wiwo.de

Wirtschafts Woche

49

6.12.2010 | Deutschland €4,30

- **Gerne arbeiten**
  Die besten Arbeitgeber
- **Ewig zahlen**
  Die Euro- und Bankenkrisen
- **Zittern, ob sie zahlen**
  Wie sicher Ihre Lebensversicherung noch ist

Wann ist Ihre Firma dran?

Wikileaks' Datenklau war erst der Anfang

Schweiz CHF 7,50 | Österreich €4,60 | Benelux €4,80 | Bulgarien BGN 11,- | Dänemark DKK 40,- | Griechenland €5,60 | Großbritannien GBP 4,70 | Italien €5,30 | Polen PLN 26,50 (€4,40) | Portugal €5,60 | Slowakei €5,40 | Spanien €5,30 | Tschechische Rep. CZK 192,- | Türkei YTL 13,- | Ungarn FT 1 900,-

Virtuelle Marschflugkörper

CYBERWAR | Die Enthüllungen von Wikileaks zeigen, wie verwundbar Staaten und Unternehmen durch das Internet geworden sind. Dabei ist Datenspionage nur der Anfang. Im Zeitalter digitaler Kriege lassen sich Wasserversorgung, Handynetze und sogar Kraftwerke über das Netz lahmlegen. Deutschland ist erschreckend schlecht geschützt.

So also sieht ein Staatsfeind Nummer eins aus: blond, leicht gerötete Wangen und das Lächeln eines Buben. Der 23-jährige US-Obergefreite Bradley Manning hat gerade die ganze Welt in Aufregung versetzt. Er erleichterte US-Behörden um Abertausende brisante Depeschen, die Botschaften in aller Welt an das State Department in Washington geschickt hatten. Jetzt kann jeder auf der Internet-Seite der Organisation Wikileaks nachlesen, was die USA über Spitzenpolitiker in aller Welt denken.

Der diplomatische Scherbenhaufen ist das Ergebnis eines einzigen virtuellen Anschlags im fernen Irak. Während seines Einsatzes nutzte Manning Sicherheitslücken in einem speziellen, von den Geheimdiensten überwachten Regierungsnetz und zapfte den Datenaustausch zwischen dem Verteidigungs- und dem Außenministerium an. Der begabte Computerexperte kopierte die Daten auf eine CD und schickte sie an Wikileaks.

Diese CD versetzte nicht nur die internationale Diplomatie in Aufruhr. Sie zeigt zugleich, wie verwundbar das Internet Staaten und Konzerne gemacht hat. Erst vor wenigen Tagen kündigte Wikileaks-Gründer Julian Assange zudem an, die nächsten Enthüllungsgeschichten kämen aus der Bankenwelt. Seither fürchten Wall-Street-Manager, die Informationen könnten ihre Branche erneut ins Chaos stürzen. Alle fragen sich: Wer ist der Nächste? Und vor allem: Wie sicher sind unsere Daten im Netz?

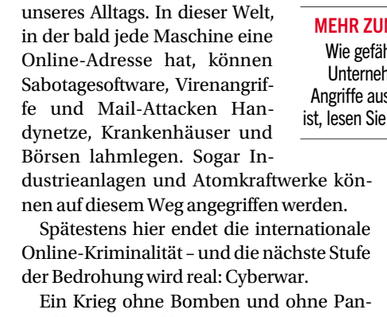
Die schlechte Nachricht: Cyber-Spionage ist nur der Anfang. Mittlerweile zeichnet sich eine noch viel größere Gefahr ab. Denn vernetzte Computer prägen alle Bereiche unseres Alltags. In dieser Welt, in der bald jede Maschine eine Online-Adresse hat, können Sabotagesoftware, Virenangriffe und Mail-Attacken Handynetze, Krankenhäuser und Börsen lahmlegen. Sogar Industrieanlagen und Atomkraftwerke können auf diesem Weg angegriffen werden.

MEHR ZUM THEMA
Wie gefährdet Ihr Unternehmen für Angriffe aus dem Netz ist, lesen Sie ab Seite 86

Spätestens hier endet die internationale Online-Kriminalität – und die nächste Stufe der Bedrohung wird real: Cyberwar.

