CYBER-KRIEG. Hochspezialisierte Hacker machten es möglich, dass zwölf israelische F15 unentdeckt in den syrischen Luftraum eindringen konnten.

WER AN DEN REGLERN DREHT...

Wer die Regler der modernen Kommandozentralen kontrolliert, hat die Macht. Das wissen die *modernen Kriegsführer* genauso gut wie kriminelle Hacker. Ein neuer Kampf um die Netze hat begonnen.

Von Alfons Flatscher

Am 29. und 30. Jänner 2013 drangen zwölf israelische Kampfflugzeuge, darunter F15-E-Jets, in syrischen Luftraum ein und bombardierten einen LKW-Konvoi, der SA-17 Boden-Luftraketen an die libanesisches Hisbollah liefern sollte. In der darauf folgenden Nacht zerstörten die Jets das militärische Forschungszentrum Jamraya in der Nähe von Damaskus, was erst bekannt wurde, als ein syrischer General in einem Interview mit dem katarischen Fernsehsender Al Jazeera den Verlust beklagte. Die Israelis selbst gaben sich über Ablauf, Ziel und Erfolg der Angriffe völlig zugeknöpft. Verteidigungsminister Ehud Barak, der zu der Zeit an der Münchner Sicherheitskonferenz teilnahm, erklärte nur so viel: »Es ist eine weitere Bestätigung dafür, dass wir meinen, was wir sagen.« Wie die zwölf Kampfflugzeuge unbemerkt bis direkt vor Damaskus eindringen konnten, blieb zunächst ein Rätsel. Es kam der Verdacht auf, die Israelis hätten Tarnkappenbomber, also für Radar nicht sichtbare Fluggeräte, eingesetzt.

Der Verdacht wurde genährt, weil erst im Oktober 2012 das Regime von Bashar Al Assad vom einzigen noch verbliebenen Verbündeten, den Russen, mit einem völlig neuen Radarsystem ausgestattet worden war. Neueste Radartechnologie war im Einsatz – trotzdem schlugen die Sensoren in jener Nacht nicht an. Das System der Syrer schien zunächst völlig normal zu funktionieren. Als die Kampfflugzeuge der Israelis schon zu hören waren, tauchten auf den Radarschirmen plötzlich Anzeigen auf: Hunderte Flugzeuge wurden nun geortet. Auf den Radarschirmen sahen die Assad-Treuen nur, was die hochspezialisierten Hacker ihnen zu sehen gaben: zuerst nichts, dann viel zu viel. Die Kontrolle der elektronischen Leitsy-

FOTO: PHOTOS.COM

steme war gekapert worden, das Radar manipuliert und die Mission der F15-Jets ein voller Erfolg. Wer die Kommandozentrale kontrolliert, hat die Macht und immer öfter sind es die Cyberkrieger, die teure Ausrüstung zum Tarnen und Täuschen missbrauchen.

Auch das iranische Atomprogramm wurde auf diese Weise um Jahre zurückgeworfen. Stuxnet, ein Computerwurm, von israelischen und amerikanischen Spezialisten entwickelt, hatte gezielt Siemens-Software und Ausrüstung, die Teheran im Einsatz hatte, außer Gefecht gesetzt.

»Vom Militär zu den Cyberkriminellen«

»Diese militärischen Erfolge liefern jetzt das Modell für Kriminelle«, erklärt Ed Skoudis, ein führender Sicherheitsexperte auf der RSA-Konferenz 2013 in San Francisco, Kalifornien. »Sie machen es den Militärs nach und sie übernehmen immer öfter die Kontrolle von Leitsystemen – dort, wo es am wenigsten erwartet wird.«

Art Coviello, der Chef der weltgrößten IT-Sicherheitsfirma RSA, fasste das bei der Eröffnungsrede in einem markanten Satz zusammen: »Die Bedrohung wird kinetisch.«

Bisher war die IT-Verteidigungsstrategie hauptsächlich darauf ausgerichtet, den Diebstahl wichtiger Daten zu verhindern. »Sogar die Militärs haben sich primär darauf konzentriert, Spionage zu verhindern, und geheime Informationen zu schützen«, so Skoudis. »Jetzt sehen wir, dass Angreifer Computer und Netzwerke angreifen, die Ausrüstungen und Geräte der wirklichen Welt kontrollieren.«

Schieber zum Beispiel – Wasserschieber: Der Wasserversorger Illinois American Water erlebte im November 2011 ein böses Erwachen. Das elektronische Leitsystem, mit dem das komplette Rohrnetz kontrolliert wird, tat nicht mehr, was die Techniker wollten. Hacker hatten das Regeln übernommen und demonstrierten ihre Macht, indem sie einen Schieber in Dauermodus setzen. Er öffnete und schloss und zwar so oft und so schnell, bis er brach. Die Hacker bewiesen damit, was sie anrichten können und das sie die komplette Kontrolle über alles haben, was elektronisch geregelt wird.

