Bundestags-Hack: Merkel und der schicke Bär

Gut möglich, dass im Wahlkampf demnächst E-Mails der Kanzlerin auftauchen. Oder vertrauliche Dokumente aus dem Bundestag. Denn vor zwei Jahren spionierten Hacker wochenlang das Computernetzwerk des Parlaments aus. Wie sind sie vorgegangen? Rekonstruktion einer spektakulären Geheimdienstaktion

Von Patrick Beuth, Kai Biermann, Martin Klingst und Holger Stark

Aus der ZEIT Nr. 20/2017

10. Mai 2017, 17:04 Uhr / Editiert am 11. Mai 2017, 15:22 Uhr.

http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland/komplettansicht

Steckt Wladimir Putin hinter dem Hackerangriff auf den Bundestag?
[M]: dpa Mikhail Metzel/Picture-Alliance; Bildagentur-online/Chromorange

Als Claudia Haydt entdeckt, dass der Deutsche Bundestag angegriffen wird, sitzt sie an ihrem Schreibtisch und ist entnervt. Ihr Büro liegt in einem Parlamentsgebäude in Berlin, Unter den Linden, erster Stock, im Innenhof blühen die Birken. Haydt, 50, leitet das Büro der Abgeordneten Inge Höger von der Linkspartei. Sie ist gerade dabei, eine Mail an einen Bekannten zu schreiben, den lieben René, aber sie scheitert schon bei der Anrede: Der kleine Strich über dem é, der Accent aigu, will nicht erscheinen. Haydt drückt die Taste. Nichts passiert. Sie drückt erneut, wieder und wieder. Keine Reaktion.

Haydt wählt die 117, die IT-Hotline des Bundestages, und schildert ihr Problem. Die Techniker, erinnert sie sich, empfehlen ihr, sie solle ihren Rechner neu starten. Auch das hilft nicht. Es ist Freitag, der 8. Mai 2015, nachmittags.

Am Montag tritt das Problem mit dem lieben René noch immer auf, ebenso am Dienstag. Endlich schaut ein Techniker des Bundestags vorbei und installiert Claudia Haydts Programme neu, doch der Accent aigu bleibt verschwunden.

Die IT-Spezialisten des deutschen Parlaments wissen jetzt, dass etwas nicht stimmt. Was sie nicht wissen, ist, dass sie längst die Kontrolle über das Rechnernetz des Bundestages verloren haben.

In jenen Tagen im Mai 2015 beginnt eine mehrwöchige digitale Schlacht[1)], wie es sie in Deutschland nie zuvor gegeben hat. Es ist, als habe eine ausländische Guerillatruppe den Reichstag gestürmt, die Zentrale besetzt, Büros aufgebrochen – nur, dass dieser Kampf digital ausgetragen wird. Am Ende sind mindestens 16 Abgeordnetenbüros durchkämmt, Postfächer kopiert, Festplatten ausspioniert, interne und vermutlich auch vertrauliche Daten abgeflossen.

Zu den Zielen der Angreifer zählen die Büros der Bundeskanzlerin Angela Merkel und des Bundestagsvizepräsidenten Johannes Singhammer von der CSU; betroffen sind auch die Sozialdemokraten Martin Rabanus und Bettina Hagedorn, die im Vertrauensgremium sitzt, das die Budgets der deutschen Geheimdienste kontrolliert.
Als der Angriff schließlich abgewehrt ist, ermittelt die Bundesanwaltschaft wegen Spionageverdachts. Angela Merkel spricht von "hybrider Kriegsführung". Im Kanzleramt werden sogar Gegenschläge erwogen. Denn die Bundesregierung ist überzeugt, dass die Eindringlinge im Auftrag eines fremden Staates handelten, genauer, dass sie aus Russland stammen, aus einer Einheit des Militärgeheimdienstes, die unter dem Namen APT28 oder auch "Fancy Bear", schicker Bär, bekannt ist.

Es sind dieselben Cyber-Spione, die im vergangenen Sommer die US-Demokraten infiltrierten und unter anderem den E-Mail-Account von Hillary Clintons Wahlkampfmanager John Podesta hackten. Eine der Mails, die wenig später an die Öffentlichkeit gelangten, zeigte, wie die Parteispitze um die damalige Vorsitzende Debbie Wasserman Schultz gegen den Kandidaten Bernie Sanders intrigierte. Der Vorfall kostete Wasserman Schultz das Amt – und belastete Hillary Clintons Wahlkampf.

Attacken der Hackergruppe "Fancy Bear"

2007

Die ersten Aktionen der Hackergruppe APT28, auch "Fancy Bear" genannt, werden bekannt. Experten stoßen auf mehrere Schadprogramme, die die Gruppe teils selbst entwickelt hat.

2008

Als die russische Armee während des Kaukasuskrieges auf georgisches Gebiet vorrückt, hackt die Gruppe mehrere georgische Ministerien.

2014

Die Hacker infiltrieren systematisch osteuropäische Staaten. Sie dringen in die Verteidigungsministerien von Bulgarien, Polen, Ungarn und Albanien ein. Gleichzeitig attackieren sie die *New York Times*.

Und in der Nacht zum vergangenen Samstag tauchten im Schlussspurt des französischen Präsidentschaftswahlkampfs plötzlich Dokumente aus der Wahlkampfzentrale Emmanuel Macrons auf einer Website auf, Mails, Rechnungen, Budgetunterlagen – kurz vor jenem Zeitpunkt, ab dem es den Kandidaten gesetzlich nicht mehr erlaubt ist, Wahlkampf zu betreiben. Macrons Leute hatten nur noch Minuten, um eine Stellungnahme abzuschicken. Auch hinter dieser Attacke steckte Fancy Bear.