Ein Krieg ohne Bomben und ohne Panzer. Um in einem Unternehmen oder einem ganzen Land Chaos anzurichten, reichen eine Handvoll Hacker, ein paar Computer und der Zugang zum Internet. Auch Terroristen horten längst Wissen darüber, wie sie mit Bits und Bytes größeren Schaden anrichten könnten als mit Bombengürteln.

Im vergangenen Jahr erst gelang es Taliban im Irak, den Datenstrom einer unbemannten Drohne vom Typ Predator anzuzapfen, sie hatten die Datenübertragung via Satellit geknackt. „In der Cyber-Welt zählen Einfallsreichtum und Flexibilität mehr als materielle Überlegenheit“, sagt Bernd Oliver Bühler, geschäftsführender Gesellschafter der Unternehmensberatung Janus Consulting. „Selbst Individuen sind nun in der Lage, ganzen Staaten erheblichen Schaden zuzufügen.“ Damit beginnt eine neue Ära der Kriegsführung.



Ein einzelner USB-Stick kann Börsen heute in den Abgrund reißen

INAKZEPTABEL VERWUNDBAR

Vor zwei Wochen hat die Nato die neue Bedrohung in ihre verteidigungspolitischen Leitlinien aufgenommen. „Wir reden hier nicht mehr über Science-Fiction“, sagt Nato-Generalsekretär Anders Fogh Rasmussen, „die Bedrohung ist real.“ Dabei diagnostiziert das neue strategische Konzept große Lücken in der Cyber-Verteidigung. „Die Verwundbarkeit ist inakzeptabel und zunehmend gefährlich.“

Auch für Deutschland. Verteidigungsminister Karl-Theodor zu Guttenberg sieht vor allem Kommunikationsnetze gefährdet. „Heutzutage kann ein USB-Stick ganze Börsen zusammenbrechen lassen“, urteilt er. Trotz solcher Bedrohungen stecke die Vorbereitung auf den Cyberwar in Deutschland „bestenfalls in den Kinderschuhen“.

Was für eine Untertreibung. Nach Ansicht von Experten ist Deutschland besonders anfällig für elektronische Attacken. Vor allem, weil die Unternehmen ihr Geschäft aus Kostengründen schneller digitalisiert haben als Wettbewerber in anderen Ländern. Dass Autokäufer ihre Karossen inzwischen online konfigurieren und Supermarkt-Tiefkühltruhen automatisch neue Ware ordern können, ist Ausdruck dieser totalen Automatisierung. »

ILLUSTRATIONEN: CHRISTOPH NIEMANN, TOM MACKINGER

© Handelsblatt GmbH. Alle Rechte vorbehalten. Zum Erwerb weitergehender Rechte wenden Sie sich bitte an nutzungsrechte@vhb.de.

» Viele Unternehmen lassen zudem Kraftwerkssteuerungen, Telefonanlagen oder Maschinen via Internet warten. Auch das erhöhe das Risiko für Cyber-Angriffe dramatisch, sagt Sicherheitsberater Bühler.

Und schließlich liegt die Verantwortung für den Schutz Deutschlands gegen digitale Angriffe – anders als in den USA – nicht beim Militär, sondern beim Innenministerium. Die Bundeswehr kümmert sich nur um den Schutz ihrer eigenen IT. Statt effizienter Gegenmaßnahmen, fürchten Experten, könne es daher im Verteidigungsfall zu Kompetenzgerangel kommen.

GEZIELT MASCHINEN ATTACKIEREN

Das könnte sich rächen. In diesem Sommer erst versetzte der technisch extrem ausgefeilte Computerwurm Stuxnet Behörden, Militärs und Industrie in Alarmzustand. Der Wurm war erstmals nicht nur für den Datenklau konzipiert, sondern darauf abgerichtet, gezielt Maschinensteuerungen in der Industrie anzugreifen. Bis heute rätseln Experten, wer hinter der destruktiven Software steckt. Vermutlich wurde er programmiert, um das iranische Atomprogramm zu sabotieren.

