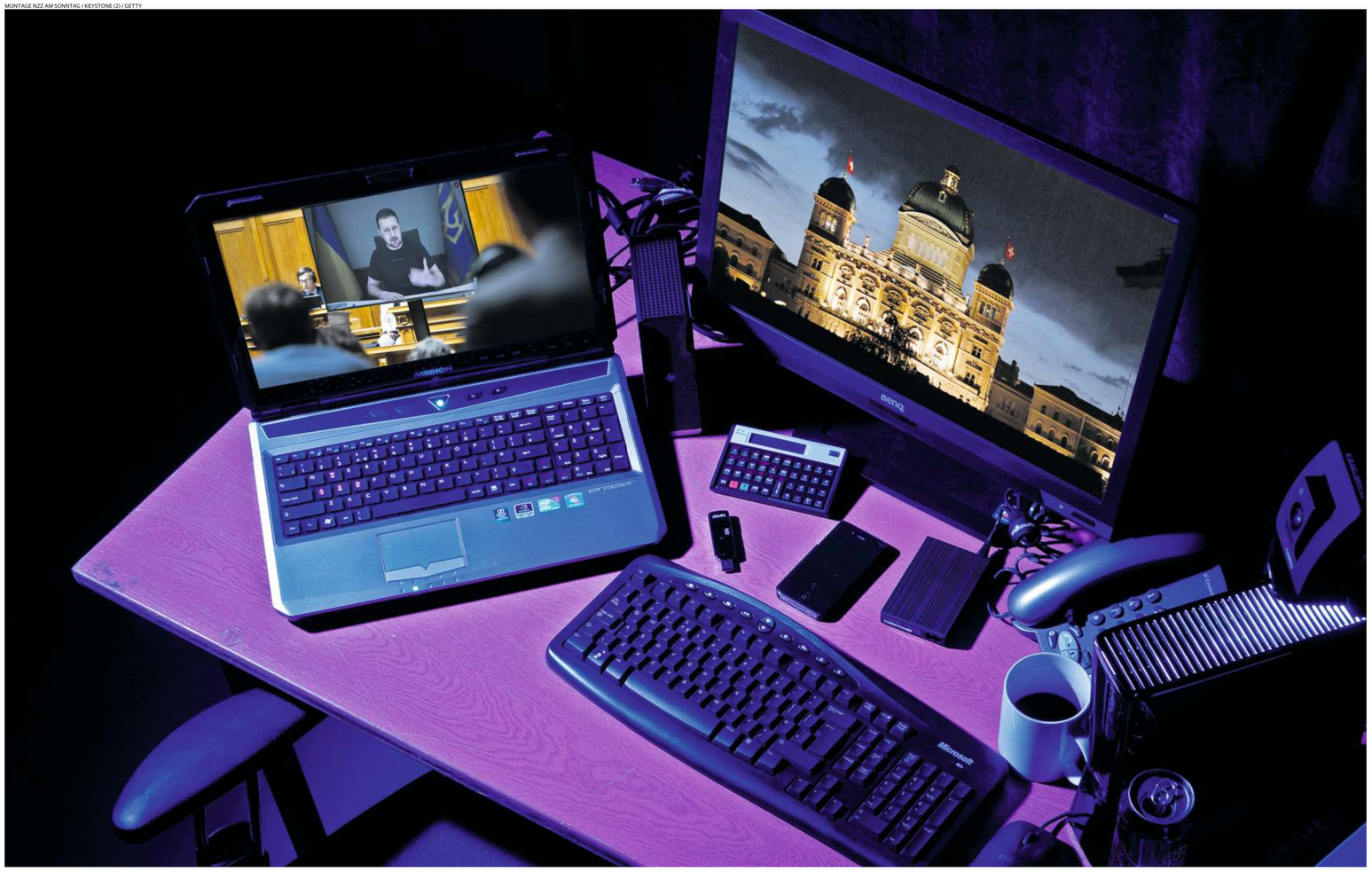
Hackerangriffe: Ungeschützt im Auge des Hurrikans

Seit Wochen wird die Schweiz im Cyberspace von russischen Hackern attackiert. Nun zeigt eine Messung, dass Zehntausende Server von Bildungs- und Gesundheitsinstitutionen sowie von Behörden gravierende Sicherheitslücken aufweisen. Der Bund reagiert nur halbherzig.