Wie arbeiten diese digitalen Einbrecher? Wie gelangten sie ins deutsche Parlament? Und werden sie in den kommenden Wochen versuchen, auch die Bundestagswahl zu beeinflussen, indem sie interne Dokumente veröffentlichen?

Es beginnt mit einer scheinbar harmlosen Mail

Am 30. April, gut eine Woche bevor Claudia Haydt ihrem Bekannten René zu schreiben versucht, erhalten mehrere Bundestagsabgeordnete gleichzeitig eine E-Mail. Die Adresse des Absenders endet auf @un.org. Die Mail sieht aus, als komme sie von den Vereinten Nationen. In Wahrheit stammt sie von den Hackern, von einem Server, den die Firewall des Bundestags nicht als problematisch erkennt. In der Betreff-Zeile heißt es: *"Ukraine conflict with Russia leaves economy in ruins"*. Der Konflikt zwischen der Ukraine und Russland ruiniert die Wirtschaft. Die Mail enthält einen Link zu einem vermeintlichen Bulletin der UN. Wer ihn anklickt, landet auf einer Internetseite, die wie eine Seite der UN anmutet, in Wahrheit aber unbemerkt eine Schadsoftware auf dem Rechner des Mailempfängers installiert, einen sogenannten Trojaner.

Wie viele Abgeordnete den Link anklicken, lässt sich nicht mehr rekonstruieren. Sicher aber ist: Die Angreifer haben mit dem Trojaner eine Art digitale Dachluke im Bundestag geöffnet. Sie sind jetzt drin im Computersystem des deutschen Parlaments.

Der Zeitpunkt des Angriffs ist nicht zufällig gewählt. Am nächsten Morgen ist der 1. Mai, Feiertag. Hinter dem Reichstag lädt der Deutsche Gewerkschaftsbund zum Tag der Arbeit und baut Hüpfburgen auf. Drinnen, im Parlament, ist nichts los. Die IT-Abteilung hat frei. Die Einbrecher können ungestört loslegen.

Nachdem sie in das System eingestiegen sind, laden sie weitere Programme ins Bundestagsnetz hoch, darunter eines, das die Arbeitsspeicher aller angeschlossenen Rechner nach Passwörtern durchkämmt. Es dauert nur ein paar Stunden, bis sie sich einen offiziellen Zugang zum Bundestagsnetz eingerichtet haben. Auf das Computersystem wirken die Angreifer jetzt wie Abgeordnete oder Mitarbeiter des Bundestags.

Den Gefahren aus der digitalen Welt fast schutzlos ausgeliefert

Eines der Programme, das sie verwenden, besteht nur aus ein paar Kommandozeilen. In der Hacker-Szene heißt es "Mimikatz", es lässt sich frei aus dem Internet herunterladen, Symbol: eine Kiwi.

Mimikatz sucht gezielt nach Administratoren-Passwörtern. Und Mimikatz ist effektiv. Diesmal dauert es zwar nicht Stunden, sondern Tage, aber dann kontrollieren die Hacker fünf der sechs Administratoren-Accounts des Bundestagsnetzwerks. Das Computersystem hält sie jetzt für Mitarbeiter der eigenen IT-Abteilung. Von nun an müssen die Einbrecher keine Türen mehr aufbrechen, sie haben einen Generalschlüssel für das Parlament. "Silver Ticket" wird diese Art von universellem Zugang in der Fachsprache genannt.

Das Netzwerk des Bundestags hat die Ausmaße einer digitalen Kleinstadt, im Frühjahr 2015 umfasst es mehr als 5,600 Computer, 500 Kopierer und 130 Drucker. Knapp 12.000 Nutzer sind registriert.

210 Techniker sind dafür zuständig, dieses Netzwerk zu warten und zu sichern. Als Claudia Haydt am 8. Mai bei ihnen anruft und von ihren Schwierigkeiten mit dem Accent aigu berichtet, haben sie von den Einbrechern in ihrer Kleinstadt noch nichts bemerkt.

Einer Sicherheitsfirma mit Büros in Großbritannien und Litauen aber ist etwas aufgefallen. Das Unternehmen beobachtet seit Längerem einen ausländischen Server, von dem aus bereits mehrere Hacker-Angriffe gesteuert wurden.

Jetzt steht dieser Server in Kontakt mit zwei Rechnern des Bundestages. Irgendetwas geht vor sich. Am 11. Mai alarmiert die Firma den deutschen Verfassungsschutz.

Am 12. Mai, dem Tag, als ein Techniker an Claudia Haydts Computer vergeblich nach einem Fehler sucht, leiten die Verfassungschützer die Warnung an den Bundestag und das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn weiter. Doch es dauert drei lange Tage, ehe die Warnung durch die Bürokratie gewandert ist. Erst am 15. Mai schickt das BSI ein Notfallteam von Bonn nach Berlin. Seit Claudia Haydts erstem Anruf ist eine Woche verstrichen.

Das BSI beschäftigt 660 Mitarbeiter, nur 15 aber besitzen das spezielle Wissen, um einen Angriff abwehren zu können, wie er gerade im Bundestag stattfindet. Diese Fachleute sind rund um die Uhr für die Sicherheit des Computersystems der Regierung zuständig. Für den Bundestag kann das BSI daher selbst in dieser Krise nur drei von ihnen entbehren.

