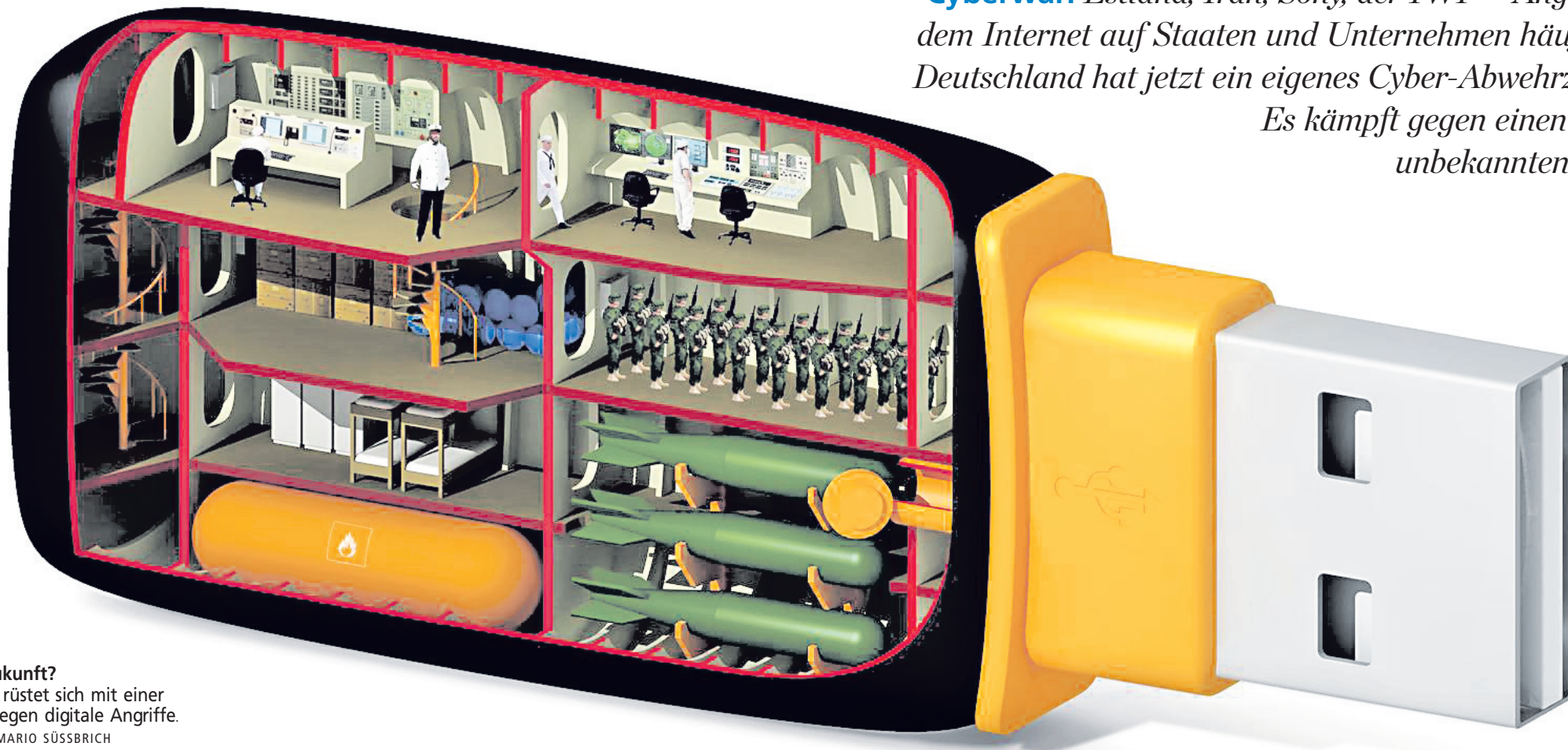


Die virtuelle Gefahr ist real

Cyberwar: Estland, Iran, Sony, der IWF – Angriffe aus dem Internet auf Staaten und Unternehmen häufen sich. Deutschland hat jetzt ein eigenes Cyber-Abwehrzentrum. Es kämpft gegen einen starken, unbekanntem Gegner.



