

Die Zauberwaffe

Der Virus „Stuxnet“, mit dem der Mossad das iranische Atomprogramm attackierte, ist das erste digitale Kampfgerät von geopolitischer Bedeutung.

programms. Die Kluft sei groß, die Ergebnisse seien nicht immer sichtbar. Aber: „Es ist trotzdem wichtig, dass wir hier sind.“

Genau das stellt Kurti in Frage. Sein Erfolg geht einher mit enttäuschten Erwartungen an die Staatengemeinschaft.

Das Grenzgebiet im Norden bleibt ein gesetzloser Raum, die Rechtsstaatsbeauftragten der EU sind ohnmächtig dort. Der Wahlfarce im Dezember hatten sie nichts weiter entgegenzusetzen als die Aufforderung an Thaçi, keine Personen, gegen die ermittelt werde, in seine Regierung einzubinden.

Obwohl die EU mit der Eulex-Mission seit 2008 im Kosovo wirkt, hat die Korruption in den Parteien und im Parlament laut Transparency International zugenommen. Kosovo nutzt zwar für Mobilfunkverbindungen die Vorwahl Monacos, des Steuerparadieses an der Côte d'Azur; die Arbeitslosigkeit aber liegt nach wie vor bei 50 Prozent.

Etwa vier Milliarden Euro hat die Staatengemeinschaft seit dem Kriegsende 1999 für das kleine Land aufgebracht; es gibt kaum Industrie, selbst Zwiebeln und Knoblauch werden aus China importiert. Die meisten Kosovaren leben von den Überweisungen aus der Diaspora. Und die Misswirtschaft, der auch die Uno-Verwaltung keinen Einhalt geboten hat, hält an. Jetzt baut die Regierung eine Autobahn in die albanische Hauptstadt Tirana, den Zuschlag für das Großprojekt bekam das US-Konsortium Bechtel-Enka. Für Beton, Sand und Kies soll Kosovo nun mehr als das Doppelte des Marktpreises zahlen.

Die Misere ist groß, der Frust in der Bevölkerung auch. Kosovo ist ein junges Land, die Hälfte der Kosovaren sind unter dreißig.

Dass die Ausrichtung der Politik im Kosovo eine Generationenfrage ist, das sagt nicht nur Albin Kurti, der junge Oppositionsführer. Das sagt auch Edita Tahiri, die stellvertretende Regierungschefin.

Tahiri, 55, sitzt hinter trübem Spiegelglas in ihrem Büro im Regierungsgebäude. Über ihr hängt goldgerahmt das Harvard-Diplom, daneben ein Faksimile der Unabhängigkeitserklärung. Sie sagt: „Wir waren es, die den Krieg gekämpft und die Freiheit gebracht haben.“ Politik bedeute mehr, als nur zu kritisieren. Für Tahiri gelten die alten Koordinaten: Ziel Kosovos müsse die Nato-Mitgliedschaft sein, einzig verlässlicher Partner seien die USA. Die Frage der Selbstbestimmung scheidet tatsächlich die Generationen.

An einer Hauswand in Priština, nicht weit vom Regierungsgebäude, steht gesprüht: „Vetevendosje! ist die Zukunft“.

Daneben, leicht verblasst, aber trotzdem lesbar: „Tito, wir vermissen dich“.

JULIA AMALIA HEYER

Der Gebäudekomplex auf der Anhöhe an einer Kreuzung des Highways von Tel Aviv nach Haifa heißt in Israel nur „der Hügel“. Das Gelände ist mehrere Fußballfelder groß, hermetisch abgeschottet mit hohen Mauern und Stacheldraht, eine moderne Festung für den Überlebenskampf Israels im Nahen Osten. Der Zutritt zu dieser Festung ist tabu, für Politiker wie für Journalisten, sie ist das Hauptquartier des israelischen Auslandsgeheimdienstes Mossad, und es ist der Mossad, der Hausbesuche macht, nicht umgekehrt.

