Nr. 391 / Juni 2020
Analysen & Argumente

KONRAD ADENAUER STIFTUNG

Coronaperspektiven

Die Auswirkungen von COVID-19 auf Cyberkriminalität und staatliche Cyberaktivitäten

Johannes Wiggen

- Die COVID-19-Pandemie illustriert durch die gestiegene Nutzung digitaler Angebote und den Einsatz weniger geschützter, privater IT-Geräte im Home-Office digitale Sicherheitsrisiken und verdeutlicht die Notwendigkeit adäquater Maßnahmen zum Schutz von IT-Systemen in kritischen Infrastrukturen.
- Cyberkriminalität profitiert gegenwärtig von der Unsicherheit und dem Informationsbedürfnis der Menschen
- Staaten nutzen vermehrt Cyberspionage, um Informationen über Maßnahmen zur Bekämpfung des Coronavirus, potentielle Impfungen und Behandlungsmethoden zu erlangen.
- Cybergefahren können nur mit einem Bündel an Maßnahmen auf ein annehmbares Maß reduziert werden: Mit Blick auf Cyberkriminalität gilt es z. B. das Aufklärungs- und Präventionsangebot sowie Digitalbildung zu stärken und die Ressourcen der Strafverfolgungsbehörden zur Prävention sowie Aufklärung von Cyberkriminalität durch gezielte Nachwuchsgewinnung auszubauen; staatliche Cyberaktivitäten sollten mit politischen und wirtschaftlichen Sanktionen oder Anklagen sowie Cyberdiplomatie adressiert werden.

Inhaltsverzeichnis

Die Pandemie hat dazu geführt, dass digitale Anwendungen verstärkt genutzt werden, Unternehmen und Behörden ganze Arbeitsprozesse ad hoc ins Internet verlagerten und Krankenhäuser noch mehr als sonst auf das ordnungsgemäße Funktionieren ihrer IT-Systeme angewiesen sind. Was bedeutet das für die Cybersicherheit?

Hintergrund

Zur Eindämmung des Coronavirus haben Regierungen im März 2020 weltweit Kontaktbeschränkungen oder Ausgangssperren erlassen. Wo möglich, schickten die meisten Arbeitgeber ihre Mitarbeiter ins Home-Office. Dort werden vermehrt private IT-Geräte für dienstliche Zwecke eingesetzt. Diese vergrößerte IT-Oberfläche ist oftmals weniger geschützt als beruflich genutzte IT-Geräte. Unter Zeitdruck werden neue Programme, z. B. für Telefon- und Videokonferenzen, meist ohne ausreichende Sicherheitsprüfung eingeführt. Außerdem mehren sich Berichte über Cyberattacken auf Organisationen aus dem Gesundheitssektor, auf dessen ordnungsgemäßes Funktionieren Staaten und Gesellschaften gerade noch mehr als sonst angewiesen sind. Welche Auswirkungen hat die COVID-19-Pandemie auf die Cybersicherheit, Cyberkriminalität und staatliche Cyberaktivitäten?[1] Wie kann die Politik Cyberbedrohungen reduzieren bzw. mit diesen umgehen?

Gestiegene Internetnutzung und Home-Office erhöhen digitale Sicherheitsrisiken

COVID-19 führt zu Rekord-Internetnutzung

Digitale Informationsangebote, soziale Medien, Streaming- und Clouddienste, E-Mails und Telefon- bzw. Videokonferenzprogramme werden verstärkt genutzt.[2] Dies schlägt sich in der Auslastung des Internets nieder: Mitte März vermeldete der nach Datendurchsatz weltweit größte, in Frankfurt ansässige Internetknoten DE-CIX, in dem Datenströme von verschiedenen Internetdienstanbietern zusammenlaufen, in der Spitze einen Datenverkehr von 9,1 Terabit (TBit) in der Sekunde.[3] Das entspricht in etwa dem Datenvolumen von 1.800 heruntergeladenen HD-Filmen. Dieser Rekordwert ist der größte Anstieg im Datenverkehr, den das Unternehmen vom bisherigen Spitzenwert, 8,3 TBit, je zu verzeichnen hatte und den es aufgrund der zunehmenden Internetnutzung sowie saisonaler Schwankungen erst für Ende des Jahres erwartet hatte. Grundsätzlich bieten die intensivere Nutzung des Internets und neue, d. h. unerfahrene Nutzer, kriminellen bzw. heimtückischen Akteuren mehr Möglichkeiten für ihre Aktivitäten.

Unsichere IT-Oberfläche

Hinzu kommt, dass sich die weniger gut geschützte IT-Oberfläche, seitdem Millionen von Menschen kurzfristig von zu Hause aus arbeiten, vergrößert hat. In großen Unternehmen, Behörden und Organisationen gibt es in der Regel einen institutionalisierten Schutz von IT-Systemen. Hier werden im Optimalfall IT-Sicherheitsstandards mit entsprechenden Maßnahmen implementiert, Schwachstellen in genutzter Software regelmäßig durch das Aufspielen von Herstellerupdates geschlossen und das interne Netzwerk geschützt. Private IT-Geräte sind oftmals unsicherer. Heimnetzwerke sind in der Regel weniger gesichert, auf privaten Computern fehlen häufig professionelle Virenschutzprogramme oder Firewalls. Außerdem kann auf Privatgeräten Software laufen, die grundlegende Sicherheitslücken aufweist, deren Sicherheitslücken durch ein nicht durchgeführtes Update des Herstellers nicht geschlossen wurden oder deren Software schlicht am Ende ihres Lebenszyklus ist und die damit keine sicherheitsrelevanten Updates mehr bekommt. Letzteres ist z. B. bei dem Betriebssystem *Windows* 7 der Fall, für das Microsoft Anfang 2020 den Support eingestellt hat, das aber immer noch millionenfach verwendet wird – u. a. beispielsweise. auf 8.000 Rechnern der Hamburger Polizei.[4] Gleichzeitig werden durch das Home-Office unter Zeitdruck vermehrt Schnittstellen zum Fernzugriff auf das interne Netzwerk der jeweiligen Organisation oder Institution eingerichtet. Dies erschwert es den IT-Experten der jeweiligen Institution oder Organisation, unrechtmäßige Netzwerkverbindungen ausfindig zu machen, und bietet Hackern eine Möglichkeit, Zugriff auf interne Netzwerke zu erlangen. Umgekehrt werden Arbeitscomputer, auf denen sich z. B. sensible Daten befinden können, im Home-Office teilweise für private Zwecke verwendet, was ebenfalls ein Einfallstor für Hacker sein kann. All dies resultiert in einer gestiegenen Anzahl an Sicherheitsrisiken.