VERSUCHSLABOR. *Der israelische Verteidigungsminister Ehud Barak gab sich zugeknöpft, mit welchen Technologien das Militär arbeitet.*

»Erpressung als Geschäftsmodell«

Manchmal ist Aufmerksamkeit das Einzige, was Hacker erreichen wollen. Sie beweisen, wozu sie technisch in der Lage sind, begnügen sich mit diesen Triumphen, ohne wirklich Schaden zuzufügen. Für andere aber ist das Geschäftsmodell Erpressung und hier sind die beliebten Opfer in Industrien zu finden, an denen bisher die Diskussion um IT-Sicherheit ziemlich spurlos vorüber gegangen ist, weil sie sich schlicht und einfach nicht bedroht fühlten.

Im Dezember 2011 etwa fiel die Eisenbahngesellschaft Pacific Northwestern einen Cyberangriff mit sehr realen Auswirkungen zum Opfer: Das Leitsystem der Pendlerzüge wurde lahmgelegt, enorme Verspätungen waren die Folge und die Arbeit stand in vielen Betrieben für Stunden still. Das Personal steckte in den Zügen fest.

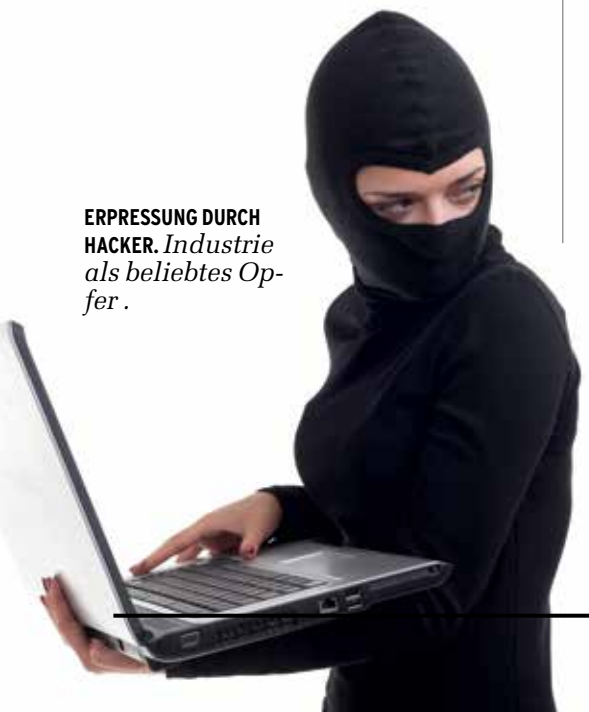
Im Herbst 2012 nutzte eine Bande die zunehmende Digitalisierung der Stromzähler, um Smart Meter zu hacken und damit Millionen von Dollars abzuzocken.

Die Erpresser suchen sich die leichtesten Opfer und während in der Finanzindustrie IT-Sicherheit eine immer bedeutendere Rolle spielt, befinden sich Wasser- und Energieversorger, Krankenhäuser und Verkehrsunternehmen noch im Sicherheits-Nirwana. Das zieht Kriminelle an.

Ed Skoudis meint dazu: »Betroffene Firmen halten sich meist sehr bedeckt, weil sie zum materiellen Schaden nicht auch noch den PR-Gau haben wollen. Wir leben im Zeitalter von Wikileaks, aber bewegen uns ins Zeitalter, in dem an den physischen Reglern, die unsere industrialisierte Welt bewegen, gedreht wird.«

Um die Bedrohung zu simulieren, hat Skoudis das Projekt Cybercity entwickelt. Auf zehn Quadratmetern wurde eine Ministadt gebaut, die über ein SCADA-kontrolliertes Stromnetz verfügt, ein elektronisch gesteuertes Verkehrsnetz hat, moderne Wasserversorgung, ein Bahnnetz, Internetprovider, Banken, Kaffeehäuser und so weiter. Jedes Viertel hat seine eigene PLC-Steuerung – von Siemens, Allen Bradley, General Electric und anderen.

Cyberkrieger werden beauftragt, die Stadt lahmzulegen. Skoudis und seine Truppe sind für die Abwehr zuständig. Das Ziel ist, den Angreifern immer einen Schritt voraus zu sein. »Das ist schwierig«, meint Sicherheitsexperte Skoudis, »aber der ganze Sinn des Projektes ist, zu beweisen, dass wir bei aller Verwundbarkeit die Technologie beherrschen können.« ■



ERPRESSUNG DURCH HACKER. *Industrie als beliebtes Opfer .*