Staaten im Cyberkrieg: Digitales Sperrfeuer

- 01.06.2021
- Manuel Heckel

Staaten im Cyberkrieg: Digitales Sperrfeuer

Ob Pipeline oder Politik: Immer häufiger werden kritische Infrastrukturen oder staatliche Systeme Ziel von Cyberangriffen. Oft werden die Hacker:innen dabei selbst von Staaten finanziert. Um den Angriffen standzuhalten, setzen Behörden auf Künstliche Intelligenz, Koordination – und Konzepte aus historischen Krisen.

Die Angreifer:innen waren geduldig: Spätestens im Herbst 2019 hatten sie sich einen ersten Pfad in die Systeme von Solarwinds geschlagen. Das US-Unternehmen entwickelt Software, mit der große Firmen und Organisationen das Durcheinander ihrer eigenen IT-Systeme verwalten und koordinieren können. Mit jedem Update kamen die Schädlinge näher an diese Kunden heran. Dabei blieben sie lange unentdeckt. Erst kurz vor Weihnachten 2020 flogen die Hacker:innen auf. Bis dahin hatten sie schon einige Zeit in den Datenbanken von mehreren US-Ministerien verbracht, inklusive dem Pentagon, dem Außenministerium oder der Behörde für die nationale Nuklearsicherheit.

Das Entsetzen war groß. Die USA schlug zunächst verbal zurück: Der damalige Außenminister Mike Pompeo machte zügig Hackergruppen mit Verbindungen zur russischen Regierung für den Cyberangriff verantwortlich. Sein Chef Donald Trump opponierte, doch die neue Regierung unter US-Präsident Joe Biden schloss sich dieser Spur an. Im April dieses Jahres folgte die Reaktion – mit klassischer Diplomatie: Zehn russische Diplomat:innen wurden ausgewiesen, gegen sechs verdächtige russische Staatsbürger:innen wurden Sanktionen verhängt.

Das Beispiel zeigt: Der digitale Krieg ist in erster Linie ein kalter – und meist ein stiller. Im Verborgenen arbeiten Hacker:innen zunächst daran, sich einen Zugang zu den Systemen von Regierungen, Behörden oder zentralen Infrastruktureinrichtungen zu sichern. Dann bieten sich zahlreiche Optionen: Manchen reicht das Mitlesen und Abgreifen von Informationen, andere verschlüsseln notwendige Daten kurzerhand. Doch immer wieder drücken die Akteure aus der Ferne auch unerlaubt den Aus-Knopf. Dann sorgen digitale Angriffe für reale Schäden, wie das Schadprogramm Stuxnet, das 2010 iranische Atomaufbereitungsanlagen zerstörte. Oder die Hackergruppe BlackEnergy, die 2015 und 2016 dafür sorgte, dass das ukrainische Stromnetz ausfiel.

Digital verschwimmen die Grenzen der Landesverteidigung

Die Staaten wissen, welches Gefahrenpotenzial durch digitale Angreifer:innen droht: „Es gibt keine Unterscheidung mehr zwischen Online- und Offline-Bedrohungen“, heißt es etwa von der EU-Kommission, „digitale und physische Risiken sind inzwischen untrennbar miteinander verbunden.“ Die Herausforderung für Regierungen und Militärs weltweit: Wie sieht eine wirksame virtuelle Verteidigungsstrategie aus? „Im Cyberspace fehlen physische Grenzen, das macht es viel schwieriger, bestehende völkerrechtliche Regeln durchzusetzen“, sagt Thomas Reinhold, wissenschaftlicher Mitarbeiter am Lehrstuhl für Wissenschaft und Technik für Frieden und Sicherheit der TU Darmstadt.

Wenn feindliche Flugzeuge nur wenige Meter in den eigenen Luftraum eindringen, lassen Staaten Abfangjäger aufsteigen. Im digitalen Raum ist schon die Identifikation des Feindes deutlich schwieriger. Die meisten Angreifer:innen agieren als eine Art Guerilla-Truppe: Expert:innen sind sicher, dass Nationalstaaten die Hacker:innen finanzieren, unterstützen und dirigieren. Doch formal streiten Regierungen jeglichen Bezug ab. Eine Studie des Kriminologen Mike McGuire von der Universität Surrey zeigt, dass es seit 2009 über 200 Cyberattacken gab, in die Staaten direkt oder indirekt involviert waren, die allermeisten davon in den vergangenen drei Jahren.

