Cyberangriffe

Innenministerium plant drei neue Internet-Eingreiftruppen

Deutschlands Cyberabwehr soll vollständig umgebaut werden. Der ambitionierte Plan dafür liegt ZEIT ONLINE und Deutschlandfunk vor. Er scheint kaum umsetzbar.

Von **Kai Biermann**, **Patrick Beuth** und **Falk Steiner**

7. Juli 2016, 7:58 Uhr / 93 Kommentare

Techniker ist informiert... © Arno Burgi/dpa

Mimikatz hat den Abgeordneten des Bundestages einen gehörigen Schrecken eingejagt. Die frei verfügbare Software [https://github.com/gentilkiwi/mimikatz] mit dem niedlichen Namen hatten Kriminelle im vergangenen Jahr genutzt, um das interne Netz des Bundestags auszuspähen [https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#abschlussbericht_bsi_20151103].

Die Angreifer stahlen nicht nur die Passwörter der Administratoren. Ihre Attacke legte vor allem offen, wie hilflos das Verfassungsorgan den Kriminellen ausgeliefert war: Verfassungsschutz und das Bundesamt für Sicherheit in der Informationstechnik (BSI) suchten hektisch nach den Lecks. Weil beide Behörden nicht genug Fachleute schicken konnten, musste eine private Firma aushelfen. Es dauerte drei Wochen, bis die Parlamentscomputer wieder abgedichtet waren.

Das soll sich nicht wiederholen. Bundesinnenminister Thomas de Mazière will die Behörden komplett umbauen, die digitale Angriffe erkennen und abwehren sollen. **Das geht aus einem vertraulichen Plan namens "Cybersicherheitsstrategie für Deutschland 2016" hervor, der ZEIT ONLINE und dem Deutschlandfunk vorliegt.** Das Papier wird gegenwärtig zwischen den zuständigen Ministerien abgestimmt. Im Herbst soll es vom Kabinett verabschiedet werden. Dann bekäme Deutschland eine neue Sicherheitsarchitektur für den digitalen Raum.

Schnelle Eingreiftruppen

Entstehen soll eine größere und fast militärische Struktur aus verschiedenen Behörden, die nicht nur beraten, sondern zum ersten Mal auch schnell handeln können. Das Bundesamt für Sicherheit in der Informationstechnik, das bislang nahezu alleine kämpft, wenn es um digitale Sicherheit geht, wäre nach diesen Plänen nur noch eine von mehreren Säulen der staatlichen Cybersicherheit. Gleich drei Eingreiftruppen sollen entstehen, verschiedene Gremien und Behörden ausgebaut, Polizei, Bundeswehr, Regierung und Wirtschaft stärker miteinander vernetzt werden.

Auf 33 Seiten beschreibt der Plan die neue Cyberstrategie. Ihr Kern: Das BSI und das Cyberabwehrzentrum des Bundes in Bonn werden stark ausgebaut. Außerdem soll eine weitere Institution gegründet werden, um sofort auf eventuelle Angriffe reagieren zu können: ein Computer Emergency Response Team (CERT) – Fachleute, die möglichst schnell Probleme analysieren und bei der Lösung helfen können. Solche CERTs gibt es schon an deutschen Universitäten und beim BSI. Nun soll ein nationales CERT entstehen.

Wird der Plan umgesetzt, wird es in Zukunft unter dem Dach des Innenministeriums drei Arme der zivilen Cyberabwehr nebeneinander geben. Das CERT wäre so etwas wie das Lagezentrum. Dorthin könnten sich Behörden und Unternehmen wenden, die angegriffen wurden. Dort würde auch die Abwehr des Angriffs geleitet. Das BSI wäre dafür zuständig, die Methoden und Instrumente der Angreifer zu analysieren und es würde die technische Beratung übernehmen.

Zivile und militärische Zusammenarbeit

Als dritter Arm würde das Cyberabwehrzentrum alle staatlichen Behörden miteinander verbinden, angefangen von BSI und Bundeswehr über Polizeien und Geheimdienste bis hin zum Zoll. Das tut es theoretisch jetzt schon. Die Bundesregierung hatte 2011 ihre erste Cybersicherheitsstrategie vorgestellt [http://www.zeit.de/digital/internet/2011-02/cyber-abwehrzentrum]. Damals wurde das Cyberabwehrzentrum [https://de.wikipedia.org/wiki/Nationales_Cyber-Abwehrzentrum] in Bonn gegründet. Doch drei Jahre später urteilte der Bundesrechnungshof [http://www.zeit.de/digital/internet/2014-06/cyber-abwehrzentrum-bundesrechnungshof], das Abwehrzentrum sei nahezu nutzlos, weil es von keiner der beteiligten Behörden ernst genommen werde.

