Kampfesstimmung im Westen: Linke Antifaschisten in Paris geraten nach der ersten Präsidentenwahlrunde mit der Polizei aneinander. FOTO: AFP PHOTO / T. SAMSON

Endziel: Chaos

Die Hacker-Jägerin Laura Galante über die Angriffe gegen Emmanuel Macron, den Bundestag, die Demokratische Partei in den USA und was Putin mit all dem bezweckt

INTERVIEW: ANDRIAN KREYE

Nur mal für den Kontext, wer sich hinter dem bürokratischen Wort „Cybersicherheitsexpertin“ verbirgt – im Kalten Krieg wäre Laura Galante eine prima James-Bond-Figur gewesen, die feindliche Spione zur Strecke bringt. Nur dass solche Jägerinnen heute nicht mehr durch neblige Metropolen und exotische Länder schleichen, sondern sich in die Tiefen hochkomplexer Computercodes vorarbeiten. Als Direktor für „Global Intelligence“ der Firma FireEye kommandierte sie die Mannschaften, die erst die chinesischen Wirtschaftsspione und dann die russischen Hackertruppen Fancy Bear (APT28) und Cozy Bear (APT29) überführten. Das Gespräch fand vor einer Woche während der Ted Conference in Vancouver statt. Die Fragen zu Macron wurden an diesem Wochenende per E-Mail geklärt.

SZ: Hat Sie der Macron-Hack überrascht?
Laura Galante: Der war schon sehr dreist. Aber – nein. Die zögerlichen Reaktionen der USA auf die Angriffe dort waren allerdings auch nicht besonders abschreckend.

Was wissen Sie denn über den Macron-Hack?
Die Firma Trend Micro hat festgestellt, dass die Hackergruppe Pawn Storm dahintersteckt. Das ist dieselbe Gruppe wie APT28, die der russischen Regierung nahestehen und die man auch als „Cozy Bear“ kennt. Ansonsten weiß ich bisher auch nur, was in den Medien steht.

Die Angriffe in den USA auf die Demokratische Partei? Spuren weisen nach Russland

Wie lange dauert es, bis man Angreifer identifizieren kann?
Das kommt darauf an, wie viele Schadprogramme man sicherstellen kann.

Als eine Bedrohung im Cyberkrieg galt bisher, dass man die Angreifer nicht erkennen kann. Hat sich das geändert?
Ja, da haben wir in den letzten fünf Jahren enorme Fortschritte gebracht. Die kritische Masse haben diese neuen Methoden 2013 erreicht, als China der Industriespionage überführt wurde. Da war unser Team damals daran beteiligt.

Was sind das für Methoden?
Nach einem Hack oder einem Datendiebstahl schaut man erst einmal nach, was für Programme die Gegenseite benutzt hat. Wenn Angreifer beharrlich über längere Zeit arbeiten, werden sie zwar ihre IP-Adressen immer wieder ändern. Das sind die digitalen Äquivalente zu Briefkästen. Aber sie können nicht jedes Mal ihre gesamte Operation verändern. Da sucht man dann eben nach gemeinsamen Nennern. Und weil die chinesischen Hackergruppen damals so überaus produktiv waren, haben sie auch eine große Menge brauchbarer forensischer Spuren hinterlassen.

Wie produktiv waren die denn?
Das war wirklich erstaunlich, was die da zwischen ungefähr 2010 und Mitte 2013 alles gemacht haben. Das waren mehrere Einbrüche bei Fortune, 500-Firmen pro Tag. Alles geistiger Diebstahl. Die haben damals viel über grüne Energie gestohlen und was sonst noch in ihren damaligen Fünfjahresplan gepasst hat.

Dann waren das Hacker der chinesischen Regierung?
Ja, das war die Volksbefreiungsarmee, vor allem die PLA-Einheit 61398.
Wie haben Sie die denn überführt?
Zunächst sind es Fehler, durch die Hacker Spuren hinterlassen. Und bei einem solchen Volumen unterlaufen denen immer Fehler. So haben wir in mühsamer Kleinarbeit Details sammeln können.