So soll der russische Militärgeheimdienst eine Truppe steuern, die unter Namen wie Sofacy Group, APT28 oder Fancy Bear hinter zahlreichen Angriffen auf US-Systeme steckt. Nordkorea verfügt mit dem „Büro 121“ über hunderte staatliche Hacker, die unter anderem im Frühjahr versucht haben sollen, an Impfstoff-Daten des Pharmakonzerns Pfizer zu gelangen. Und in diesem Frühjahr griff Amnesty International die vietnamesische Regierung scharf an: Die Gruppe „Ocean Lotus“ mit Verbindungen nach Hanoi soll die Webseiten und Social-Media-Profile von Menschrechtsaktivisten angegriffen haben. Statt milliardenschwerer Rüstungsprogramme reichen vergleichsweise kleine Digitaltruppen für

gezielte Angriffe: „Auch kleinere Staaten, die sich keine schlagkräftige Armee leisten können, können so aktiv werden“, sagt Reinhold.

Komplexe Koordination gegen die Cyberangreifer
Machtlos sind die Staaten jedoch keineswegs. Doch die Strategien im Cyberkrieg unterscheiden sich. Die USA setzen etwa seit vielen Jahren explizit auf das Konzept „defend forward“ – also eine aktive Vorwärtsverteidigung. Im Cyberraum heißt das: Das Militär sucht und schafft sich selbst Zugänge zu relevanten IT-Systemen. Das ermöglicht zum einen, selbst gegen Staaten oder staatliche Gruppen vorgehen zu können. Und zum anderen etabliert die USA so eine Drohkulisse im virtuellen Raum: „Nur wenn man selbst in den Systemen steckt, kann man anderen glaubhaft versichern, dass man Angreifern das Licht ausknipsen kann“, sagt Reinhold, der dem amerikanischen Abschreckungskonzept kritisch gegenüber steht.

Die EU-Kommission setzt vor allem auf Defensive. Sie hat im vergangenen Dezember ihre Pläne für eine neue Cybersicherheitsstrategie vorgestellt. Neue Richtlinien sollen künftig ein höheres Schutzniveau für Krankenhäuser, Energienetze, Verkehrswege und staatliche Rechenzentren vorgeben. Mithilfe von Künstlicher Intelligenz solle zudem ein „Cybersicherheitsschutzschild“ etabliert werden – so könnten abweichende, verdächtige Datenbewegungen frühzeitig erkannt werden. Ein neues Kompetenzzentrum entsteht bald in Bukarest.

Eine Ebene darunter bauen die Mitgliedsstaaten ihre Verteidigungslinien auf: Frankreich hat in diesem Februar einen „1-Milliarde-Euro-Plan für Cybersicherheit“ vorgestellt . Die sollen zum einen dem Aufbau von staatlichen Strukturen, zum anderen jedoch auch Start-ups finanzieren, die im Bereich der IT-Sicherheit aktiv sind. In Deutschland wurde Anfang Mai das „IT-Sicherheitsgesetz 2.0“ vom Bundesrat verabschiedet. „Die Digitalisierung durchdringt alle Lebensbereiche, die Pandemie hat diesen Prozess noch einmal enorm beschleunigt“, sagte Innenminister Horst

Seehofer. „Unsere Schutzmechanismen und Abwehrstrategien müssen Schritt halten – genau dazu dient das IT-Sicherheitsgesetz 2.0“.

Jenseits der großen Strategien zeigt sich jedoch: Die Abwehr gegen die agilen Angreifer:innen zu koordinieren, ist eine große Herausforderung. Die Stiftung Neue Verantwortung (SNV) aktualisiert seit vielen Jahren ein Dokument, in dem alle relevanten Akteure der deutschen Cybersicherheitsarchitektur präsentiert werden. Die aktuelle Version hat 105 Seiten – von der Agentur der Europäischen Union für Cybersicherheit (ENISA) bis zum Hessen Cyber Competence Center (Hessen3C). Grundsätzlich sei solch ein komplexer Aufbau jedoch richtig und hilfreich, sagt Sven Herpig, Leiter für Internationale Cybersicherheitspolitik bei der SNV: „Es ist wichtig für Behörden und Unternehmen, auch lokal einen Ansprechpartner zu haben“. In den Ebenen darüber geht es dann um den Austausch zu Angreifern und Einfallstoren – oder darum, technische Standards zu entwickeln, die diese Tore etwas dichter abschließen.