Krieg der Zukunft?
Deutschland rüstet sich mit einer Cyber-Unit gegen digitale Angriffe.
ILLUSTRATION: MARIO SÜSSBRICH

Von unserem Redaktionsmitglied
BENJAMIN STAHL

Satelliten geraten außer Kontrolle und verschwinden im All. Flugzeuge stürzen vom Himmel. Aus Chemiefabriken entweichen tödliche Chlordämpfe. In Raffinerien brechen Großfeuer aus. Erdgaspipelines explodieren. Atomkraftwerke schalten sich automatisch ab. Die Stromversorgung bricht zusammen. Banken können kein Bargeld mehr auszahlen. Die Verkehrsinfrastruktur kommt zum Erliegen. Lebensmittellieferungen bleiben aus. Es kommt zu Plünderungen. Der Beginn der Apokalypse? Nein. Das Unheil kam durch die Glasfaserkabel, die die Erde umspannen.

So stellt sich Richard Clarke, ehemaliger Sicherheitsberater von insgesamt vier US-Präsidenten, in seinem Buch „World Wide War“ einen groß angelegten Cyber-Angriff – eine elektronische Attacke aus dem Internet auf die IT-Systeme von Behörden und Unternehmen – vor. Auch wenn es nach Science-Fiction klingt: Spätestens seitdem „Stuxnet“ 2010 eine iranische Urananreicherungsanlage angegriffen hat, ist das Thema im Bewusstsein vieler Staaten angekommen. Der Computer-

wurm hatte rund 1000 Zentrifugen der Anlage zerstört, indem er die Frequenzen, mit denen sie rotieren, manipulierte.

Bereits 2007 wurde Estland Opfer eines Cyber-Angriffs. Hacker legten damals unter anderem Websites von Regierung und Medien lahm. Auch Handynetzbetreiber und das größte Finanzinstitut des Landes waren betroffen. 2011 machten unter anderem Angriffe auf Sony und den Internationalen Währungsfonds (IWF) Schlagzeilen.

Seit Jahren sieht sich auch Deutschland zunehmend elektronischen Angriffen auf IT-Systeme von Behörden und Wirtschaftsunternehmen ausgesetzt: Im Jahr 2010 zählte das Bundesamt für Verfassungsschutz (BfV) nach eigenen Angaben allein 2100 Angriffe auf Rechner von Bundesbehörden – im Vergleich zu 2009 ein Anstieg um 40 Prozent.

Die Bundesregierung reagierte: Im April 2011 nahm das Nationale Cyber-Abwehrzentrum seine Arbeit auf. Zehn Experten – Mitarbeiter des Bundesamts für Sicherheit in der Informationstechnik (BSI), des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe und des BfV – sollen künftig von Bonn aus im Fall eines Cyber-Angriffs schnell die Lage bewerten und Behörden sowie Firmen Handlungsempfehlungen geben.

Wo die Hacker sitzen, die hinter den Attacken aus dem Netz stecken, und in wessen Auftrag sie handeln, bleibt häufig ungeklärt. Meist gelingt es den Angreifern, ihre Spuren im Wirrwarr der Datenautobahnen zu verwischen. Art, Herkunft und Ausrichtung der Angriffe sprächen jedoch häufig dafür, „dass ausländische Nachrichtendienste dahinterstecken“, sagte jüngst BfV-Präsident Heinz Fromm in einem Interview. „Nicht selten“, so Fromm weiter, „sei dabei eine regionale Zuordnung möglich, wobei China und auch Russland besonders ins Auge fallen.“

„Ein Land lahmzulegen ist möglich.“

Marco Di Filippo,
Internet-Sicherheitsexperte

Experten unterscheiden bei den Angriffen zwischen politischen und ökonomischen Motiven (siehe Interview). So teilt das BfV auf Anfrage dieser Zeitung mit, dass es meist Ziel sei, strategische Informationen aus Politik und Wirtschaft zu bekommen: Wie ist die Haltung der Bundesregierung zum Thema X? In welchem Bereich forscht das Unter-

nehmen Y?

Natürlich gibt es aber auch Hacker, die nicht für einen Geheimdienst arbeiten. „Sie verabreden sich in Internet-Foren zu einem Angriff, beispielsweise auf ein bestimmtes Unternehmen“, erklärt der Internet-Sicherheitsexperte Marco Di Filippo. „Die einen wollen sich profilieren, die anderen wollen damit Geld verdienen.“ So suchten sogenannte Cracker zum Beispiel gezielt nach Sicherheitslücken. Landen sie einen Treffer, verkauften sie ihr Wissen darüber. Entweder an den Hersteller des entsprechenden Programms – oder an den Meistbietenden...