Von René Donzé, Georg Humbel, Mirko Plüss

MONTAGE NZZ AM SONNTAG / KEYSTONE (2) / GETTY



Am Donnerstagmittag um 13.22 Uhr erscheint im Telegram-Kanal der Hacker-Gruppe mit dem kryptischen Namen «NoName057(16)» eine neue Meldung: «Die Website des Schweizerischen Privatbankierverbandes hat unseren Angriff nicht überlebt.» In den Stunden zuvor hatten die Hacker bereits die Online-Auftritte von Schweiz Tourismus, den Zürcher Verkehrsbetrieben, der Swiss ID und des Rüstungskonzerns Ruag lahmgelegt. 45 000 Abonnenten zählt ihre Telegram-Gruppe, die Erfolgsmeldungen werden mit «Daumen hoch»- und Flammen-Emojis garniert.

Am gleichen Tag, kurz nach 14 Uhr, erscheint im Nationalratssaal in Bern auf mehreren Bildschirmen Wolodimir Selenski. Der ukrainische Präsident wendet sich mit einer Videobotschaft ans Parlament. «Ich danke dir, liebe Schweiz», sagt er in seiner kurzen Rede. Im Telegram-Chat ist die Wortwahl weniger freundlich: «Wir können die gesamte Internet-Infrastruktur der Schweiz zur Hölle schicken», schreiben die Hacker.

Löchrig wie ein Käse

Die neutrale Schweiz ist unter Attacke – zumindest digital. Und es droht noch viel grösseres Unheil. Je länger der Krieg andauert, je mehr die Schweiz Farbe bekennen muss, desto wahrscheinlicher werden auch Cyberangriffe. Dazu kommt, dass die Zahl der Hackerangriffe wieder steigt, nachdem sie bei Kriegsausbruch etwas eingebrochen war. Und noch immer sind Zehntausende Server in der Schweiz nicht geschützt. Was bedeutet das für die Sicherheit unserer Daten? Und für die Demokratie?

Rückblende. Wir schreiben den 15. März 2022, und im eleganten Empire Saal des Restaurants «Zum Äusseren Stand» in Bern treffen sich hohe Militärs, Politikerinnen und Politiker, Cyber-Fachleute zum Nachtessen an runden, reich gedeckten Tischen zur Gründung der parlamentarischen Gruppe Cyber. Von solchen Politikergruppen, die sich um ein Thema kümmern, gibt es Dutzende in Bern, von Wandern über Textilwirtschaft bis zum nachhaltigen Finanzsystem. Nun also auch eine zu Cyber. Es ist Tag 20 des russischen Angriffskriegs auf die Ukraine. Bundesrätin Viola Amherd betont vor den Anwesenden die Wichtigkeit der Cyber-Abwehr, Divisionär Alain Vuitel erklärt, was die Schweizer Armee unternimmt.

Und einer warnt: Nicolas Mayencourt, Chef der Schweizer Firma Dreamlab Technologies, die sich international in der Cybersicherheit engagiert. Die Bilder, die er auf die Leinwand projiziert, sind erschreckend: Die Schweizer Cyber-Landschaft ist löchrig wie ein Käse. Über 116 000 Sicherheitslücken haben die Messungen der Schweizer Server aufgezeigt. «Wir müssen sowohl als Nation als auch als einzelne Akteure proaktive Sicherheitsmassnahmen ergreifen», sagt er und beendet den Vortrag mit: «Stop being naive.»