Abwehr stärken statt Angriffe reiten

Ebenso wichtig jedoch: „Das Ganze kann nur funktionieren, wenn auch die zentralen Akteure wirksam arbeiten“, so Herpig. Das gelingt aus Sicht von Expert:innen in Deutschland nicht immer. Die staatliche „Agentur für Sprunginnovationen in der Cybersicherheit“ wurde vor knapp drei Jahren ins Leben gerufen. Forschungsprojekte hat sie bislang noch nicht auf den Weg gebracht – und Anfang Mai hatten sowohl der Forschungs- als auch der kaufmännische Direktor die Agentur verlassen. Auch das Beratungsgremium Cyber-Sicherheitsrat hat noch keine großen Erkenntnisse vermeldet. Beobachter Herpig wünscht sich, dass die wichtigen Gremien über einen „Arbeitsmuskel“ verfügen, einen „vernünftigen, mit passenden Fachkräften ausgestatteten, Unterbau“. Immerhin: Das Cyber-Abwehrzentrum in Bonn soll künftig deutlich mehr Stellen bekommen – hier arbeiten IT-Expert:innen von Bundeskriminalamt, Bundeswehr und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen.

Der Bundesnachrichtendienst hat vor wenigen Wochen eine eigene Kampagne gestartet, um Nachwuchskräfte mit Code-Kenntnissen zu finden. Gesucht werden neue Mitarbeiter mit der „License to hack“. Grundsätzlich sind die deutschen und europäischen Vorhaben jedoch deutlich stärker auf Verteidigung ausgerichtet als etwa die der USA. „Der aussichtreichste Weg ist es, die eigenen Systeme so sicher wie möglich zu machen“, sagt Informatiker Reinhold. In einem Wettrüsten um die besten eigenen Angriffsmöglichkeiten fehlt nämlich häufig – trotz Werbekampagnen –eine wichtige Ressource: Informatiker:innen und Datenspezialist:innen. Denn die Behörden suchen ebenso wie Unternehmen nach diesen Fachkräften – sind aber in der Regel an die Tarifverträge des öffentlichen Dienstes gebunden.

Abrüstung im virtuellen Raum

Auch aus rechtlichen Gründen plädieren viele Expert:innen eher für eine defensive Strategie. „Überwachungswerkzeuge sind nicht sinnvoll investiertes Geld, wenn wir die IT-Sicherheit stärken wollen“, warnt Herpig. Die Bundeswehr etwa müsste sich in der Theorie etwa auch Cyberangriffe vom Parlament absegnen lassen. Das entspräche der Verfassung – aber würde wirkungsvolle digitale Präventivschläge so gut wie unmöglich machen. „Im Prinzip müsste die Bundeswehr schon in Friedenszeiten in den Systemen und damit auf dem Boden fremder Staaten aktiv sein“, sagt Reinhold. „Dazu müsste dringend eine Klärung auf gesetzlicher Ebene stattfinden.“ Ein grundsätzliches großes Problem aus seiner Sicht: Sobald staatliche Akteure sich Schlupflöcher in fremde Systeme suchen, ist deren Integrität verletzt.

Auf lange Frist haben Staaten und Verbände auch die Hoffnung auf eine politische Lösung nicht aufgegeben. „Die EU wird ihr Instrumentarium für die Cyberdiplomatie weiter stärken“, heißt es in dem Entwurf der EU-Kommission. Wie das genau umgesetzt werden soll, steht jedoch noch nicht fest. Eine idealistische Idee: Eine Art globaler Abrüstungsvertrag für den digitalen Raum. „Natürlich ist es schwierig, damit auch nicht-staatliche

Akteure einzufangen“, räumt Reinhold ein, „aber man kann die Hoffnung haben, dass die Länder das aus einem gewissen Eigennutz dann auch durchsetzen“. Wie bei anderen Waffengattungen könnte das durch gegenseitige Einblicke in das Hacker-Arsenal abgesichert werden – und so nach einiger Zeit zu einem Gleichgewicht der Cyber-Angriffskapazitäten führen.

Titelbild: Getty Images