DIE ZEIT

Z+ Cyberangriffe

"Teile der kritischen Infrastruktur sind längst unterwandert"

Die Hackerin Chris Kubecka findet Sicherheitslücken in Kraftwerken, der Wasserversorgung und im Stromnetz. Sie sagt: Europas Feinde haben sich bereits eingenistet.

Interview: Tim Geyer

Aktualisiert am 4. Oktober 2025, 6:04 Uhr

Dieser Artikel ist Teil von ZEIT am Wochenende [https://www.zeit.de/we], Ausgabe 40/2025.

Chris Kubecka ist eine der bekanntesten Hackerinnen der Welt. Gerade spricht die

US-Amerikanerin auf einer Konferenz in Athen vor Sicherheitsexperten darüber, wie Russland in Europa Teenager für sich spionieren lässt. Zwischen zwei Panels hat sie Zeit für einen Videocall.

DIE ZEIT: Frau Kubecka, Bundesverteidigungsminister Boris Pistorius sagte kürzlich: "Wir sind nicht im Krieg, aber auch nicht mehr im Zustand des vollständigen Friedens."

Chris Kubecka: Wir befinden uns längst mitten in einem Kalten Cyberkrieg.

ZEIT: Was meinen Sie damit?

Kubecka: Wie im Kalten Krieg gibt es aktuell keine direkte militärische Konfrontation zwischen Russland und dem Westen. Aber auf digitaler Ebene kocht der Konflikt überall hoch. Windkraftanlagen, Waffensysteme, Flugzeuge: All das können Ziele von Cyberangriffen sein. Nur ein paar Beispiele aus jüngerer Zeit: Vergangenes Jahr wurden die E-Mail-Konten mehrerer deutscher Behörden und Unternehmen, auch aus der Rüstungsindustrie, gehackt – von einer dem russischen Militärgeheimdienst unterstellten Hackergruppe. Seit Monaten werden in Ostdeutschland Drohnen gesichtet, die Routen für Waffenlieferungen in die Ukraine ausspähen. Und im September griffen Hacker die Check-in- und Abfertigungssysteme am BER und anderen europäischen Flughäfen an.

ZEIT: Für die Angriffe an Flughäfen könnten auch einfach Kriminelle verantwortlich sein.

Kubecka: Es ist nicht unwahrscheinlich, dass Russland dahintersteckt. Aber solche Zuordnungen müssen Regierungen treffen, nicht ich. Wissen Sie, in den Hinterzimmern haben sich Politiker seit Russlands Angriff auf die Ukraine schon mit weit schlimmeren Cyberangriffen beschäftigt, ohne dass über diese öffentlich berichtet wurde. Aber auf diesem Level muss man sich immer fragen, ob man wirklich etwas öffentlich machen will und dann vielleicht gezwungen ist, den Nato-Artikel 4 auszurufen, so wie das Estland kürzlich aufgrund der Verletzungen seines Luftraums getan hat.

Chris Kubecka

Die US-amerikanische Cybersicherheits-Expertin berät mit ihrem Unternehmen HypaSec Regierungen und Behörden, hält Vorträge vor der UN und EU, Europol und Interpol. Nachdem 2012 ein Cyberangriff 35.000 Computer des weltweit größten Erdölunternehmens Saudi Aramco mit einem Virus infiziert hatte, wurde Kubecka beauftragt, die Systeme wiederherzustellen. Danach verantwortete sie für mehrere Jahre die digitale Sicherheit und nachrichtendienstliche Aufklärung der Unternehmensgruppe. Sie lebt in den Niederlanden.

ZEIT: Der besagt, dass sich die Nato-Parteien beraten, wenn ein Land die Unversehrtheit seines Gebiets oder die eigene Sicherheit bedroht sieht. Im schlimmsten Fall könnte die Nato auch bei einem Cyberangriff den Bündnisfall ausrufen.

Kubecka: Verständlicherweise will man sich die Möglichkeit für eine friedliche Lösung offen halten. Dennoch ist klar: Solche Cyberangriffe nehmen zu.

