Die sittsamen Verbrecher im «Silicon Wadi»

Der Cyber-Tech-Sektor in Israel boomt und bringt dem Land Milliarden und Ansehen

ULRICH SCHMID, TEL AVIV

Die Weissen sind die Guten. Die Schwarzen sind evil, und sie treffen sich im Dunkeln, im Darknet zum Beispiel, dem virtuellen Tummelplatz all jener, die Diskretion lieben, also auch der Verbrecher. In diese attraktive Finsternis hinab steigt heute Alex, Mitarbeiter der Consulting-Firma White Hat in Tel Aviv, ein Ritter der edlen Gestalt zweifellos, wenn auch ohne weiss schimmernde Rüstung, dafür jung, cool und ausgestattet mit Computerkenntnissen, die in der Branche grosse Anerkennung finden. Er sucht nicht das Allerschlimmste. Er könnte Drogen kaufen, Waffen und Sexsklaven, es wäre ihm ein Leichtes, einen Mord nach seinem Gusto live in Szene zu setzen. Doch Alex ist den «Black Hats» auf der Spur, jenen Kriminellen, die Daten klauen, Viren säen und ihre Opfer erpressen. Sie will er ausspionieren.

Alex heisst Alex, aber das wär's dann auch schon, einen Nachnamen gibt's nicht. Reut Menashe indessen heisst so. Ihre Wurzeln liegen in Iran, sie ist Chief Technology Officer bei White Hat, eine junge Frau, die ihre Liebe zu Computern schon als Kind entdeckt und diese Liebe zum Beruf gemacht hat. Reut erklärt, was Alex und und das gute Dutzend seiner Kolleginnen und Kollegen tun. Sie gehen online auf Tuchfühlung zu den Kriminellen. Im Darknet und auf vielen anderen solchen Webseiten versuchen sie, Avataren gleich, an die Methoden heranzukommen, mit denen die Software von Firmen geknackt wird. Das Gefundene verwenden sie, um ihren Klienten zu helfen. Manchmal, wenn sie auf Pädophilen-Netzwerke stossen zum Beispiel, benachrichtigen sie auch direkt die Polizei. White Hat boomt, man ist international unterwegs, die Löhne sind «ganz okay».

Angehörige des israelischen Militärs bei einem Cybersicherheitstraining in Beer Sheva. AMIR COHEN / REUTERS

Hightech-Weltmacht Israel

Israel ist eine High-Tech-Weltmacht. Hunderte Firmen sind hier, die Startup-Szene boomt, das «Silicon Wadi» hat längst zum «Silicon Valley» aufgeschlossen, das ganze Land befindet sich in einem wunderbaren Taumel der Innovation. Klar, dass hier auch die Hacker-Szene blüht. Viele versuchen, Online-Sicherheitssysteme zu überwinden. Und hier kommen White Hat und all die Unternehmen ins Spiel, die diese Firmen schützen. Das tun sie, wie Reut Menashe erklärt, indem sie originell («out of the box») denken und in die Gehirnwindungen von Hackern schlüpfen. Doch auch die Kunden selber werden bearbeitet. Oft muss man den Firmen klarmachen, dass eine gute Firewall und ein Antivirenprogramm längst nicht mehr genügen. Heute kommt der alles lahmlegende Virus über den neuen Drucker ins System oder über ein unscheinbares Gerät, das irgendein Mitarbeiter fernab von den grossen Computern ahnungslos in eine Buchse seines Autos steckt. Das kann genügen, um eine riesige Firma praktisch zu vernichten.