Laut dem Experten kann das Finden einer Sicherheitslücke bis zu 100 000 US-Dollar einbringen. Hacker füllen sich zudem die Taschen durch das Plündern von Online-Konten oder durch sogenanntes Auftrags-Hacking im Bereich der Wirtschaftsspionage. Gute Hacker könnten so auf ein Monatseinkommen von etwa 15 000 US-Dollar kommen. Ein lukratives Geschäft, das laut BfV-Präsident Fromm allein durch den Zweig der Wirtschaftsspionage jährlich einen zweistelligen Milliardenbetrag an Schaden anrichtet.

Doch die Angriffe stellen nicht nur eine Bedrohung im wirtschaftlichen Sinne dar, warnt Di Filippo. „Auch die Terrorgefahr ist ein The-

ma“, sagt er. Beispielsweise könnte die Manipulation des GPS-Signals das komplette Verkehrsnetz zum Erliegen bringen. „Von der Straßenbahn bis hin zum Flugzeug“, sagt Di Filippo. „Ein Land lahmzulegen ist möglich“, glaubt er. Und im Falle von Deutschland verhältnismäßig günstig. „Das gesamte deutsche Stromnetz und das Internet kann man mit verhältnismäßig kleinem Budget zum Erliegen bringen. Wer das tun will, kann das Geld dafür leicht aufbringen.“

Ob die Cyber-Verteidiger in Bonn eine solche Attacke tatsächlich abwehren könnten, ist unter Experten umstritten. „Die Schaffung einer solchen Einrichtung ist auf jedem Fall positiv zu bewerten, jedoch mit zehn Mitarbeitern zu schwach besetzt“, glaubt Di Filippo. Sicher dagegen scheint: Die Folgen einer erfolgreichen Attacke im großen Stil würden stark an Clarks Endzeitszenario erinnern. „An den jüngsten Naturkatastrophen sieht man, wie schnell eine Infrastruktur oder ein Stromnetz zusammenbrechen kann und welche Folgen das hat“, sagt Di Filippo.

ONLINE-TIPP

Hacker, Würmer, Cyberwar – unser Multimedialexikon erklärt viele Begriffe rund ums Internet: www.mainpost.de/multimedia

„Geheimdienste spionieren auch Unternehmen aus“

Gemündener IT-Experte: Wie Wirtschaft und Politik im Netz attackiert werden

Das Gespräch führte
BENJAMIN STAHL

Profi-Hacker, politische und wirtschaftliche Spionage, manipulierte Hardware. Die Gefahren im Cyber-Raum, die der Gemündener IT-Experte Thomas R. Köhler aufzählt, sind vielfältig. Dass das Cyber-Abwehrzentrum der Bundesregierung den Bedrohungen Herr werden kann, bezweifelt er.

FRAGE: Was verstehen Sie als Experte unter dem Begriff „Cyberwar“?

THOMAS R. KÖHLER: Zunächst einmal kann man in meinen Augen nicht von einem „Krieg“ sprechen. Bei dem so bezeichneten Phänomen handelt es sich meist um Spionageversuche oder um Sabotageaktionen, wie bei dem Computerwurm „Stuxnet“. Dem Begriff „Cyberwar“ stehe ich daher kritisch gegenüber. Schließlich kommt ein Stromausfall, ausgelöst durch eine Cyber-Attacke, keinem Bombenangriff gleich.

Dennoch können solche Attacken großen Schaden anrichten.

KÖHLER: Ja. Je nachdem wer die Angreifer sind und welches Ziel sie verfolgen, können die Folgen entweder auf politischer oder auf wirtschaftlicher Ebene verheerend sein.

Erklären Sie das bitte näher.

KÖHLER: Man kann davon ausgehen, dass in vielen Fällen Auslandsgeheimdienste hinter den Attacken stecken. Handelt es sich dabei um politisch motivierte Provokationen, können sie im schlimmsten Fall auch Auslöser von Konflikten auf diplomatischer Ebene sein – wie wenn ein südkoreanisches Schiff nordkoreanische Hoheitsgewässer befährt. Es gibt Hinweise, dass Hacker im Auftrag der chinesischen Regierung Angriffe auf die IT-Systeme der Bundesregierung starteten. Wenn so etwas passiert, will meist ein Land herausfinden, was ein anderes zu einer bestimmten Sache plant. Die Geheimdienste spionieren aber nicht nur aus politischem Interesse.