Cyberkriminalität profitiert von Neugierde und Informationsbedürfnis der Menschen

Schwachstelle Mensch

Maßgeblich hinzu kommt die so bislang noch nie dagewesene Situation: Ähnlich wie andere besondere Situationen – z. B. 2018 die Einführung der europäischen *Datenschutz-Grundverordnung* (*DSGVO*) – bietet die COVID-19-Pandemie die Möglichkeit, die Verunsicherung, Neugierde und das Informationsbedürfnis von Menschen gezielt für kriminelle oder heimtückische Aktivitäten auszunutzen.[5] Mit der persönlichen Gesundheit lässt sich das Informationsbedürfnis besonders wecken – vor allem, wenn es beispielsweise um Schutzmaßnahmen, angebliche Behandlungsmethoden, eine Impfung oder vermeintliche Informationen von staatlichen Stellen geht. So verlieren Internetnutzer ihren Argwohn und werden zum Opfer von Betrugsmaschen oder Schadsoftware. Dieses gezielte Manipulieren von Menschen wird auch als *Social Engineering* bezeichnet – das „Hacken von Menschen". Cyberkriminelle profitieren von der besonderen Situation und versuchen diese durch die Anpassung ihrer Aktivitäten auszunutzen, um sich zu bereichern. Eine beliebte Methode sind sogenannte Phishing-E-Mails, die in großem Stil versendet werden.[6] Mit gefälschten E-Mails sollen Internetnutzer unter einem falschen, aber möglichst glaubwürdigen Vorwand zur Eingabe von Passwörtern, sensiblen Daten oder dem Öffnen eines mit Schadsoftware infizierten E-Mail-Anhangs bewegt werden. Kriminelle Phishing-Kampagnen mit Bezug zum Coronavirus sollen der Informationssicherheitsfirma Fireeye zufolge seit Januar 2020 „dramatisch" zunehmen.[7]

Bereicherung durch Betrug

Das Bundesamt für Sicherheit in der Informationstechnik (BSI), das für die IT-Sicherheit in Deutschland zuständig ist, warnte Anfang April 2020 vor einer „Zunahme von Cyber-Angriffen mit Bezug zum Corona-Virus auf Unternehmen und Bürger".[8] Das Wirtschaftsministerium in Nordrhein-Westfalen stoppte Anfang April 2020 die Auszahlung von Soforthilfe an Selbstständige und Unternehmen, nachdem das Landeskriminalamt vor gefälschten Webseiten gewarnt hatte, auf denen Kriminelle versuchten über entsprechende Antragsformulare Daten zu sammeln, um mit diesen wiederum betrügerische Anträge auf Soforthilfen zu stellen.[9]

Die Verbraucherzentrale Nordrhein-Westfalen machte Mitte März auf eine professionelle Phishing-Kampagne aufmerksam. In authentisch aussehenden E-Mails geben sich Cyberkriminelle als Bank aus und sprechen gezielt die Emotionen von Menschen an, um diese unter dem Vorwand der Aufrechterhaltung der Kommunikation in Zeiten von geschlossenen Bankfilialen zur Eingabe sensibler Kundendaten auf einer authentisch aussehenden Webseite zu bewegen.[10] Solche Daten zur digitalen Identität, wie die E-Mail-Adresse, die Anschrift oder das Geburtsdatum, werden anschließend zur finanziellen Bereicherung genutzt. Ebenfalls gibt es Berichte über Webseiten und eine Android-App, die in Anlehnung an die populäre Karte der Johns Hopkins Universität Echtzeit-Informationen über die Ausbreitung des Virus versprechen, die Nutzer dabei aber mit Schadsoftware infizieren.[11]

Gesundheitssektor als besonders essentieller Bereich in einer Pandemie

Aktuell warnen IT-Sicherheitsexperten vor einem Anstieg von Cyberattacken auf Organisationen und Institutionen aus dem Gesundheitssektor.[12] Bei Cyberangriffen auf Krankenhäuser sind Kriminelle primär an demografischen und finanziellen Informationen interessiert, um mit Daten zur digitalen Identität Geld zu verdienen.[13] Hierbei können die IT-Systeme von Krankenhäusern absichtlich oder unabsichtlich beeinträchtigt werden. Tschechiens zweitgrößtes Krankenhaus, die Universitätsklinik Brno, wurde am 13. März das Ziel einer nicht näher spezifizierten Cyberattacke bislang unbekannter Herkunft.[14] Das Krankenhaus, das auch für Corona-Tests zuständig ist, musste Teile seines IT-Systems herunterfahren und geplante Operationen verschieben. Den Grundbetrieb konnte die Klinik weiterhin gewährleisten, seine Arbeit rund um das neue Virus wurde nicht eingeschränkt.