Die Weissen Hüte sind also die Guten. Oder etwa nicht? Doch, doch, sagt Reut Menashe. Eindeutig. Man bietet die Produkte an, man zwingt sie niemandem auf. Man macht mit beim berauschenden israelischen High-Tech-Boom, was im Grossen und Ganzen eine gute Sache ist. Das Leben ist gut. Man ist jung und hip, man chillt beim Pingpong oder auf weichen, farbigen Kissen und hört gute Musik. Und man ist in Tel Aviv, was sowieso supergut ist. Weniger in Ordnung für Reut Menashe ist, dass auch in Israel im High-Tech-Sektor noch weit weniger Frauen arbeiten als Männer. Bei White Hat sind es zwei. Was kann man tun? Das werde sich geben, sagt die Technik-Offizierin, man müsse Geduld haben. Die Regierung tue viel, um die Frauen in eine gute Ausgangslage zu befördern. Allgemein seien Frauen am Computer «positiv konnotiert». Gemeinschaftsprogramme wie «She codes», von Frauen mit dem Ziel gegründet, dafür zu sorgen, dass es unter Israels Software-Entwicklern ebenso viele Frauen wie Männer gibt, boomen. Bereits im Kindergarten lernen Knirpse, Mädchen wie Jungs, einen Computer zu programmieren und Hackerangriffe abzuwehren. «Cyber Tech ist eine nationale Aufgabe.»

Ein High-Tech-Traum ganz in Pink also? Nicht ganz. Wechseln wir kurz in die Vereinigten Arabischen Emirate. Ahmed Mansur ist Menschenrechtsaktivist. Inspiriert vom frischen Wind des Arabischen Frühlings, unterzeichnete er 2011 zusammen mit einigen Mitkämpfern eine Petition für ein demokratisch gewähltes Parlament. Er wurde verhaftet und zu drei Jahren Haft verurteilt. Um ihm auf die Schliche zu kommen, hatte Abu Dhabi Malware des Typs «Pegasus» verwendet, die von der Firma NSO Group Technologies hergestellt wird. NSO, gegründet 2010, ist eine Firma mit Sitz in Herzliya, nördlich von Tel Aviv. Dass Mansur einen Tag nach seiner Verurteilung 2011 begnadigt wurde, tut hier nichts zur Sache. Relevant ist, dass Israel Cyber-Tech-Überwachungssysteme entwickelt, die gleichsam vom Regal weg zu haben sind, und dass Regime mit üblem Ruf sie kaufen, um missliebige Journalisten zu überwachen.

Es gibt andere Beispiele. Äthiopien zählt zu den ärmsten Ländern der Welt. Nur rund 5 Prozent der Bevölkerung haben Zugang zum Internet. Doch die Regierung kontrolliert viele Dissidenten mit ausgeklügelter Software. Jeder Schritt, den die Opfer auf ihrem Computer tun, wird verfolgt, sogar Kameras und Mikrofone können fernbedient werden. Eingekauft hat die Regierung in Addis Abeba diese Technik bei Cyberbit Security Solutions, einer hundertprozentigen Tochter des in Haifa basierten, multinational agierenden Elektronikriesen Elbit Systems, dessen über 12'000 Mitarbeiter Militärtechnik, Überwachungsgerät, Drohnen, Elektrooptik und mehr herstellen. Cyberbit Security Solutions, gegründet 2015, ist in Ra'anana am Mittelmeer zu Hause und hilft laut Eigenwerbung Firmen, Bedrohungen im Internet schon im Voraus zu entdecken, und zwar «in Sekunden».

Cyber-Stadt in der Wüste

Das also ist die Kehrseite des «guten» Booms. Technik, die zerstörerische Viren findet, kann auch kritische Journalisten zum Schweigen bringen. Der Nichtregierungsorganisation «Reporter ohne Grenzen» ist dies schon vor langer Zeit aufgefallen. Bereits 2013 wies sie darauf hin, dass im Arabischen Frühling 2011 Länder wie Libyen, Tunesien, Syrien und Ägypten Journalisten mit Programmen ausspionierten, die in Deutschland entwickelt wurden. Inzwischen hat Israel Deutschland überholt. Zwar ist der Export geregelt, doch wie Figura zeigt, haben weder NSO noch Cyberbit Mühe, ihre Produkte loszuwerden. Beide Firmen geben sich widerborstig, mehr als ein «Kein Kommentar» hat ihnen der Korrespondent nicht entlocken können. Gegenüber «Citizen Lab», einer Gruppe von Wissenschaftern der Universität Toronto, haben die Verantwortlichen von Cyberbit immerhin klargestellt, man verkaufe nur an souveräne Regierungen. Für den Umgang mit diesen System seien diese selber verantwortlich.