Der Chef des Teams ist Dirk Häger, ein asketischer Beamter mit Anzug und Nickelbrille. In Berlin angekommen, machen seine Leute eine Bestandsaufnahme. Welche Systeme sind befallen? Wie tief sind die Hacker eingedrungen?

Häger lässt sich die Logdaten des Parlamentsnetzes ausdrucken. Jede Verbindung, die ein Bundestagsrechner in den vergangenen Tagen ins Internet aufgebaut hat, ist darin verzeichnet. Zeile für Zeile geht Häger die Angaben durch, liest sie, sortiert sie. "Das ist Fleißarbeit, wie bei Polizisten, die Spuren verfolgen", sagt er.

So stellt sich heraus: Die Angreifer haben so viele Computer infiltriert, dass nur noch eine radikale Maßnahme hilft. Die BSI-Leute ziehen den Stecker. Alle Rechner des Bundestages werden heruntergefahren. Auf Tausenden Bildschirmen erscheint die Nachricht, dass den Nutzern eine Minute bleibt, um Dokumente zu sichern, an denen sie gerade arbeiten. Dann werden die Bildschirme schwarz. Der Deutsche Bundestag ist jetzt offline. Nur noch so lassen sich die Eindringlinge draußen halten.

Die Abgeordneten und ihre Mitarbeiter sind schockiert. Keine E-Mail kommt mehr durch. Google funktioniert nicht mehr. Sie gehen von einem technischen Fehler aus, einem dummen Zufall. Fast niemand weiß von dem Kampf, der hinter den Kulissen tobt. Der CSU-Mann Reinhard Brandl gibt das Gefühl vieler Parlamentarier wieder: ob man nicht wenigstens fünf Minuten Vorwarnzeit hätte haben können?

Der Verfassungsschutz bietet den drei Männern vom BSI seine Hilfe an, aber das lehnen die Abgeordneten, inzwischen über den Angriff informiert, ab. Sie haben Angst, der Geheimdienst könnte sie nebenbei ausspähen. Die Bundestagsverwaltung bittet stattdessen eine private IT-Firma um Hilfe, eine Ausgründung der Universität Karlsruhe, die schon mehrfach mit dem BSI zusammengearbeitet hat. Zwei Mitarbeiter des Unternehmens durchsuchen die Server des Parlaments nach auffälliger Software.

Die Attacke hätte sich verhindern lassen

Die Eingreiftruppe des BSI versucht zu retten, was zu retten ist. Aber ihre Arbeit legt auch offen, wie unvorbereitet der Bundestag auf Gefahren des digitalen Zeitalters ist – und wie schlecht das Zusammenspiel der Behörden funktioniert.

Das BSI führt eine schwarze Liste mit weltweit etwa 160.000 als gefährlich eingestuften Servern. Da das BSI aber nur für das Computersystem der Regierung zuständig ist, nicht für das des Parlaments, hat es dieses Verzeichnis nicht an den Bundestag weitergegeben, das wird erst Monate später geschehen.

Die Bundestagstechniker haben zwar ebenfalls eine schwarze Liste, aber auf der stehen nur 5.000 Rechner. Informationen über verdächtige Server würden "den Bundestag nur verspätet oder nie erreichen", klagt der zuständige Referatsleiter der Bundestagsverwaltung.

Gegen Angreifer, die Pistolen oder Messer tragen, ist der Bundestag mit seinen Sicherheitsschleusen gut geschützt. Den Gefahren aus der digitalen Welt aber ist er fast schutzlos ausgeliefert.

"Bettina, immer schön cool bleiben!"

Wie sich später herausstellt, kannte das BSI den Server, von dem aus die Hacker agierten, sogar. Am 13. April, zwei Wochen vor dem Angriff auf den Bundestag, blockierte die Behörde alle von diesem Server stammenden Daten. Die Regierung war damit sicher, der Bundestag nicht. Hätten die Behörden früher miteinander geredet, der Angriff hätte sich verhindern lassen.

Und jetzt, da die Eindringlinge schon am Werk sind und das BSI zu helfen versucht, gehen die Probleme weiter. Weder Dirk Häger und seine Mitarbeiter noch das Unternehmen aus Karlsruhe wissen genug über das Innere des Bundestagsnetzes. Deshalb bitten sie zusätzlich einen Experten von T-Systems um Rat, einer Tochterfirma der Telekom.

Nun arbeiten also drei Mitarbeiter des BSI, zwei des Unternehmens aus Karlsruhe und einer von T-Systems daran, den Angriff der Hacker auf das deutsche Parlament abzuwehren. Sechs Männer gegen die großen Unbekannten.

Einen Tag nachdem sie den Stecker gezogen haben, lassen die IT-Spezialisten den Bundestag wieder ans Netz. Sie haben für den gesamten Datenverkehr eine kurzfristige Umleitung installiert. E-Mails und Internetkontakte des Parlaments laufen nun über das besonders gesicherte Regierungsnetz. Dieses hat nur vier Zugänge zum Internet und jeden einzelnen überwachen die BSI-Spezialisten wie Pförtner. So bekommen sie zum ersten Mal einen detaillierten Überblick, welche Daten in den Bundestag hinein- und welche aus ihm herausfließen.