An einem Donnerstag Anfang Januar ist das anders. Auf dem Parkplatz vor einem nahe gelegenen Kino fährt ein Kleinbus mit abgedunkelten Scheiben vor, eine Gruppe handverlesener Journalisten muss Handys und Diktiergeräte abgeben. Meir Dagan, der mächtige Mossad-Chef, hat geladen, es ist sein letzter Arbeitstag, nach sieben Jahren verlässt er den Dienst. Es geht an diesem Januartag um sein Vermächtnis: den Kampf des Mossad gegen das iranische Atomprogramm.

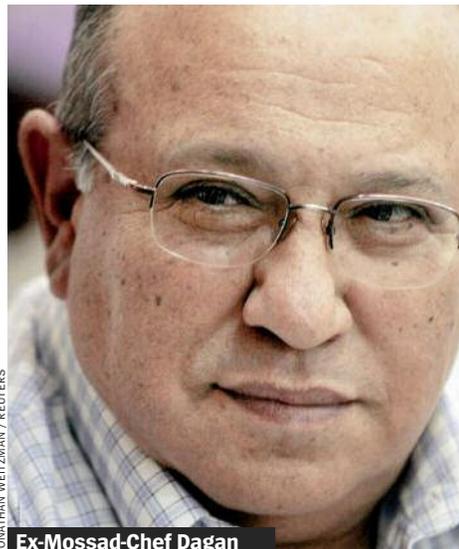
Voller Leidenschaft warnt er vor einem möglichen Militärschlag gegen Iran. Er glaubt, ein solcher Angriff müsse zu einem Flächenbrand in der Region führen, zum Krieg mit der Hisbollah und der Hamas, vielleicht auch mit Syrien. Wer denke, dass ein Militärschlag das Atomprogramm stoppen könne, der irre, sagt Dagan. Es könne nur eine Verzögerung

geben, keinen dauerhaften Erfolg. Der scheidende Mossad-Chef ist deshalb gegen Bomben, aber für alles, was das iranische Atomprogramm zurückwirft, ohne einen konventionellen Krieg zu beginnen.

Verzögerung, das ist das Zauberwort. Und Dagan hat dafür eine Zauberwaffe geschaffen, deren Name an diesem Januartag in Raum hängt, aber vom Mossad-Chef nicht ausgesprochen wird: „Stuxnet“.

Vor gut einem Jahr, im Juni 2010, hat Stuxnet die Bühne der Weltpolitik betreten – ein Computervirus, der in Hochsicherheitsrechner eindringen konnte, die nicht am Internet hängen, was als beinahe unmöglich gilt. Ein Virus, der sich durch die Steuerungscomputer im iranischen Natans gefressen hat, wo Wissenschaftler Uran anreichern; der die Zentrifugen bis zur Selbsterstörung manipulierte und damit ins Herz des Atomprogramms vorgedrungen ist.

Stuxnet ist die erste Cyberwaffe mit geopolitischer Dimension, „ein digitaler Bunkerbrecher“, wie Frank Rieger vom deutschen Chaos Computer Club sagt. Der Virus hat die moderne Kriegsführung um eine grundlegend neue Waffe erweitert: den militärischen Angriff mit einem auf ein Ziel zugeschnittenen Programmcode. Ein Jahr danach gibt es keine Sicherheitsfirma im Internet, keine Regierung eines größeren Landes, die sich nicht mit Stuxnet und den Folgen beschäftigt und ihre Schlüsse daraus gezogen hat.



Ex-Mossad-Chef Dagan

Sabotierende Software

Wie „Stuxnet“ die iranische Urananreicherung störte

1 Vermutlich über einen USB-Speicherstick gelangt die Schad-Software in das eigentlich von der Außenwelt abgeschirmte Computersystem der Urananreicherungsanlage im iranischen Natans.





ABACA / PICTURE-ALLIANCE / DPA

Iranischer Präsident Mahmud Ahmadinedschad in Natans: Ein Schlachtfeld, auf dem nicht mit Kanonen gekämpft wird

Wer mehr über Stuxnet erfahren will, wer verstehen möchte, was hinter dem Virus steckt, muss nach Israel reisen, in das Land, in dem diese Waffe erfunden wurde.

