Gekapert von einer fremden Macht

Ohne Laptop, Tablet und Smartphone geht kaum etwas im Deutschen Bundestag. Bereits seit Mitte Mai ist bekannt, dass es eine Attacke auf das IT-Netzwerk des Parlaments gibt. Aber erst jetzt zeichnet sich die Dimension ab. DPA

Es ist die bislang größte Cyberattacke auf den Bundestag. Und die Trojaner sind noch immer aktiv. Der russische Geheimdienst wird als Urheber genannt. Aber sicher ist das nicht.

VON DIRK SCHMALER

Es passierte ausgerechnet am 8. Mai. Der Bundestag erinnerte gerade mit einer Gedenkstunde an das Ende des Zweiten Weltkrieges vor 70 Jahren, als die IT-Fachleute des Parlaments erstmals bemerkten, dass ihre Computer ein Eigenleben führen. Einzelne Rechner stellten eigenmächtig Verbindungen zu Bundestagsservern her, einige luden massenhaft Daten herunter und überlasteten kurzzeitig die Systeme. Erst waren es nur wenige. Doch bald stellte sich heraus, dass die Unregelmäßigkeiten der Beginn des bisher größten Cyberangriffs auf eine öffentliche deutsche Institution seit Bestehen des Internets waren. Und er dauert unvermindert an.

Die Trojaner genannten Schadprogramme, die sich ursprünglich in 15 Computern eingenistet hatten, sind noch immer in dem Netz mit insgesamt mehr als 20 000 „Parlakom"-Rechnern vorhanden. Mehr noch: Auswertungen der IT-Spezialisten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) haben bereits vor zwei Wochen ergeben, dass es den Angreifern gelungen ist, die „Administrationsrechte für die gesamte Infrastruktur" zu bekommen. Das bedeutet: Der Angriff zielte tief ins Herz des Systems – und er ist geglückt. Irgendjemand hat nun Zugriff auf das Computersystem. Er könnte mitlesen, Daten absaugen, womöglich sogar Abgeordnete einfach vom Netz nehmen oder deren Computer fernsteuern. Der gläserne Abgeordnete, ein lang gehegter Traum mancher Bürgerrechtler, ist ausgerechnet für eine Hackergruppe weitgehend Realität geworden.

Der Bundestag, einer der wichtigsten Orte politischer Entscheidungsfindung, ist von einer fremden Macht gekapert. Selbst wenn in den vergangenen Tagen tatsächlich keine neuen Daten mehr abgeflossen sein sollten, gehen Experten davon aus, dass der Bundestag einen Gutteil der Computer austauschen und die gesamte Software neu einrichten muss. „Es handelt sich um den bisher größten Angriff auf das deutsche Parlament", sagte der Parlamentarische Geschäftsführer der Unionsfraktion, Bernhard Kaster, gestern in geradezu kriegerischem Vokabular. Noch weiß niemand, wer der Urheber dieser Attacke ist. Experten tippen auf professionelle Spione, weil der Angriff äußerst komplex und umfassend scheint. Verfassungsschutzpräsident Hans-Georg Maaßen treibt die Sorge um, „dass es sich um einen Cyberangriff eines ausländischen Nachrichtendienstes handelt" – und er erwähnte abstrakt die „hoch qualifizierten" russischen Dienste. Mehr als Spekulation scheint das aber nach Ansicht von Netzaktivisten nicht zu sein. Viele Hacker seien mittlerweile in der Lage, russische oder chinesische Programmierfetzen in den Programmcode einzubauen, um falsche Spuren zu legen. Die wahre Herkunft ist nur sehr schwierig nachvollziehbar.

> **Womöglich schreiben mir die Bürger nicht mehr von ihren Problemen.**
> Lars Klingbeil (SPD), Bundestagsabgeordneter

Greifbarer als die Täter sind die Folgen des Angriffs. Auch wenn die vertraulichen Informationen von Abgeordneten in der Regel nicht allzu sicherheitsrelevant sind, sieht etwa der SPD-Parlamentarier Lars Klingbeil, netzpolitischer Sprecher seiner Fraktion und Mitglied im Verteidigungsausschuss, seine Arbeit durch die neuen Ungewissheiten stark beeinträchtigt. Auf die Frage, was unsichere Computer für einen Abgeordneten bedeuten können, gibt er drei Beispiele aus seinem Alltag.