ZEIT: Sie haben Windkraftanlagen erwähnt, die derzeit überall in Deutschland gebaut werden, genauso wie Photovoltaikanlagen. Sind diese modernen Kraftwerke gut gegen Cyberangriffe geschützt?

Kubecka: Nein. *(lacht)* Absolut nicht. Tatsächlich eher schlechter. Niederländische Hacker haben 2024 öffentlich gemacht, dass sie einen Weg in einen großen Teil der europäischen Photovoltaik gefunden haben. Auch in all die wunderbaren Balkonkraftwerke in Deutschland. Das Steuerungssystem eines Herstellers ließ eine offene Tür zu Millionen solcher Anlagen. Und Windturbinen? Vor einigen Jahren habe ich einem britischen Nachrichtendienst demonstriert, dass in Großbritannien 82 Prozent der Windturbinen mit dem Standardpasswort "admin admin" konfiguriert waren und ich online auf sie zugreifen konnte.

ZEIT: Das war hoffentlich eine Ausnahme.

Kubecka: Nein. So etwas kommt sehr häufig vor. Die Hersteller wollen ihren Kunden das Leben möglichst leicht machen. Wenn Sie ein Gerät kaufen, das mit dem Internet verbunden ist und Sie starten es zum ersten Mal, dann wäre es eigentlich gut, wenn Sie direkt ein neues Passwort festlegen müssten. Inzwischen ist das häufig auch so. Aber das gibt es noch nicht sehr lange und auch nur bei Alltagskonsumgütern. Jetzt stellen Sie sich große Industrieanlagen vor, die in dieser Hinsicht meistens ein paar Jahre hinterherhinken und eher darauf ausgelegt sind, gut mit anderen Systemen zusammenzuarbeiten. Zwar müssen in der EU auch die bis spätestens 2027 passwortgeschützt sein. Aber entweder werden die Regeln noch nicht überall verstanden oder sie werden nicht scharf genug kontrolliert.

ZEIT: Was könnte passieren, wenn Hacker Kraftwerke in Deutschland übernehmen würden?

Kubecka: Das konnte man sich vor ein paar Jahren in der Ukraine anschauen. Vor Russlands Einmarsch verübte es zahlreiche Cyberangriffe auf die kritische Infrastruktur des Landes. Im Dezember 2015 legten russische Hacker Teile des Stromnetzes in der Westukraine lahm. Etwa 230.000 Menschen waren ohne Strom. Weil die Systeme so alt waren, konnte man sie nach drei Stunden zum Glück wieder manuell hochfahren. Bei modernen Anlagen wie in Deutschland

kann das schwieriger sein. Wer so etwas mitten im Winter in einem Land anrichtet, kann es in die Knie zwingen. Ein Angriff auf die Stromversorgung und der dadurch ausgelöste Blackout ist dann nur der Anfang.

“Teile der kritischen Infrastruktur in Deutschland und anderen Ländern sind längst durch ausländische Akteure unterwandert.”

– Chris Kubecka

ZEIT: Was passiert, wenn der Strom länger ausfällt?

Kubecka: Dann brechen nach und nach weitere Systeme zusammen – Wasserversorgung, Krankenhäuser, Kommunikations- und Zahlungssysteme. Selbst Tanken wird unmöglich. All das wirkt sich auch auf psychologischer Ebene aus. Plötzlich funktioniert etwas Zentrales nicht mehr. Das kann Ihr Vertrauen in Ihre Regierung und deren Reaktionsfähigkeit erschüttern. Für Desinformations- und Propagandakampagnen bieten sich dann ideale Ansatzpunkte.

ZEIT: Wenn es möglich ist, Kraftwerke in Deutschland oder anderen Nato-Staaten durch Cyberangriffe zu attackieren, warum ist es dann noch nicht passiert?