Gesundheitssektor unter doppeltem Druck

Krankenhäuser und andere Einrichtungen aus dem Gesundheitssektor können ferner das Ziel sogenannter *Ransomware* werden. Mit solch einer Schadsoftware verschlüsseln Kriminelle die gespeicherten Informationen ihrer Opfer, um sie anschließend zu erpressen. Das ungewisse Versprechen: Gegen eine Zahlung werden die Daten wieder entschlüsselt. In London wurde z. B. ein Labor, das bereit stand, um eine potentielle Impfung gegen das Coronavirus zu testen, Opfer einer *Ransomware*-Attacke durch eine etablierte Gruppe Cyberkrimineller.[15] Das Unternehmen konnte seine IT-Systeme erfolgreich schützen, die Angreifer konnten aber Patientenakten abfischen, die sie im Internet veröffentlichten. Das Computer-Emergency-Response-Team (CERT-FR) der französischen Regierung warnte seine Lokalbehörden Ende März ebenfalls vor einer *Ransomware*-Kampagne.[16]

Von Spionage bis Sabotage: COVID-19 und staatliche Hacker

Neben Kriminellen nutzen auch staatliche Akteure, die in der Cyberdomäne versuchen verdeckt zu operieren, um sich politischer Verantwortlichkeit zu entziehen, die Ausnahmesituation mit gezielten Phishing-Emails – dem sogenannten *Spear-Phishing* – für Spionagezwecke aus. Hackergruppen, die Russland, China und Nordkorea zugerechnet werden, setzen personalisierte E-Mails mit Bezügen zur Pandemie und deren Folgen ein, um ihre Ziele mit Schadsoftware zu infizieren oder Passwörter abzugreifen.[17] In der COVID-19-Pandemie, die erneut illustriert, dass die nationale Sicherheit nicht nur traditionell militärische Bedrohungen umfassen sollte, rücken neue Ziele in den Fokus der Informationssammlung von Nachrichtendiensten im Internet, der sogenannten *Signals Intelligence* (*SIGINT*). Klassische *SIGINT*-Ziele sind politische und militärische Institutionen, die z. B. Aufschluss über politische Entscheidungsprozesse oder militärische Fähigkeiten eines Landes geben können.[18] Ein weiteres gewichtiges Betätigungsfeld von Nachrichtendiensten im Internet ist neben der Gegenspionage, d. h. der Abwehr der Tätigkeiten anderer Nachrichtendienste, die Wirtschaftsspionage.

„Wissen ist Macht“

Gegenwärtig von besonderem Interesse für Staaten sind Informationen über die Ausbreitung des Coronavirus, staatliche Eindämmungsmaßnahmen und potentielle Medikamente sowie Impfstoffe. Solche Informationen können entscheidende strategische Vorteile bei der Bekämpfung der Pandemie bringen. Damit rücken vor allem Institutionen und Organisationen aus dem Gesundheitssektor, der Pharmazie und Biotechnik, entsprechende staatliche Stellen sowie Logistikinfrastrukturen ins Visier von Nachrichtendiensten.[19] Folglich überrascht es nicht, dass z. B. Mitarbeiter der Weltgesundheitsorganisation (WHO) im März 2020 das Ziel von *Spear-Phishing*-E-Mails waren, die dem Iran zugerechnet werden.[20] Mitte Mai 2020 warnten das US-amerikanische Federal Bureau of Investigation (FBI) und die Cybersecurity and Infrastructure Security Agency (CISA) zusammen vor China zugerechneten Hackergruppen und „non-traditional collectors“.[21] Sie sollen US-Einrichtungen, die zum Coronavirus forschen, mit dem Ziel der Identifikation und Erlangung geistigen Eigentums sowie öffentlicher Gesundheitsdaten mit Bezug zu Impfungen, Behandlungen und Coronatests digital aufklären und teilweise auch schon in deren Netzwerke eingedrungen sein. Zwei Gruppen, die ebenfalls China zugerechnet werden, sollen E-Mails mit angehängten Dokumenten, die wahre Gesundheitsinformationen enthalten, an Ziele in Vietnam, der Mongolei und den Philippinen versendet haben, um diese mit Spionagesoftware zu infizieren. Ähnlich soll eine russische Gruppe aktiv sein, die gegen ukrainische Ziele operiert.[22]

Neue Kommunikationswege sind anfällig für Spionage und Wirtschaftsspionage

Eldorao für staatliche Spione

Da physische Besprechungen gegenwärtig nicht stattfinden können, weichen Unternehmen, Regierungen und Behörden oftmals kurzfristig nach Verfügbarkeit und Benutzerfreundlichkeit auf Programme für Telefon- und Videokonferenzen aus. Diese Programme können unsicher oder ihr Hersteller nicht vertrauenswürdig bzw. von Nachrichtendiensten unterwandert sein. In der Vergangenheit waren solche Kommunikationskanäle für Nachrichtendienste ein attraktives Ziel, wie zuletzt das Beispiel der Schweizer Crypto AG zeigte.[23] Regierungen und Behörden verfügen in der Regel über sichere Gesprächskanäle. In einem Szenario, wie gegenwärtig in der COVID-19-Pandemie, in dem viele Regierungsmitglieder und Behördenmitarbeiter räumlich getrennt voneinander arbeiten, ist diese sichere Kommunikationsinfrastruktur aber häufig zahlenmäßig unzureichend.