Der damalige BSI-Chef Michael Hange sagt gegenüber dem Ältestenrat der Abgeordneten, die Angreifer seien "tief in den Systemen verankert und würden sich inzwischen sogar recht auffällig bewegen, da sie aus Erfahrung nicht mehr fürchten müssten, mit einfachen Mitteln entfernt zu werden".

Immerhin kann das Notfallteam einzelne Opfer der Hacker identifizieren, zum Beispiel die SPD-Abgeordneten Martin Rabanus und Bettina Hagedorn und den Bundestagsvizepräsidenten Johannes Singhammer von der CSU.

Rabanus sitzt erst seit 2013 im Bundestag, er kommt aus Fulda, sein Büro liegt im Paul-Löbe-Haus des Parlaments, ganz oben in der Ecke. Von dort aus kann er das Glasdach des Hauptbahnhofs sehen, daneben das Kanzleramt.

Ein paar Monate vor dem Angriff der Hacker, im Dezember 2014, war Rabanus mit einer Delegation des Bundestages nach Kiew und Moskau gereist. In der Ukraine hatten sich die Delegationsmitglieder mit dem Minister für Bildung und Wissenschaft getroffen und die "völkerrechtliche Annexion der Krim" gerügt, in Moskau forderten sie eine Lösung des Ukraine-Konflikts.

Nun erfährt Rabanus durch ein Telefonat mit seiner Sekretärin, dass sein Büro ausspioniert wurde. Die Bundestagsverwaltung wird ihm später mitteilen, es seien zwei Tage lang Daten vom Rechner seines Vorzimmers kopiert worden.

Der Abgeordnete ist perplex. "Ich bin nie auf die Idee gekommen, dass es bei dem Angriff gezielt um mein Büro oder um mich als Person ging", sagt er. Aber Rabanus kann sich auch vorstellen, was das Ziel des Spionageangriffs gewesen sei: "Vielleicht wollte jemand Munition sammeln, um Entscheidungsträger persönlich zu diffamieren."

Seine Fraktionskollegin Bettina Hagedorn, eine gelernte Goldschmiedin aus Schleswig-Holstein, sitzt für die SPD im Vertrauensgremium des Bundestages. Die neun Mitglieder dieser Runde sind die einzigen Abgeordneten, die wissen, wie viel Geld die deutschen Geheimdienste wofür erhalten. Hagedorn kennt die Wünsche und Projekte des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes und des Bundesamts für Verfassungsschutz.

Von Nachrichtendiensten versteht Hagedorn viel, von Computern wenig. "Technisch", sagt sie, "bin ich eine völlige Niete." Die Nachricht, dass da jemand tief in ihre Rechner eingedrungen ist, ihre Mails liest und ihre Notizen verfolgt, setzt ihr zu. Als sie von dem Einbruch erfährt, atmet sie tief durch und sagt sich: "Bettina, immer schön cool bleiben!"

In den Wochen und Monaten danach fährt Hagedorn oft nach Hause zu ihren Wählern, auf die Ostseeinsel Fehmarn etwa und in die Marmeladenstadt Bad Schwartau. Sie meidet Berlin, sosehr sie kann, vor allem den Bundestag. "Selbstschutz" nennt sie das. Mit Hagedorn ist es wie mit vielen Opfern von Wohnungseinbrüchen: Sie fühlt sich in ihren eigenen vier Wänden nicht mehr sicher. Sollte es den Angreifern darum gegangen sein, die deutschen Volksvertreter zu verunsichern, ist ihnen das bei Bettina Hagedorn gelungen.

Hatten sie es aber auf die geheimen Dokumente des Vertrauensgremiums abgesehen, sind sie gescheitert. Denn diese werden prinzipiell nicht digital verschickt, sondern per Boten, auf Papier, wie vor der Erfindung des Computers. Bettina Hagedorn musste eigens einen Tresor aus Stahl in ihrem Büro aufstellen. "Aber das konnten jene, die sich für mich interessierten, nicht ahnen", sagt sie.

Bei Bundestagsvizepräsident Johannes Singhammer standen damals, im Mai 2015, plötzlich IT-Techniker im Büro und bauten den Computer ab. Offenbar gerade noch rechtzeitig. Von seinem Rechner scheinen keine Daten abgeflossen zu sein. Singhammer ist trotzdem aufgewühlt: "Wir dürfen das in keiner Form unterschätzen."

Die Verbindung nach Moskau

Auf dem Rechner der Linkspartei-Mitarbeiterin Claudia Haydt finden die IT-Spezialisten später ein weiteres Spionageprogramm, das die Angreifer aus der Ferne installiert haben. Es nennt sich "XTunnel". Dieses Programm lässt sich nicht einfach aus dem Internet herunterladen wie Mimikatz, es wurde speziell für Attacken dieser Art programmiert. Es trägt eine Handschrift. Später wird es auch beim Hack der Demokratischen Partei in den USA eingesetzt.

Die Spur der Angreifer führt nach Moskau

Die Linkspartei bittet Claudio Guarnieri, 29, um Hilfe, einen gebürtigen Mailänder, der in Berlin lebt. Sie traut der offiziellen Untersuchung des BSI nicht. Guarnieri war früher selbst Hacker, heute arbeitet er für Amnesty International. Er hat sich in der Szene einen Namen gemacht, weil er nicht nur für die Opfer digitaler Überwachung streitet, sondern auch Spähprogramme mit der kühlen Präzision eines Gerichtspathologen sezieren kann.

