NURPHOTO / ZUMA PRESS / ACTION PRESS

Simulation eines digitalen Angriffs bei Nato-Übung: Massive Aufrüstung der Bundeswehr angepeilt

Hacker mit Dienstausweis

Cyberabwehr Deutschland ist immer öfter Opfer von Attacken. Jetzt wollen die Sicherheitskräfte offensiv zurückschlagen – Politiker und Experten warnen.

Die Hacker fielen bei der Kontrolle am Flughafen von Atlantic City nicht auf. Sie hatten keine ungewöhnlichen Geräte im Handgepäck und wirkten auf die Sicherheitsbeamten ganz normal.

Das Ziel ihrer Attacke parkte draußen auf dem Rollfeld: eine Passagiermaschine vom Typ Boeing 757, die 200 bis 300 Menschen transportieren kann. Von diesem Modell sind Hunderte im Einsatz. Auch US-Präsident Donald Trump besitzt ein solches Flugzeug, mit Goldarmaturen und Schlafzimmern.

Nur wenig Zeit brauchten die Hacker, dann waren sie drin, mitten im elektronischen Herz der Maschine. Offenbar nutzten sie dafür keine teure Spezialtechnik, sondern unter anderem ein Gerät, das jeder für ein paar Dollar im Internet bestellen kann. Noch beunruhigender: Die Angreifer programmierten ihre Attacke im Terminal, sie brauchten nicht einmal Zutritt zur Maschine. Sie hätten die Boeing wohl vom Boden aus fernlenken können.

Als vor rund zwei Jahren ein Hacker behauptete, er habe sich im Flugzeug von seinem Sitz aus über das Entertainmentsystem in die Steuerungssysteme gehackt und in einem Fall sogar die Flugbewegungen manipuliert, hagelte es Dementis, von Boeing wie von Flugexperten. Die Systeme seien streng abgeschirmt, hieß es, ein erfolgreicher Angriff sei undenkbar.

Diesmal allerdings waren Dementis kaum möglich: Der Staat selbst hatte, wie diesen Monat bekannt wurde, das Flugzeug in einem kontrollierten Experiment gehackt. Als die Staatshacker des US-Heimatschutzministeriums kommerziellen Piloten ihren erfolgreichen Angriff vorstellten, waren die entsetzt: Von der Schwachstelle hatte keiner etwas gewusst.

Gehackte Flugzeuge, die in Atomkraftwerke gesteuert werden; U-Bahnen, die ferngelenkt aufeinander zurasen; lahmgelegte Strom- oder Wasserversorger in Metropolen: Es sind diese Horrorbilder, die gemalt werden, wenn es um die Verletzbarkeit moderner Gesellschaften geht – und um die Frage, wie diese Gesellschaften verhindern können, dass solche Bilder Wirklichkeit werden.

Glaubt man den Experten in den Sicherheitsbehörden, dann reichen die Maßnahmen zur Cyberabwehr nicht aus: Statt sich zu verteidigen, müsse der Staat in Einzelfällen selbst zum Angreifer werden. Der sogenannte Hackback, also das staatliche Zurückhacken, ist rechtlich allerdings bedenklich und politisch umstritten. Denn die Zerstörung eines fremden Servers ist

nichts anderes als ein Angriffsmanöver in einem virtuellen Krieg. Soll in einem solchen Krieg der deutsche Staat mehr dürfen als nur abwehren?

Der Streit um die staatlichen Befugnisse wird die nächste Regierung beschäftigen. In den gescheiterten Sondierungsgesprächen von Union, Grünen und FDP gab es zaghafte Annäherungen. Man sei sich von Grün bis Schwarz einig gewesen, dass man sich dem „Mega-Problem“ dringend widmen müsse, heißt es aus Verhandlungskreisen. Die staatliche Abwehr von Cyberattacken müsse ausgebaut und konzentriert werden. Ob Deutschland auch virtuelle Angriffe starten soll, wurde allerdings noch nicht geklärt.

Und nun? „Wir müssen das Thema Cyberabwehr unbedingt angehen, egal, in welcher Regierungskonstellation“, sagt Stephan Mayer, der innenpolitische Sprecher der Unionsfraktion. „Und dabei müssen wir dringend auch die Zuständigkeiten klären.“ Bisher sei bei militärischen Attacken die Bundeswehr zuständig, bei Angriffen durch Kriminelle das Bundeskriminalamt. „Was aber, wenn der Hintergrund unklar ist?“, fragt Mayer.