Das zeigt sich daran, dass z. B. die britische Regierung das Videokonferenz-Programm Zoom des gleichnamigen US-Unternehmens für ein digitales „Kabinettstreffen“ verwendete. Das Unternehmen, für das in China ca. 700 Menschen im Bereich Forschung und Entwicklung arbeiten, konnte die Zahl seiner Nutzer von ca. 10 Millionen am Tag im Dezember 2019 auf über 200 Millionen Nutzer am Tag im März 2020 steigern.[24] Zoom warb damit, dass sein Dienst Ende-zu-Ende verschlüsselt ist, d. h. nur die daran beteiligten Personen im Stande sind, die ausgetauschten Informationen zu lesen. Das Unternehmen stand aufgrund unzureichender Datenschutzstandards und einer mangelhaften Verschlüsselung von übertragenen Gesprächen Anfang April 2020 öffentlich in der Kritik.[25] Auf die Missstände reagierte Zoom umgehend mit Maßnahmen zur Erhöhung der Transparenz, des Datenschutzes, der Bereitstellung erster Softwareupdates sowie einem umfassenden Plan, wie Datenschutz und die Sicherheit des Programms, u. a. durch die geplante Implementation einer echten Ende-zu-Ende-Verschlüsselung, zukünftig verbessert werden können.[26]

Folglich können Nachrichtendienste die COVID-19-Pandemie nutzen, um sensible Kommunikation, die gerade vermehrt online stattfindet, abzugreifen. Das Auswärtige Amt (AA) verbot einem Bericht zufolge nach einer eigenen Prüfung von Zoom dessen Nutzung auf mobilen

Geräten für die Mitarbeiter des eigenen Hauses.[27] Da viele Partner des Außenministeriums das Programm nutzten, sei ein gänzlicher Ausschluss zurzeit aber nicht möglich. Eine einheitliche Regelung zur Nutzung des Dienstes gebe es in der Bundesregierung aber nicht.

Cybersabotage

Auch indirekte Auswirkungen von Cyberattacken können beträchtlichen Schaden verursachen.

Neben der Spionage können Staaten Cyberoperationen in Friedenszeiten auch zum Zweck der Sabotage, d. h. der Beeinträchtigung von Software und Betriebsprozessen zur Schwächung eines ökonomischen oder politischen Systems nutzen.[28] So soll eine gegebene Situation zum Vorteil des sabotierenden Staates beeinflusst werden.[29] In einer bestehenden Krise wie einer Pandemie könnten solche Cyberattacken, z. B. auf die IT-Systeme von kritischen Infrastrukturen, die ohnehin angespannte Lage zusätzlich verschärfen. Das Beispiel *NotPetya* hat 2017 gezeigt, dass Cyberattacken auch ohne direkte physische Auswirkungen zu verursachen weitreichende Folgen haben können, indem sie die Funktionalität von Computern negativ beeinflussen: Die russische Schadsoftware verschlüsselte für das Funktionieren von Windows-Computern essentielle Daten irreversibel und machte betroffene Computer so unbrauchbar.[30] Schwerpunktmäßig betroffen war die Ukraine, die US-Administration bezifferte den Gesamtschaden von *NetPetya* auf zehn Milliarden US-Dollar. Mitte April 2020 warnte die tschechische National Cyber and Information Security Agency (NUKIB) ihre Verbündeten vor einer bevorstehenden Welle von Cyberangriffen auf Krankenhäuser und kritische Infrastrukturen des Landes eines „ernsten" und technisch versierten Angreifers, die ebenso gezielt Windows-Computer unbrauchbar machen sollte.[31] Am nächsten Tag wurden u. a. die IT-Systeme von zwei tschechischen Krankenhäuser das Ziel von nicht näher spezifizierten Cyberattacken unbekannter Herkunft, die aber beide erfolgreich abgewehrt werden konnten.[32]

Wie umgehen mit Cyberkriminalität, Cyberspionage und Cybersabotage?

Differenzierung zwischen Kriminalität und staatlichen Aktivitäten hilfreich

Die COVID-19-Pandemie verdeutlicht bestehende Cyberbedrohungen und Sicherheitslücken. Wie in der „realen" Welt gibt es auch in der Cyberdomäne keine einhundertprozentige Sicherheit. Gefahren können nur mit einem Bündel an Maßnahmen auf ein annehmbares Maß reduziert werden. Mit Blick auf den Umgang von Cyberbedrohungen ist es hilfreich zwischen den Aktivitäten krimineller Akteure, die meist aus dem Motiv der Bereicherung agieren, und staatlichen Akteuren, die in Friedenszeiten mit Cyberoperationen versuchen strategische Vorteile zu erlangen, zu unterscheiden.

Aufklärung, Prävention, Digitalbildung & finanzielle Förderung

Grundsätzlich ist zu erwarten, dass Cyberkriminalität durch die fortschreitende Digitalisierung weiter an Bedeutung gewinnen wird. Betrugsmaschen mit Bezug zum Coronavirus bzw. daraus resultierenden Entwicklungen werden für die Dauer, in der das Virus die Schlagzeilen bestimmt, auf einem hohen Niveau bleiben. Cyberkriminelle werden ihre Aktivitäten dem weiteren Verlauf der Pandemie anpassen. Die Gefahr, die hiervon ausgeht, lässt sich nur zusammen mit den Bürgerinnen und Bürgern sowie Unternehmen und Organisationen auf ein annehmbares Niveau reduzieren. Da der Mensch beim S*ocial Engineering* im Vordergrund steht, gilt es, die Aufklärungs- und Präventionsarbeit, die z. B. das BSI, das Bundeskriminalamt (BKA) oder die Polizeien der Länder betreiben, zu verstärken.[33] Groß angelegte Sensibilisierungskampagnen, die auf die Gefahren vor Phishing-E-Mails hinweisen, könnten hier ebenso eine adäquate Maßnahme sein wie der Ausbau von Angeboten zur Digitalbildung in Schulen, Universitäten und der Erwachsenenbildung. Kleine und mittelständische Unternehmen (KMU), die oftmals nicht über ausreichend Ressourcen verfügen, gilt es außerdem gezielt zu fördern, damit diese ihre IT-Systeme besser schützen und ihr Personal schulen können.