Was sind das für Fehler?
Kleinigkeiten wie Zeitmarken. Die chinesischen Hackergruppen tauschten ihre Werkzeuge immer wieder untereinander aus. Da fanden sich dann immer wieder die Zeitzonen von Peking und Shanghai. Oder man fand im Code Spracheinstellungen für Mandarin. Oder sogar ISPs in Shanghai. Man geht da genauso vor, wie bei regulären Schadprogrammen. Man schaut sich das nicht an und sagt, ich glaube, das kommt aus China. Man fragt sich, was bedeutet dieser Code denn überhaupt? Dann baut man den nach und findet so all die kleinen Details, die man dann zusammensetzen kann.
Und dann?
Irgendwann konnten wir die Chinesen konfrontieren: Schauen Sie, wenn Sie uns erklären können, warum Tausende Hacker in Shanghai das tun, dann erklären Sie uns das mal, hier ist die Beweislage. Nach dem Druck aus dem Westen haben sie ihre Aktivitäten massiv zurückgefahren. Eigentlich arbeiten sie nur noch gegen Dissidenten.

Warum machen Hackergruppen denn solche Fehler? Warum ändern die ihre Codes nicht einfach gründlicher?
Das kann man sich bei APT28 auch fragen. Am besten vergleicht man das mit Silicon Valley. Es dauert Jahre, bis das große Softwarepaket eines Konzerns in einer neuen, überarbeiteten Version auf den Markt kommt. Es ist ein ungeheuerer Aufwand an Zeit und Ressourcen, eine komplette Codebase zu verändern. APT28 haben ihre Codebase zum Beispiel 2007 geschrieben. Die ist jetzt wie das Chassis eines Autos. Das wird immer wieder benutzt.

Und das erkennen Sie immer wieder?
Ja.
Wenn man Hacks inzwischen so klar beweisen kann, wieso hat noch jemand Zweifel daran, dass die Russen während des US-Wahlkampfes die Dateien der Demokratischen Partei gehackt haben?
In der Sicherheitsindustrie zweifelt niemand daran, dass das die russischen Gruppen APT28 und APT29 waren. Man hat APT28-Schadprogramme gefunden. Und niemand, der sich die Datensätze angesehen hat, zweifelt ernsthaft daran, dass APT28 gleichbedeutend mit der russischen Regierung sind. Die Firma Crowdstrike hat die Untersuchungen damals geleitet und die Schadprogramme damals vier, fünf anderen Firmen gegeben. Unter

Die Juristin **Laura Galante** (31) war Direktorin der Abteilung für globale Informationsbeschaffung bei der Sicherheitsfirma FireEye. Nun hat sie nahe Washington die Firma Galante Strategies gegründet, die auch Regierungen berät. FOTO: OH

anderem uns. Wir haben uns das angeschaut und haben herausgefunden, dass sich die Programme mit denen decken, die wir von APT28 kannten. Diese Programme sind auch nie im nicht staatlichen Hacker-Untergrund zirkuliert. Die wurden wirklich nur von APT28 eingesetzt.

Bauen Sie eine Datenbank mit digitalen Fingerabdrücken wie von APT28 auf?
Ja, das ist allerdings eine kollektive Anstrengung von Forschungseinrichtungen, Regierungen, Geheimdiensten und Strafverfolgungsbehörden. FireEye gehört da dazu, Semantic, CrowdStrike, TrendMicro, bei Ihnen sind das der Bundesnachrichtendienst, der Verfassungsschutz.
Nutzen die das schon?
Ja natürlich. Als die deutsche Regierung im Dezember verkündete, dass in Rechner des Bundestages und der CDU eingebrochen wurde, haben sie sich auf APT28 bezogen. Genauso wie die französischen Behörden nach dem Angriff auf den Fernsehsender TV5 Monde. Obwohl es da zunächst Bekennerschreiben des IS gab. Das war ein besonders interessanter Fall.
Wieso?
Niemand weiß bisher, wie genau das ablief. Aber APT28 hat es im Mai 2015 geschafft, TV5 Monde komplett lahmzulegen – den Sender selbst, seine Webpräsenz. Und dann posteten sie die Verkündung eines Cyber-Kalifats im Namen des IS. Das war der erste destruktive Cyberangriff unter falscher Flagge. Auch wenn alle Spuren dann zu APT28 führten.

Was war die Motivation?
Die meisten Experten glauben, dass das nur ein Versuchsballon war, auch um zu beweisen, dass sie sich trauen, Aktionen in Frankreich zu lancieren.