Tel Aviv, 15 Autominuten vom Flughafen Ben Gurion entfernt. In einem gesichtslosen Neubaukomplex residiert die israelische Dependence der US-amerikanischen Computersicherheitsfirma Symantec. Sam Angel, der Chef von Symantec Israel, holt Besucher in der Tiefgarage ab und führt sie in einen Konferenzraum in den dritten Stock. Angel startet einen Powerpoint-Vortrag, er sagt: „Stuxnet ist die ausgefeilteste Attacke, die wir jemals gesehen haben, ein solcher Angriff auf ein ausgereiftes, abgeschottetes Industriesystem ist absolut ungewöhnlich.“ Angels Beamer wirft eine Weltkarte an die Wand, es erscheinen die Länder, in denen dieser Angriff stattgefunden hat: Iran, Indonesien, Malaysia etwa, und Weißrussland,

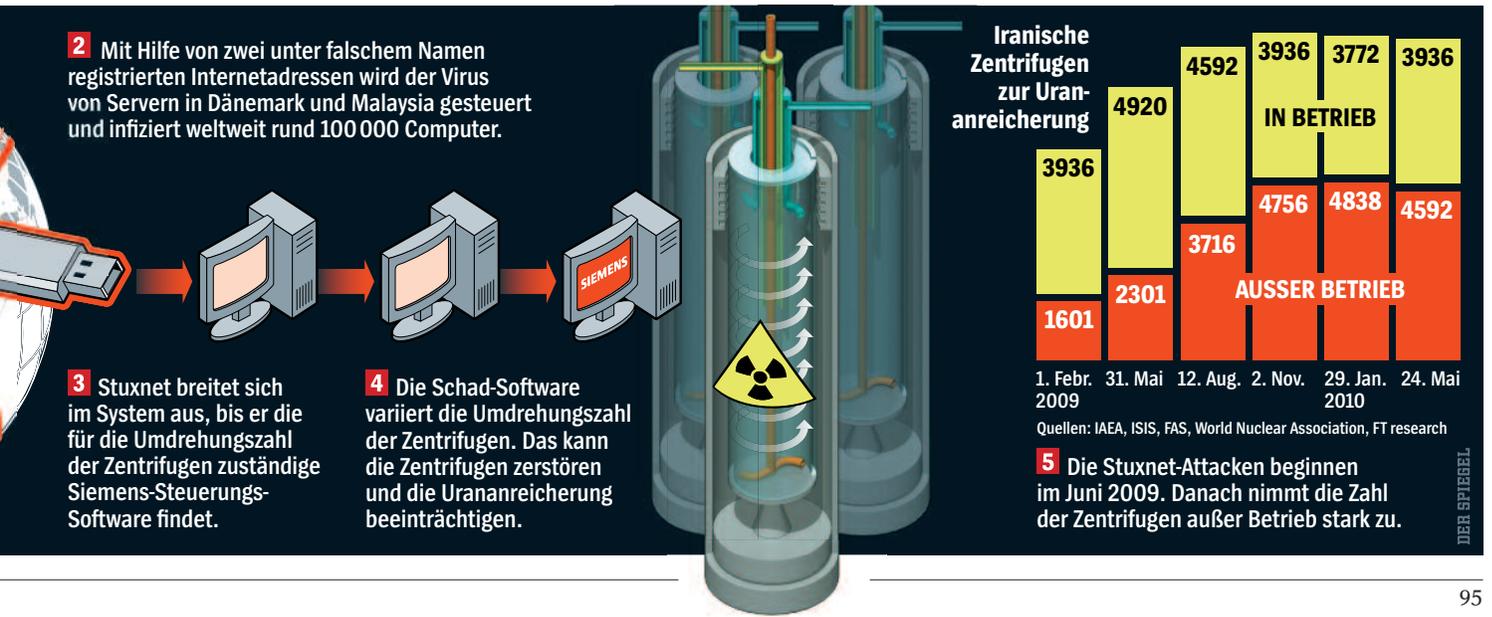
wo ein Mann namens Sergej Ulasen Stuxnet entdeckt hat.