Klar jedenfalls ist, dass Stuxnet für die Industrie gefährlich ist wie kein Virus zuvor. Er gilt als Blaupause für künftige, noch gefährlichere virtuelle Marschflugkörper und markiere daher „eine neue Dimension der Bedrohung“, urteilt August Hanning, bis Dezember 2005 Präsident des Bundesnachrichtendienstes (siehe Interview Seite 85).

Audun Lødemel, Sicherheitsexperte beim norwegischen IT-Security-Dienstleister Norman, nennt den Programmcode „ein Präzisionsgewehr in der Hand eines Scharfschützen“. Für Unternehmen wie Wasser-, Öl- und Gasversorger sowie Eisenbahnen bedeute das „Alarmstufe Rot“.

»Hacker könnten Atomkraftwerke per Software-angriff abschalten«

Besonders gefährdet sind große Stromversorger wie E.On und RWE. Sie stecken mitten im Umbau ihrer Infrastruktur: Dabei verschmelzen sie Stromleitungen, Steuerungselektronik und IT. Schon bald wollen sie mithilfe der Technik Tarife anbieten, die entsprechend der verfügbaren Strommenge mal billig und mal teurer sind. Doch das vom Kunden bis zum Kraftwerk digitalisierte Stromnetz bietet digitalen Angreifern auch ganz neue Angriffspunkte. Hackern in den USA etwa gelang es im März 2007, einen Dieselgenerator, wie er in Kraftwerken zum Einsatz kommt, per Computervirus zur Selbstentzündung zu bringen und damit zu zerstören. Das war zwar nur ein Test des US-Energieministeriums. Aber nächstes Mal ist es vielleicht schon der Ernstfall.

Kraftwerke sind nur einer von vielen Schwachpunkten: Von der Netzsteuerung bis zur Sabotage des grenzüberschreitenden Stromaustauschs bieten sich elektronisch Angreifenden zahlreiche Ziele. Bereits kleine Störungen dieses empfindlichen Systems der Stromversorgung können Dominoeffekte auslösen, die das gesellschaftliche Leben zum Erliegen bringen, heißt es in der „Nationalen Strategie zum Schutz kritischer Infrastrukturen“ von Bundesinnenminister Thomas de Maizière.

Wie das genau aussehen würde, versuchen nun die Forscher des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag herauszufinden. Seit Monaten arbeiten sie an Szenarien für einen flächendeckenden Stromausfall, wie ihn eine eine massive Cyber-Attacke auslösen kann. Am Beispiel von Baden-Württemberg haben die Experten des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe in Bonn schon einmal durchgerechnet, wie rasch das Alltagsleben nach einem Ausfall der Stromversorgung aus dem Ruder laufen kann (siehe Übersicht Seite 81).

NACH EINER WOCHE AUFRUHR

Binnen weniger Stunden würden die ersten Kommunikationsnetze, das Internet und selbst Teile der Treibstoff-Versorgung versagen. Kurz darauf wird das Trinkwasser knapp. Ohne Strom versagen Kassen und Türen der Supermärkte. Nach dem Ausfall der Notstromaggregate müssten nach wenigen Tagen selbst Krankenhäuser ihren Betrieb einschränken und Industrieunternehmen die Produktion drosseln. Vor allem aber kommt spätestens nach dem Ausfall von Geldautomaten und Bank-Rechenzentren der Wirtschaftskreislauf zum Erliegen. Nach einer Woche, so die Prognose, herrschen Aufruhr und Ausnahmezustand.

In Estland hat man das schon erlebt. Dort brach im April 2007 der sogenannte „Web War One“ aus. So nennen Sicherheitsexperten den ersten politisch motivierten Hackerangriff auf die Internet-Infrastruktur eines Staates: Unzählige automatisierte Anfragen, sogenannte Denial-of-Service-Attacken, zwangen die Internet-Seiten von Ministerien, Medien und Banken des Baltenstaats in die Knie. Binnen kurzer Zeit waren Schulen und Behörden nicht mehr erreichbar. Drei Viertel aller Bank-Transaktionen

FOTOS: PHOTOTHEK/THOMAS TRUTSCHEL, LAIF/GEO; BLOOMBERG NEWS; ILLUSTRATION: CHRISTOPH NIEMANN

World Wide War Mobiles Rechenzentrum der Bundeswehr als digitales Angriffsziel

waren blockiert, Unternehmen konnten keine Löhne mehr zahlen.