Was sie dann auch getan haben. War der Macron-Hack dann die nächste Aktion?
Nein, zunächst waren es die selben Methoden wie im amerikanischen Wahlkampf. Sie haben mit Strohmanngruppen die Narrative gepusht, die sich gegen Macron gerichtet haben. Sie haben aber eben nicht Le Pen unterstützt. Die Taktik ist eher, dass sie das gesamte politische System so weit schwächen, dass sich die Wähler irgendwann nach einem starken Mann sehnen. In diesem Fall eben nach einer starken Frau.

Und jetzt der Macron-Hack. Mit dem strategisch brillanten Zeitpunkt kurz vor dem Informations-Blackout, den das französischen Wahlgesetz vorschreibt. Sind Hackergruppen inzwischen strategisch so gewitzt?
Diese Gruppen, vor allem APT28, zeigen kontinuierlich, dass sie die politische Landschaft ihrer Zielländer sehr gut kennen. Was der Öffentlichkeit nicht so bewusst ist, ist, wer die Befehle gibt, solche gehackten E-Mail-Konvolute zu veröffentlichen.

Wer gibt diese Befehle denn?
Operationen der russischen Regierung in Europa verlangen zumindest nach Zustimmung auf allerhöchster Ebene. „Rechtzeitig“ ist in Papieren des russischen Militärs und der russischen Regierung ein häufiger Begriff, wenn es um die Anwendung von Informationsstrategien geht. Das sehen wir nun am verheerenden Beispiel Macron.

Warum wird immer wieder Wikileaks bei solchen Hacks vorgeschoben?
Die werden sich im Kreml schon überlegt haben, wie solche Informationen am breitflächigsten angenommen werden. Das ist ja das Geniale und das Beängstigende an Wikileaks. Journalisten können die einfach als Quelle angeben und dann alles aufschreiben. Ich nehme an, dass die russischen Geheimdienste erkannt haben, dass Wikileaks von westlichen Medien als legitime Quelle angesehen wird. Mit Julian Assange, der jetzt schon so lange in der ecuadorianischen Botschaft sitzt.

Aber all diese Leaks sind keine Fake News, die die Debatte in den vergangenen Monaten so bestimmt haben.
Nein, die Dateien aus der Parteileitung der Demokraten waren authentisch. Aber Fake News und Leaks sind Teil der russischen Strategie der „reflexive control“. Letztlich geht es darum, Zielpersonen oder ganze Bevölkerungen dazu zu bringen, von sich aus so zu denken, wie man das haben will.

Nutzen westliche Geheimdienste und Regierungen das denn auch?
Nein, die russischen Staatsorgane können sehr viel flexibler operieren. Nach dem westlichen Modell bekommt ein Soldat einen Auftrag, den er erfüllt, da wird nicht lange darüber nachgedacht, was das übergeordnete Ziel ist. Da sind die Werkzeuge, da ist der Auftrag. Russische Organe überlegen sich dagegen erst, was das Endziel ist und dann erst, wie sie das erreichen.

Das klingt aber sehr viel wirkungsvoller. Warum setzen westliche Staaten das nicht auch ein?
Weil das in jeder Hinsicht unethisch, verfassungsfeindlich und illegal wäre. Das funktioniert nur in Staaten, die bereit sind, jedes nur mögliche Mittel einzusetzen.

Was ist denn Putins Ziel in Ländern wie den USA, Frankreich oder Deutschland?
Es geht zunächst einmal darum, Chaos zu verursachen. Trump verursacht zum Beispiel in der amerikanischen Politik vor allem Chaos. Er steht aber auch für die Zweifel an der Elite und zeigt, dass das gesamte westliche Modell korrumpiert ist. Das kann er dann wiederum für sich nutzen.

Dann war die Wahl Trumps so etwas wie ein Regimewechsel?

Es geht nicht nur um Daten und Meinungen, sondern auch um Rohstoffe, Energie und um Finanzpolitik

Ich glaube nicht, dass Putin Regimewechsel in den USA will. Das geht zu weit. Nein, wenn er Stück für Stück die westlichen Demokratien aushöhlen kann, wenn er das Leuchtfeuer der Demokratie dämpfen und die moralische Deutungshoheit des Westens schwächen kann, reicht das schon.

