„Die Hütte brennt“

Spionage Misstrauen, Sorglosigkeit, Gezänk: Die Cyberattacke auf den Bundestag ist auch deshalb so verheerend, weil das Krisenmanagement versagt.

Im Ältestenrat des Bundestags sitzen „sehr erfahrene“ Abgeordnete, die für einen „möglichst reibungslosen Arbeitsablauf“ im deutschen Parlament sorgen sollen. So steht es auf der Website des Gremiums. In Plenarwochen kommt es donnerstags zusammen.

Es muss viel passieren, bis der Ältestenrat die Schlagzahl erhöht – der größte Cyberangriff in der Geschichte des Bundestags gehört wohl nicht dazu. Man muss ja nicht hektisch werden, nur weil ausländische Geheimdiensthacker das wichtigste Verfassungsorgan attackieren.

Nach zwei sitzungsfreien Wochen tagte der Ältestenrat am Donnerstag wieder turnusgemäß. Sicherheitsexperten hatten die Sitzung förmlich herbeigesehnt. Anschließend ließ Bundestagspräsident Norbert Lammert (CDU) die Abgeordneten wissen, Teile des attackierten Bundestagsnetzes würden nun „rasch“ neu installiert. Zügig werde man sich weitere Hintergrundinformationen zur Cyberattacke beschaffen.

Doch ein schnelles Ende der beispiellosen Affäre ist auch nach fünf Wochen nicht absehbar. Verantwortlich ist das ausgefeilte Angriffswerkzeug einer Hackergruppe, die anscheinend mühelos bis in die Prozesssteuerung des Bundestagsnetzes Parlakom vorgedrungen ist und dort seither fast nach Belieben schalten und walten kann.

Allerdings haben die Fraktionen im Deutschen Bundestag die Hacker geradezu zum Datenraubzug eingeladen. Über Jahre nahmen selbst Sicherheitspolitiker die Datensicherheit im Parlament auf die leichte Schulter. Privatgeräte wurden zugeschaltet, eigene Server aufgebaut und nicht zureichend gewartet. Wäre das Parlakom-Netz ein Haus, es hätte zahllose Erker, einfach verglaste Fenster und Anbauten mit Wellblechdach, in denen Dokumente dürftig geschützt herumliegen.

Unglücklich agierte zudem Bundestagspräsident Lammert. Statt die Abgeordneten sofort zu informieren, wartete der Christdemokrat zunächst ab. Von Ratschlägen, das Bundestagsnetz abzuschalten, um noch Schlimmeres zu verhindern, wollte seine Verwaltung nichts wissen. Dabei musste dem Präsidenten von Anfang an klar sein, dass nichts weniger als die Funktionsfähigkeit des deutschen Parlaments auf dem Spiel steht.

Bereits am 8. Mai hatten IT-Spezialisten des Bundestags „Anomalien“ im internen Datennetz Parlakom festgestellt, auf die sie sich zunächst keinen Reim machen konnten. Fast zeitgleich ging beim Bundesamt für Verfassungsschutz (BfV), Abteilung Spionageabwehr, eine beunruhigende Meldung ein: Eine Quelle berichtete, dass Hacker das Computersystem des deutschen Parlaments angegriffen hätten.

Die Verfassungsschützer prüften die Angaben und hielten den Fall für so gravierend, dass sie ihn zur Chefsache erklärten: Am 12. Mai informierte BfV-Präsident Hans-Georg Maaßen das Bundesamt für Sicherheit in der Informationstechnik (BSI) über die Cyberattacke, das wiederum das Parlament alarmierte.

Die Ermittlungen förderten Brisantes zutage. So lokalisierten IT-Spezialisten zunächst einen Bundestagsrechner der Unionsfraktion sowie einen Computer der Linken, die immer wieder Server in Osteuropa anwählten. Da diese im Visier von Geheimdiensten sind, weil sie von organisierten Kriminellen genutzt werden, flog die Sache auf. Die Parlamentscomputer wurden offensichtlich von fremden Profis ferngesteuert – ein beispielloser Vorgang (SPIEGEL 23/2015).

Wie schwer der Spionageangriff den Bundestag tatsächlich getroffen hat, kam danach scheibchenweise ans Licht: In mehreren Angriffswellen drangen die Hacker immer tiefer ins Parlakom-Netz ein und gelangten sogar bis zu dessen Prozesssteuerung. Experten nennen das Advanced Persistent Threat, eine ausgefeilte, hartnäckige Bedrohung.

Die Angreifer hatten damit potenziell Zugriff auf alle 20 000 ans Parlakom-Netz angeschlossene Accounts, darunter jene in den Bundestagsbüros von Kanzlerin Angela Merkel und weiteren Regierungsmitgliedern. Angeblich wurden bislang 15 befallene Rechner eindeutig identifiziert, bei mindestens 5 von ihnen wurden Datenabflüsse festgestellt. Die Schadsoftware dauerhaft zu beseitigen gilt als nahezu unmöglich.

Einen derart perfekten Angriff kann nach Auffassung von Experten nur ein Geheimdienst durchführen. Nach Analyse der Schadwerkzeuge spricht vieles dafür, dass der russische SWR hinter der Attacke steht. Es gibt zudem auffällige Parallelen zum Cyberangriff auf den französisch-

sprachigen Fernsehsender TV5 Monde am 9. April. Zwar brüstete sich seinerzeit das „Cyber-Kalifat" des „Islamischen Staates" mit dem Hack. Tatsächlich weisen aber auch in diesem Fall die Spuren in Richtung Russland.