Nun ist die Schweiz schmerzhaft erwacht. Seit zwei Wochen jagt eine DDoS-Attacke die nächste. Dabei werden Websites mit automatisierten Anfragen überhäuft, bis sie zusammenbrechen. Solche Angriffe entfalten keine langfristige Wirkung, aber sie verunsichern Hunderttausende Userinnen und User. Es traf das Parlament, das Justizdepartement, Flughäfen, Verkehrsbetriebe, Städte und Gemeinden in allen Landesteilen. Es ist eine digitale Bestrafungsaktion dafür, dass die Schweiz Selenski nur schon anhört.

Wo die Gefahr am grössten ist

Anteil der kritischen Sicherheitslücken in Servern nach Branche

Quelle: Dreamlab Technologies AG

Klumpenrisiko beim Bund

Und beinahe gleichzeitig wird bekannt, dass Hacker rund ein Terabyte Daten von der Interlakner Firma Xplain gestohlen haben - einer Anbieterin von Behördensoftware. Darunter befindet sich potenziell heikles Material diverser Bundesstellen. Wie kann das sein? Warum sorgte der Bund nicht dafür, dass die Daten aufgeteilt und separat verschlüsselt wurden? Hatte niemand ein solches Klumpenrisiko auf dem Radar?

Mit Verweis auf laufende Untersuchungen wollte dazu niemand etwas sagen. Die Berner Staatsanwaltschaft hat ein Verfahren wegen Erpressung und unbefugter Datenbeschaffung eröffnet. Auch die Bundesanwaltschaft ist aktiv geworden. Die Ermittler wollen wissen, wie die Behördendaten zu Xplain gelangt sind, und befragen wohl auch Angestellte des Bundes und der Firma.

Vordergründig haben die DDoS-Attacken, die relativ einfach abgewehrt werden können, und der viel raffiniertere Ransomware-Angriff auf Xplain nichts miteinander zu tun. Das eine ist politisch motiviert, das andere ein Angriff der organisierten Cyberkriminalität. «Beides zeigt aber, wie schlecht die Schweiz aufgestellt ist, wenn es um die Verteidigung des Landes im virtuellen Raum geht», sagt Mayencourt heute. Schlimmer noch: Seit seinem Auftritt in Bern vor 15 Monaten hat sich die Lage kaum verbessert. Noch immer zählen die Sicherheits-Scans von Dreamlab im Schweizer Netz 106 000 Server mit Sicherheitslücken, dies bei einer Gesamtzahl von 3,5 Millionen Servern. Rund die Hälfte der Lücken, also etwa 50 000, sind gemäss internationalen Normen als «gravierend» einzustufen – sie befinden sich auf einer Skala von 0 bis 10 bei über 9. Das heisst: Man kann mit leicht zugänglichen Tools relativ einfach dort eindringen, und der potenzielle Schaden ist erheblich. «Das Schiff ist am Sinken, und wir müssen gemeinsam alle Anstrengungen bündeln, um diese Löcher zu stopfen», sagt Mayencourt.

Während der ukrainische Präsident Wolodimir Selenski zum Schweizer Parlament spricht, drohen die Hacker in ihren Chats: «Wir können die gesamte Internet-Infrastruktur der Schweiz zur Hölle schicken.»

In Bern sitzt ein Mann, der das ziemlich anders sieht. Florian Schütz wird oft auch als Mr. Cyber bezeichnet, da er das Nationale Zentrum für Cybersicherheit NCSC leitet. Die Schätzung von 50 000 lückenhaften Servern sieht er kritisch. «Da könnten zum Beispiel auch private Websites mitgezählt werden, die schon seit Jahren inaktiv sind.» Schütz sagt aber auch: «Leider ist es so, dass viele Firmen, Behörden und Private ihre IT-Schwachstellen zu spät oder gar nicht schliessen.» Das NCSC weise immer wieder auf Schwachstellen hin und habe in den vergangenen Jahren mehrere tausend eingeschriebene Briefe an gefährdete Firmen verschickt. Allerdings: «In einigen Fällen erhalten wir darauf gar keine Rückmeldung, und die Lücken existieren weiterhin.» Schütz verweist deshalb auch auf die Sorgfaltspflicht von Unternehmen: «Die eigenen Daten zu schützen, ist auch im Cyberraum eine Pflicht.»