Bei den Strafverfolgungsbehörden sollten die Kapazitäten und das Wissen zur Prävention und Aufklärung von Cyberkriminalität ausgebaut werden. Wie in den Ministerien und Bundesbehörden, in denen von 2.800 Stellen für IT-Sicherheit jede vierte unbesetzt ist, mangelt es oftmals an entsprechend ausgebildetem Personal.[34] Hier gilt es mit gezielten Maßnahmen zur Ausbildung von IT-Fachkräften gegenzusteuern. Beispielhaft ist die Schaffung einer Fortbildung von vorgebildeten Fachkräften zu Cyberkriminalisten durch das BKA oder die Einrichtung eines Studiengangs Cyberkriminalistik zur Ausbildung von speziell geschulten Polizisten in Hessen.[35]

Identifikation neuer schutzbedürftiger Einrichtungen & Evaluation bestehender Schutzmaßnahmen

Zum Schutz Kritischer Infrastrukturen (KRITIS) wie z. B. von Kraftwerken, elementarer Bestandteile des Staates und der Verwaltung oder Krankenhäusern hat die Europäische Union 2016 die *Network and Information Security*-Richtlinie verabschiedet.[36] Mit ihr wurden die Betreiber „essentieller Dienstleistungen" durch die Mitgliedsstaaten u. a. zur Einführung und Einhaltung von organisationalen und technischen Sicherheitsstandards in Bezug auf die Sicherheit von IT-Systemen verpflichtet.[37] Die COVID-19-Pandemie illustriert gegenwärtig, welche Organisationen und Institutionen in einer Krise wirklich kritisch sind. Da Krankenhäuser vergleichsweise weiche Ziele sind, die oftmals unter Sparzwängen stehen, was sich in veralteten und unsicheren IT-Systemen widerspiegelt, könnte ein Ansatzpunkt sein, diese für den Schutz ihrer IT-Systeme finanziell besser auszustatten. Ebenfalls kann COVID-19 als Ausgangspunkt zur Identifikation neuer, schutzbedürftiger Organisationen bzw. der Evaluation der bisherigen Schutzmaßnahmen dienen.

Vorhaltung sicherer Kommunikationskanäle für Regierungen und Behörden essentiell

Mit Blick auf staatliche Cyberaktivitäten ist zu vermuten, dass die *SIGINT*-Aktivitäten von Nachrichtendiensten künftig Gesundheitsthemen vermehrt berücksichtigen und in ihrem Ausmaß zunehmen werden.[38] Grundsätzlich muss bei der Nutzung von Programmen zur Kommunikation oder dem Austausch von Daten berücksichtigt werden, ob bzw. wie sehr die betreffenden Informationen schutzbedürftig sind. Zoom z. B. für ein Gespräch mit Freunden zu nutzen ist unproblematisch, seine Verwendung in der gegenwärtigen Version für den Austausch sensibelster Geschäftsgeheimnisse oder Kabinettssitzungen hingegen ein Risiko. Die Pandemie zeigt damit die Notwendigkeit der Vorhaltung sicherer und zuverlässiger Kommunikationskanäle für vertrauliche Informationen auch für die Breite von Mitarbeitern – vor allem von Regierungen und Behörden. Ähnlich wie in der Causa *5G*, bei der es eine rege Diskussion um das Für und Wider der Beteiligung chinesischer Unternehmen am Aufbau des neuen Mobilfunkstandards gibt, sollte die Politik eine grundsätzliche und umfassende Diskussion über die Abwägung möglicher Sicherheitsrisiken bei der Nutzung von Informations- und Kommunikationstechnik in sensiblen Bereichen führen. Denn mit Blick auf Sicherheitsrisiken muss berücksichtigt werden, dass ein staatlicher Akteur, der z. B. durch Updates Einfluss auf etablierte Soft- oder Hardware nehmen kann, seine Intentionen in einer Krise jederzeit verändern kann.

Eskalationsrisiko vermeiden

Über die möglichen Risiken einer immer weiter ausufernden Informationssammlung und die Rolle zunehmend aggressiver agierender Nachrichtendienste für das künftige Verhalten von Staaten in der Cyberdomäne sollte diskutiert werden, um sich zuspitzende staatliche Interaktion in der Cyberdomäne zu vermeiden.[39] Staaten sollten Cyberspionage oder Cybersabotage nicht mit dem Eindringen in die Netzwerke des Gegners oder neutraler IT-Systeme beantworten. Solche sogenannten Maßnahmen der Aktiven-Cyberabwehr sind je nach Kontext in der Praxis meist wenig effektiv: Sie können die Erreichung des Ziels eines laufenden Angriffs – z. B. den Diebstahl von Daten, die sich leicht kopieren lassen – oftmals nicht mehr stoppen und bergen das Risiko von Kollateralschäden sowie der ungewollten Eskalation.[40] Stattdessen sollten die wenigen vorhandenen IT-Fachkräfte schwerpunktmäßig mit defensiven Aufgaben wie dem Schutz von IT-Systemen betraut werden.

