

Middle East Diary

17.01.2012

Dr. Gil Yaron

Krieg ohne Tote

www.dias-online.org

Duesseldorf Institute for Foreign and Security Policy
c/o Juristische Fakultät der Heinrich-Heine-Universität
Universitätsstr. 1, 40225 Duesseldorf, Germany

Der nächste Nahost-Krieg hat längst begonnen. Jüdische und arabische Hacker liefern sich im Internet schwere Gefechte. Seit Jahresbeginn will Israel sich mit einem „Cyber“ Kommando vor Angriffen auf die Infrastruktur schützen. Auch Israels Feinde leiden unter Virus- und Wurmattaken.

Das neue Jahr beginnt für Israel mit einer bisher unbekanntem Art von Krieg. Seit zwei Wochen werden israelische Webseiten immer wieder Angriffsziele arabischer Hacker. Montagfrüh fielen die Webseiten des Flugunternehmens „El Al“ und der Börse in Tel Aviv für Stunden aus. Eine harmlose Nachricht verkündete: „Wegen Wartungsarbeiten im Augenblick nicht zugänglich“, doch dahinter stand eine Attacke des saudischen Hackers „0xOmar“, der israelische Verbraucher bereits seit Wochen plagt und auch seinen neuesten Angriff im Vorfeld bei israelischen Medien angekündigt hatte. Dabei vermuten die meisten israelischen Experten hinter dem Namen keine Einzelperson, sondern gleich ein ganzes Netzwerk von Hackern, die entweder ideologisch hoch motiviert oder für ihre umfangreiche Arbeit bezahlt werden.

Das Hackernetzwerk, das sich „0xOmar“ nennt, rückte erstmals vor zwei Wochen ins Rampenlicht. Damals veröffentlichte es die Daten von rund 20.000 israelischen Kreditkarten und forderte Internetnutzer dazu auf, die Konten der ahnungslosen Kunden zu plündern: „Dies ist der Anfang eines Cyberkriegs“, verkündete 0xOmar damals. „Ihr seid nicht mehr sicher. Wir werden israelische Server für verschiedene Zwecke angreifen, um geheime und heikle Informationen zu veröffentlichen oder um Seiten zu löschen.“ Der finanzielle Schaden soll damals gering gewesen sein, doch es war nur der Auftakt. Nachdem israelische Hacker Revanche übten und die Bankdetails hunderter Saudis preisgaben, schlug 0xOmar erneut zu. Am Wochenende griffen Hacker aus Gaza die Webseite der israelischen Feuerwehr an, ersetzten sie mit einem verunstalteten Bild des stellvertretenden Außenministers und der Botschaft „Tod für Israel!“. Damit schienen sie einem Aufruf von Hamassprecher Sami Abu Suhri in Gaza gefolgt zu sein, der am Freitag erklärt hatte: „Das Hacken israelischer Webseiten stellt die Eröffnung einer neuen Front des Widerstands dar, und den Beginn eines elektronischen Kriegs gegen die israelische Besatzung.“

Dass ihr Staat ausgerechnet von arabischen Hackern angegriffen wird, wurmt hier viele. Israel gilt als High-Tech Nation mit einer der höchsten Dichten an Patenten und Ingenieuren weltweit. Gern preist man sich mit der technologischen Überlegenheit gegenüber seinen Nachbarn. Dennoch schien Benjamin Netanjahus Regierung Cyberangriffe erwartet zu haben. Schon Mai 2011 richtete sie einen „Stab für Internetkriegsführung“ ein. Der nahm seine Arbeit unter der Führung von Dr. Avitar Matanyia aber erst zu Jahresbeginn auf und soll noch Monate benötigen, bevor er Israels Infrastruktur vor Cyberangriffen schützen kann. Da das Land im hohen Grade vernetzt ist, gilt es als besonders anfällig für Internetangriffe. Die Staatsbank wies Israels Banken an, jeden Zugriff aus Saudi Arabien, Iran und Algerien zu stoppen, andere Banken gingen sogar einen Schritt weiter und blockierten jeden Zugriff aus dem Ausland. Dabei soll mindestens die Hälfte der Angriffe von israelischen Rechnern ausgegangen sein, nachdem die Angreifer sie insgeheim gekapert und umprogrammiert haben, sagte der israelische Internetsicherheitsexperte Gil Schwed der Tageszeitung „Haaretz“: „So eine Attacke kommt nicht von einem Computer in Saudi Arabien, sondern tausende aus aller Welt“, die mit einem „bot“ infiziert wurden, sagte Schwed.

Die Armee rekrutierte in vergangenen Monaten hunderte Computerfachleute, um Spezialeinheiten wie die „8200“ der militärischen Aufklärung auf einen Cyberkrieg vorzubereiten. Dabei begann der spätestens Juni 2010, als der „Stuxnet“ Virus weltweit auf Siemensmaschinen entdeckt wurde. Israelische und amerikanische Experten sollen ihn erfunden und mit Hilfe infizierter Laptops ins iranische Atomprogramm eingeschleust haben, um Zentrifugen unbrauchbar zu machen. So sollte die Anreicherung von Uran ohne einen militärischen Einsatz gestoppt werden.

The Dusseldorf Institute for Foreign and Security Policy e.V. (DIAS)

The Dusseldorf Institute for Foreign and Security Policy (DIAS) e.V., founded in 2003 at the Heinrich-Heine-University Dusseldorf, is an independent, interdisciplinary forum whose purpose is to analyze the field of foreign and security policy from economic and historical perspectives, as well as within the context of public international law. The Institute provides the academic public with the chance to exchange theoretical ideas in relation to issues of foreign and security policy and additionally seeks to provide the interested public with discussions and information necessary for the understanding of international relations. The Institute's activities also include lectures, presentations, moderated discussions, seminars and academic trips, as well as a publication series.

© Copyright 2012, The Dusseldorf Institute for Foreign and Security Policy e.V. (DIAS),
Universitaetsstr. 1 Geb. 24.91, 40225 Duesseldorf, Germany, www.dias-online.org