Sicherheit: „Als Mitglied im Verteidigungsausschuss bekomme ich wöchentliche vertrauliche Lageberichte über die Auslandseinsätze der Bundeswehr", erklärt Klingbeil. Das seien sehr sensible Informationen, „die in den falschen Händen die Sicherheit von Soldaten gefährden könnten".

Vertraulichkeit: „Ich bekomme regelmäßig vertrauliche Hinweise von einfachen Soldaten über Missstände in der Truppe – etwa in der Debatte um das Sturmgewehr G 36", sagt Klingbeil. Wenn die Hinweisgeber nicht sicher sein könnten, dass der Kontakt zu ihrem Abgeordneten vertraulich bleibt, verändere das die Gesprächssituation und wirke einschüchternd. „Womöglich schreiben mir die Bürger nicht mehr von ihren Problemen."

Offenheit: Die Kommunikation der Abgeordneten ist gehemmt. „Wenn jeder weiß, mit wem wir uns wann worüber austauschen, bedroht das unsere Freiheit als Abgeordnete." Ein anderer Abgeordneter berichtete gestern sogar von der Möglichkeit der Erpressung durch angedrohten Verrat von Informationen.

Zwar warnen vor allem Bundesbehörden und Politiker seit Jahren vermehrt vor den Gefahren aus dem Netz – die eigene Verwundbarkeit allerdings hat sich das Parlament und seine Verwaltung bisher anscheinend nicht eingestanden. Gestern haben sich die Bundestagsgremien offenbar zumindest dazu durchgerungen, das Bundesamt für Sicherheit in der Informationstechnik (BSI) und den Verfassungsschutz enger einzubinden. Mittelfristig, da sind sich die Experten einig, muss der Schutz vor Cyberattacken deutlich steigen – nicht nur im Parlament. Der Bundestag macht heute einen Anfang – wenn der Termin auch zufällig ist. Nach langer Planung wollen die Abgeordneten das IT-Sicherheitsgesetz beschließen. Damit sollen Firmen verpflichtet werden, Cyberangriffe zu melden, wenn sie dazu angetan sind, die Funktionsfähigkeit kritischer Infrastruktur wie etwa Stromnetze zu beeinträchtigen.

Schleswig-Holstein hat keine Angst vor Hackern

VON ULF B. CHRISTEN

Die Regierung und der Landtag in Schleswig-Holstein sehen sich gegen Hacker gut geschützt. „Ich glaube, dass so etwas wie in Berlin in Schleswig-Holstein nicht passieren kann", betont der Leiter des Zentralen IT-Managements, Sven Thomsen. Seine Zuversicht erklärt der Herr über mehr als 20 000 Regierungs- und Landtags-Computer mit einem ausgeklügelten und erfolgreichen Sicherheitssystem. „Wir haben durchaus einige Angriffe gehabt, die aber schnell abgewehrt werden konnten." Trojaner und Viren seien „Tagesgeschäft".

Uli König (Piraten) traut dem Frieden nicht. EIS

„Wir fühlen uns gut geschützt", bestätigt der Sprecher des Landtags, Tobias Rischer. Bei der Landtagsverwaltung mit ihren 120 Computern habe es in der Vergangenheit kleinere „Störungen" wie etwa Portscans oder Mailbombing gegeben. „Cyber-Angriffe wie aktuell auf den Bundestag haben wir noch nicht registriert." Die Fraktionen mit ebenfalls rund 120 PCs haben unterhalb des Regierungs- und Landtagsschutzschirms eigene Datennetze, die extra geschützt sind – gegen Angriffe von außen ebenso wie gegen Attacken von innen, etwa von der politischen Konkurrenz.