Ulasen arbeitet in der Forschungs- und Entwicklungsabteilung der Sicherheitsfirma VirusBlokAda in Minsk, und die E-Mail, die er am 17. Juni 2010 erhielt, klang banal: Eine iranische Firma klagte, ihre Rechner verhielten sich merkwürdig. Die Computer würden sich permanent ausschalten und neu starten. Ulasen prüfte zusammen mit einem Kollegen eine Woche lang die Maschinen. Dann hatten sie Stuxnet gefangen. VirusBlokAda informierte die Branche, darunter Symantec.

Die Techniker bei Symantec machten sich an die Arbeit und stießen auf zwei Rechner, welche die Angriffe zentral gesteuert hatten. Einer der Server stand in Malaysia, der andere in Dänemark, sie waren unter den Adressen www.todaysfutbol.com und www.mypremierfutbol.com erreichbar. Die Adressen waren über eine

der weltgrößten Internet-Registrierfirmen im amerikanischen Arizona angemeldet worden, unter falschem Namen, mit einer gefälschten Kreditkarte. Symantec leitete die ein- und ausgehende Kommunikation der beiden Server auf ihr Rechenzentrum in Dublin um und überwachte so die Aktivitäten des Virus. Wer auch immer Stuxnet in die Welt gesetzt hatte, war zwar entkommen. Aber Symantec konnte zumindest die Spuren verfolgen.

Die Umleitung der Kommunikation ermöglicht einen Überblick darüber, in welchen Ländern der Virus aktiv war. Demnach hat Stuxnet bis Herbst 2010 rund 100 000 Computer weltweit infiziert. Mehr als 60 000 dieser Rechner stehen in Iran, mehr als 10 000 in Indonesien, mehr als 5000 in Indien. Die Erfinder haben Stuxnet so programmiert, dass der Virus den beiden Steuerungsservern zuerst die Frage beantwortet, ob darauf die indu-



strielle Siemens-Software Step 7 läuft, mit der Zentrifugen im iranischen Natans gesteuert werden.

Die Anlage bei Natans, 250 Kilometer südlich von Teheran in der Wüste gelegen, ist geschützt wie eine Militärbasis. Die Zentrifugen in den Bunkern bestehen aus Aluminium, sie sind 1,80 Meter hoch und haben einen Durchmesser von zehn Zentimetern. Die Schleudern sollen den Anteil des spaltbaren Isotops 235 im Uran schrittweise erhöhen. In den Zentrifugen befindet sich ein Rotor, der sich 1000-mal pro Sekunde dreht. Das gasförmige Uranhexafluorid wird geschleudert, so dass sich das spaltbare Isotop 235 im Zentrum sammelt. Dieser Prozess wird von einer Siemens-Anlage gesteuert, die mit Microsofts Windows-Betriebssystem läuft.

Der Kniff, der den Angriff möglich macht, ist so simpel wie genial. Stuxnet nutzt dazu eine Lücke in Windows aus, die die Manipulation des Systems ermöglicht. Dieser Programmierfehler erlaubt es, den Virus etwa über einen USB-Stick einzuschleusen. Kaum ist der Stick angeschlossen, startet unbemerkt die Installation.

Anfangs sucht Stuxnet nach Anti-Viren-Programmen. Der Code soll sie umgehen – oder, wenn das nicht möglich ist, sich deinstallieren. Keine Spuren, das ist lange Zeit eine Priorität.

In einem zweiten Schritt nistet Stuxnet sich in jenem Teil des Betriebssystems ein, das USB-Sticks verwaltet, und erstellt eine Prüfsumme, deren genauer Zweck unklar ist. Jedenfalls bricht die Infektion ab, wenn diese Summe den Wert 19790509 erreicht. Symantec spekuliert, ob es sich dabei um eine Art Code handelt: Die Zahl könnte, rückwärts gelesen, für den 9. Mai 1979 stehen. An jenem Tag wurde der jüdische Unternehmer Habib Elghanian in Teheran hingerichtet. Zufall? Eine Provokation? Oder eine absichtlich gelegte falsche Spur?