Kubecka: Möglicherweise wäre damit eine rote Linie überschritten, was zu einer erheblichen Eskalation führen könnte. 2019 haben wir so ein Szenario in Brüssel bei einer Cybersecurity-Übung mit Vertretern von Nato- und EU-Staaten durchgespielt. Manche sprachen in der Simulation nur eine diplomatische Rüge aus. Andere Länder entschieden hingegen, als Reaktion eine Nuklearwaffe in der oberen Atmosphäre über dem angreifenden Land zu zünden, um mit einem Elektromagnetischen Impuls deren Strom- und digitale Kommunikation auszuschalten. Aber unabhängig von solchen Planspielen denke ich: Teile der kritischen Infrastruktur in Deutschland und anderen Ländern sind längst durch ausländische Akteure unterwandert.

ZEIT: Das heißt, Russland, China oder ein anderer Staat sitzt in unserem Stromnetz und wartet nur darauf, einen Schalter umzulegen?

Kubecka: Nein, so ist es nicht. Es geht dabei eher darum, Systeme auszuspähen und Informationen zu gewinnen, auch im Zuge von Industriespionage.

ZEIT: Was macht Sie so sicher?

Kubecka: Das weiß ich aus Gesprächen mit EU-Abgeordneten, aber ich habe es auch einfach schon so häufig selbst gesehen. Wie schon gesagt ist es extrem einfach, in manche Systeme einzudringen. Und wenn mir das gelingt, wäre es naiv anzunehmen, dass andere das nicht auch können. Über vieles davon kann ich nicht öffentlich sprechen. Aber diese Dinge geschehen. Deshalb sollten wir Pläne und Strategien festlegen, um gegebenenfalls schnell reagieren zu können. Das Leid, das allein bösartiger Code anrichten kann, habe ich aus nächster Nähe gesehen.

ZEIT: Bitte erzählen Sie.

Kubecka: Am 20. Februar 2022 bin ich in die Ukraine gereist, vier Tage vor dem russischen Angriff. Ich war dort als Beraterin für Cybersicherheit, eine ukrainische Sicherheitsfirma hatte mich für den Fall engagiert, dass es zu einem Cyberangriff auf eine Nuklearanlage kommen sollte. Doch dann wurde ich informiert, dass ich nicht länger sicher sei und das Land verlassen müsse. Später an der Grenze erfuhr ich, dass ich angeblich auf einer russischen Liste von Personen stand, die bei einer Invasion gezielt entführt werden sollten. Ich galt als hochrangiges Ziel.

ZEIT: Was geschah dann?

Kubecka: Am 25. Februar erreichte ich die Grenze zu Rumänien. Dort herrschte das absolute Chaos. Russland hatte in den beiden Tagen davor mit sogenannter Wiper-Schadsoftware, die ganze Festplatten löscht, zahlreiche ukrainische Behörden angegriffen, darunter die Grenz- und Zollbehörden. Davon erfuhr ich aber erst später.

ZEIT: Wie war die Situation vor Ort?

Kubecka: Es war bitterkalt. Tausende Menschen drängten sich dort. Manche Leute versuchten, zu Fuß zu flüchten. Ich sah Mütter mit Babys im Kinderwagen und Menschen im Rollstuhl. Es war ein Bild der Verzweiflung. Es gab nur eine Tankstelle mit einer Toilette, nur begrenzte Mengen an Essen und Wasser. Irgendwann kamen Gerüchte auf, die Russen würden den Grenzübergang mit Artillerie beschießen. Aber wir konnten nirgendwohin, weil alles blockiert war. Aus russischer Sicht hat dieser Cyberangriff den konventionellen Angriff perfekt ergänzt.

ZEIT: Was genau war passiert?

Kubecka: Die Grenzbeamten mussten nicht nur die Pässe prüfen, sondern auch, ob Männer im wehrfähigen Alter ausreiseberechtigt sind. Die entsprechenden Datenbanken waren aber gelöscht worden. Ebenso einige Identitäts-Datenbanken. Wer floh und nicht alle Geburtsurkunden seiner Kinder dabeihatte, konnte Probleme bekommen. Auch die ukrainische E-

Government-App Diia war betroffen – viele hatten dort ihre Dokumente gespeichert und konnten sie nicht vorzeigen. Also blieben dem Grenzschutz nur Stift und Papier. Am frühen Morgen des 26. Februar erfuhr ich von dem Cyberangriff. Ich konnte mich zu einem Grenzkommandanten durchschlagen und ihm erklären, dass ich helfen könnte. Gemeinsam verschafften wir uns einen Überblick. Er übergab mir eine Probe der Schadsoftware, die ich zur Analyse an Kollegen schickte. Dann konnten wir ausreisen. Es war surreal.