Erst als die Esten ihre Server vom Internet trennten, ebbten die Angriffe nach drei bis vier Tagen ab.

Das soll nie wieder passieren. Die Nato betreibt daher in der estnischen Hauptstadt Tallinn das Cooperative Cyber Defence Center, ein Abwehrzentrum gegen digitale Angriffe. Auf deren Arbeit allein aber will sich die Bundeswehr nicht verlassen. Sie baut mittlerweile eine eigene Abwehr auf – unter anderem in einer Kaserne am Rande von Rheinbach, einer Kleinstadt rund 15 Kilometer südwestlich von Bonn.

Von Unterholz überwuchert und mit Laub bedeckt, reihen sich im Rheinbacher Stadtwald Bombenkrater an Bombenkrater. Im Unterholz liegen noch immer die Fundamente der Munitionslager, denen im Zweiten Weltkrieg die Luftangriffe der Alliierten galten. Ein paar Schritte durchs Gehölz nur trennen die Spuren vergangenen Konflikte von dem Ort, an dem sich Soldaten auf die neue Art der Kriegsführung vorbereiten: Mehrfach abgeschottet von der Außenwelt, trainieren in der Tomburg-Kaserne Elektronikexperten der Gruppe Computernetzwerkoperationen den Einsatz von Computern und Software als Waffe – und ihren Schutz gegen elektronische Angriffe aus dem Netz.

Doch den Bundesbürgern hilft das im Ernstfall wenig: Die Hacker in Oliv sollen nur die Bundeswehr fit machen gegen die Bedrohung aus dem Netz. Für den Schutz der Zivilisten sind nicht sie zuständig, sondern Innenminister de Maizière.

Doch dessen Einfluss ist begrenzt: Viele ehemals staatliche Infrastrukturbetreiber nämlich sind heute im Besitz ausländischer Investoren. Der schwedische Energieversorger Vattenfall etwa verkaufte sein Stromnetz in Ostdeutschland im März an ein Investorenkonsortium. Reine Finanzinvestoren jedoch „haben ein eingeschränktes Bedürfnis an kostenintensiven Schutzmaßnahmen“, sagt Professor Alexander Huber, Sicherheitsexperte an der Beuth Hochschule für Technik in Berlin.

Oft fehlt zudem das Wissen. „Viele Verantwortliche in Unternehmen sind sich der Gefahr digitaler Angriffe nicht bewusst“, sagt Ex-BND-Chef Hanning. Die Bundesregierung versucht zwar, die Sicherheitslücken auf freiwilliger Basis durch Gesprächskreise und Empfehlungen zu schließen. Was dabei herauskommt, kann sich jeder denken: „Jeder kann machen, was er will, und es wird auch nicht überprüft, ob die Vorgaben umgesetzt werden“, moniert Sicherheitsexperte Huber.

Helfen könnte nach Ansicht von Janus-Chef Bühler ein Nationaler Sicherheitsrat, der alle mit dem Schutz vor Cyber-Angriffen beschäftigte Institutionen – Unternehmen, Regierungsstellen, Sicherheitsbehörden und Dienstleister – an einen Tisch holt.

NACHBARN RÜSTEN AUF

Andere Staaten gehen zielstrebiger vor: Sie haben den Cyberspace als militärisches Gefechtsfeld definiert und rüsten auf. Am entschiedensten marschieren die USA voran. Präsident Barack Obama ordnete den Aufbau einer neuen Spezialeinheit an und ernannte den Vier-Sterne-General Keith Alexander zum obersten Befehlshaber des neuen US Cyber Command. Die neue Elitetruppe umfasst 30 000 Netzkrieger, die ausschließlich im Web operieren sollen.

Der britische Verteidigungsminister Nick Harvey plant sogar, abschreckende Online-Erstschlagskapazitäten aufzu- »

Cyber-Attacken

Von Blockade bis Sabotage – die Überraschungsangriffe der Hacker gegen Regierungen und Militärs.