Bis heute ist ungeklärt, wie die Israelis den Virus nach Natans tragen konnten. In der Sprache der Computerexperten heißen Sicherheitslücken wie das Loch im Windows-Betriebssystem Zero-Day-Exploits, bislang unbekanntes Sicherheitslücken. Die Suche danach ist eine Mischung aus Hacker-Sport und Geschäftsmodell, das Wissen ist kostbar, es gibt einen Schwarzmarkt, auf dem ein solcher Fehler 100.000 Dollar oder mehr wert sein kann. In Stuxnet sind gleich vier dieser digitalen Juwelen kombiniert.

Symantec-Mann Angel glaubt, dass es unmöglich ist, einen Code wie Stuxnet zu schreiben, ohne intime Kenntnisse der Siemens-Anlage zu haben. „Es gibt für Exploits der Siemens-Software keinen Schwarzmarkt“, sagt er. „Dafür ist die Verbreitung zu gering.“ Aber wie ist der Mossad an die Informationen über die in Natans verwendete Technik gekommen?



Symantec-Mann Angel: „Ausgefällteste Attacke, die wir je gesehen haben“

Öffentlich ist darüber spekuliert worden, dass die Amerikaner dem Mossad geholfen haben könnten. In Idaho existiert ein Forschungsinstitut der US-Regierung, das sich mit der Siemens-Steuerungstechnik beschäftigt, die auch in Iran eingesetzt wird; dort könnte die Grundlagenforschung für Stuxnet stattgefunden haben. Anschließend sei der Virus in Dimona getestet worden, dem israelischen Atomzentrum in der Negev-Wüste.

Israelische Gesprächspartner, die die Hintergründe des Angriffs kennen, legen dagegen Wert darauf, dass Stuxnet eine „blue-and-white operation“ gewesen sei, so genannt nach den Nationalfarben Blau und Weiß und damit ein rein israelischer Angriff. Einen Teil des Codes soll eine geheime Eliteeinheit des militärischen Nachrichtendienstes programmiert haben,

Der Angriff beginnt im Sommer 2009 und verläuft in drei Wellen, er trifft die Iraner hart.

den Rest der Mossad, der auch für die Einschleusung in Natans verantwortlich gewesen sei. Der Mossad habe sogar verborgen versucht, eine Kaskade von Zentrifugen auf dem Schwarzmarkt aufzukaufen. Mit Hilfe ausländischer Geheimdienste sei es einer israelischen Rüstungsfirma schließlich gelungen, ein Modell von Natans nachzubauen. Dort soll Stuxnet getestet worden sein.

Im Sommer 2009 ist es so weit: Die Angreifer lassen Stuxnet am 22. Juni 2009 um 16.31 Uhr von der Leine. Insgesamt stehen fünf iranische Organisationen im Fokus des Angriffs, sie werden in drei

Wellen attackiert. Nach der ersten Welle folgt im März 2010 ein zweiter Schlag, der die Iraner hart trifft, im April folgt die dritte Welle. Nach Angaben von Symantec haben die Ziele nicht direkt mit dem Nuklearprogramm zu tun, aber einige Unternehmen seien auf Sanktionslisten der Vereinten Nationen verzeichnet. Allein in diesen fünf Organisationen werden 12.000 Rechner infiziert.

Stuxnet ist so programmiert, dass es sich auf dem USB-Stick nach der dritten Infektion von selbst löscht – vermutlich um eine explosionsartige Verbreitung, die alsbald aufgefallen wäre, zu verhindern. Die Cyberwaffe soll nachhaltig sabotieren, nicht spektakulär.

