Warum können wir uns nicht besser vor Cyberangriffen schützen?

Der israelische Sicherheitsexperte Gabi Siboni sagt: Hacker können Banken lahmlegen und Kraftwerke unter ihre Kontrolle bringen. Europa muss die Bedrohung aus dem Netz endlich ernst nehmen

DIE ZEIT: Beim Angriff auf die ukrainische Gasfirma Burisma Anfang des Jahres haben offenbar russische Hacker die gleiche Taktik angewendet wie bei der Attacke auf die E-Mails der US-Demokraten im Jahr 2016. Wie genau funktioniert ein solcher Hack?

Gabi Siboni: Das sogenannte Phishing ist keine besonders ausgefallene Methode. Die Angreifer verschicken gefälschte E-Mails, die so aussehen, als stammten sie von einem vertrauten Absender. Diese enthalten dann maliziöse Links, die, wenn sie geöffnet werden, dem Angreifer ein Einfallstor in den Zielcomputer bieten. Und die letzte Verteidigungslinie ist nun einmal die Person, die vor dem Computer sitzt. Im amerikanischen Fall war es Clintons oberster Berater John Podesta, der sich seine Passwörter offenbar so hat abnehmen lassen.

ZEIT: In den vergangenen Jahren hat Europa eine Vielzahl folgenreicher Hacks erlebt, etwa den Angriff auf den Bundestag im Jahr 2015 oder auf das Wahlkampfteam von Emmanuel Macron zwei Jahre später. Tun wir zu wenig, um unsere Daten zu schützen?

Siboni: Es gibt keine technische Lösung, die vor allen potenziellen Gefahren im Netz schützt. Wenn ein Mensch einen Fehler macht, kommt es immer wieder zu solchen Vorfällen. Und das ist offenbar auch im Fall dieser ukrainischen Firma geschehen.

ZEIT: Wie also lassen sich Netzwerke besser absichern?

Siboni: Viele Leute glauben, dass es bei Cyberverteidigung um Technologie geht. Aber das stimmt nicht. Die Netz-Infrastruktur eines Staates ist wie ein Ballon, der Angreifer braucht nur eine einzige Nadel, und Sie müssen versuchen, die gesamte Oberfläche zu schützen. Jedes einzelne Gerät und jeder einzelner Nutzer sind ein potenzieller Zugang. Wenn Sie immer mehr Nutzer in einem Netzwerk zusammenschalten und nicht jedes Mitglied dieses Netzwerks ein intensives Training absolviert hat, können Angreifer mit einfachen Mitteln große Wirkung gegen Ihr System erzielen. Sie müssen definieren, welche Infrastruktur besonders wichtig ist und besonders geschützt werden muss, brauchen funktionierende Krisenstäbe und intensive Simulationen, um das System auf Schwachstellen zu testen.

ZEIT: Bislang sind kaum Details über den Angriff auf Burisma und eine weitere Cyberattacke auf Österreichs Außenministerium bekannt. Welche Absichten könnten hinter diesen Hacks stecken?

Siboni: Das ist schwer zu sagen. Es ist wichtig, zu verstehen, dass Ziele eines Angriffs oft nur Teile einer Kette sind: Nur weil ein Ministerium angegriffen wird, heißt das nicht, dass sich die Operation auch gegen ebendieses Ministerium richtet. Vielleicht benötigt der Angreifer nur diesen Zugang oder einige bestimmte Informationen, um sich später gegen ein anderes Ziel wenden zu können.

ZEIT: Warum passiert den Europäern so etwas immer wieder?

Siboni: In meinem israelischen Verständnis ist eine ganze Reihe an Schritten notwendig, um die eigenen Netzwerke schützen. Aus meiner Perspektive und nach Gesprächen mit meinen europäischen Kollegen kann ich nicht erkennen, dass Europa diese Schritte unternimmt. Es wirkt so, als ob das Problem nicht wirklich ernst genommen wird.

ZEIT: Was macht Israel anders?