Damit soll es nun offensichtlich vorbei sein. Die Bundesregierung will das Abwehrzentrum mit mehr Geld und Einfluss ausstatten. Es soll Informationen über Angriffe verteilen und auch die Bundeswehr mit ihrer Cybertruppe [http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYyxEoIwEES_hQ8wB9qgHYiFjYWNxu4ImXgMSZjzgMaPNyncndli3-zCC5IDruRQKAac4Ana0KnfVO9Xp8a4cGqVp0AfsUyLh0feDFaZGKzkFBuEUjpGiazmyDJlsjAnomgAXVZdW1blX9W32V9ux3NdH7pre8-HM6PzCDrEnUHztjB7X29NUfwASe2Amw!!/] einbeziehen. Wie genau, das bleibt allerdings unklar. Im Ministerpapier steht lediglich, dass die zivil-militärische Zusammenarbeit zwischen Abwehrzentrum und Bundeswehr neu konzipiert werden müsse.

Der Plan des Innenministeriums sieht außerdem vor, dass drei Behörden jeweils eine digitale Eingreiftruppe aufbauen, die jederzeit ausrücken kann. Wie der Angriff auf den Bundestag gezeigt hat, ist das die bisher größte Schwäche: Keine Sicherheitsbehörde hat Mitarbeiter, die sie schnell irgendwohin schicken kann, um Rechner zu analysieren und Hacker zu jagen.

Einsatz rund um die Uhr

Das Bundesamt für Verfassungsschutz, das Bundeskriminalamt und das BSI sollen nun jeweils eine Quick Reaction Force bekommen. Der Name stammt vom Militär und bezeichnet kleine, mobile Teams, die möglichst innerhalb von Stunden bei jedem Opfer sein können. Im Konzept des Innenministeriums steht dazu der Ausdruck "24/7" – rund um die Uhr, an jedem Tag der Woche.

Im BSI soll dieses Team Mobile Incident Response Team (MIRT) heißen. Seine Aufgabe soll es sein, kritische Infrastrukturen zu reparieren. Die Eingreiftruppe des Verfassungsschutzes firmiert bislang unter "Cyber-Team". Sie soll anrücken, wenn Geheimdienste oder Terroristen angreifen. Die Einheit des BKA, Quick Reaction Force genannt, soll Strafverfolger unterstützen und als digitale Polizei bei kriminellen Angriffen Daten sicherstellen.

Das Problem: Es ist bei Hacks nur schwer bis gar nicht zu erkennen, wer sie mit welchem Motiv ausführt. Bis heute ist nicht klar, wer vor einem Jahr den Bundestag angegriffen hat und was er wollte. Waren es Kriminelle? Terroristen? Ein fremder Geheimdienst? Oder waren es Kriminelle im Auftrag eines Geheimdienstes, wie der Verfassungsschutz glaubt [https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#abschlussbericht_bsi_20151103]?

Die Eingreifteams könnten sich also schon bald gegenseitig auf die Füße treten und miteinander um die Zuständigkeit rangeln. Dieser Punkt sei leider noch vollkommen ungeklärt, sagt ein Sicherheitsfachmann, der an dem Konzept beteiligt ist.

Netz überwachen

Kritisch ist die Idee, dass das Innenministerium zusammen mit den Providern die "Sensorik im Netz ausbauen" will, um Cyberangriffe und Infektionen besser erkennen zu können und laufende Angriffe abzuschwächen. Mit Sensoren im Netz könne man viele Angriffe erkennen, sagt Klaus Landefeld. Er ist Mitglied im Vorstand des Internetverbandes eco und im Beirat des DE-Cix, des weltweit größten Internetverbindungsknotens. Doch sollte das Innenministerium mit der Sensorik die sogenannte Deep Packet Inspection [http://www.zeit.de/digital/internet/2011-11/internet-downloads-kontrolle] meinen, also das Durchsuchen aller in den Leitungen transportierten Daten, dann ist Landefeld klar dagegen. "Das ist nun einmal etwas, was man verfassungsrechtlich nicht will. Die Verkehre sind geschützt, man darf in die Daten nicht hineinsehen." Das Verbot aufzuweichen, sei gefährlich.