Wie komplex die Konstruktion ist, zeigt ein weiterer Trick, der dem Virus den Anschein des Legalen verleiht. Im Internet werden Zertifikate durch Firmen ausgestellt, die die Aktivität eines Servers oder eines Programmcodes prüfen und als eine Art Treuhänder eine Unbedenklichkeitsbescheinigung ausstellen. Wer ein solches Zertifikat vorweisen kann, darf passieren. Die taiwanischen Firmen Realtek Semiconductor und JMicon Technology sind solche Treuhänder.

Im Januar 2010 taucht eine Stuxnet-Variante auf, die mit einem Zertifikat von Realtek signiert ist. Im Juli 2010 folgt eine Version, die ein Zertifikat von JMicon aufweist. Beide Zertifikate sind gestohlen. Allein dieser Diebstahl ist eine Operation, die entweder einen physischen Einbruch in die Zentralen der beiden Firmen erfordert oder einen Hacker-Angriff, wie ihn weltweit nur wenige Programmierer beherrschen. Denn die Zertifikate sind besonders gesichert und verschlüsselt.

In einer als „secret“ eingestuften Analyse eines europäischen Geheimdienstes, die der SPIEGEL einsehen konnte, heißt es, für die Entwicklung von Stuxnet habe ein Programmierer mindestens drei Jahre gebraucht, und sie habe einen zweistelligen Millionenbetrag gekostet. Symantec schätzt sogar, dass allein die Tests in der Modellanlage fünf bis zehn Programmierer für ein halbes Jahr beschäftigt haben. „Nichtstaatliche Akteure“, so die Geheimdienstanalyse, könnten als Erfinder von Stuxnet „so gut wie ausgeschlossen werden“. Das glauben auch die Mitglieder des Bundessicherheitsrats, der am 25. November 2010 in Berlin zusammentritt.

Stuxnet zeige, was alles passieren könne, wenn man potente Angreifer habe, sagt der damalige Innenminister Thomas de Maizière. Wer so viel Geld und Ressourcen investiere, der wisse, was er tue. Dahinter, darin ist sich die Runde einig, könne nur ein Staat stecken.

De Maizières Leute haben zusammengetragen, dass täglich 15 Lücken in Standardcomputerprogrammen gefunden würden. Mehrere zehntausend Web-Seiten würden täglich weltweit infiziert. Am Ende der Sitzung beschließt der Bundessicherheitsrat, ein Nationales Cyberabwehrzentrum zu gründen. „Die Erfahrungen mit dem Schadprogramm Stuxnet zeigen, dass auch wichtige industrielle Infrastrukturbereiche von gezielten IT-Angriffen nicht mehr ausgenommen sind“, wird es später in der Kabinettsvorlage der Bundesregierung heißen.

Der Virus hat die Sicht auf digitale Angriffe grundlegend verändert. Die amerikanische Regierung hat vor kurzem eine neue Cyberwar-Doktrin erlassen, wonach

ein solcher Angriff wie ein konventioneller Überfall zu einem Kriegsgrund werden kann. Der öffentlich zugängliche Code von Stuxnet, warnte Roberta Stempfley vom US-Heimatschutzministerium vergangene Woche, könne Nachahmer inspirieren.

Auch die britische Regierung hat im vergangenen Jahr eine neue Sicherheitsstrategie beschlossen und dafür 650 Millionen Pfund bereitgestellt. Die Cyberwelt werde in Konflikten zwischen Staaten immer wichtiger, erläuterte im Februar Dan Meridor, Israels Vize-Ministerpräsident, bei einem Vortrag in Jerusalem. „Das ist ein neues Schlachtfeld, auf dem nicht mit Kanonen, sondern mit etwas anderem gekämpft wird.“

Der Mossad betrachtet Stuxnet als großen Erfolg, vergleichbar mit dem Knacken der deutschen Chiffriermaschine Enigma durch Polen und Briten im Zweiten Weltkrieg. Das israelische Militär ist weniger euphorisch. Dass Stuxnet aufgefliegen ist, sei ein hoher Preis gewesen, trotz des Rückschlags für das Mullah-Regime.