Er durchsucht die beiden befallenen Rechner der Linkspartei.

Neben dem Programm XTunnel entdeckt Guarnieri eine weitere Software, die die Eindringlinge nutzten. Er zerlegt sie in ihre Einzelteile. In einer Kommandozeile stößt er auf die Adresse des Servers, von dem aus die Angriffe gesteuert, die E-Mails verschickt, die Schadprogramme installiert wurden: 176.31.112.10.

Im Internet erhält jeder Rechner eine individuelle Zahlenkombination, IP-Adresse genannt, ähnlich einem Autokennzeichen. Die IP-Adresse 176.31.112.10 ist zum Zeitpunkt des Berliner Angriffs bei dem französischen Internet-Unternehmen OVH in Paris registriert, unweit der Seine. Guarnieri findet jedoch heraus, dass die Franzosen einen Untermieter haben: Tatsächlich verwaltet den Server eine pakistanische Firma aus der Kleinstadt Kakra Town, südöstlich von Islamabad.

Den Ermittlungen deutscher Sicherheitsbehörden zufolge tarnt sich der Server bei seiner Kommunikation mit dem Bundestag unter dem Namen bitcoin-dns.hosting – der Name soll unverdächtig klingen, als handele es sich um einen Anbieter der Internet-Währung Bitcoin. Auch dieser Rechner ist später am Angriff auf die US-Demokraten beteiligt, außerdem am Hack der internationalen Anti-Doping-Agentur Wada sowie an einem gescheiterten Angriff auf die Berliner CDU-Parteizentrale im April und Mai 2016. Heute ist er abgeschaltet.

Ein Server in Paris, eine Firma in Islamabad – von wo aus werden die Attacken wirklich gesteuert?

Es fällt auf, dass alle Attacken den außenpolitischen Interessen Russlands dienten. Das allein ist noch kein Beleg, dass Fancy Bear von Moskau aus operiert. Auch die Spuren, die die Hacker im Bundestag hinterlassen, sind nur Indizien, keine Beweise, die vor einem Gericht Bestand hätten. Und doch sind dem schicken Bären über die Jahre mehrere Fehler unterlaufen.

Einer der Server, den die Gruppe für ihre Angriffe benutzt, lässt sich laut deutschen Geheimdiensten auf einen Russen zurückführen, den die Ermittler für einen Strohmann des russischen Militärgeheimdienstes GRU halten.

In einem Excel-Dokument aus dem Macron-Hack taucht in den Metadaten, also jenen Informationen, die anzeigen, wer ein Dokument bearbeitet hat, der Name Georgi Petrowitsch Roschka auf. Roschka, ein junger Russe, arbeitet offenbar für eine Moskauer Sicherheitsfirma namens Eureka CJSC, die enge Kontakte zu den russischen Geheimdiensten und dem Militär unterhält. Eine Mail der *ZEIT* an Roschka mit Bitte um Stellungnahme blieb unbeantwortet.

Bei einem früheren Angriff von Fancy Bear geschah etwas Unerwartetes: Die Menge an gestohlenen Daten war so groß, dass sie über einen Cloud-Server umgeleitet werden musste. Zeitweise, berichten IT-Experten, sei keine Verschlüsselung aktiv gewesen. Plötzlich gab es eine offene Verbindung – in den Nordosten Moskaus, wo auch der russische Geheimdienst GRU residiert, in einem Gebäudekomplex, der intern "Aquarium" genannt wird. Das Programm, mit dem die Angreifer damals die Daten nach Moskau abtransportierten, war einer der Schädlinge, der auch auf den Rechnern des Bundestags und der US-Demokraten gefunden wurde.

Der GRU ist der wohl mächtigste russische Nachrichtendienst, sein Chef Igor Korobow, ein bulliger General, zählt zu den Beratern von Staatschef Wladimir Putin. Unter den GRU-Mitarbeitern kursiert ein Bonmot, das viel über das Selbstverständnis des Geheimdienstes aussagt. Welche Fischarten schwimmen im "Aquarium"? Nur eine. Piranhas.

Als die neue Geheimdienstzentrale am nordwestlichen Stadtrand Moskaus 2006 eingeweiht wurde, landete Putin mit einem Hubschrauber auf einem Heliport, der das Dach des Hauptquartiers krönt. Bilder des russischen Staatsfernsehens zeigen den ehemaligen KGB-Mann Putin, wie ihm ein vermummter Agent in Tarnuniform eine Pistole reicht. Lässig tritt der Staatschef auf den Schießstand, die linke Hand in der Hosentasche seines Anzugs, hebt die Waffe und feuert einhändig auf die Zielscheibe. Einmal Geheimdienst, immer Geheimdienst.

Die Agenten des GRU seien "Augen und Ohren" des russischen Militärs rund um den Globus, sagte Putin damals.

1996 erklärte der damalige Chef des amerikanischen Geheimdienstes NSA "die Kontrolle der Informationstechnologien" zum "Schlüssel zur Macht im 21. Jahrhundert". Wenig später infiltrierten die Russen erstmals online die amerikanische Navy, das US-Energieministerium sowie die Nasa. Die Operation ging unter dem Codenamen "Moonlight Maze" in die Geschichte ein.