Doch soll überhaupt der komplette Netzwerkverkehr automatisiert überwacht werden? Ein kleiner Zusatz im Ministerpapier legt das nahe: "Die Pseudonymisierung solcher Erkenntnisse ist dabei ein wirksames Mittel, um die Rechte der Betroffenen zu schützen", heißt es dort. Übersetzt könnte das bedeuten: Alle Daten werden auf verdächtige Aktivitäten hin überprüft und die Privatsphäre indirekt geschützt, indem Klarnamen durch Nummern ersetzt werden. Eine solche Pseudonymisierung kann aber immer rückgängig gemacht werden.

Strafrecht erweitern

Auch bei anderen Punkten bleibt das Konzept im Ungefähren. So wird gefordert, das Strafrecht auszubauen. Neue Taten bräuchten neue Gesetze und neue Befugnisse für die Sicherheitsbehörden, schreibt das Innenministerium. Der Katalog der Straftaten, bei denen der Paragraf 100 a der Strafprozessordnung greife, müsse erweitert werden. Paragraf 100 a regelt [https://dejure.org/gesetze/StPO/100a.html], wann die Telekommunikation überwacht, wann Telefone abgehört, wann E-Mails mitgelesen werden dürfen. Die Cyberstrategie sagt dazu lediglich, es müssten jene Straftaten berücksichtigt werden, "die online und konspirativ verübt werden".

Was genau damit gemeint ist, wissen nicht einmal Strafrechtsexperten. "Angesichts der vagen Formulierungen ist schwer zu bestimmen, welche konkreten Ziele die Bundesregierung verfolgt", sagt Tobias Singelnstein, Professor für Strafrecht und Strafverfahrensrecht an der Freien Universität Berlin. Er warnt, dass der Paragraf 100 a nur bei schweren Straftaten zum Einsatz kommen dürfe. Im Übrigen sei Cyberkriminalität gut durch bestehende Gesetze erfasst.

Nutzer identifizieren

Die neue Cyberstrategie sieht auch eine "Anpassung" der Mitwirkungspflichten von Unternehmen vor, etwa bei der Identifizierung von Nutzern. Als Beispiel wird die Verifizierungspflicht für Prepaidhandys genannt, die mit dem jüngst vom

Bundestag beschlossenen Anti-Terror-Paket [http://www.n-tv.de/politik/Prepaid-Karten-Kauf-nur-noch-mit-Ausweis-article18038161.html] eingeführt wird. Ob es ähnliche Pflichten auch für deutsche Anbieter von anonymen Internetdiensten geben könnte, lässt sich aus dem Dokument nicht direkt ableiten, vorstellbar wäre es aber.

Ebenfalls heikel ist der Vorschlag, der Staat müsse sich stärker für private Sicherheitsdienstleister öffnen, weil es an Fachkräften mangele. Aufgaben von Polizei, Geheimdiensten und Militär zu privatisieren, ist stark umstritten. Trotzdem will das Innenministerium mehr private Sicherheitsfirmen einsetzen. Auch die Bundeswehr solle darüber nachdenken, Cybersöldner einzukaufen. Zumindest sei Unterstützung durch zivile Akteure "zulässig und denkbar", heißt es in dem Konzept.

Aufrüsten

Im Innenministerium soll außerdem eine zentrale Stelle entstehen, die Cyberwaffen beschafft und entwickelt. So zumindest kann die unscharfe Formulierung verstanden werden, nach der diese Stelle "technische Unterstützung für nationale Sicherheitsbehörden im Hinblick auf deren operative Cyberfähigkeiten" leisten soll.

Dafür würde sprechen, dass die staatliche Abwehr die gleichen Werkzeuge nutzen muss, die auch Angreifer verwenden. Das ist im Internet nicht anders als auf dem Schlachtfeld. Trotzdem gibt es viele Kritiker, die fordern, Deutschland solle sich nicht am internationalen Wettrüsten digitaler Waffen [http://www.nzz.ch/meinung/kommentare/geheimes-wettruesten-im-cyberspace-1.18443493] beteiligen. Diese Stabsstelle, die "bedarfsbezogen und zukunftsorientiert Methoden, Produkte und Strategien für die operative Umsetzung der Cyberfähigkeiten in den Sicherheitsbehörden erarbeitet", könnte aber genau das tun.

