aviv würdigt Sam Angel, der Chef der israelischen Niederlassung der amerikanischen Computerfirma Symantec, Stuxnet wie folgt: «Stuxnet ist die ausgefeilteste Attacke, die wir jemals sahen. Ein derartiger Angriff auf ein abgeschottetes Industriesystem ist absolut ungewöhnlich.»

Angel zeigt auf einer Weltkarte, wo Stuxnet angriff: im Iran, in Indonesien, in Malaysia und in Weissrussland, wo ein Techniker namens Sergej Ulasen das Virus entdeckte.

Ulasen arbeitet in der Sicherheitsfirma VirusBlokAda von Minsk. Am 17. Juni 2010 erhielt er eine Nachricht aus Teheran. Eine iranische Firma klagte: «Unsere Computer schalten sich permanent selber aus. Und sie starten selber neu.»

Zwei Server

Ulasen prüfte eine Woche lang die iranischen Maschinen. Dann fing er Stuxnet. Er informierte die Branche, darunter Symantec. Die Symantec-Techniker stiessen auf zwei Rechner, welche den Angriff zentral steuerten:

- Einer der Server stand in Malaysia und war unter *www.todaysfutbol.com* erreichbar.

Die iranische Atomanlage bei Natans: Für den Mossad ein militärisches Ziel.

- Der andere Server befand sich in Europa, in Dänemark, und trug die Adresse *www.mypremierfutbol.com*.

Auf der Spur

Die Adressen waren über eine Registrierfirma in Arizona angemeldet worden – unter falschem Namen, mit einer gefälschten Kreditkarte.

Symantec leitete alles, was über die beiden Server lief, auf ein Rechenzentrum in Dublin um und überwachte fortan das Virus. Wohl war der Mossad als Urheber entkommen; aber nun verfolgte Symantec die Spuren.

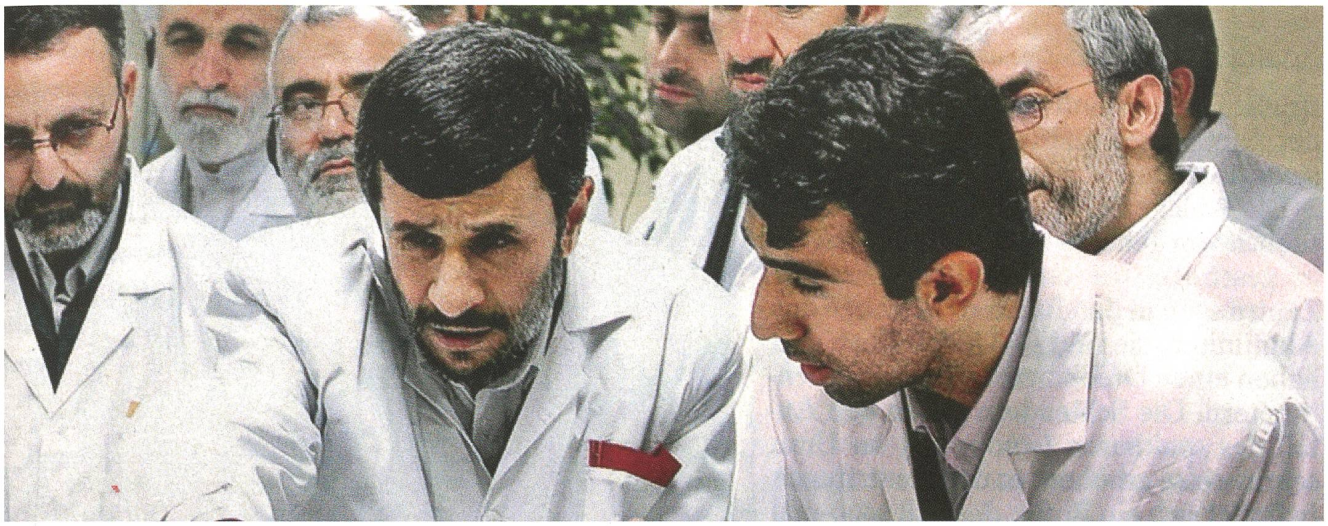
Im Herbst 2010 hatte Stuxnet rund 100 000 Computer infiziert. Mehr als 60 000 dieser Rechner stehen in Persien, mehr als 10 000 in Indonesien, mehr als 5000 in Indien. Der Mossad programmierte Stuxnet so, dass der Virus den beiden Steuerungsservern zuerst die Frage beantwortet, ob darauf die Siemens-Software *Step 7* läuft, welche die Zentrifugen im iranischen Natans steuert.

So einfach wie genial

Natans, 250 Kilometer südlich von Teheran mitten in der Wüste, ist militärisch hochgeschützt. Die Aluminium-Zentrifugen in den Bunkern sind 1,80 Meter hoch und haben einen Durchmesser von zehn Zentimetern.

Die Schleudern erhöhen den Anteil des spaltbaren Isotops 235 im Uran Schritt für Schritt. In den Zentrifugen dreht sich ein Rotor 1000 Mal pro Sekunde. Das gasförmige Uranhexafluorid wird geschleudert, so dass sich das spaltbare Isotop 235 im Zentrum sammelt.