Ob solches Verhalten mehr Entrüstung verdient als beispielsweise der grosszügige Verkauf von «Rüstungsgütern» – man könnte auch «Kriegsgerät» sagen – aus der Schweiz oder Deutschland an Länder wie Saudiarabien oder Katar, darüber liesse sich diskutieren. In Beer Sheva aber interessieren solche Fragen kaum. Nirgendwo in Israel ist die Begeisterung über High Tech und Cyber Tech grösser als in dieser eigenartigen, faszinierenden Wüstenstadt. Hier befindet sich das neue nationale Cyber-Tech-Zentrum, und gerne erinnert man sich daran, dass schon Ben Gurion sagte, die Zukunft Israels liege im Negev. Netanyahu will, dass Beer Sheva zum Magneten für Firmen aus Israel und der ganzen Welt wird. Wer kommt, erhält Steuererleichterungen. Und alle sind da. Das Militär hat seine grössten und prestigeträchtigsten Anlagen hierhergebracht, ganz in die Nähe der Ben-Gurion-Universität. Dell EMC, Lockheed Martin, Paypal und die Deutsche Telekom sind in Beer Sheva, und selbstverständlich auch das Israeli National Cyber Bureau.

Dies ist der richtige Ort, um sich nach den Gründen und Voraussetzungen des israelischen Cyber-Tech-Booms zu erkundigen. Amos Stern ist Mitbegründer und Geschäftsführer der Firma Siemplify und ehemaliger Anführer einer Computer-Sondereinheit der Armee. Sein Lebenslauf erklärt im Grunde schon alles. Viel, fast alles eigentlich, was sich heute im Startup-Sektor etabliert, hat in der Armee oder beim Mossad, dem Geheimdienst, angefangen. Stern hat die Erkenntnisse, die er im Militär gewonnen hat, auf den Zivilsektor übertragen. Seine Produkte reduzieren oder eliminieren Hintergrundgeräusche. Die anderer neuer Firmen konzentrieren sich auf den Empfang schwacher, weit entfernter Signale, auf die säuberliche Trennung sich überlagernder Geräuschquellen oder auf das Sehen ohne Licht.

Den Russen auf der Spur

Das zweite ist die konsequente staatliche Förderung. Man kann Netanyahu viel vorwerfen, aber nicht, dass er die Bedeutung des Sektors verkennt. Schon 2011 gab er die Losung aus, Israel in einer konzertierten Aktion zu einem der fünf mächtigsten Cyber-Staaten zu machen. Die National Cyber Defense Authority koordiniert Kontakte zwischen der Regierung, dem Sicherheits-Establishment und dem Privatsektor zum Wohle des Landes, wobei die Behörde laut Netanyahu die klare Aufgabe hat, nationale Sicherheitsbedürfnisse und demokratische Grundrechte gegeneinander aufzuwiegen. Dass dies immer gelingt, glauben nicht alle, aber in dieser Hinsicht steht Israel wahrhaftig nicht allein da. Der Mossad befeuert den Ideenreichtum noch zusätzlich mit Lockangeboten. Im Sommer 2016 kreierte er einen Investment-Fonds für neue Spionage-Techniken. Vielversprechende Erfinder erhalten bis zu 2 Millionen Schekel pro Projekt.