"Wir sollten uns auch Russlands Schwächen bewusst machen"

ZEIT: Sie beraten Regierungen und Unternehmen zum Thema Cybersicherheit, sind aber auch als White-Hat-Hackerin tätig. Was kann man sich darunter vorstellen?

Kubecka: Cybersicherheit wird häufig eher reaktiv finanziert. Erst wenn es brennt, zieht man los und kauft einen Feuerlöscher. Das führt dazu, dass ich mit meinem Wissen jederzeit jede Menge offen zugängliche kritische Systeme finden kann – zum Beispiel Windkraftanlagen. Anders als Kriminelle oder staatliche Hacker informiere ich diejenigen, bei denen ich die Sicherheitslücken finde. Leider ist das nicht in allen Ländern legal möglich.

ZEIT: Wo haben Sie noch solche offenen Türen entdeckt?

Kubecka: Vor ein paar Jahren konnte ich über ein Testsystem, das eigentlich nicht online sein sollte, ins EU-Stromnetz eindringen. Die Belege habe ich vor der EU-Kommission präsentiert. Und ich gelangte in 72 Stromerzeugungssysteme in den USA und Kanada. Die USA haben dieses Programm danach eingestellt. Außerdem hatte ich Zugriff auf ein italienisches Aquädukt, dessen Steuerung offen im Internet lag – ohne Login. Man stand quasi da wie ein Leittechniker, konnte Knöpfe drücken, den Druck und Mischverhältnisse ändern. Wenn in Wasser die falschen Chemikalien sind, können schädliche Stoffe aus den Rohren gelöst werden. In den USA gab es 2014 in Flint, Michigan, den Fall, dass – wohl aus Kostengründen und Unkenntnis – jemand die chemische Mischung geändert hat und Blei aus den Rohren gelöst wurde. Einige Menschen erlitten eine Bleivergiftung.

ZEIT: Warum müssen solche Systeme online sein?

Kubecka: Sie müssen nicht online sein. Aber gerade bei vielen kritischeren Systemen können die Hersteller aus der Ferne Diagnosen stellen und die Geräte warten. Übrigens auch bei Kernkraftwerken, Waffensystemen und Flugzeugen. Das hat offensichtliche Vorteile. Manchmal muss es schnell gehen, und einen Ingenieur zu schicken, würde zu lange dauern. Aber leider sind einige dieser Fernverbindungen nicht die neuesten. Ein Anbieter könnte für alle Kunden – sprich alle Kraftwerke, alle Waffensysteme – denselben

Benutzernamen und dasselbe Passwort verwenden, um sich die Administration zu erleichtern. Gleichzeitig gibt es keine Verpflichtung zu unabhängigen Sicherheitstests oder Zertifizierungen.

ZEIT: Das scheint fahrlässig.

Kubecka: Es kostet Zeit und Geld, Risiken zu senken. Das gilt auch für zusätzliche Tests oder eine externe Stelle, die all das prüft und zertifiziert. Im Grunde sind viele Waffensysteme oder auch Kraftwerke Teil des Internets der Dinge. Wie die vernetzten Geräte, die Sie vielleicht auch in Ihrem Haushalt haben. Auch die sind ein potenzielles Einfallstor für Hacker.

ZEIT: Haben Sie ein Beispiel?

Kubecka: Je mehr Daten Unternehmen bei Ihnen sammeln, desto mehr Profit können sie damit machen. Denken Sie an die Smart Meter, die digitalen Strommessgeräte, mit denen in Deutschland bis 2032 jeder Haushalt ausgestattet werden muss. Wer darauf Zugriff hat, kann abhängig von Tageszeit und Stromverbrauch herausfinden, wie viele Personen wie oft und wann im Haushalt sind. Kriminelle haben in den USA solche Informationen genutzt, um den perfekten Zeitpunkt für Einbrüche zu bestimmen. Solange solche Geräte von keiner unabhängigen Stelle auf Sicherheit und Datenschutz geprüft werden, würde ich sie nicht bei mir zu Hause haben wollen.