Es war also kein Alarmismus, als das BSI die Bundestagsverwaltung nach ersten Analysen darauf hinwies, eine sichere Kommunikation der 631 Parlamentarier und ihrer Mitarbeiter könne nicht mehr garantiert werden. Erstaunlicherweise dauerte es nach dem Aufdecken der Attacke trotzdem sieben Tage, bis die Verwaltung einzelne Fraktionen über den „Sicherheitsvorfall" im Parlakom-Netz in Kenntnis setzte. Seither wurden die Abgeordneten nur tröpfchenweise ins Bild gesetzt.

Am Morgen des 21. Mai berichtete BSI-Chef Michael Hange dem Parlament, man müsse von einer „breiten Kompromittierung der Netzinfrastruktur" des Bundestags ausgehen. Am Nachmittag desselben Tages verschickte Lammert eine Rundmail an die Abgeordneten, in der es hieß, das Ausmaß des Angriffs habe „bis zur Stunde nicht vollständig ermittelt" werden können. Die IT-Systeme stünden „grundsätzlich zur Verfügung".

Am Donnerstag dieser Woche gab es von den Verantwortlichen im Bundestag erneut widersprüchliche Aussagen: Während Lammert in einer Mail an die Abgeordneten versicherte, die Aufräumarbeiten seien „nicht mit einem Austausch von Hardware verbunden", hieß es aus seiner Verwaltung: Teile der Hardware müssten zu Untersuchungszwecken „übergangsweise stillgelegt und ersetzt" werden. „Die Informationspolitik gegenüber den Abgeordneten in dieser Angelegenheit ist völlig indiskutabel", sagt der Linke André Hahn.

Inzwischen wächst der Missmut auch in Lammerts eigener Fraktion: Die Innenpolitiker der Union haben den Präsidenten für kommenden Dienstag in ihre Runde geladen. Dort solle er endlich zusammenhängend erläutern, wann und wie der Schaden eigentlich behoben werden soll. Bislang ist nur klar: Es wird Monate dauern und womöglich Millionenbeträge kosten.

Offen ist dagegen, wer bei den Aufräumarbeiten an vorderster Stelle stehen wird. Außen vor blieb zunächst das Bundesamt für Verfassungsschutz, zu dessen Kernaufgaben die Spionageabwehr zählt. Weil aber das Parlament die Geheimdienste kontrolliert, und nicht umgekehrt, und weil derzeit ein Untersuchungsausschuss die Verstrickungen von NSA, CIA, BND und BfV beleuchtet, gibt es in Teilen des Bundestags massive Bedenken dagegen, den Inlandsgeheimdienst an sensible Datenströme zu lassen.

Anfang Juni drängte Verfassungsschutzchef Maaßen bei der Bundestagsverwaltung darauf, ins Boot geholt zu werden. Am vergangenen Donnerstag gab der Ältestenrat nach: Nun soll Maaßens Behörde zumindest genügend Informationen bekommen, um eigene Analysen durchführen zu können.

Mit ähnlichen Schwierigkeiten kämpft das BSI, das einst aus dem Bundesnachrichtendienst hervorging. Dass die Behörde inzwischen einen Teil der Bundestagskommunikation über das vergleichsweise sichere Netz der Bundesregierung umgeleitet hat, halten Abgeordnete für bedenklich.

Auch hier steht der Verdacht im Raum, eine Behörde der Exekutive könne den Schaden nutzen, um insgeheim den Datenverkehr von Parlamentariern auszuspähen. „Die Hütte brennt, und wir streiten darüber, wer löschen darf", sagt ein Abgeordneter resigniert.

Das heißt: Eigentlich streitet nur ein kleiner Teil der Volksvertreter. Dem großen Rest scheint der Cyberangriff auf das digitale Rückgrat der Demokratie schlicht egal zu sein.

Gemessen an anderen Aufregerthemen im politischen Berlin jedenfalls firmierte der Hack wochenlang eher als Lappalie. Es gibt keine Sondersitzungen des Plenums, keine aktuelle Stunde – nichts, was die Erregungsrepublik sonst in Atem halten würde. Und die Verantwortlichen im Bundestag hielten es bis Donnerstag offenbar nicht für nötig, Strafanzeige zu erstatten, etwa wegen Ausspähens von Daten.

Es ist wie im Herbst 2013, nachdem bekannt geworden war, dass die NSA ein Mobiltelefon von Kanzlerin Merkel im Visier hatte. Schon damals warnten Fachleute, es wäre kein Wunder, wenn weitere deutsche Politiker abgehört würden. Schließlich nutzten die meisten private, kaum gesicherte Handys und machten es damit fremden Geheimdiensten einfach.

In der Folge wurde halbherzig darüber debattiert, Parlamentarier mit Kryptohandys auszustatten. Die Mitglieder des NSA-Untersuchungsausschusses, die ihr Mobiltelefon vor Beratungssitzungen in einem Metallkasten wegsperrten, wurden von Kollegen als leicht paranoid belächelt. Danach ging man zur Tagesordnung über.

Von „digitaler Sorglosigkeit" sprach Bundesinnenminister Thomas de Maizière (CDU) jüngst auf dem BSI-Sicherheitskongress in Bonn. Kurz davor hatte es BSI-Vize Andreas Könen als „Glück" bezeichnet, dass es in Deutschland noch keinen Cyberangriff mit weitreichenden Folgen gegeben habe.

Wie es scheint, ist die Glückssträhne vorbei.

Maik Baumgärtner, Peter Müller, Sven Röbel, Jörg Schindler