Das Resultat aller dieser Bemühungen sind Firmen wie White Hat und Eldorados der Innovation wie Beer Sheva, Haifa oder Tel Aviv. Cyber Tech blüht. Israel hat weltweit die zweithöchste Dichte an Cyber-Tech-Firmen nach den USA. Ein Viertel aller mit Venture Capital finanzierten Startups weltweit befindet sich in Israel. Der Wert der aufsummierten Anti-Hacking-Exporte beträgt derzeit um die 5 Milliarden Dollar. Und das alles ist nur ein Teil des boomenden High-Tech-Bereichs mit seiner mittlerweile bekannten, geradezu notorischen Risikobereitschaft. Was illustrierte es besser als der Begriff Venture Capital? Was im Englischen grandios nach Abenteuer klingt, nach Eroberung und neuen Horizonten, wird im Deutschen zu «Risikokapital», zu etwas potenziell Gefährlichem also, das man besser vermeidet. In Israel nimmt man einen, der nicht schon zwei, drei Firmen in den Sand gesetzt hat, gar nicht erst ernst, und Venture Capital fliesst auch nach der fünften Pleite. Das ist günstig, denn der Weltmarkt ist gigantisch, und er lässt sich leichter erobern, wenn man mehrere Anläufe nehmen kann. Laut «Forbes» wird der Weltumsatz im Cyber-Tech-Bereich bis 2020 auf 170 Milliarden Dollar anwachsen. Mindestens.

Ein indirektes Erbe des Holocausts

USd. · Dass die Israeli gute Hacker sind, weiss die Welt inzwischen sehr genau. Es waren Mossad-Beamte, die herausfanden, dass sich die russischen Regierungs-Hacker, die sie gerade ausspionierten, auf Antiviren-Software der Firma Kaspersky stützten. Diese Software wird von 400 Millionen Usern weltweit verwendet, aber auch von amerikanischen Regierungsstellen. Die Israeli informierten umgehend die Amerikaner, und die Welt war um eine Internet-Sensation reicher. Als Antonio Forzieri, Sicherheitschef des Software-Giganten Symantec, sagte, er habe Hacker auf der ganzen Welt gesehen, aber die israelischen seien die besten. Sie seien jünger, schneller und gescheiter als fast alle andern, da wurde dies von Haifa bis Eilat zitiert, und das Einzige, was die Menschen verblüffte, war dieses irritierende «fast» in Forzieris Lob. Eben war der frühere CIA-Chef David Petraeus in Tel Aviv an der alljährlichen Cyber-Tech-Konferenz. Es ist ein Riesen-Event, aus 80 Ländern kamen 15 000 Aficionados angereist, und die Israeli hörten stolz, dass Petraeus ihnen attestierte, sie seien eine «Cyber-Supermacht». Allerdings: Wer viel austeilt, muss auch einstecken. Israel ist eines der am meisten im Internet attackierten Länder der Welt.

Aber warum? Genügen die Hinweise aufs Militär, den Mossad und den spendablen Staat wirklich? Warum soll ausgerechnet dieses winzige Mittelmeerland, fern von den übrigen Zentren der Forschung, eine solche Expertise entwickeln? Wir fragen bei Daniel Cohen nach, dem Leiter der Sicherheitsabteilung von RSA Security, einer amerikanischen Cyber-Firma, die 1992 in Bedford, Massachusetts, von Adi Shamir, Ron Rivest und Leonard Adleman gegründet wurde. Cohen stellt sich im Netz als «Maker of ways, paver of paths» vor und nennt zunächst ebenfalls die üblichen Verdächtigen, das Militär, den Staat, die Risikobereitschaft. Doch dann räumt er ein, dass natürlich auch die einzigartige Geschichte der Juden ein Grund sei, weshalb der Cyber-Tech-Sektor derart blüht. Und nun schwebt schon etwas Pathos durch den Raum. Die prägende Wirkung des Holocausts könne gar nicht überschätzt werden, sagt Cohen. Juden hätten halt stets die persönliche Sicherheit im Kopf. Sie sei ihr Mantra. «Den andern einen Schritt voraus zu sein: Das ist unsere Lebensversicherung.»