Verschlüsselung knacken

Solche Janusköpfigkeit zeigt sich auch beim Thema Verschlüsselung. Einerseits will das Innenministerium, dass Deutschland die besten Verschlüsselungswerkzeuge der Welt entwickelt. Andererseits sollen Geheimdienste und Polizei jedes Programm und jede Kommunikation knacken können.

Cybersicherheit entstehe vor allem, wenn Anwender sichere Systeme einsetzten, heißt es in der Einleitung des Papiers. Viele Angriffe könnten so bereits abgewehrt werden. Wenige Absätze später wird sogar gefordert, alle Anwender müssten die Chance haben, vertrauenswürdige und sichere Systeme zu nutzen. Die Verschlüsselung privater Kommunikation müsse zum Standard werden und nicht mehr nur die Ausnahme sein.

Gleichzeitig plant das Ministerium jedoch abseits der hier formulierten Strategie, eine weitere Behörde aufzubauen. Deren einziges Ziel: Verschlüsselte Daten zu knacken, damit Dienste und Behörden sie trotzdem lesen können. Bis 2020 sollen 400 Mitarbeiter bei dieser Zentralen Stelle für Informationstechnik im Sicherheitsbereich (Zitis) [http://www.sueddeutsche.de/digital/sicherheitspolitik-neue-behoerde-soll-fuer-regierung-verschluesselte-kommunikation-knacken-1.3047884] arbeiten.

Die Cybersicherheitsstrategie erwähnt den Zitis-Plan nirgendwo, aber sie fasst diese beiden, sich widersprechenden Forderungen in einem Satz zusammen: "Die deutsche Kryptostrategie umfasst Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung."

"Kryptierung von Kommunikation ist eine der Grundvoraussetzungen für die Digitalisierung", sagt Martin Schallbruch. Er war viele Jahre lang IT-Direktor im Innenministerium und dort zuständig für digitale Sicherheit. Verschlüsselung dürfe weder durch Hintertüren noch durch unsichere Algorithmen angebohrt werden. Natürlich müssten Sicherheitsbehörden auch im digitalen Raum ermitteln und dazu technisch aufrüsten, sagt Schallbruch. "Es ist jedoch nicht ratsam, Verschlüsselung abzuschwächen. Das würde unserer gesamten digitalen Gesellschaft auf die Füße fallen."

Haftung für schlechte Software

Immerhin gibt es in dem Cyberplan auch Forderungen, die aus Sicht der Bürger und Internetnutzer uneingeschränkt positiv sind.

So prüft die Bundesregierung demnach, ob Hersteller haftbar gemacht werden können, wenn sie Sicherheitsmängel in ihrer Software und ihrer Hardware nicht beheben. Die Industrie wehrt sich bislang mit allen Mitteln gegen solche Ansprüche. Es sei unmöglich, Software ohne Fehler zu produzieren, ist ihr Argument, Haftungsansprüche würden die Entwicklung neuer Produkte verhindern und Firmen ruinieren.

Ähnlich schwer erreichbar scheint ein anderes Ziel. Digitale Bildung "muss zu einem festen Bestandteil des Bildungskanons werden", steht in dem Konzept. "Jede Schulabgängerin und jeder Schulabgänger sollte Grundkenntnisse von Informatik haben."

Das zu erreichen, ist ein weiter Weg. Wie überhaupt der ganze Plan an einem Problem krankt: Es gibt in Deutschland gar nicht genug Fachleute, um all die gewünschten Gremien zu besetzen. Sie auszubilden, wird Jahre dauern. Vielleicht steht in dem Cyberkonzept deshalb auch keine Jahreszahl, bis wann eines der genannten Ziele erreicht sein soll.

Mehr dazu finden Sie auch beim Deutschlandfunk

Haben Sie Informationen zu diesem Thema? Oder zu anderen Vorgängen in Politik und Wirtschaft, von denen die Öffentlichkeit erfahren sollte? Wir sind dankbar für jeden Hinweis. Dokumente, Daten oder Fotos können Sie hier in unserem anonymen Briefkasten deponieren