Die Gefahren sind real, wie der Fall der gehackten Boeing zeigt: Bei vielen, zum Teil jahrzehntealten Technologien spielte alles Mögliche eine Rolle, nur nicht die Sicherheit gegen virtuelle Angriffe von heute. Sie rückwirkend dagegen „zu härten“, wie es im Expertenjargon heißt, ist teuer und langwierig. Wie der IT-Experte Sandro Gaycken von der Berliner Hochschule ESMT in dieser Woche auf der Digital-Society-Konferenz sagte, müsste man die gesamte 757-Flotte ein Jahr lang stilllegen, um sie nachzurüsten.

Hacker bedrohen nicht nur Rechner und Maschinen, sondern auch den eigenen Körper, wie in diesem Jahr mehr als 400 000 Träger eines Herzschrittmachers erfahren haben: Der Hersteller St. Jude Medical aus den USA musste sie zum „Firmwareupdate“ bitten, nachdem die amerikanische Aufsichtsbehörde FDA in den Geräten kritische Schwachstellen ausgemacht hatte. So hätten Hacker die Batterien entladen und sogar den Herzschlag der Patienten verändern können. Der damalige US-Vizepräsident Dick Cheney hatte bei seinem Schrittmacher schon im Jahr 2007 Schnittstellen für drahtlose Zugriffe deaktivieren lassen, aus Sorge vor einem Cyberattentat.

Auch in Deutschland gab es beängstigende Fälle. 2014 wurde bekannt, dass Hacker den Hochofen eines Stahlwerks massiv beschädigten. Im August 2016 erhielt das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Hinweis: Durch eine Schwachstelle könnten Baustellenampeln über das Internet manipuliert werden. Der Fehler wurde rechtzeitig behoben. Im selben Jahr legte ein britischer Hacker über eine Million Telekom-Router lahm. Selbst der Bundestag wurde schon überfallen: 2015 knackte ein den russischen Geheimdiensten nahestehendes Hackerkollektiv mehrere Abgeordnetenrechner. Bislang wurden die gestohlenen Daten nicht veröffentlicht

Wie es um die virtuelle Gefahrenlage in Deutschland steht, erfährt man von einem Mann mit randloser Brille. Arne Schönbohm ist der Präsident des BSI und stellt einmal im Jahr den Lagebericht seiner Behörde vor.

In diesem Jahr fiel die Bilanz gemischt aus. Von Juli 2016 bis Juni 2017 war die Zahl der Angriffe gegen Regierungsnetze im Vergleich zum Vorjahreszeitraum um

Die gezählten Schwachstellen bei industriellen Großanlagen sind rasant gestiegen.

18 Prozent gestiegen. Im Monat zählte die Behörde durchschnittlich 52 000 E-Mails mit angehängter Schadsoftware. Seit Anfang des Jahres ging die Zahl der Angriffe aber wieder zurück. Vor allem sogenannte Ransomware verschickten die Hacker, eine Schadsoftware, die Daten auf den Rechnern der Opfer verschlüsselt und angeblich gegen Lösegeld freigibt. 2017 legten Angriffskampagnen mit den Namen „Wannacry“ und „Petya“ Firmen, Behörden und Krankenhäuser lahm. Anzeigetafeln der Deutschen Bahn funktionierten nicht mehr.

Ernst zu nehmende Angriffe gegen die sogenannten kritischen Infrastrukturen im Energie-, Gesundheits- oder Transportsektor gab es zwar keine. 34-mal aber meldeten Unternehmen solche Versuche ans BSI. Ursache waren meist menschliche Fehler oder Hardwaredefekte. Die gezählten Schwachstellen bei industriellen Großanlagen sind in den vergangenen Monaten allerdings rasant gestiegen, auf 110 in der ersten Hälfte dieses Jahres. Die Bedrohung existiert, die Frage ist, wer sie abwehren und bekämpfen soll.

Wenn es um offensive Angriffe geht, bringt sich die Bundeswehr gern ins Spiel. Schon bald nach Amtsantritt Ende 2013 hat Ursula von der Leyen (CDU) das Thema Cyber besetzt, über fast nichts redet die Ministerin so gern, am liebsten vor internationalem Publikum auf großen Konferenzen.