Aber hat er nicht geholfen, Trump an die Macht zu bringen? Zum Beispiel mit den geleakten Mails, die FBI-Direktor Comey wenige Tage vor der US-Wahl veröffentlichte? So wie nun in Frankreich die Macron-Mails kurz vor der Wahl herauskommen?
Wahlergebnisse haben so viele Faktoren. Die Leute haben Hillary Clinton ja wirklich nicht leiden können. Wie viel Prozent Anteil die Comey-Leaks an Trumps Sieg hatten? Wirklich schwer zu sagen.

All diese Leaks sind aber, wie Sie sagen, authentisch. Wie soll denn die Presse damit umgehen? Es ist ja ihre Kernaufgabe, Dokumente zu veröffentlichen.
Da kommt eine neue Aufgabe auf die Medien zu. Es geht nicht mehr nur darum, solche Inhalte zu veröffentlichen. Es gehört genauso zu einer Geschichte, wer solche Fakten veröffentlicht und wann.

Um die Mechanismen der „reflexive control“ aufzuzeigen?
Das ist der Anfang. Aber was sind denn die Ziele hinter Putins Ziel, den Westen dumm dastehen zu lassen? Das steckt zum einen in seiner Millenniums-Botschaft vom Silvesterabend 1999, als er seinen Etatismus definierte. Da ist kein Platz für Demokratie daneben. Auf der anderen Seite geht es natürlich auch um Finanzpolitik, um Energie und Rohstoffe. Wir sollten nicht nur den Cyberkrieg untersuchen, sondern das große Panorama, wie unkalkulierbar der russische Staat seine Interessen mit „reflexive control“ durchsetzt. Es würde sicher schon helfen, wenn sich der Westen von seinen Abhängigkeiten von Russland befreit. Vor allem in Energiefragen.

Noch ein Tipp für die Bundestagswahl?
Ich fand das geschickt, wie der Bundesnachrichtendienst im Dezember die Flucht nach vorne angetreten und verkündet hat, schaut, APT28 hat uns kompromittiert. Das und das wird nun herauskommen. Das ist die beste Verteidigung. Das ist ein bisschen wie ein Zauberer, der seinen Trick verrät. Der Überraschungsmoment ist vorbei. Man schaut sich das vielleicht noch an, aber man lässt sich davon nicht mehr verstören. Wenn ich Merkel wäre, würde ich Standleitungen zu allen deutschen Zeitungen und Medien einrichten und sie über alles, aber auch wirklich alles informieren. Davon mal abgesehen, wird man den digitalen Schutz ausbauen müssen. Sie brauchen digitale Grenzschützer.

Bühne des Bundes

An diesem Montag wird der Hauptstadtfinanzierungsvertrag unterzeichnet. Die Berliner Kultur bekommt zusätzliche Millionen

Berlin kann sich wieder einmal über Bundesmillionen freuen, mehr Geld für die Sicherheit und mehr Geld für Kultur. Zusätzlich zu den vielen Einrichtungen in der Stadt, die der Bund bereits seit Jahren fördert – von der Akademie der Künste über die Stiftung Deutsche Kinemathek bis hin zum Martin-Gropius-Bau, dem Haus der Kulturen der Welt und der Stiftung Jüdisches Museum – wird nun auch die Barenboim-Said-Akademie institutionell gefördert. An diesem Montag wird der Hauptstadtfinanzierungsvertrag dazu unterzeichnet.

Aber das ist längst noch nicht alles an Förderungen. Die Opernstiftung, einst gegründet, um alle drei Opernhäuser zu erhalten, erhält ab dem Jahr 2018 zehn Millionen Euro vom Bund. Der Hauptstadtkulturfonds zur Förderung wichtiger Projekte gesamtstaatlicher Repräsentation in Berlin wird mit 15 Millionen Euro jährlich ausgestattet. Bislang waren es knapp zehn Millionen. Außerdem beteiligt sich der Bund in Zukunft an der bisher allein vom Land Berlin getragenen Stiftung Berliner Philharmoniker. Vorgesehen ist ein Bundeszuschuss von 7,5 Millionen Euro jährlich. Der Bund tritt dem Stiftungsbeirat bei. Gegen seine Stimme kann in Budgetfragen künftig nichts entschieden werden. Auch im Humboldt-Forum entlastet der Bund die Stadt. Berlin muss sich nicht an den Umzugs- und Betriebskosten für die Flächen der Stiftung Preußischer Kulturbesitz beteiligen. Eigentlich hätte das Land 25 Prozent der Betriebs- und Programmkosten aufbringen müssen.