Siboni: Die nationale Sicherheit spielt grundsätzlich für uns eine viel größere Rolle, das gilt auch für den digitalen Raum. Darüber hinaus sind unsere Streitkräfte – die Israeli Defense Forces (IDF) – ein riesiges Ausbildungszentrum für hoch qualifizierte Fachkräfte im Cyberbereich, sowohl mit defensiven als auch mit offensiven Kapazitäten. Wir haben einen mehrjährigen verpflichtenden Wehrdienst. Unsere jungen Leute gehen zur Armee, etwa in die Elite-Cyber-Einheit 8200, und wenn sie danach im ersten Job-Interview gefragt werden, ob sie irgendeine Erfahrung haben, können sie diese Frage klar mit Ja beantworten. Jedes Jahr tritt auf diese Weise eine hohe Zahl von Fachkräften in den freien Markt ein. So ist Israel zu einem der führenden Staaten auf diesem Gebiet geworden.

Professor Gabi Siboni leitet das Cyberprogramm beim Institute for National Security Studies

ZEIT: Gegen welche Staaten muss Europa sich verteidigen?

Siboni: Ich denke, die Europäer sollten sich um Russland Sorgen machen. Und zwar nicht nur um direkte Angriffe staatlicher russischer Cybereinheiten, sondern auch um Proxies, also Stellvertreter, die unter russischer Führung agieren. Auch China und der Iran haben meiner Einschätzung nach großes Interesse daran, was in Europa passiert. Zudem gibt es Gruppen wie den »Islamischen Dschihad« oder den »Islamischen Staat«, nicht staatliche Akteure, die den europäischen Cyberspace bedrohen.

ZEIT: Warum sind Staaten wie Russland, China und der Iran besonders aktiv auf diesem Gebiet?

Siboni: Weil wir es mit einem kosteneffizientes Werkzeug zu tun haben. Cyberangriffe sind günstig und zum Teil schwer zurückzuverfolgen. Ganz anders als bei kinetischen Waffen, etwa einer Bombe. Der Aufwand ist gering, der Ertrag oft groß.

ZEIT: Welche Gefahren bringt der Hack eines Ministeriums oder eines Unternehmens mit sich?

Siboni: Der Diebstahl von Daten kann erhebliche Auswirkungen haben, ein Angreifer kann sensibles Material veröffentlichen oder es nutzen, um einen Gegner zu erpressen. Auch droht durch einen Hack die Manipulation und die Zerstörung von Informationen. Eine weitere Eskalation wäre ein Angriff auf die Funktionsfähigkeit bestimmter Dienste, etwa im Bankensektor. Dann können Transaktionen blockiert oder auf andere Konten umgeleitet werden. Die wohl größte Bedrohung besteht durch Attacken auf Raffinieren und Kraftwerke, plötzlich geht der Strom aus, oder bestimmte Waffensysteme funktionieren nicht mehr.

ZEIT: Zahlreiche europäische Staaten beraten derzeit darüber, ob sie die Dienste der chinesischen Firma Huawei beim Aufbau ihrer neuen 5G-Datennetze in Anspruch nehmen. Halten Sie das für eine gute Idee?

Siboni: Nur wenige Staaten haben sich bislang dazu entschieden, chinesische Konzerne vom Aufbau ihrer Netze auszuschließen, etwa die USA und Australien. Bevor sich ein Staat jedoch anders entscheidet, sollte er überlegen, ob er dafür garantieren kann, dass seine Daten und die Daten seiner Unternehmen in einem chinesischen Netz wirklich sicher sind.

ZEIT: Zwei Ihrer israelischen Kollegen haben im Jahr 2018 eine Studie veröffentlicht, die nahelegt, dass ein anderer staatlicher chinesischer Telekommunikationskonzern Teile des globalen Datenverkehrs abgezweigt und zuerst nach China umgeleitet hat. Und trotzdem halten Sie sich bei Huawei mit einem Urteil zurück?

Siboni: Sie wollen eine ehrliche Antwort?

ZEIT: Bitte!

Siboni: Ich denke, die digitale Infrastruktur auf diese Weise auszulagern wäre keine gute Idee.