Juli 2001
Angriff auf das Weiße Haus

Der Computerwurm Code Red nutzt eine Lücke im Betriebssystem Windows aus und legt den Server, auf dem die Web-Seiten des Weißen Hauses laufen, mit einer Flut von Anfragen zeitweise lahm.

September 2007
Luftabwehr manipuliert

Die US Air Force manipuliert mit der Software Suter die Empfangsantennen der gegnerischen Luftabwehrsysteme im Irak und in Afghanistan. Auf diese Weise können Phantomziele eingespeist werden oder aber sichtbar gemacht werden, was der Gegner gerade auf seinem Radar sieht.

September 2007
Behörden blockiert

Erste Cyber-Attacke auf Bundesbehörden in Deutschland: Per digitalem Beschuss durch

ein sogenanntes Botnet aus 350 gekaperten und zusammengeschalteten Rechnern werden der Internet-Zugang und der E-Mail-Verkehr von zehn Bundesbehörden blockiert. Unter der Last des elektronischen Angriffs steigt der digitale Datenverkehr im Kommunikationsnetz der Bundesverwaltung für kurze Zeit um den Faktor 1000 an.

Dezember 2009
Drohne angezapft

Talibankämpfern im Irak gelingt es, den Datenstrom einer unbemannten Predator-Drohne (siehe rechts) zum Satelliten anzuzapfen. Die US Air Force bemerkt den Zwischenfall erst, als sie auf dem Laptop eines Schiiten Videoaufnahmen aus den Kameras der Drohne entdeckt.

April 2010
Verkehr umgeleitet

Im Auftrag chinesischer Regierungsstellen kapern Hacker 15 Prozent des weltweiten Internet-Verkehrs und leiten ihn für 18 Minuten nach China um. Darunter befinden sich riesige Datenpakete vom Pentagon, anderen amerikanischen Regierungs- und Militärstellen sowie vom US-Softwareriesen Microsoft und dem US-Computerbauer Dell.

September 2010
Kraftwerk sabotiert

Virenattacke auf das iranische Atomkraftwerk Bushehr (siehe unten). Der mit hohem Aufwand entwickelte Cyber-Schädling Stuxnet sabotiert die Steuerung von Industrieanlagen. Das Virus ist so raffiniert, dass es sogar ein bereits desinfiziertes System erneut befallen und danach unentdeckt bleiben kann.

© Handelsblatt GmbH. Alle Rechte vorbehalten. Zum Erwerb weitergehender Rechte wenden Sie sich bitte an nutzungsrechte@vhb.de.

» bauen. Künftig soll das britische Militär Kontrahenten mittels Cyber-Attacken erledigen können. Umgerechnet rund eine Milliarde Euro will Großbritannien in den nächsten Jahren für die Cyberwar-Vorbereitungen ausgeben.

Das reicht nicht aus, um Europa zu schützen: „Es besteht kein permanenter Dialog auf nationaler oder europäischer Ebene zwischen Regierungen, Wirtschaft und Militär“, heißt es in einem Positionspapier von Janus Consulting. Und auch auf EU-Ebene fand erst Anfang November die erste internationale Cyberwar-Übung der europäischen IT-Sicherheitsbehörde Enisa statt. Laut Beobachtern war es eher ein besseres Kennenlernen als ein hochgerüstetes IT-Treffen. Kein Wunder: In manchen EU-Staaten war nicht einmal festgelegt, welche Behörde bei Internet-Angriffen mit den übrigen EU-Partnern zusammenarbeitet.

Die Gefahr, glauben viele Sicherheitsexperten, kommt vor allem aus dem Osten. Der russische Geheimdienst FSB beispielsweise nutzt Hacker lieber für eigene Zwecke, anstatt sie zu bekämpfen. Nikita Kislizin weiß, welchen Schaden sie anrichten können. Er ist Chefredakteur einer russischen Fachzeitschrift für IT-Sicherheit und lernte als Student am Moskauer Institut für IT-Sicherheit das Handwerkszeug der Cyber-Krieger. „Selbst die Abschaltung eines Atomkraftwerks ist technisch kein Problem“, sagt er, „der Auftraggeber muss nur genug Geld lockermachen.“

Eine der gefährlichsten Waffen des FSB ist ein junger Mann, der sich Boris Iwanow nennt. Es braucht Fantasie, sich den leicht übergewichtigen Mittzwanziger als Cyber-Söldner vorzustellen, der Rechenzentren fremder Regierungen lahmlegt und hochbrisante Daten von fremden Geheimdiensten stiehlt.