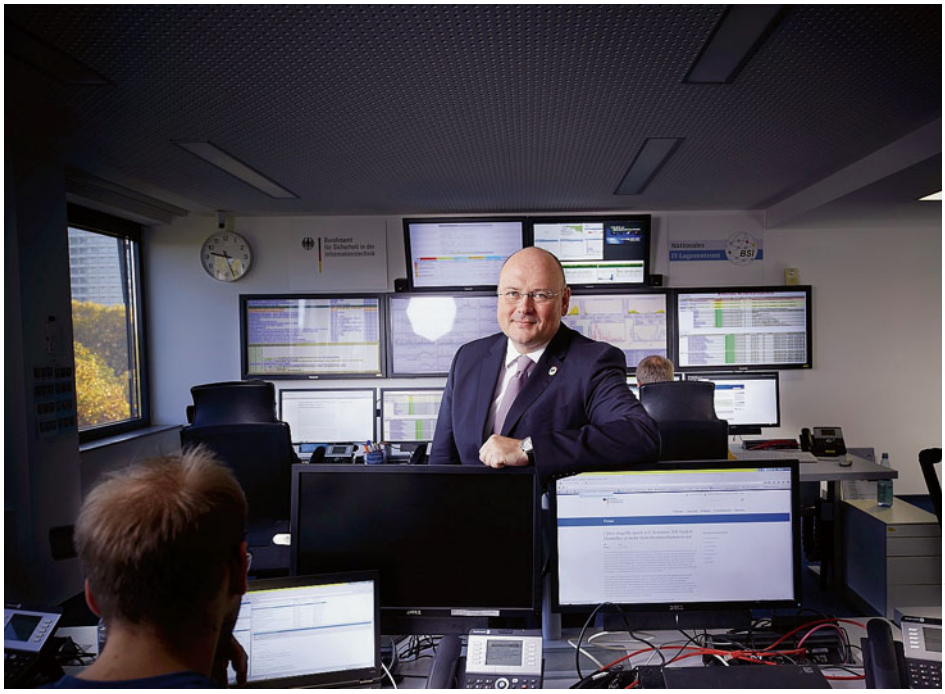
Von der Leyen erkannte, dass Cyber nicht nur modern ist, sondern auch ein Feld, auf dem sie sich in der deutschen Sicherheitsarchitektur einen Namen machen kann. Im April 2015 billigte sie eine geheime Strategie, die eine massive Aufrüstung der Bundeswehr anpeilt. In dem Papier fordern die Militärs offensive Cyberfähigkeiten. Sie seien als „Wirkmittel“ für die Truppe genauso nötig wie Bomben oder Gewehre. Mit dem Papier strebt die Bundeswehr erkennbar eine Führungsrolle bei der „gesamtstaatlichen Sicherheitsvorsorge“ im Cyberraum an.

Bisher aber ist die Abteilung Attacke in der Bundeswehr noch recht klein. Von rund 14 000 Soldaten, die von der Leyen in ihr Cyberkommando verschob, sind nur rund 80 echte Hacker. Sie sitzen hinter hohen Mauern in der Tomburg-Kaserne am Rand der Eifel. So ziemlich alles an der Einheit „Computer Netzwerk Operationen“ (CNO) wird als geheim eingestuft.

Derzeit, so die offizielle Version, agieren die Hacker in Uniform noch unter Laborbedingungen, spielen Cyberattacken und Hackbacks nur in der Simulation mit Rechnern durch, die nicht online sind. In der Truppe aber raunt man, dass man in der

OLIVER DIETZE / DPA

Behördenchefs Münch, Maaßen, Minister de Maizière: Zuständigkeiten klären



THOMAS RABSCH / LAIF

BSI-Präsident Schönbohm im IT-Lagezentrum: Beängstigende Fälle

echten Welt sicherlich schlagkräftig sei, wenn der Befehl nur endlich käme.

Wie schwierig ein Einsatz der Bundeswehr als Cyberarmee ist, zeigte sich bei der bisher einzigen scharfen Mission. Im Herbst 2015 hatte der Krisenstab des Außenamts um Hilfe in einem heiklen Entführungsfall gebeten. Da man zwar mit den Kidnappern um Lösegeld verhandelte, ihnen aber nicht vertraute, wandte man sich an die Bundeswehr. Dort war man zunächst skeptisch: Rechtlich ist das Penetrieren fremder Netze ohne Mandat ein Tabu.