Sondern?

KÖHLER: Sie spionieren auch Unternehmen aus und stellen das so gewonnene Know-how dann einheimischen Firmen zur Verfügung. Man spricht dabei von Wirtschaftsspionage. Das ist ein großes Tabuthema, es findet aber statt.

Wirtschaftsunternehmen, Geheimdienste – haben wir ein falsches Bild von Hackern, die uns in Filmen ja immer als fettleibige Computerfreaks verkauft werden, die aus Spaß Passwörter knacken oder Viren programmieren?

KÖHLER: Früher waren das wirklich Leute, die sich aus Spaß an der Freude intellektuell daran gemessen haben, wer sich wo einhacken kann. Die Hackerszene hat sich in den letzten zehn Jahren aber dramatisch professionalisiert. Und heute kann man damit viel Geld verdienen, vor allem im Bereich der Wirtschafts- und Industriespionage: Unternehmen A will etwas über Unternehmen B wissen – wer's rausbekommt kassiert.

Also ist die Einrichtung des Cyber-Abwehrzentrums der Regierung eine sinnvolle Maßnahme?

KÖHLER: Das schon, zumindest als eine Art Koordinationsstelle. Es kann helfen, einen Überblick darüber zu bekommen, was im Internet alles passiert. Ich bezweifle allerdings, dass es effektiv arbeiten kann, weil man mehrere Hundert Fachleute beschäftigen müsste, um der Flut von Bedrohungen auch nur annähernd Herr zu werden. Und so viele Leute hat das Zentrum nicht. Ich glaube daher, es wird dort mehr überwacht, als wirklich abgewehrt werden kann.

Sind Viren, Würmer und andere Schadprogramme die einzige Gefahr für die Datensicherheit, die im Internet lauert?

KÖHLER: Leider geht man in Fachkreisen inzwischen davon aus, dass die größte Gefahr

schon nicht mehr von Viren und Co. ausgeht, sondern von manipulierter Hardware: In vielen Netzwerkkomponenten ist die Spionagevorrichtung sozusagen schon eingebaut. So steht zum Beispiel ein großes chinesisches Unternehmen, das solche Netzwerkkomponenten herstellt und zum Großteil der chinesischen Armee gehören soll, unter Spionageverdacht. Deren Komponenten sind in zahlreichen Unternehmen und Telekommunikationsanbietern auch hierzulande im Einsatz. Und erstaunlicherweise hat ein kleinerer japanischer Hersteller gerade zugegeben, dass er in diesem Sinne „fehlerhafte Hardware“ produziert und geliefert hat.

Thomas R. Köhler

Der 42-jährige Gemündener gilt als einer der führenden IT-Experten im deutschsprachigen Raum. Köhler leitet die Strategieberatung CE21 und hat zahlreiche Bücher zu Internet- und Technologiethemen verfasst. Sein aktuelles Werk „Die Internetfalle“ beschäftigt sich unter anderem mit den Chancen und Risiken der Onlinewelt.



FOTO: JOACHIM WENDT

Wie funktioniert die „mitgelieferte Spionage“?

KÖHLER: Die manipulierten Geräte sind mit sogenannten „Backdoors“ (Hintertüren, d. Red.) ausgestattet, die gezielt durch eine bestimmte Befehlskette – die das Gerät über das Internet erreicht – geöffnet werden können. Durch die geöffneten „Backdoors“ sendet das Gerät dann Daten. In den USA gibt es für Anbieter sogar eine Verpflichtung, derartige „Backdoors“ einzubauen. Offiziell für Regierungsstellen zur Verbrechensaufklärung und Terrorbekämpfung. Von wem und zu welchem Zweck das aber letztendlich wirklich genutzt wird, kann man nicht überprüfen.

Was wäre für Sie der „Cyber“-Super-GAU?

KÖHLER: Ein Angriff auf die Trinkwasser- oder die Energieversorgung. Hacker könnten in einer konzertierten Aktion versuchen, Steuerungs- und Regleinrichtungen so zu beeinflussen, dass Kraftwerke runterfahren müssen. Denken Sie an ausbrechende Chaos, wenn große Städte unter Umständen tagelang ohne Strom wären. Wie groß das Risiko für einen derartigen Vorfall aktuell tatsächlich ist, ist aber auch unter Fachleuten umstritten.