Schutzlos ausgeliefert

Wie sich das Angebot von Deutschlands IT-Sicherheits-Know-how entwickelt

Sicherheitssparte	Angebot durch deutsche Unternehmen	
	heute	in 3 bis 5 Jahren
Netzwerksicherheit	gut	schlecht
Endgeräteabsicherung	durchschnittlich	schlecht
Web-Browser-Schutz	keine	keine
Anwendungs-/ Softwaretests	schlecht	schlecht
Hochsicherheitstechnik	sehr gut	gut
Datenübertragung/ -verschlüsselung	durchschnittlich	schlecht
Identitätssicherung/ -kontrolle	sehr gut	sehr gut

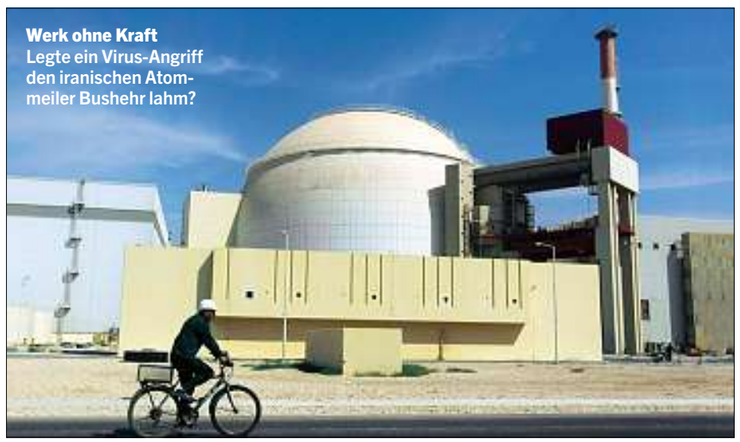
Quelle: Bundeswirtschaftsministerium

Doch genau das ist sein Job. Wer ihn bezahlt, ist Iwanow egal. „Die Klienten melden sich übers Internet“, sagt er. „Ein paar Wochen später liegt ein Umschlag mit Geld in meinem Briefkasten.“

Auch China wird zunehmend zur Gefahr in der Cyber-Welt. Westliche Geheimdienste machen das Pekinger Regime für Cyber-Angriffe auf Computernetzwerke in Indien, Taiwan, Deutschland und den USA verantwortlich: Fast täglich dringen Hacker mit oder ohne Regierungsauftrag in die Rechner westlicher Staaten ein, um Geheiminformationen auszuspähen und Hintertüren in die Computernetze einzubauen. IT-Sicherheitsberater schätzen die Zahl der chinesischen Cyber-Krieger inzwischen auf 50 000. Mindestens.

Erst im April kaperten die Chinesen 15 Prozent des weltweiten Internet-Verkehrs und leiteten die Bits und Bytes für 18 Minuten auf ihre Rechner um. Darunter riesige Datenpakete des Pentagons, der US-Regierung sowie von Microsoft und Dell.

Aber auch die USA ziehen inzwischen in den virtuellen Krieg. US-Militärs etwa legen mit ihrem Luftangriffssystem „Suter“ gezielt gegnerische Kommunikationssysteme lahm. Über eine Schadsoftware können die Amerikaner beispielsweise irreführende Daten als Phantomziele in feindliche Radarsysteme einspielen oder verfolgen, was der Gegner momentan auf seinem Radarschirm sieht. So kann die US-Luftwaffe kontrollieren, ob ihre Tarnkappen-Bomber „Stealth“ tatsächlich unentdeckt bleiben.



Werk ohne Kraft
Legte ein Virus-Angriff den iranischen Atommeiler Bushehr lahm?