Eine Siemens-Anlage steuert den Prozess. Der Stuxnet-Trick ist so simpel wie ge-



Archivbilder

Der iranische Präsident Mahmud Achmadinedschad inspiziert Natans. Noch hat Persien die Atombombe nicht gezündet.

nial. Stuxnet nutzt eine Lücke in Windows aus, um das System zu manipulieren. Der Programmfehler erlaubt es, das Virus etwa über einen USB-Stick einzuschleusen.

- Zuerst sucht Stuxnet Anti-Viren-Programme. Entweder umgeht der Code die Programme – oder er schaltet sie aus. Die oberste Priorität lautet: Keine Spuren hinterlassen!
- Dann nistet sich Stuxnet in jenem Teil des Betriebssystems ein, das USB-Sticks verwaltet. Stuxnet erstellt eine Prüfsumme, deren genauer Zweck unklar ist.

Schwarzer Markt

Jedenfalls bricht die Infektion ab, wenn die Summe 19790509 erreicht. Rückwärts gelesen, ergibt die Zahl den 9. Mai 1979. An diesem Tag richtete Persien in Teheran den jüdischen Unternehmer Habib Elghanian hin. Zufall? Provokation? Absichtlich gelegte Spur? Wir wissen es nicht.

Wie trug der Mossad das Virus nach Natans? Die Computerfachleute nennen Sicherheitslücken wie das Windows-Loch *Zero-Day-Exploits*. Das Wissen darüber ist kostbar, auf dem schwarzen Markt kann ein solcher Fehler 100 000 Dollar wert sein. Stuxnet verbindet gleich vier dieser digitalen Juwelen miteinander. Ohne intime Kenntnisse der Siemens-Anlage lässt sich ein Code wie Stuxnet nicht schreiben.

Wie aber kam der Mossad, noch immer einer der raffiniertesten Geheimdienste der Welt, an die in Natans verwendete Technik?

- Die eine Theorie geht davon aus, dass die Amerikaner dem Mossad halfen. In Idaho beschäftigt sich ein Forschungsinstitut mit der Siemens-Technik, welche die Perser anwenden.
- Dort könnten die Grundlagen zu Stuxnet gelegt worden sein – mit anschliessender Überprüfung in Dimona, im israelischen Atomzentrum in der Wüste Negev.
- Dem widersprechen die Israeli. Stuxnet sei vollständig eine Blau- und Weiss-Operation gewesen: benannt nach Israels Nationalfarben ein rein israelischer Angriff.

Einen ersten Teil des Codes programmierte eine geheime Elite-Gruppe des militärischen Nachrichtendienstes Aman, der hinter dem legendären Mossad immer etwas verschwindet, aber nicht zu unterschätzen ist. Den Test programmierte der Mossad, der Stuxnet in Natans einschleuste.

Der Mossad baute in einer israelischen Firma Natans nach. So testete er Stuxnet. Mitte 2009 war es soweit. Am 22. Juni um 16.31 Uhr liessen die Angreifer Stuxnet von der Leine. In drei Wellen attackierten sie das iranische Ziel: Die erste Welle rollte im Sommer 2009, die zweite Welle im März 2010, die dritte im April 2010.

Der Mossad programmierte Stuxnet so, dass sich das Virus nach der dritten Infektion selber löscht. Die Israeli wollten eine explosionsartige Verbreitung vermeiden. Ihre Wunderwaffe sollte das gegnerische Atomprogramm *nachhaltig* sabotieren, aber nicht spektakulär.

1000 Geräte zerstört

Der Mossad betrachtet Stuxnet als Erfolg. Eine iranische IR-1-Zentrifuge dreht sich mit 1064 Hertz. Als die Rotoren verrückt spielten, erhöhten sie die Frequenz eine Viertelstunde lang auf 1410 Hertz.

Später bremste Stuxnet die Rotoren 50 Minuten lang auf eine Frequenz von wenigen 100 Hertz. Die Aluminiumröhren wurden gedehnt, die Zentrifugen brachen. Sechs Kaskaden mit jeweils 164 Zentrifugen gingen kaputt. Rund 1000 Geräte fielen Stuxnet zum Opfer. *spi/hst.*

1. Mai 2011, Abbottabad: Drei Navy Seals spürten Osama Bin Laden auf

Zur Erschiessung von Osama Bin Laden werden Details bekannt. Demnach spürten am 1. Mai 2011 drei Navy Seals den Terrorführer auf. Sie hatten ihm den Codenamen «CRANKSHAFT» (Kurbelwelle) gegeben. Zuerst stellten sich zwei seiner Frauen schützend vor Bin Laden. Einer Frau schoss ein Soldat in die Wade. Dann überwältigte er beide Frauen. Aus Angst, sie könnten Sprengstoffgürtel tragen, behielt er beide hart im Griff.

Ein zweiter Seal richtete sein M-4-Gewehr auf Bin Ladens Brust. Bin Laden trug ein Hemdgewand und eine Gebetskappe. Es sei nie die Rede davon gewesen, Bin Laden zu ergreifen oder in Haft zu nehmen. Es sei keine Sekundenentscheidung gewesen, ihn sofort zu erschiessen. Niemand wollte Gefangene machen. Die erste Kugel traf Bin Laden in die Brust, eine zweite in den Kopf. Der Chef der Seals meldete: «Für Gott und unser Land – Geronimo EKIA. Enemy killed in action, Feind im Gefecht getötet.»