ZEIT: Die Gefahr von Cyberangriffen wirkt abstrakt. Kann man sich als Einzelperson überhaupt davor schützen?

Kubecka: Da gibt es eine sehr einfache Maßnahme. Wann haben Sie zuletzt Ihren Internetrouter neu gestartet?

ZEIT: Das ist schon eine Weile her.

Kubecka: 2022 hat man festgestellt, dass russische Hackergruppen gezielt schlecht gesicherte oder veraltete Heimrouter und kleine Firmenrouter in Europa angegriffen haben. Die niederländische Regierung hat damals empfohlen, Heimrouter mindestens einmal im Monat neu zu starten und Handys mindestens einmal pro Woche. Ich halte das für sinnvoll.

ZEIT: Das scheint fast ein wenig zu einfach.

Kubecka: Es gibt dieses Konzept der "Persistenz", wenn es darum geht, die Kontrolle über ein digitales Gerät aufrechtzuerhalten – sei es Ihr Router oder Ihr Telefon. Wenn Sie das Gerät neu starten, unterbrechen Sie diese laufende Angriffs-Session. Dann müssen Angreifer Sie erneut finden. Dadurch verbrauchen sie Ressourcen. Sie machen den Angriff kostspieliger – nur durch

das Neustarten dieser beiden Geräte. Allerdings gilt das nicht für alle Arten von Angriffen. Es gibt hoch entwickelte Spionagesoftware wie zum Beispiel Pegasus, gegen die Aus- und Einschalten nicht hilft.

ZEIT: Im James-Bond-Film *Skyfall* von 2012 manipuliert ein Hacker die Gasversorgung der MI6-Zentrale und jagt das Gebäude in die Luft. Sind das reine Hollywood-Fantasien?

Kubecka: Das ist gar nicht so weit weg von der Realität. 2014 veröffentlichte das Bundesamt für Sicherheit und Informationstechnik einen Bericht über einen Cyberangriff auf ein deutsches Stahlwerk. Die Angreifer waren über das Büro-IT-Netzwerk in die Steuerungssysteme des Werks eingedrungen. Der Angriff führte dazu, dass ein Hochofen nicht mehr kontrolliert heruntergefahren werden konnte und dadurch schweren Schaden nahm. Wer dahintersteckte, wurde nie veröffentlicht.

ZEIT: Seit dem Angriff Russlands scheinen die Berichte über Cyberangriffe in der Ukraine zurückgegangen zu sein. Spiegelt das die Realität wider?

Kubecka: Natürlich liegt Russlands Fokus stärker auf physischen Angriffen. Gleichzeitig kenne ich einige Leute, die in der Ukraine ständig damit beschäftigt sind, die digitale Infrastruktur nach Cyberangriffen wieder aufzubauen. Unternehmen, Stromnetze, Telekommunikation, Banken – alles. Sie leisten unglaublich gute Arbeit, viele davon übrigens Frauen. Wenn jemals Frieden herrschen sollte, müssen all diese Ukrainerinnen und Ukrainer als Top-Sicherheitsleute eingestellt werden.

“Wir sollten uns auch Russlands Schwächen bewusst machen.”

– Chris Kubecka

ZEIT: Welche übergeordnete Strategie verfolgt Russland mit seinen Cyberangriffen?

Kubecka: Teil der russischen Außenpolitik ist, bestimmte Regionen zu isolieren, zu spalten und gegen andere auszuspielen. Kürzlich wurde mir ein Leak von Russlands militärischer Drohnendoktrin zugespielt. Ein Teil davon besagt, dass Russland mittels Drohnen zivile Bereiche weichklopfen und psychologische Effekte erzeugen möchte. Meine Schlussfolgerung ist, dass die Bevölkerung so dazu gebracht werden soll, Druck auf ihre Regierungen auszuüben, eine beschwichtigende Haltung einzunehmen.