Bloss sind es nicht in erster Linie Private oder Unternehmen, sondern überwiegend Behörden oder behördennahe Anbieter, die prekär unterwegs sind (siehe Grafik): Betroffen sind rund 21 000 Bildungs-Server, 10 000 Behörden-Server und 10 000 Server der Gesundheitsbranche, zu der etwa auch Spitäler gehören.

Wie sicher ist E-Voting?

Der Angriff trifft die Schweiz in einer besonders heiklen Woche. Diesen Sonntag wird in drei Kantonen erstmals seit Jahren auch wieder digital abgestimmt. Und ausgerechnet die Post, welche die E-Voting-Plattform betreibt, wurde ebenfalls Ziel der Hacker. Betroffen war unter anderem der Log-in-Bereich. Zwar blieb die Plattform selbst unangetastet, doch war die Nervosität gross. Wie mehrere Seiten bestätigen, sprachen sich Bund, Post und Kantone zu möglichen Bedrohungsszenarien ab. Denn: Obwohl DDoS-Angriffe keinen grossen wirtschaftlichen oder technischen Schaden anrichten: Sie beschädigen das Vertrauen in die Systeme. Und diese sind ohne Vertrauen nichts wert. «Sogar wenn man das sicherste E-Voting-System hat: Es reicht, wenn Zweifel an dessen Resultaten gestreut werden können», sagt Gazmend Huskaj vom Geneva Centre for Security Policy. Aus diesem Grund etwa hat sich Schweden gegen E-Voting entschieden. Was er ebenfalls sagt: Es war zu erwarten, dass die Zahl der Angriffe auf Schweizer Server zunimmt im Vorfeld der Rede des ukrainischen Präsidenten.

Niemand weiss, was Selenskis Videorede vor dem Parlament politisch bewirkte, ob Bewegung in die Grabenkämpfe um Waffenlieferung, Neutralität, Sanktionen kommt. Sicher aber ist, die begleitenden Cyberattacken haben die Politik getroffen. Am Morgen lag der Übersetzungsdienst des Parlaments zwei Stunden lahm. Vielen in der Wandelhalle im Bundeshaus ist es mulmig. Während bei realen Staatsbesuchen das Sicherheitsdispositiv hochgefahren wird, scheint es im virtuellen Raum kaum ein solches zu geben.

«Wir hatten als Land viel zu wenig auf dem Radar, dass auch wir plötzlich im Auge des Hurrikans sein könnten», sagt SVP-Nationalrat Franz Grüter. Der Präsident der Aussenpolitischen Kommission ist selber Verwaltungsratspräsident einer IT-Firma und weiss, wovon er spricht, wenn er sagt: «Ich hoffe, dass diese Angriffe wachrütteln.» Von links bis rechts scheint man sich für einmal einig. FDP-Sicherheitspolitikerin Maja Riniker sagt: «Wir sind in Sachen Cybersicherheit offensichtlich nicht dort, wo wir sein müssten», und spricht von einer «grossen sicherheitspolitischen Herausforderung». Der grüne Nationalrat und IT-Unternehmer Gerhard Andrey sagt: «Wir müssen die Cyberabwehr auf ein höheres Niveau heben.» Und er bestätigt auch, was die Dreamlab-Analyse zeigte: Besser geschützt sind die Banken, die von der Aufsichtsbehörde Finma seit Jahren aufgefordert werden, Cyberrisiken aktiv zu minimieren. «Deutlich schlechter geschützt sind Schulen, Gemeinden, Strom- und Wasserversorgung und Spitäler. Das sind sehr sensible Bereiche. Aber sie haben noch keine digitale Sicherheitskultur.»