Im Februar 2013 skizzierte der Generalstabschef der russischen Streitkräfte, Waleri Wassiljewitsch Gerassimow in einem Aufsatz seine Vision einer modernen Armee. Politische Ziele, so Gerassimow, seien im vernetzten Zeitalter nicht mehr nur mit konventioneller militärischer Macht zu erreichen, sondern durch den "breit gestreuten Einsatz von Desinformation", die das Protestpotenzial der Bevölkerung verstärken solle – zum Beispiel durch geleakte Dokumente.

Für die einstige Weltmacht Russland bietet das Internet optimale Möglichkeiten der politischen Einflussnahme. Ein instabiler Westen, dessen Widersprüche durch veröffentlichte Interna der Eliten offen zutage treten, hilft dem Kreml nicht nur politisch, sondern auch moralisch. Schmutzige Details wie jene über Hillary Clintons Auftritte vor Großbanken erleichtern es Putin, die Vorhaltungen des Westens über vermeintliche Demokratiedefizite zu kontern. Seine Botschaft: Kommt uns nicht mit Vorträgen über Menschenrechte und Demokratie, schaut lieber, wie es um euer eigenes Haus bestellt ist.

Eine Destabilisierung der Europäischen Union, die noch immer auf Sanktionen gegen Moskau beharrt, würde eine Verschiebung der geopolitischen Koordinaten zugunsten Russlands bedeuten. Donald Trump hat die Aussöhnung mit Russland zu einem seiner wichtigsten außenpolitischen Anliegen erklärt. Marine Le Pen möchte die EU erklärtermaßen "zerstören" und Frankreich aus der Westbindung lösen.

Direkt vom Kreml autorisiert

Aus russischer Sicht gab es also viele Gründe, aufseiten Trumps und Le Pens in den Wahlkampf einzugreifen, auch wenn es in Frankreich nicht für einen Sieg gereicht hat. "Der Westen hat noch immer nicht verstanden, welche Möglichkeiten der Cyberspace bietet", sagt Dmitri Alperowitsch.

Alperowitsch ist ein kleiner, kräftiger Mann mit blondem Seitenscheitel, der an diesem Abend in einem zu weit geschnittenen sandfarbenen Anzug an der Bar eines Münchner Hotels steht. Alperowitsch verfolgt die Bewegungen der russischen Nachrichtendienste im Internet seit 2007. Er ist es, der der russischen Hacker-Gruppe den Namen "Fancy Bear" gab.

Alperowitsch wurde in Moskau geboren, er war 13 Jahre alt, als seine Eltern in die USA auswanderten. Heute ist er Mitte 30, sein genaues Alter will er nicht verraten. Er fürchtet, die Russen könnten seine persönlichen Daten für einen Spionageangriff nutzen. Mit einem Geburtsdatum, kombiniert mit Details wie der amerikanischen Sozialversicherungsnummer, könne man online viel Schaden anrichten.

Als im Frühjahr 2016 der Verdacht aufkam, die Demokratische Partei in Washington könnte gehackt worden sein, riefen die Demokraten nicht das FBI. Sie riefen Alperowitsch und dessen IT-Unternehmen CrowdStrike. Trump hat CrowdStrike dafür mehrfach öffentlich als eine Firma diffamiert, "über die viele schlechte Dinge" im Umlauf seien.

Sechs Wochen lang kämpften Alperowitschs Leute damals mit Fancy Bear. Der Angriff ähnelte dem Bundestagshack.

Mehrere Tausend Mitarbeiter seien im "Aquarium", der Zentrale des GRU, in Online-Operationen wie jene in Washington und Berlin eingebunden, schätzt Alperowitsch. Das Internet hat eine neue Form der Spionageindustrie geschaffen.

Vermutlich haben selbst die Russen nicht daran geglaubt, dass Trump tatsächlich die Wahl gewinnen könnte. Aber mittlerweile, das hört Alperowitsch von seinen russischen Kontakten, seien sie in Moskau überzeugt davon, den Ausgang der Wahl tatsächlich zugunsten von Trump beeinflusst zu haben.

Nun hat Clinton in erster Linie nicht wegen Fancy Bear verloren, sondern weil sie einen schlechten Wahlkampf führte. Aber das Durchsickern von Mails aus ihrem Stab trug im vergangenen Herbst dazu bei, die Stimmung im Land zu drehen. "Die historische Lektion für Putin lautet: Du kannst es tun, und du kommst damit durch", sagt Alperowitsch.

Gilt das auch für Deutschland?

Der Abwehrkampf der BSI-Leute dauert bis zum 20. Mai 2015. Rechner für Rechner beseitigen sie die Schadprogramme. Die Diebe erbeuten noch am letzten Tag Daten aus dem Büro des SPD-Abgeordneten Martin Rabanus.

Bei den meisten ausspionierten Abgeordneten gibt es eine Erklärung, warum sie für Hacker aus Russland interessant sein könnten. Martin Rabanus war kurz zuvor in Kiew und Moskau. Bettina Hagedorn verfügt über Geheimwissen der deutschen Nachrichtendienste. Johannes Singhammer hat als Vizepräsident des Bundestags Einblick in viele interne Vorgänge. Inge Höger von der Linkspartei gilt als Sympathisantin Moskaus. Die Kanzlerin ist immer interessant, auch wenn es sich nur um ihr Abgeordnetenbüro handelt. Trotzdem ist es überraschend, dass die Angreifer nicht in die Rechner sämtlicher Mitglieder des Auswärtigen Ausschusses eingedrungen sind. Auch die Fraktionschefs wurden nicht gehackt.

Oder vielleicht doch?