Am Ende nahm sich ein General ein Herz und stellte auf eigene Faust fest, der Schutz der entführten Entwicklungshelferin Käthe B. sei vom Afghanistan-Mandat der Bundeswehr gedeckt. Die CNO-Einheit fand eine Schwachstelle im System des afghanischen Mobilfunkbetreibers und konnte die Geodaten der Kidnapper-Telefone auslesen. Live verfolgte man nun mit, wie die Entführer ihre Geisel wie verabredet zu einem Treffpunkt brachten, dort warteten Elitesoldaten mit einer Sporttasche voller Dollarnoten auf sie. Der Vorgang wird bis heute nur in geheimen Sitzungen thematisiert.

Die Militärs drängen immer wieder auf eine Aufrüstung ihrer Cyberfähigkeiten. So verfolgten die Geheimdienste bei der Militärübung „Zapad“ live mit, wie die Russen dort die technische Störung aller Kommunikation, einschließlich der Militärnetze, testeten. Genau dafür müsse man sich wappnen, heißt es in der Truppe. In den Sondierungsgesprächen drängten die Grünen darauf, dass die Cyberabwehr nicht gänzlich militarisiert werde. Auch in der Bundesregierung sieht man Grenzen: Schließlich dürfe die Truppe nur in Aus-

„Erhebliche völkerrechtliche Probleme, da der Gegner meist im Ausland sitzt.“

nahmen im Inneren tätig sein. Wolle man die Cybermacht der Soldaten ausweiten, sei wohl eine Grundgesetzänderung nötig.

Der Bundessicherheitsrat gab Gutachten in Auftrag, um die Optionen auszuloten. Sie sind noch nicht fertig, aber erste Ergebnisse wurden kürzlich bekannt. Demnach setzt man im Bundesinnenministerium auf fünf Stufen einer künftigen Cyberstrategie. Erstens: Prävention, zweitens: das Umleiten von Daten eines Angreifers, wenn man ihn rechtzeitig erkennt, drittens: das Aufklären des Angriffs. All das soll ohne Gesetzesänderungen möglich sein.

Heikel wird es bei Stufe vier und fünf: dem Löschen der gestohlenen Daten auf dem fremden Server und am Ende dessen Zerstörung. Dies müsse in den Gesetzen derjenigen Behörden geändert werden, die dafür zuständig sind – zum Beispiel im Gesetz über den Bundesnachrichtendienst (BND). Allerdings gibt es in der Regierung Bedenken, dem Geheimdienst eine derartige operative Macht zu überantworten.

Sollte die Polizei die Aufgaben übertragen bekommen, müsste das in den Polizeigesetzen der Länder festgeschrieben werden. Mehrere Bundesländer hätten aber signalisiert, heißt es aus der Bundesregierung, dass sie die Kompetenz der Cyberabwehr lieber beim Bund sähen, also beim Bundeskriminalamt (BKA) unter dessen Präsidenten Holger Münch. Dafür aber wäre vermutlich auch eine Grundgesetzänderung nötig.

Staatliches Hacken ist schon lange Thema in den Behörden, wie vertrauliche Papiere zeigen, die dem SPIEGEL vorliegen. Bereits 2004 hatte das BSI ein „Gutachten zur rechtlichen Bewertung“ von Hackbacks erstellt, 2008 eine Analyse zur „aktiven Netzverteidigung“. Dass erst jetzt das Thema die politische Öffentlichkeit erreicht, liegt an den spektakulären Cyberangriffen der letzten Monate und an Behördenchefs wie Hans-Georg Maaßen, dem Verfassungsschutzpräsidenten, der bei jeder Gelegenheit „niedrigschwellige Möglichkeiten“ für die Cyberabwehr fordert. Bundesinnenminister Thomas de Maizière (CDU) unterstützt die Forderung, die er „aktive Abwehr“ bei Angriffen nennt.

Auch der frühere Geheimdienstmann Wilfried Karl hält es für notwendig, dass staatliche Behörden digital zurückschlagen können. Karl baut in München gerade aus dem Nichts eine neue Behörde auf, die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis). Sie soll einmal 400 Leute beschäftigen, die Grundlagenarbeit für die neuen digitalen Ermittlungstechniken leisten sollen, als Dienstleister für BKA, Bundespolizei und den Verfassungsschutz.