Das ist viel Geld, zumal für die Baukosten der Stiftung Preußischer Kulturbesitz, etwa die Sanierungen auf der Museumsinsel, seit 2003 allein der Bund aufkommt; zumal mit den Filmfestspielen und den Berliner Festspielen aufwendige Programme finanziert werden und obendrein ein neues Museum der Moderne vom Bund bezahlt wird, der auch den Löwenanteil für das Humboldt-Forum im Schloss aufbringt; zumal der Bund auch das Deutsche Historische Museum und Gedenkstätten in der Stadt unterhält. Andernorts müssen Theater und Museen um sehr viel kleinere Summen und ihre Existenz bangen. Das wird den Berlinern gern vorgerechnet. Sie können sich damit trösten, dass zur Rollenbeschreibung einer europäischen Hauptstadt gehört, jenseits des Stadtgrenzen für Verschwendung und Arroganz kritisiert zu werden. Auch gibt es keine Rechtsgrundlage, die es dem Bund erlauben würde, außerhalb Berlins bedrohten Einrichtungen dauerhaft zu helfen. Und es sollte doch eine Selbstverständlichkeit sein, dass sich die reiche Republik in der Hauptstadt auch als Kulturnation darstellt.

Der Senator will sich seine Kulturpolitik nicht vorschreiben lassen. Aber was will er dann?

Allerdings geht das seit dem Regierungsumzug immerfort wachsende Engagement des Bundes mit strukturellen Schwächen der Landespolitik einher. Die ersten Einrichtungen wurden übernommen, als die Stadt nach dem Bankenskandal pleite war und es galt, Kahlschlag zu verhindern. Warum der Bund nun in die Stiftung Berliner Philharmoniker eintritt, ist auch für Freunde des Orchesters nicht recht einzusehen. Welche Vorteile soll eine weitere Institution mit verteilten Zuständigkeiten bringen? Da werden Wünsche geweckt, die nur durch eine Änderung des gesamten Systems der Kulturfinanzierung zu erfüllen wären.

Das Internationale Literaturfestival, das in jedem Jahr erneut einen Antrag auf Förderung stellen muss, fordert in einem offenen, von vielen Autoren unterschriebenen Brief an die Kulturstaatsministerin Monika Grütters eine gesicherte Finanzierung durch den Bund. Aus der Bundeskulturbehörde heißt es, man sei in Gesprächen mit Berlin, suche pragmatische Lösungen, aber das sei gar nicht so einfach. Schließlich gebe es in Berlin nicht nur ein Literaturfestival. Es gibt auch mehrere Orchester in der Stadt. Warum erhalten nicht andere ebenfalls, was den Philharmonikern zugestanden wird?

Monika Grütters, die zugleich Vorsitzende der Berliner CDU ist, und der linke Kultursenator, Klaus Lederer, kommen, wie man hört, gut miteinander aus. Die Frage aber, was Berliner Kulturpolitik unter den komfortablen Bedingungen des Hauptstadtkulturvertrages will, ist bis jetzt noch nicht beantwortet.

In den vergangenen Jahren schien es, als sei die Landespolitik allzu bereit, die Stadt anderen Akteuren als Bühne zu überlassen. Rings ums Humboldt-Forum oder am Kulturforum, wo das Museum der Moderne erstehen soll, schwiegen die Berliner Interessen. Sie schwiegen so eindringlich, dass der Haushaltsauschuss des Bundes mit allerlei Finanzierungsversprechen Kulturpolitik zu machen versuchte. Eines dieser Geschenke, das „House of Jazz“ in der Alten Münze, hat Klaus Lederer selbstbewusst zurückgewiesen (*SZ vom 22. April*). Er wolle sich seine Kulturpolitik nicht vorschreiben lassen. Gut, aber was nun? Bislang haben die Bundesmillionen auf Berliner Seite vor allem zu konzeptioneller Zurückhaltung und sporadischen Trotzgesten geführt. Beides bekommt der Stadt schlecht. JENS BISKY

HEUTE

› *www.sz.de/kultur*