Als das Rettungsteam des BSI auf den Plan trat, waren die Hacker schon seit zwei Wochen am Werk. Der Verkehr im Bundestagsnetz wird aber nur für sieben Tage protokolliert. Danach verschwinden die Daten. Was in den ersten Tagen des Einbruchs genau geschah, weiß niemand.

Es lässt sich nicht rekonstruieren, welche Abgeordneten oder Mitarbeiter den vermeintlichen Link der Vereinten Nationen anklickten, mit dem der Angriff begann. Und es ist nicht bekannt, wie viele Rechner die Hacker letztlich durchkämmten. Bei 16 Abgeordneten ist sich das BSI sicher, dass ihre Büros infiziert wurden, an mindestens 25 Orten installierten die Angreifer Schadsoftware. Die gestohlenen Daten, 16 Gigabyte, wurden an neun über die ganze Welt verstreute Server übertragen.

Da die Daten verschlüsselt verschickt wurden, wissen die Ermittler bis heute nicht, was alles abfloss. Zumindest sind sie sicher, dass "gezielt nach lokal abgelegten Outlook-Dateien" sowie Office-Dokumenten gesucht wurde.

"Die abgeflossenen Daten", sagt Dirk Häger, der BSI-Notfallchef, seien "in erster Linie komplette Mailpostfächer gewesen". Was die Abgeordneten in ihren Mails geschrieben haben, wissen nur sie selbst. Und die Hacker.

Wie soll die Bundesregierung reagieren?

Im Januar 2016, rund zwei Monate nachdem das BSI seine Untersuchung abgeschlossen hat, bitten Merkels Leute zu einer Besprechung ins Kanzleramt. Eingeladen ist neben dem Bundesnachrichtendienst (BND) und dem Verfassungsschutz auch das Bundesinnenministerium, später stoßen das Auswärtige Amt und das Verteidigungsministerium hinzu. Es geht um die Frage, wie Deutschland auf den Angriff der russischen Hacker reagieren soll.

Die Geheimdienste werden beauftragt, ein Lagebild über Russlands Konfrontationskurs zu erstellen, Merkel persönlich will die Hintergründe wissen. Kurz vor Weihnachten 2016 präsentieren BND und Verfassungsschutz ein "amtlich geheim gehaltenes" Dossier. Darin steht, es sei "festzustellen, dass das moderne Russland Beeinflussungsaktivitäten gegen den Westen zentral koordiniert". Cyber-Operationen wie gegen den Bundestag, "welche Beeinflussung, vermutlich auch Desinformation und Propaganda in großem Stil als Ziel haben", dürften "direkt von der Präsidialadministration im Kreml autorisiert und zur Durchführung den Diensten überlassen werden". Anders gesagt: Die deutschen Geheimdienste sind überzeugt, hinter Fancy Bear steht Wladimir Putin.

Welche Optionen hat die Bundesregierung? Höhere, bessere digitale Mauern? Mehr Wachpersonal beim BSI? Oder sogar Gegenschläge? Letzteres könnte einen Cyberkrieg mit den Russen entfesseln. In einer solchen Form der Auseinandersetzung hat Deutschland keine Erfahrung und wäre hoffnungslos unterlegen. Darüber nachgedacht wird trotzdem.

Schlägt Deutschland zurück?

Das Auswärtige Amt bewertet den Bundestagshack "als eine Verletzung der Souveränität Deutschlands, wenn nicht sogar als einen Versuch der Einmischung in die inneren Angelegenheiten des Landes". So formuliert es Dirk Roland Haupt, der im Auswärtigen Amt für Cyber-Außenpolitik zuständig ist. Wenn der Angriff eindeutig einem Staat zugerechnet werden könne, argumentiert Haupt, "dann hätte Deutschland das Recht auf Gegenmaßnahmen". Intern läuft die Diskussion in der Bundesregierung unter dem Stichwort "Hackback".

Schlägt Deutschland zurück?

Das Auswärtige Amt legt seine Einschätzung der Kanzlerin vor, aber Merkel und ihr Kanzleramtschef Peter Altmaier entscheiden sich gegen Vergeltungsschläge. Niemand weiß, wie Putin reagieren würde.

Ende März 2017 allerdings beschließt der Bundessicherheitsrat, dem neben dem Kanzleramt die wichtigsten Ministerien angehören, ein Gesetz für digitale Gegenschläge zu erarbeiten, für künftige Fälle.

Auch bei dem Geheimdienst-Dossier, das den Kreml als Drahtzieher benennt, macht das Kanzleramt einen Rückzieher. Eigentlich sollte es in einer gekürzten Fassung veröffentlicht werden, die Bundesregierung wollte ein deutliches Signal nach Moskau senden. Aber mittlerweile ist Donald Trump im Weißen Haus eingezogen, es ist nicht mehr ganz klar, wo Deutschlands Freunde sitzen und wo seine Feinde. Altmaier will keine weitere Eskalation. Das Dossier bleibt unter Verschluss.

Stattdessen überbringt ein Emissär des Kanzleramts bei einem Besuch in Moskau eine Warnung: Die Deutschen würden die Spionage nicht länger hinnehmen. Die Russen weisen alle Anschuldigungen zurück.

Heute, zwei Jahre nach dem Angriff, belastet der Bundestagshack noch immer die deutsch-russischen Beziehungen. In der vergangenen Woche flog Merkel zum ersten Mal wieder nach Russland. In Putins Sommerresidenz in Sotschi sprach sie das Thema erneut an. Russland mische sich "nie in die inneren Angelegenheiten anderer Staaten ein", antwortete ein kalt lächelnder Putin.