Es ist, als ob man verpasst hätte, bei einer Villa Türen und Fenster zu schliessen. Zumindest will man nun eine Alarmanlage einbauen.

Wenig Geld für Mr. Cyber

Doch geht nun ein Ruck durch Bern? Im Moment deutet wenig darauf hin. Zwar wird per 1. Januar 2024 aus dem Nationalen Zentrum für Cybersicherheit ein eigenes Bundesamt, das vom Finanz- ins Verteidigungsdepartement wechselt. Das Budget wird nur leicht erhöht, von 13,7 auf 14,5 Millionen Franken, damit können gerade einmal vier zusätzliche Vollzeiteinheiten finanziert werden. Ein Ausbau sieht anders aus. Das bestätigt auch Mr. Cyber Florian Schütz: «Mit mehr Mitteln kann man auch mehr erreichen. Es ist jedoch wichtig, nicht nur Mittel aufzustocken, sondern diese auch effizient einzusetzen», sagt er. «Im Vergleich zu anderen Ländern ist die Schweiz eher moderat mit Mitteln ausgestattet.»

Immerhin müssen Hackerangriffe auf kritische Infrastrukturen bald obligatorisch gemeldet werden. Auf eine solche Meldepflicht haben sich Bundesrat und Parlament geeinigt. Und kommende Woche berät die Sicherheitspolitische Kommission sogar eine Meldepflicht für schwerwiegende Schwachstellen, die entdeckt werden, bevor etwas passiert. Allerdings sind dort die Mehrheiten nicht klar. «Ich verlange, dass man nicht nur Angriffe melden muss, sondern auch Schwachstellen und Sicherheitslücken», sagt der Grüne Gerhard Andrey. «Wir brauchen im digitalen Raum eine Sicherheitskultur, wie es sie in der Luftfahrt heute schon gibt.»

Auch Dreamlab-Chef Mayencourt wäre grundsätzlich für eine solche Meldepflicht. «Damit würde die Schweiz einen grossen Schritt in Richtung einer vernünftigen Cyber-Abwehr machen», sagt er.

Davon sind wir laut Statistiken noch weit entfernt: In einem globalen Ranking zur Cybersicherheit steht die Schweiz auf Rang 42, der detaillierte National Cyber Security Index der estnischen E-Governance Academy gesteht ihr immerhin Platz 27 zu (gerade noch vor Bulgarien). Null Punkte gab es dort für die Schweiz etwa für die Bereiche «Cybersicherheitsstandards für den öffentlichen Sektor» und «Kompetente Überwachungsautoritäten». Das ist für eines der reichsten und innovativsten Länder der Welt eine gefährliche Position: Als ob man es verpasst hätte, bei einer Luxusvilla die Türen und Fenster zu schliessen. Zumindest will man bei dieser Villa mithilfe der nationalen Meldepflicht nun wenigstens eine Alarmanlage einbauen.

Verhandeln mit Erpressern

Warum gewisse Firmen zahlen

Manche geben sich phantasievolle Namen wie DarkSide, REvil oder Play, andere treten als seriöse Geschäftspartner auf: «Guten Tag, wir haben eine Schwachstelle in Ihrer IT-Architektur entdeckt und können Ihnen helfen, sich in Zukunft besser zu schützen», heisst es dann in einer E-Mail. Das Geschäftsmodell ist in beiden Fällen dasselbe: Hacker schleusen sich in IT-Systeme von Firmen ein, kopieren Daten, drohen mit der Veröffentlichung und verlangen Lösegeld.