INTERNATIONAL ABGESCHLAGEN

Deutschland dagegen verliert technologisch den Anschluss (siehe Tabelle). Das Innovationstempo im Internet bestimmen vor allem US-Web-Riesen wie Google, Microsoft, Apple und Cisco. Gegen die übermächtige Konkurrenz sind deutsche IT-Sicherheitsspezialisten wie Secunet oder Genua nur noch Nischenanbieter. „Deutsche Sicherheitsunternehmen sind bereits heute international abgeschlagen“, sagt Sicherheitsexperte Huber. „Unternehmen mit kritischen Infrastrukturen sind zunehmend auf ausländische Produkte angewiesen.“

Lediglich im Hochsicherheitsbereich konnten deutsche Firmen ihre Führungsrolle mit staatlicher Hilfe verteidigen. Denn beim Versand von streng vertraulichen Dokumenten vertraut die Bundesregierung nur deutschen Verschlüsselungssystemen, in die ausländische Geheimdienste keine Hintertüren eingebaut haben. So werden etwa die Auslandseinsätze der Bundeswehr über das Führungskräfteinformationssystem der Streitkräfte mit Secunet-Technik verschlüsselt.

Ganz vorsichtige Unternehmen indes wählen einen noch radikaleren Weg und koppeln Teile ihrer IT inzwischen wieder vom Internet ab. Ob sensible Maschinensteuerung oder vertraulicher Austausch zwischen Niederlassungen – wenn es wirklich wichtig wird, läuft die Kommunikation über ein separates Netz ohne Zugang zum öffentlichen Internet.

Die ursprüngliche Idee allerdings, alle und alles kostengünstig und komfortabel via Internet miteinander verbinden zu können, verkehrt sich damit – aus Sicherheitsgründen – plötzlich ins Gegenteil. ■

thomas.kuhn@wiwo.de, juergen.berke@wiwo.de, florian willershausen | moskau, matthias kamp | Peking

FOTOS: IMAGO/ UPI PHOTO, WAZ FOTOPOOL /MATTHIAS GRABEN ; ILLUSTRATION: CHRISTOPH NIEMANN

»Neue Bedrohung«

INTERVIEW | August Hanning Der Ex-Präsident des Bundesnachrichtendienstes über Schwierigkeiten beim Schutz vor Cyber-Angriffen.

Bei Sicherheitsexperten gilt das Internet als fünftes militärisches Gefechtsfeld neben Boden, Luft, Wasser und Weltraum.

Dennoch seien die westlichen Staaten nur unzulänglich gegen digitale Angriffe geschützt. Wie gefährdet ist Deutschland?

Hanning: Sehr. Die Entwicklung der vergangenen 20 Jahren hat unsere Gesellschaft technisch revolutioniert. Vernetzte Computer prägen den Alltag. Sie sind existenziell für das Funktionieren unserer Gesellschaft. Das hat enorme Auswirkungen auf die Szenarien der Kriegführung. Auch das Militär selbst ist computerisiert und damit ein potenzielles Ziel von IT-Attacken.

Sind digitale Angriffe wie etwa der auf die IT der Bundesverwaltung Vorboten der neuen Bedrohung?

Hanning: Ja. Und die Bedrohung wird zunehmen. Ich glaube, dass wir unsere Regierungsnetze wirksam schützen. Doch im Bereich der Wirtschaft, speziell bei kleineren und mittleren Unternehmen, haben wir noch erhebliche Defizite. Viele Verantwortliche dort sind sich der Gefahr digitaler Angriffe nicht bewusst.

Und die privaten Infrastrukturen, ob Energieversorgung, Telekommunikation, Wasserversorgung oder Gesundheitswesen: Kann der Staat die überhaupt sichern?

Hanning: Effizienter Schutz ist weniger eine Frage rechtlicher Kompetenzen als einer vernünftigen Kooperation zwischen Staat und Wirtschaft. Die Bundesregierung hat zum Schutz dieser Infrastrukturen mit der Wirtschaft einen „Leitfaden Risiko- und Krisenmanagement“ entwickelt, um den Verantwortlichen im Ernstfall Hilfen zu geben. Trotz aller Maßnahmen von Staat und Privaten nach dem 11. September 2001, wir bleiben verwundbar. Man kann ein Industrieland wie die Bundesrepublik nicht 100-prozentig schützen. Sie können Angriffe nur erschweren und die Auswirkungen begrenzen.