Sie gehe davon aus, "dass die deutschen Parteien ihren Wahlkampf untereinander ausmachen können", entgegnete Merkel spitz.

Noch ist aus dem gestohlenen Datenpaket nichts aufgetaucht, "aber wir warten darauf", sagt Andreas Könen, Leiter des Bereichs Cybersicherheit im Bundesinnenministerium. Oft sind es in einer E-Mail geäußerte Halbsätze über Kollegen, die öffentlich große Wellen schlagen. Oder unzulässig verwendete Gelder, von denen ein Schriftverkehr handelt.

Werden solche Worte, solche Zahlen demnächst auch in Deutschland auftauchen, von den Russen an die Öffentlichkeit gebracht?

Der Wahlkampf könne schmutzig werden, so hat Merkel ihre Kollegen im CDU-Präsidium neulich gewarnt.

Vielleicht kommen die Daten aber auch nie wieder ans Licht, vielleicht sind die E-Mails, die sich deutsche Abgeordnete schreiben, schlicht zu langweilig. Im Vergleich zu Washington, wo politische Verschwörungen an der Tagesordnung sind, wirkt das politische Berlin manchmal wie ein Freizeitheim. Vielleicht haben die Russen derzeit auch kein Interesse, die Debatte weiter anzuheizen.

Wahrscheinlich ist, dass die Spione all die Mails, Word-Dokumente und PDF-Dateien aus dem Bundestag längst ausgeschlachtet haben, um neue Spionageziele zu identifizieren. Seit vergangenem Jahr soll der GRU mehr als 70 neue Cyber-Angriffe in Deutschland verübt haben. In mehreren Wellen griff Fancy Bear am 15. und 24. August vergangenen Jahres die SPD-Fraktion im Bundestag an, die Linkspartei und den Landesverband Saar der CDU. Auch die grüne Bundestagsabgeordnete Marieluise Beck wurde attackiert. Die Bären sind längst auf der Suche nach neuen Opfern.

Der digitale Einbruch im deutschen Parlament sei ein "Weckruf" gewesen, sagt der neue BSI-Präsident Arne Schönbohm. "Nun können wir uns auf das nächste Mal vorbereiten."

Schönbohm sagt nicht: Nun *sind* wir vorbereitet. Und das offenbar mit gutem Grund. Denn Anfang 2017 untersuchte die Firma secunet Security Networks im Auftrag des Bundestags das Parlamentsnetz. In einem als geheim eingestuften Bericht, den die *ZEIT* einsehen konnte, simulierte sie ein ähnliches Szenario wie vor zwei Jahren und kam zu dem Ergebnis, dass sich ein Angreifer unter Umständen noch immer "ungestört im Netz bewegen und Informationen beschaffen" könne. Noch immer gebe es ungesicherte Zugänge über die USB-Anschlüsse, die "ein Einfallstor für Malware und die Möglichkeit darstellen, Informationen abfließen zu lassen". Und noch immer seien viele der Datenleitungen im Bundestag nicht verschlüsselt.

Hinter der Geschichte Merkel und der schicke Bär

Ausgangsfragen: Wer sind die Hacker, die 2015 den Bundestag ausspionierten? Wie gingen sie vor? Und steht Deutschland ähnlich wie den USA eine Beeinflussung des Wahlkampfs durch geleakte Dokumente bevor?

Die Recherche: Vier Monate lang wertete ein ZEIT-Team Unterlagen des Bundestages aus. Die Reporter hatten ebenfalls Einsicht in teils geheime Dokumente der Sicherheitsbehörden. Sie sprachen mit betroffenen Abgeordneten und ihren Assistenten, interviewten deutsche und amerikanische IT-Experten, analysierten die Codierung der Schadsoftware und befragten Regierungsmitarbeiter.

Das Fazit: Im Internet ist die Beweisführung schwer, aber viele Spuren führen nach Russland. Ein deutscher Geheimdienstbericht macht sogar den Kreml direkt verantwortlich.

In Washington veröffentlichten die Angreifer einen Teil ihrer Informationen aus der Demokratischen Partei via WikiLeaks, andere Teile auf einer Seite namens dcleaks.com, die sie eigens dafür eingerichtet hatten. In Frankreich, wo es um Macrons Bewegung En Marche ging, traten sie als "emleaks" auf.

Vor ein paar Monaten, am 13. Januar, haben Unbekannte eine Seite namens btleaks.com registriert, der Name steht womöglich für "Bundestags-Leaks".

Noch ist sie nicht ans Netz gegangen.

Mitarbeit: Alice Bota

Kommentar

In Sachen Datensicherheit verwies Innenminister de Maizière 2014 auf die "Eigenverantwortung des mündigen Bürgers". Und wenn es nicht klappt: Heulen und auf den Russen deuten, das kommt bei weiten Teilen der Bevölkerung zunehmend besser an. Löst natürlich kein Problem. Wir sollten uns die Frage stellen, wie jemand den Bundestag hacken konnte. Sind unser IT-Experten am Ende vielleicht die teuersten, aber deshalb noch lange nicht die besten? Was kann Russland bieten, was Deutschland nicht bieten kann?

[1)] http://www.zeit.de/digital/datenschutz/2015-05/hackerangriff-bundestag-sommerpause