Und der war schmerzhaft. Eine iranische Zentrifuge vom Typ IR-1 dreht sich normalerweise mit 1064 Hertz. Als die Rotoren verrücktzuspielen begannen, erhöhten sie ihre Frequenz 15 Minuten lang auf 1410 Hertz, um dann zur normalen Frequenz zurückzukehren. 27 Tage später übernahm der Virus erneut die Kontrolle, diesmal bremste er die Rotoren über 50 Minuten lang auf eine Frequenz von ein paar hundert Hertz. Die Aluminiumröhren wurden durch die übermäßige Fliehkraft gedehnt, die Gefahr stieg, dass Teile sich berühren und die Zentrifugen zerbrechen.

Sechs Kaskaden mit jeweils 164 Zentrifugen sollen auf diese Weise zerstört worden sein. Rund tausend Geräte habe Stuxnet zerstört, das glauben Kenner des iranischen Atomprogramms wie David Albright vom Washingtoner Institut Isis. Iran hat eingeräumt, dass das Nuklearprogramm zurückgeworfen wurde, mit „potentiell großen Schäden“, wie Gholamreza Dschalali, der Chef der iranischen Zivilverteidigung, zugibt.

Dagan hat sein Ziel erreicht, das Atomprogramm zu sabotieren, ohne dass es darüber zu einem neuen Nahost-Krieg kam. Aber Iran hat noch 8000 weitere Zentrifugen, und die moderneren Geräte der zweiten Generation IR-2, die mit Kohlefaserrotoren ausgestattet sind, laufen auch bei 1400 Hertz rund, sie sind von dieser Version der Sabotage-Software nicht betroffen. Der Mossad könnte bald einen neuen Virus brauchen. Es wäre die nächste Runde im geheimen Cyberkrieg.

Tel Aviv, eines der modernen Cafés der Stadt, am Tisch sitzen zwei junge Israelis, die indirekt für den Staat arbeiten: Sie haben eine eigene Firma, die Jobs für den Mossad und den Inlandsgeheimdienst Schin Bet übernimmt. Sie lächeln, sie sagen, ihre Disziplin sei der digitale Angriff, nicht die Abwehr, sie gehören zur globalen Hacker-Elite. In Jerusalem und Tel Aviv kursiert das Gerücht, die beiden hätten dem Mossad bei Stuxnet zugearbeitet, Recherchen im Vorfeld übernommen.

„Die Leute haben so etwas wie Stuxnet bislang nur in Filmen gesehen“, sagt einer der Hacker. „Jetzt sehen sie, dass es real ist.“ Aus seiner Stimme spricht Stolz, als er sagt: „In der kleinen Gemeinde der Angreifer ist nichts davon wirklich neu gewesen.“ Fast jede der Schwachstellen sei schon einmal bei einer Attacke eingesetzt worden, aber niemals alle gemeinsam. Die wirkliche Herausforderung für einen Angriff mit einem Virus wie Stuxnet sei die Aufgabe, in ein System einzudringen, das nicht am Internet hänge.

Was die Folgen von Stuxnet seien?

Die beiden schweigen, ihre Sicht ist die Perspektive der Angreifer. „Die Entdeckung von Stuxnet hat uns schwer geschadet“, sagt einer der beiden. „Für uns ist das bitter, weil eine erfolgreiche Methode enthüllt wurde.“

Die Erfinder von Stuxnet hatten offenbar noch viel vor mit ihrem Produkt. Inzwischen hat Symantec eine weitere Version des Stuxnet-Virus gefunden, die einen noch komplexeren Code beinhaltet und auf moderne Siemens-Steuerungstechnik zielen sollte, aber bislang nicht aktiviert war. Stuxnet, sagen die Symantec-Leute, „ist die Art von Bedrohung, von der wir hoffen, dass wir sie nie wiedersehen“.

Die Hoffnung dürfte nicht in Erfüllung gehen.

HOLGER STARK



Iranische Atomanlage bei Natans: „So etwas gab es bislang nur in Filmen“