Der Stuxnet-Virus, der das iranische Atomprogramm sabotieren sollte, gilt als Prototyp künftiger High-Tech-Angriffe.

Hanning: Das sehe ich auch so. Ein so professionell erstelltes Virus ist eine neue Dimension der Bedrohung. Damit wurde offenkundig versucht, in sensible Systeme von Industrieanlagen einzudringen.

Wären im Kalten Krieg Panzer über Grenzen gerollt, hätte das Krieg bedeutet. Wo aber endet im digitalen Zeitalter Computerkriminalität, und wo beginnt Cyberwar?

Hanning: Ich glaube, hier versagen die klassischen Kategorien für die Definition eines Verteidigungsfalles. Natürlich drängt sich in Fällen wie Estland oder Georgien, wo Angriffe aus einem bestimmten Land festgestellt wurden, der Eindruck gezielter Aktionen auf. Aber selbst da ist der Nachweis der Verantwortung bestimmter Staaten sehr schwierig.

Wer könnte Interesse an einem elektronischen Angriff auf Deutschland haben?

Hanning: Bisher war für uns weniger ein IT-Angriff von außen ein Problem, sondern die Nutzung des Internets durch Terroristen und die organisierte Kriminalität. So haben die sogenannten Sauerland-Attentäter das Internet intensiv genutzt. Auch islamistische Dschihadisten verbreiten darüber terroristisches Know-how.

Die USA haben eine eigene Militäreinheit geschaffen, das US Cyber Command, die das Land gegen digitale Angriffe schützen soll. In Deutschland gibt es bisher nichts Vergleichbares. Ist das nicht leichtsinnig?

Hanning: Meines Erachtens beschäftigt sich neben den deutschen Sicherheitsbehörden auch die Bundeswehr mit dem Schutz ihrer Einrichtungen. Es gibt eine enge Zusammenarbeit in der Nato. Außerdem hat auch die Bundeswehr Kräfte in das Cyber-Verteidigungszentrum der Nato in Estland entsandt.

Lassen sich denn bei elektronischen Angriffen die Aufgaben von Bundeswehr und Polizei noch sinnvoll abgrenzen?

Hanning: Die virtuelle Welt hat keine nationalen Grenzen. Damit verliert die Trennung von innerer und äußerer Sicherheit ihre Bedeutung. Nur glaube ich nicht, dass man dieser Bedrohung mit klassischen militärischen Mitteln wirksam begegnen kann. Deswegen ist es nicht zielführend, an dieser Stelle den Einsatz der Bundeswehr im Inneren zu diskutieren.

Laut Koalitionsvertrag sollen die Kompetenzen für die Abwehr von IT-Angriffen beim Bundesinnenministerium gebündelt werden. Ist das die richtige Stelle?

Hanning: Der Schutz der Infrastruktur ist zunächst eine zivile Aufgabe, die zu Recht beim Innenministerium liegt. Natürlich kann man streiten, ob ausreichend Ressourcen zur Verfügung stehen. Sicherheitsbehörden müssen sich immer neuen Herausforderungen stellen und ihre Schwerpunkte an die Bedrohungslagen anpassen. Deshalb erwarte ich, dass künftig der Abwehr von IT-Angriffen größere Aufmerksamkeit gewidmet wird. »

thomas.kuhn@wiwo.de

STAATSSCHÜTZER

Hanning, 64, war von 1998 bis 2005 Chef des deutschen Auslandsgeheimdienstes Bundesnachrichtendienst. Anschließend wurde er Staatssekretär unter Ex-Bundesinnenminister Wolfgang Schäuble. Schäubles Nachfolger, Thomas de Maizière, versetzte den Juristen nach der Bundestagswahl 2009 in den Ruhestand.

© Handelsblatt GmbH. Alle Rechte vorbehalten. Zum Erwerb weitergehender Rechte wenden Sie sich bitte an nutzungsrechte@vhb.de.