Die Fragen stellte **Paul Middelhoff**

Siehe auch **Wirtschaft, Seite 23**

Illustration: Delia Wilms für DIE ZEIT; kl. Foto: privat

Attacken auf die Daten

Wie Hacker in Österreich und der Ukraine zuschlugen **VON FLORIAN GASSER UND PAUL MIDDELHOFF**

Die Attacken kamen aus dem Netz: Rund um den Jahreswechsel drangen Hacker in das Netzwerk des ukrainischen Gaskonzerns Burisma ein. Analysten der US-Sicherheitsfirma *Area 1* zufolge handelt es sich bei den Angreifern um Angehörige russischer Militäreinheiten, die im Auftrag des Kreml arbeiten. Fast zur selben Zeit vermeldete auch das Außenministerium in Wien, es sei Ziel eines »schwerwiegenden Cyberangriffs« geworden. Es gibt keine Hinweise darauf, dass die beiden Hacks miteinander in Verbindung stehen. Und doch machen sie deutlich, dass es der EU und ihrem östlichen Nachbarn an einer wirksamen Cyber-Verteidigung mangelt.

Der Fall von Burisma reicht bis nach Washington. Denn Hunter Biden, Sohn von Joe Biden, dem derzeitigen Favoriten im Rennen um die demokratische Präsidentschaftskandidatur, saß von 2014 bis 2019 im Aufsichtsrat des Konzerns. Trump wirft Joe Biden vor, als Vizepräsident unter Barack Obama Einfluss auf die ukrainische Politik genommen zu haben, um drohende Ermittlungen von der Firma seines Sohnes abzuwenden – Beweise gibt es dafür allerdings nicht.

Nun interessieren sich offenbar auch russische Hacker der berüchtigten staatlichen Cyber-Einheit »Fancy Bear« für Burisma. Ein amerikanischer Regierungsbeamter berichtet laut *New York Times* davon, dass russische Spione zeitgleich auf analogem Wege versuchten, in ukrainischen Regierungskreisen an Informationen über die Bidens zu gelangen. Zwar ist nicht bekannt, ob Burisma Informationen gestohlen wurden und wonach die Hacker eigentlich suchten. Doch seit Moskau 2016 mit Falschinformationen und geleakten E-Mails der Demokraten in den US-Wahlkampf eingegriffen hatte, steht nun zu befürchten, dass Russland versuchen könnte, auch die Wahlen in diesem Herbst zu beeinflussen.

In Österreich war bis Redaktionsschluss dieser Ausgabe kaum etwas über den Hackerangriff auf das Außenministerium bekannt, nur dass er schwerwiegend sei, ließ die Regierung wissen. Sebastian Kurz, der zum Zeitpunkt des Hacks noch gar nicht wieder als Bundeskanzler im Amt war, sagte, das sei »kein Kavaliersdelikt«, sondern »eine moderne Form des Angriffs«. Es klang alles ein wenig ratlos.

Überhaupt nimmt Österreich die Landesverteidigung seit Jahrzehnten nicht sonderlich ernst – weder in der analogen noch in der digitalen Welt. Das Bundesheer spart, wo es kann, und auch die digitale Abwehrbereitschaft hatte vor ein paar Jahren eigentlich aufgestockt werden sollen. Im Jahr 2013 wurde dazu eigens die »Österreichische Strategie für Cyber Sicherheit« vorgestellt. »Sehr große Staaten«, erklärte damals Klaus Naumann, der ehemalige Vorsitzende des Nato-Militärausschusses, dürften ab 2020 in der Lage sein, »kleinere Staaten teilweise oder sogar ganz elektronisch auszuschalten«.

Das Jahr 2020 hat mittlerweile begonnen, die früheren Pläne sind nicht weit gediehen. Cyberattacken oder einem Black-out sei das Bundesheer »fast schutzlos ausgeliefert«, sagte Thomas Starlinger, der Verteidigungsminister der Übergangsregierung im vergangenen August. Und offenbar ist nicht nur das Bundesheer bedroht, sondern, wie sich nun zeigt, auch Teile der Regierung.