Sanktionen, Anklagen und weitere Verrechtlichung

Auf politisch-strategischer Ebene sollte die Politik mit Maßnahmen wie politischen und wirtschaftlichen Sanktionen und bzw. oder Anklagen zum Isolieren und Stigmatisieren eines Akteures auf Cybervorfälle eines anderen Staates reagieren, um langfristig auf Veränderung dessen Verhaltens hinzuwirken.[41] Ein wie von der EU mit der *Cyber-Diplomacy-Toolbox* 2017 beschlossenes Rahmenkonzept hierfür kann die eigene Reaktion anleiten und auf andere Staaten eine Signalwirkung für nicht akzeptiertes Verhalten entfalten.[42] Langfristig könnte die COVID-19-Panedmie, die für alle Staaten gleichermaßen die Relevanz eines funktionierenden Gesundheitssektors illustrierte, die Chance sein, den 2017 ins Stocken geratenen Prozess der Verrechtlichung und Normensetzung beim staatlichen Einsatz von Informations- und Kommunikationstechnologie (IKT) auf Ebene der Vereinten Nationen wiederzubeleben.[43] Hierzu sollte die deutsche bzw. europäische Cyberdiplomatie mit gleichgesinnten Staaten ein Verständnis über nicht akzeptiertes staatliches Verhalten beim Einsatz von IKT herausbilden und auf dessen Grundlage mit nicht-gleichgesinnten Ländern einen Dialog über rote Linien und den Umgang mit staatlichen Cyberattacken führen.

1 Cybersicherheit beruht im Kern auf der Vertraulichkeit, Integrität und Verfügbarkeit von Daten (vormals IT-Sicherheit genannt). Durch die Durchdringung nahezu aller gesellschaftlicher Bereich mit IKT hat der Begriff Cybersicherheit neben der technischen auch eine soziale, rechtliche, politische, militärische, wirtschaftliche und kulturelle Dimension erhalten. Cybersicherheit kann ebenfalls einen Zustand bezeichnen, d. h. die Abwesenheit bzw. Reduzierung von Bedrohungen auf ein annehmbares Niveau. Referenzobjekt ist dabei die Cyberdomäne, d. h. das technische Medium Internet, mit ihm verbundene und nicht verbundene IT-Geräte sowie die soziale Dimension, die sich aus der Nutzung der Technologien ergibt (vgl. Sven Herpig: Anti-War and the Cyber Triangle. Strategic Implications of Cyber Operations and Cyber Security for the State, Hull: University of Hull 2016, S. 49 f.). Vereinfacht gesagt befasst sich Cybersicherheitspolitik bzw. Cyberverteidigungspolitik – wenn Maßnahmen in das Aufgabengebiet des Militärs fallen – mit defensiven wie offensiven Maßnahmen zum Schutz der Cyberdomäne.

2 Vgl. Ella Koeze/Nathaniel Popper: The Virus Changed the Way We Internet, in: The New York Times 07.04.20, online unter: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html?action=click&module=Editors%20Picks&pgtype=Homepage; Statista: Media consumption increase due to the coronavirus worldwide 2020, by country, online unter: https://www.statista.com/statistics/1106766/media-consumption-growth-coronavirus-worldwide-by-country/.

3 DE CIX: Highest jump ever: DE-CIX Frankfurt reaches 9.1 Tbps, 11.03.20, online unter: https://www.de-cix.net/de/news-events/news/de-cix-frankfurt-reaches-9-1-tbps.

4 Vgl. Ed Bott: It's 2020: How many PCs are still running Windows 7, in: zdnet.com 07.01.20, online unter: https://www.zdnet.com/article/how-many-pcs-are-still-running-windows-7-today/; Gabi Probst: Den digitalen Anschluss verpasst, in tagesschau.de 16.04.2020, online unter: https://www.tagesschau.de/investigativ/kontraste/kriminaltechnik-bundesrepublik-101.html.

5 Danny Palmer: Phishing alert: GDPR-themed scam wants you to hand over passwords, credit card details, in: zdnet.com 03.05.18, online unter: https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/.

6 Bundeskriminalamt: Cybercrime. Bundeslagebild 2018, Stand Oktober 2019, S. 17, online unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.pdf?__blob=publicationFile&v=3; Symatec: Internet Security Threat Report, Volume 24, February 2019, S. 21 ff.; online unter: https://www.symantec.com/content/dam/symantec/docs/re- ports/istr-24-2019-en.pdf.

7 Patrick Howell O'Neill: Chinese hackers and others are exploiting coronavirus fears for cyber espionage, in: MIT Technology Review 12.03.20, online unter: https://www.technologyreview.com/2020/03/12/916670/chinese-hackers-and-others-are-exploiting-coronavirus-fears-for-cyberespionage/.

8 Bundesamt für Sicherheit in der Informationstechnik: Cyber-Kriminelle nutzen Corona-Krise vermehrt aus 02.04.20, online unter: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html.

9 FAZ.net: NRW stoppt Auszahlung von Soforthilfen, 09.04.20, online unter: https://www.faz.net/aktuell/wirtschaft/nrw-stoppt-auszahlung-von-soforthilfen-wegen-betrugsverdacht-16718743.html.

10 Verbraucherzentrale Nordrhein-Westfalen: Achtung, Phishing! Wie Betrüger die Corona-Krise in E-Mails nutzen 18.03.20, online unter: https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/achtung-phishing-wie-betrueger-die-coronakrise-in-emails-nutzen-45714.