E-Mails von Leuten, die irgendetwas behaupten und fordern, finden sich täglich in den Mailboxen von Firmen. Doch manche sind mehr als Bluff. Die Abwehr ist geknackt, die Daten sind weg. Das ist der Moment, in dem der Zürcher Anwalt Christian Laux ins Spiel kommt. Seine Kanzlei ist auf IT-Recht spezialisiert. Dazu gehört die Beratung von Firmen, die Opfer von Datendiebstählen wurden. Wie geht man mit Verbrechern um? Soll man zahlen oder das Risiko eingehen, dass die Daten im Darknet landen? Mit solchen Fragen kommen Firmen zu Laux.

Zuerst erledigt der Anwalt das Handwerkliche: Innerhalb von 72 Stunden müssen diverse Behörden informiert werden – Datenschützer, das Nationale Zentrum für Cybersicherheit, je nach Branche auch die Finanzmarktaufsicht und Behörden in der EU. Das ist Routinesache, knifflig wird's danach. «Ein Cyberangriff ist wie ein Überfall in einer dunklen Unterführung. Man sieht den Angreifer nicht, doch plötzlich liegt man am Boden», sagt Laux. Entscheidend sei, möglichst schnell in einen professionellen Handlungsmodus zu kommen. Das gilt auch für das Verhältnis zum Angreifer. Diesen generell zu ignorieren, hält Laux für keine intelligente Idee. «Mit den Erpressern zu kommunizieren, kann Vorteile haben.» Denn so habe man eine Chance, Informationen über die Gegenseite herauszufinden.

«Manche erzählen Geschichten, die bedrohlich klingen. Dann stellt man aber fest, dass die geschilderte Datenlage gar nicht möglich ist. Das kann ein entscheidender Vorteil für die weiteren Verhandlungen sein», sagt Laux. Möglich sind solche Erkenntnisse allerdings nur, wenn die angegriffenen Firmen im Vorfeld ihre Hausaufgaben gemacht haben. Wer keine Übersicht über seine Daten hat, ist leichter erpressbar.

Mit den Verhandlungen gewinnt Laux auch Zeit für die nächsten Schritte. Einen Verteidigungsring aufbauen, den Schaden minimieren und die wohl heikelste Aufgabe angehen: die Kunden informieren, dass heikle Daten von ihnen im Darknet landen könnten. «Ein Verlust von Kundendaten bleibt zwar eine unangenehme Situation für ein Unternehmen, die Folgen lassen sich aber entschärfen», sagt Laux. Die Kunden können etwa ihre Passwörter ändern.

Damit nähert sich Laux der entscheidenden Frage: Zahlen oder hart bleiben? «Rein rational gibt es keinen Grund zu zahlen», sagt er. Zu gross ist die Ungewissheit, dass dies nicht nur der Anfang für weitere Erpressungen ist. Dennoch steigen viele Unternehmen auf die Erpressung ein. Auch Laux hat schon Kunden geraten zu zahlen. Nicht die Phantasiebeträge, die die Angreifer ursprünglich verlangten, sondern eine moderate Summe. «Solche Zahlungen können taktische Gründe haben, sie können ein Signal sein, dass man kooperationswillig ist», sagt Laux. Die Angreifer wollten ernst genommen werden. «Wenn man die Daten zurückverlangt und dann einen Betrag überweist, kann man zu einem Deal kommen, der Bestand hat», sagt Laux.

Mit der Geldüberweisung manövrieren sich Firmen allerdings in eine delikate Situation. Denn damit machen sie sich mitverantwortlich, dass das Geschäftsmodell Erpressung funktioniert. Frankreich hat deshalb das Zahlen von Lösegeldern verboten, in der Schweiz ist es erlaubt.

Obwohl er Zahlungen nicht ausschliesst, ist Laux überzeugt, dass sein Verhandlungsansatz dem Geschäftsmodell Erpressung ebenfalls den Boden entzieht. «Indem das Opfer gestärkt wird und Handlungsoptionen erhält, sinkt der Druck, Lösegeld zu zahlen.» Je nach Fall erhalten die Erpresser zwar ein Entgelt, doch den Jackpot können sie nicht mehr knacken.

Guido Schätti