Die Piraten trauen dem Cyber-Frieden nicht. „Wenn ein Hacker in das Landessystem will, dann kommt er da auch rein", meint ihr Datenschutzexperte Uli König. Im Internet gebe es die Möglichkeit, „Sicherheitslücken" für gängige Systeme zu kaufen. Habe man Zugriff etwa auf den „Verzeichnisdienst", sei das System geknackt. In dem Dienst seien die Benutzer samt Zugriffsberechtigungen und Passwort aufgelistet. „Dann kann man sich selbst Administratorrechte einräumen", sagt der Informatiker.

Der Piraten-Politiker empfiehlt Regierung und Landtag, sich von „Windows" zu verabschieden und stärker auf offene Software wie Linux zu setzen. Außerdem hat er einen ganz praktischen Tipp: Die Putzkolonnen sollten abends im Landeshaus stärker darauf achten, dass nicht zu viele Büros mit Computern offenständen. König geht davon aus, dass es so oder so keine hundertprozentige Sicherheit gibt. Aber: „Das Land ist bei den Hackern bestimmt nicht das Ziel Nummer eins."

Späher und Hacker halten den Bundestag weiter in Atem

Ermittlungen zum ausgespähten „Merkelphone“ eingestellt – IT-Gesetz neu aufgestellt

VON DIANA NIEDERNHÖFER

KARLSRUHE/BERLIN. Vorerst wird es keine weiteren Ermittlungen zum mutmaßlichen Ausspähen des Mobiltelefons der Bundeskanzlerin geben. Generalbundesanwalt Harald Range stellte das seit einem Jahr laufende Ermittlungsverfahren aus Mangel an Beweisen ein. Der US-Geheimdienst NSA soll über Jahre das Handy von Angela Merkel (CDU) abgehört haben. Der Angriff eines wohl anderen Geheimdienstes auf das Computernetz des Bundestages führte unterdessen zu einer Erweiterung des IT-Sicherheitsgesetzes.

„Wir haben das Ermittlungsverfahren eingestellt, weil wir bei dem Verdacht letztlich die Vorwürfe, die im Raum stehen, nicht gerichtsfest beweisen können“, sagte Range gestern. Die Bundesanwaltschaft hatte im Juni 2014 Ermittlungen wegen des Anfangsverdachts der Spionage und der Agententätigkeit eingeleitet.

Doch die Behörde kam offenbar nicht weiter: So hätten von dem ehemaligen NSA-Mitarbeiter Edward Snowden veröffentlichte Dokumente keine gerichtsfesten Nachweise für eine Überwachung des Mobiltelefons enthalten. Ein angebliches NSA-Beweisdokument habe nicht beschafft werden können.

Die Unterlagen des NSA-Untersuchungsausschusses des Bundestags hätten auch kaum weiter geführt, sagte Range. Von einer Vernehmung Snowdens habe man Abstand genommen, weil keine neuen Erkenntnisse zu erwarten gewesen seien. Dennoch seien die Ermittlungen nicht chancenlos gewesen: „Sonst hätten wir das Verfahren ja nicht eingeleitet und hätten auch unsere Ermittlungen nicht über ein Jahr geführt.“

➡ Generalbundesanwalt Range konnte gegen den US-Geheimdienst NSA keine gerichtsfesten Beweise finden.

SMS von der NSA? Angela Merkel checkt ihr Smartphone. DPA

Während die Bundesregierung eine Stellungnahme ablehnte, kritisierte die Opposition die Einstellung scharf. Grünen-Innenexperte Hans-Christian Ströbele bezeichnete den Schritt als „schlechten Witz“ und forderte Range auf, „erstmal Ermittlungen zum Sachverhalt durchzuführen“. Auch die Linke-Obfrau des NSA-Untersuchungsausschusses, Martina Renner, warf Range ein „falsches Signal“ in der Aufklärung von Geheimdienst-Spionage vor.

Nach dem Hackerangriff eines mutmaßlich ausländischen Geheimdienstes auf das Computersystem des Bundestages hat die Regierung dagegen Konsequenzen gezogen: Das gestern vom Bundestag verabschiedete IT-Sicherheitsgesetz verpflichtet nicht nur Unternehmen, sondern auch Bundesbehörden, Mindestanforderungen an die Computersysteme zu erfüllen. Diese soll das Bundesamt für Sicherheit und Informationstechnik (BSI) festlegen.