11 Dan Goodin: The Internet is drowning in COVID-19-related malware and phishing scams, in arstechnica.com 16.03.20, online unter: https://arstechnica.com/information-technology/2020/03/the-internet-is-drowning-in-covid-19-related-malware-and-phishing-scams/; World Economic Forum: Hackers are using coronavirus maps to spread malware 14.03.20, online unter: https://www.weforum.org/agenda/2020/03/hackers-are-using-coronavirus-maps-to-spread-malware?fbclid=IwAR1OSDE-Yf__vchx1qcUONrJZeYz23LhMpUZEaxOSuxTfo3MaC0efjBW1Sg.

12 Vgl. Matt Burgess: Hackers are targeting hospitals crippled by coronavirus, in: wired.co.uk 22.03.20, online unter: https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing.

13 Caroline Brooks/Xuefeng Jiang: Here's the Kind Of Data Hackers Get About You From Hospitals, in: Michigan State University 23.09.19, online unter: https://msutoday.msu.edu/news/2019/heres-the-kind-of-data-hackers-get-about-you-from-hospitals/.

14 Sean Lyngaas: Czech Republic's second-biggest hospital is hit by cyberattack, in: cyberscoop.com 13.03.20, online unter: https://www.cyberscoop.com/czech-hospital-cyberattack-coronavirus/.

15 Davey Winder: COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online, in forbes.com 23.03.20, online unter: https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#ad64a7618e55.

16 Computer Emergency Response Team France: Rapport Menaces et Incidents du CERT-FR. Attacks involving the Mespinoza/Pysa ransomware 01.04.20, online unter: https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-003/.

17 Catalin Cimpanu: State-sponsored hackers are now using corovirus lures to infect their targets, in zdnet.com 13.03.20, online unter: https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/; Shannon Vavra: Cybercriminals, nation-states increasingly tailoring coronavirus spearphishing campaings, in cyberscoop.com 12.03.20, online unter: https://www.cyberscoop.com/coronavirus-phishing-scams-iran-china/.

18 Ben Buchanan: The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations, Oxford: Oxford University Press 2017, S. 89–96.

19 Sandra Joyce: Limited Shifts in the Cyber Threat Landscape Driven by COVID-19, in: Fireeye.com 08.04.20, online unter: https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html.

20 Joseph Menn/Christopher Bing/Raphael Satter/Jack Stubbs: Exclusive: Hackers linked to iran target WHO staff emails during coronavirus – sources, in reuters.com 02.03.20, online unter: https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC.

21 Federal Bureau of Investigation/Cybersecurity and Infrastructure Security Agency: People's Republic of China (PRC) Targeting of COVID-19 Research Organizations 13.05.20, online unter: https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.pdf.

22 Patrick Howell O'Neill: Chinese hackers and others are exploiting coronavirus fears for cyber espionage.

23 Elmar Theveßen/Peter F. Müller/Ulrich Stoll: #Cryptoleaks: Wie BND und CIA alle täuschten, in: zdf.de 11.02.20, online unter: https://www.zdf.de/nachrichten/politik/cryptoleaks-bnd-cia-operation-rubikon-100.html.

24 Kalila Sangster: Zoom users surge from 10m to 200m as world works from home, in: yahoo Finance UK 02.04.20, online unter: https://uk.finance.yahoo.com/news/zoom-users-surge-from-10-m-to-200-m-as-world-works-from-home-110022110.html.

25 Bill Marczak/John Scott-Railton: Move Fast and Roll Your Own Crypto. A Quick Look at the Confidentiality of Zoom Meetings, in: citizenlab.ca 03.04.20, online unter: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/; Micah Lee/Yael Grauer: Zoom Meetings Aren't End-To-End Encrypted, Despite Misleading Marketing, in: theintercept.com 31.03.20, online unter: https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

26 Eric S. Yuan: A Message to Our Users 01.04.20, online unter: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/. Mitte April 2020 gab Zoom mit der Version „5.0" u. a. die Verwendung eines höheren Verschlüsselungsstandards bekannt. Ebenfalls führte Zoom für Geschäftskunden die Möglichkeit ein auszuwählen, wo die Server sind, die für ein Gespräch genutzt werden, sodass Schlüssel zur Ver- und Entschlüsselung von Gesprächen ohne einen Teilnehmer in China nicht mehr wie zuvor teilweise von chinesischen Servern übertragen werden sollen (Colleen Rodriguez: Zoom Hits Milestone on 90-Day Security Plan, Releases Zoom 5.0 22.04.20, online unter: https://blog.zoom.us/wordpress/2020/04/22/zoom-hits-milestone-on-90-day-security-plan-releases-zoom-5-0/). Nach wie vor werden die Schlüssel aber von Zoom-Servern generiert, wodurch das Unternehmen theoretisch auf die Inhalte zugreifen bzw. dazu verpflichtet werden könnte die Schlüssel auf rechtmäßige Anfragen von Sicherheitsbehörden herauszugeben. Durch seine Geschäftspräsenz in China könnte das Unternehmen aufgrund der dortigen Rechtslage zur Zusammenarbeit verpflichtet werden. Zoom arbeitet weiter an einer echten Ende-zu-Ende-Verschlüsselung, die es künftig in seiner kostenpflichtigen Version anbieten möchte und bindet in diesen Prozess die Zivilgesellschaft, Kryptografie-Experten und seine Kunden mit ein (Eric S. Yuan: Zoom Acquires Keybase and Announces Goal of Developing the Most Broadly Used Enterprise End-to-End Encryption Offering 07.05.20, online unter: https://blog.zoom.us/wordpress/2020/05/07/zoom-acquires-keybase-and-announces-goal-of-developing-the-most-broadly-used-enterprise-end-to-end-encryption-offering/).