„Als Bürger erwarte ich, dass unser Staat auch bei neuartigen digitalen Bedrohungen handlungsfähig bleibt“, sagt Karl. Als Beispiel nennt er den Bundestagshack im Jahr 2015: „Wäre es nicht wünschenswert, entwendete Dateien und Dokumente zumindest auf den Servern der Diebe zu löschen?“

Das Schweizer Gesetz erlaube den dortigen Geheimdiensten solche Hackbacks bereits unter bestimmten Voraussetzungen. Noch weiter gehe ein Gesetzentwurf aus den USA, der es Unternehmen gestatten würde, gegen Cyberattacken offensiv vorzugehen, also zurückzuhacken. Letzteres hält Karl für keine gute Idee: „Derlei offensive Maßnahmen sollten staatlichen Behörden vorbehalten bleiben.“

Experten vergleichen die diskutierten Methoden gern mit dem Polizeialltag. Kommt das Umleiten der Angreiferdaten einem Platzverweis gleich, sei das Zerstören des fremden Servers wie ein Todesschuss aus der Polizeiwaffe, bevor der Täter schieße.

Der Vergleich hinkt allerdings. Der Cyberraum sei viel komplexer, sagt Timo Kob. Der Gründer der Sicherheitsfirma Hi-Solutions und Professor für Wirtschaftsschutz und Cybersecurity sieht „erhebliche verfassungs- und völkerrechtliche Probleme, da der Gegner meist im Ausland sitzt“. Wie aber finde man heraus, auf welchem Server der Täter seine Daten verstecke? Beim Bundestagshack hätten die Täter absichtlich unsichere Software benutzt. Sie hätten sich mit anderen Identitäten später selbst gehackt, um die Spur der Daten zu

verschleiern. „Das ist wie ein geraubtes Fluchtauto, das man verfolgt, obwohl das gestohlene Geld längst aus dem Fenster geworfen wurde“, sagt Kob. Die Gefahr, den Falschen zu treffen, sei groß.

Dramatisch werde es, wenn die Hacker zum Beispiel zur Tarnung den Server eines Krankenhauses für ihre Angriffe nutzten. Werde der von staatlichen Akteuren vernichtet, sei der Kollateralschaden riesig. „Dann haben wir eine Regierungskrise.“ Zum Hacken fremder Server benötigten die Behörden zudem Sicherheitslücken, die sie von Dritten meist einkaufen müssten. „Damit wird ein Markt beflügelt, den andere Behörden gern austrocknen würden“, sagt Kob.

Kritische Stimmen gibt es auch in großen IT-Firmen. Brad Smith, Präsident und Chefjustiziar von Microsoft, fordert die Einführung einer „Digitalen Genfer Konvention“. Microsoft werde nicht dabei helfen, Kunden anzugreifen, sagt Smith und gibt die Devise aus: Hundert Prozent Verteidigung, null Prozent Angriff. „Selbst in einer Welt des wachsenden Nationalismus muss der globale Techniksektor bei der Cybersicherheit als eine Art neutrale digitale Schweiz agieren“, so Smith. Einig ist sich der Microsoft-Mann in dieser Frage mit Konstantin von Notz, dem stellvertretenden Fraktionsvorsitzenden der Grünen im Bundestag. „Verteidigung ist im Cyberbereich die beste Verteidigung“, sagt der Politiker und beschreibt die künftige Linie seiner Partei. „Angriffe sind rechtlich wie praktisch maximal problematisch und sollten nicht legalisiert werden.“

Was aber, wenn Deutschland tatsächlich vor einer Katastrophe steht? Wenn Hacker glaubhaft mit einer Kernschmelze in einem Reaktor drohen? Brauchen die Behörden für diesen Fall nicht eine rechtliche Grundlage für einen Angriff aus Notwehr?

Sven Herpig, IT-Experte der Stiftung Neue Verantwortung, sagt, natürlich müsse es dafür einen Rechtsrahmen geben. Dazu müsse man aber das Thema auch öffentlich diskutieren und nicht ausschließlich in Geheimgremien der Bundesregierung und des Bundestags. Außerdem sei es eine Ressourcenfrage: „Da richtig gute Leute bei uns rar sind, würde ich sie lieber für den Schutz unserer Netze und Systeme eingesetzt sehen. Sonst ist das nichts anderes als digitales Räuberschach.“

Gutes Personal sei in Deutschland sehr schwer zu finden, sagte auch IT-Sicherheitsforscher Sandro Gaycken diese Woche auf der Digital-Society-Konferenz. Eine aktuelle Analyse einer Personalberatungsagentur habe ergeben, dass gerade einmal 40 bis 50 Spezialisten in der Lage seien, besonders gesicherte und „gehärtete“ IT-Systeme zu knacken. Deutschlandweit.

Maik Baumgärtner, Matthias Gebauer, Martin Knobbe, Marcel Rosenbach, Wolf Wiedmann-Schmidt