Das Computersystem des Bundestags wurde nach dem letzten Stand der Ermittlungen bei der seit rund vier Wochen laufenden schweren Cyber-Attacke mit Hilfe von Links durch E-Mails an zwei Computer im Bundestag angegriffen. Die Links führten zu einer Webseite, die mit Schadsoftware präpariert war.

S 26.5.2020

Hackerangriff kam wohl aus Russland

Behörden identifizieren offenbar einen Mitarbeiter des Militärgeheimdienstes GRU als Täter

VON MARKUS DECKER

BERLIN. Fünf Jahre nach dem Angriff auf das Computernetzwerk des Deutschen Bundestages ist es den Ermittlern offenbar gelungen, einen der Täter zu identifizieren. Nach Informationen von WDR, NDR und „Süddeutscher Zeitung" handelt es sich um einen 29-jährigen Russen namens Dmitrij Badin. Er soll als Hacker für den russischen Militärgeheimdienst GRU arbeiten. Gegen ihn habe der Generalbundesanwalt beim Bundesgerichtshof einen internationalen Haftbefehl erwirkt, heißt es.

Im Frühjahr 2015 waren Hacker in das IT-System des Bundestags eingedrungen und hatten mehr als 16 Gigabyte Daten gestohlen – darunter zahlreiche E-Mails von Abgeordneten. Aus Sicherheitsbehörden verlautet, der Cyberangriff sei vermutlich Teil einer Spionagekampagne.

Die US-Bundespolizei FBI geht dem Bericht zufolge davon aus, dass der Russe auch an den Hackerangriffen auf die Demokratische Partei im Vorfeld der US-Präsidentschaftswahlen 2016, die zulasten der demokratischen Präsidentschaftskandidatin Hillary Clinton ausgingen, und auf die Welt-Anti-Doping-Agentur (Wada) mitwirkte. In den USA wird er deshalb ebenfalls gesucht.

Gezielter Angriff: 2015 wurden von Bundestagsservern massenhaft Daten gestohlen. FOTO: THOMAS TRUTSCHEL/IMAGO IMAGES

Dass der Hacker in Deutschland oder den USA vor Gericht gestellt werden kann, gilt als unwahrscheinlich, da er sich kaum aus Russland herausbegeben dürfte. Allerdings gilt Badins Identifizierung zumindest als Prestigeerfolg, weil sich die Richtung, aus der ein Hackerangriff kommt, selten zweifelsfrei feststellen lässt – geschweige denn eine Person, die daran unmittelbar beteiligt war.

Der stellvertretende Vorsitzende der Grünen-Bundestagsfraktion, Konstantin von Notz, sagte dem Redaktions-Netzwerk Deutschland (RND): „Wir müssen dem Thema IT-Sicherheit noch sehr viel mehr Aufmerksamkeit schenken." Es sei besorgniserregend, wie Wahlen manipuliert und die Demokratie geschwächt würden.

Unterdessen nähern sich die Ermittlungen gegen einen damals 20-jährigen Hacker aus Homberg (Hessen), der Hunderte Politiker und andere Prominente ausspioniert hatte und Anfang 2019 aufgeflogen war, offenbar ebenfalls dem Ende. Eine Abschlussentscheidung darüber, ob Anklage erhoben werde, liege noch nicht vor, sagte die Wiesbadener Staatsanwältin Julia Bussweiler. In vier Wochen könne es etwas Neues geben. „Mein Eindruck ist, dass wir uns dem Ende nähern."

Nach offiziellen Angaben gibt es rund 1000 Betroffene und 50 schwerwiegende Fälle, bei denen umfangreiche und teilweise sehr private Informationen für alle sichtbar ins Netz gestellt wurden. Zu den Hauptgeschädigten zählten seinerzeit unter anderem der Grünen-Vorsitzende Robert Habeck und der ZDF-Satiriker Jan Böhmermann.