27 Reuters.com: German foreign ministry restricts use of Zoom over security concerns 08.04.20, online unter: https://www.reuters.com/article/us-health-coronavirus-germany-zoom/german-foreign-ministry-restricts-use-of-zoom-over-security-concerns-report-idUSKBN21Q1SC.

28 Thomas Rid: Cyber War Will Not Take Place, in: Journal of Strategic Studies 1 (2012), S. 5–32.

29 Ben Buchanan: The Hacker And The State, Harvard: Harvard University Press 2020, S. 8.

30 Andy Greenberg: The Untold Story of NotPetya, The Most Devasting Cyberattack in History, in: Wired 22.08.18, online unter: https://www.wired.com/story/notpetya-cyberattack-ukraine- russia-code-crashed-the-world/.

31 Jason Hovet/Christopher Bing/Jack Stubbs: Czechs warn of imminent, large-scale cyberattacks on hospitals, in: http://reuters.com 17.04.20, online unter: https://uk.reuters.com/article/uk-czech-cyber/czechs-warn-of-imminent-large-scale-cyberattacks-on-hospitals-idUKKBN21Z00N.

32 Reuters.com: Czech hospitals report cyberattacks day after national watchdog's warning 17.04.20, online unter: https://www.reuters.com/article/us-czech-cyber-ostrava/czech-hospitals-report-cyberattacks-day-after-national-watchdogs-warning-idUSKBN21Z1OH?__twitter_impression=true.

33 Vgl. Bundesamt für Sicherheit in der Informationstechnik: Social Engineering – der Mensch als Schwachstelle o. A., online unter: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html; Bundeskriminalamt: Forschungs- und Beratungsstelle Cybercrime o. A., online unter: https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsUndBeratungsstellen/Cybercrime/Cybercrime.html.

34 Dominik Rzepka: Jede vierte Stelle für IT-Sicherheit unbesetzt, in zdf.de 12.02.20, online unter: https://amp.zdf.de/nachrichten/politik/cyberabwehr-bundesregierung-it-sicherheit-stellen-unbesetzt-100.html?__twitter_impression=true.

35 Bundesministeriums des Innern, für Bau und Heimat: Verstärkung im Kampf gegen die Cyberkriminalität 02.10.19, online unter: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/10/aenderung-krimLV-cyberkrim.html; FAZ.net: Polizei bildet Spezialisten aus 19.04.20, online unter: https://www.faz.net/aktuell/rhein-main/cyberkriminalitaet-polizei-bildet-spezialisten-aus-16731824.html.

36 2016/1148/EU: Directive of the European parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, in: Official Journal of the European Union L194, 19.07.16, S. 1–30, online unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=NL).

37 In Deutschland ist das BSI zuständig für die Umsetzung bzw. Einhaltung der sogenannten NIS-Richtlinie (vgl. Bundesamt für Sicherheit in der Informationstechnik: Gesetz zur Umsetzung der NIS-Richtlinie o. A., online unter: https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html).

38 Glenn S. Gerstell/Michael Morell: Four ways U.S. intelligence efforts should change in the wake of the coronavirus pandemic, in: washingtonpost.com 07.04.20, online unter: https://www.washingtonpost.com/opinions/2020/04/07/four-ways-us-intelligence-efforts-should-change-wake-coronavirus-pandemic/.

39 Vgl. Alexandra Paulus/Sven Herpig: Covid-19: Why states now need to consider self-restraint in the cyber domain, in: aboutintel.eu o. A., online unter: https://aboutintel.eu/covid-cyber-china/.

40 Vgl. Sven Herpig: Zurückhacken ist keine Lösung, in: Zeit.de 21.04.17, online unter: https://www.zeit.de/digital/internet/2017-04/cyberangriffe-bundesregierung-hackback-gegenangriff/komplettansicht.

41 Exemplarisch für „naming and shaming" ist der Haftbefehl der Bundesanwaltschaft gegen einen Angehörigen des russischen Militärgeheimdienstes GRU, der am Hack des Bundestagsnetzwerkes 2015 beteiligt gewesen sein soll und der bereits 2018 von einem US-Gericht für seine Involvierung in den sogenannten DNC-Hack angeklagt wurde. Deutschland ist nach den USA erst das zweite Land, dass Anklage gegen einen Angehörigen einer staatlichen Cybereinheit erhoben hat. (Florian Flade/Georg Mascolo: Bärenjagd, in: SZ.de 05.05.20, online unter: https://www.sueddeutsche.de/politik/hack-bundestag-angriff-russland-1.4891668).

42 Rat der Europäischen Union: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, 13007/17, Brussels, 9 October 2017, online unter: http://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.

43 Vgl. Kubo Mačák/Laurent Gisel/Tilman Rodenhäuser: Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?, in: justsecurity.org 27.03.20, online unter: https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

Letzter Abruf für die genannten Internet-Links: 29.05.2020

Impressum

Der Autor

Johannes Wiggen ist Referent für Cybersicherheit in der Abteilung Internationale Politik und Sicherheit der Konrad-Adenauer-Stiftung e.V.

Konrad-Adenauer-Stiftung e. V.

Johannes Wiggen
Referent für Cybersicherheit
Analyse und Beratung
T: +49 30 / 26 996-3934
johannes.wiggen@kas.de

Postanschrift: Konrad-Adenauer-Stiftung e. V., 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2020, Berlin
Gestaltung: yellow too Pasiek Horntrich GbR
Satz: Janine Höhle, Konrad-Adenauer-Stiftung e. V.
Die Printausgabe wurde bei copy print Kopie & Druck GmbH, Berlin klimaneutral produziert und auf FSC-zertifiziertem Papier gedruckt.
Printed in Germany.

ISBN 978-3-95721-677-9