ZEIT: In der vergangenen Woche sollen Drohnen im Großraum Kiel Einrichtungen der kritischen Infrastruktur ausgespäht haben, darunter ein

Kraftwerk und eine Militärwerft. Könnte es sich dabei um Vorbereitungen für Militärschläge handeln?

Kubecka: Das glaube ich nicht. Vor allem dürfte das Ziel gewesen sein, Informationen über die Reaktionszeiten und Fähigkeiten der Deutschen zu sammeln. Wenn Drohnen, wie in diesem Fall, in parallelen Bahnen ein bestimmtes Muster abfliegen, geht es außerdem sehr wahrscheinlich darum, Messdaten zu sammeln. Russische Drohnen können für diesen Zweck mit allerlei Sensoren ausgestattet werden.

ZEIT: Was können wir aus Russlands Vorgehen lernen?

Kubecka: Wir müssen unsere Erkenntnisse auf nationaler und internationaler Ebene miteinander teilen. Denn unsere Gegner machen es schon längst. Der Iran und Russland tauschen sich zum Beispiel über den Einsatz von Drohnen aus. Aber wir sollten uns auch Russlands Schwächen bewusst machen.

ZEIT: Welche sind das?

Kubecka: Russland leidet unter einem gewaltigen Braindrain von Fachkräften. Aufgrund der Eskalation des Krieges wird Russlands digitale kritische Infrastruktur immer schwächer. Wir sehen immer verwundbarere Systeme. Wegen der wirtschaftlichen Lage können sie nicht einmal grundlegende Gehälter zahlen, um etwa die Systeme der Airline Aeroflot zu warten. Das sollten wir strategisch als Vorteil nutzen, zum Beispiel durch offensive Cyber-Operationen – sofern sie legal sind.

ZEIT: An welche Gegenmaßnahmen denken Sie dabei?

Kubecka: Russland ist sehr gut darin, Desinformation zu streuen. Wir sollten darauf mit gezielten Aufklärungskampagnen antworten und uns dabei an all diese frustrierten Menschen in Russland richten. Früher gab es dafür Hollywood, heute müssen wir neue Wege suchen, um die Herzen und Köpfe zu gewinnen.

ZEIT: Wie können wir uns als Gesellschaft besser gegen Cyberangriffe rüsten?

Kubecka: Wir sehen immer mehr Jugendliche und junge Erwachsene, die für Cyberkriminalität und Spionage angeworben und manipuliert werden. Für etwas Kryptogeld setzen sie GPS-Störsender ein oder fliegen mit Drohnen über sensible Standorte. Oft ohne zu wissen, für wen sie das wirklich tun. Vor ein paar Tagen wurden zwei 17-jährige Niederländer verhaftet, weil sie versucht haben sollen, im Auftrag prorussischer Hacker Daten aus den WLAN-Netzen von Europol, Eurojust und der kanadischen Botschaft in Den Haag abzugreifen. Die Eltern hatten keine Ahnung. Dass ein Kind in Onlinespielen oder auf Telegram von einem Staat rekrutiert werden könnte, klingt nach seltsamem James-Bond-Stoff. Aber genau das passiert. Wir müssen dafür ein Bewusstsein

schaffen und ein Klima, in dem es möglich ist, darüber zu sprechen. Und wir sollten technikinteressierten jungen Menschen Möglichkeiten bieten, wie in den Niederlanden, wo sie der Polizei helfen können, vermisste Personen zu finden. Dabei erhalten sie auch eine Ausbildung. In Deutschland gibt es solche Programme nicht.

ZEIT: Was kann Deutschland außerdem besser machen?

Kubecka: Koordination. Es gibt viele Dutzende Organisationen und Behörden auf Länder- und Bundesebene in Deutschland, die sich mit dem Thema Cyberwarfare beschäftigen. Aber nur ganz wenige sprechen miteinander. Deutschland diskutiert darüber, offensive Cyberfähigkeiten aufzubauen, kann diese Programme aber nicht koordinieren. Das halte ich für katastrophal. Bei einem Angriff auf die kritische Infrastruktur müssen sämtliche Kräfte zusammenkommen und gemeinsam antworten. Anders geht es nicht.