N1

Titel	Cybersicherheit
AntragstellerInnen	Berlin
Zur Weiterleitung an	

☐ angenommen ☑ mit Änderungen angenommen ☐ abgelehnt

Cybersicherheit

2Der Großteil unserer Gesellschaft nutzt vernetzte Dienste und das Internet täglich, sei es bewusst zur Recherche von Informationen oder unbewusst beim Bezahlen mit der Kreditkarte. Äußerungen auf sozialen Plattformen sind Teil des politischen Diskurses und gehören folglich auch zum öffentlichen Raum. Nicht nur die Kommunikation, auch Dienstleistungen werden teilweise oder komplett online erbracht. Teile der Infrastruktur, die das gesellschaftliche Zusammenleben ermöglichen, wie die Strom- und Wasserversorgung, Gesundheitsinfrastruktur oder auch Finanzdienstleistungen und insbesondere der Zahlungsverkehr gelten aufgrund ihrer Vernetzung und Abhängigkeit von sicheren Datenströmen als besonders schützenswert und werden unter dem Begriff der kritischen Infrastruktur zusammengefasst.

Der Cyberspace dient als virtueller Ort an dem Daten und Informationen ausgetauscht und verbreitet werden sowie als Infrastruktur, die gesellschaftliches Zusammenleben erleichtert und muss daher auch wirksam geschützt werden. Der Schutz des Cyberspace wird als Cybersicherheit bezeichnet.

Eine sinnvolle Definition von Cybersicherheit umfasst jedoch nicht nur die Sicherheit des Cyberspace, sondern alle Elemente, die im Cyberspace interagieren oder mit diesem verknüpft sind. Elemente des Cyberspace können unter anderem Daten, Informationen und die notwendige Infrastruktur sein. Aber auch zwischenmenschliche Kommunikation, Geräte des Internet der Dinge sowie die kritische Infrastruktur eines Staates können Elemente des Cyberspace sein.

Zur umfassenden Gewährleistung von Cybersicherheit werden sowohl defensive als auch offensive Maßnahmen diskutiert.

Zu defensiven Maßnahmen zählen z.B. die grundlegende Verbesserung von Hard- und Softwarequalität (sowohl des Endproduktes als auch des Entwicklungsprozess), die Implementierung einer sicherheitswahrenden Architektur, sowie die schnelle Beseitigung von Sicherheitslücken (Patchmanagement). Ferner müssen im Notfall auch aktive Maßnahmen zur Abwehr eines laufenden Angriffs ergriffen werden können, z. B. durch Umleiten oder Blockieren von Datenverkehr. Bildungsmaßnahmen sind ebenfalls essentieller Bestandteil einer defensiven Sicherheitsstrategie. So erfolgen Angriffe nicht nur in digitaler Form. Die gezielte Manipulation von Menschen (sog. Social Engineering) zählt deshalb ebenfalls zum Repertoire von Angrei-

24fer*innen.

Zu Offensivkapazitäten zählen Maßnahmen, bei denen ein Angriff erfolgt. Dies umfasst die Infektion mit/Injektion von Schadsoftware in ein fremdes System, das Einbringen einer Sicherheitslücke in Hardwaredesigns, das Manipulieren von Kommunikation oder die gezielte Störung eines Systembetriebes (Denial of Service).

Der Aufbau von vermeintlicher Offensivkapazität wird gerade in jüngerer Zeit von insbesondere rechtskonservativen Politiker*innen gefordert. Alleine aus technischen Gründen senkt schon der Aufbau einer theoretischen Angriffskapazität das allgemeine Sicherheitsniveau.

Derzeit gibt es in der Bundesrepublik Deutschland eine Vielzahl von Bundes- und Landesbehörden, deren Aufgabe es im engeren oder weiteren Sinne ist, für die Cybersicherheit der Bundesrepublik zu sorgen. Dazu gehören neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bayerische Landesamt für Sicherheit in der Informationstechnik, die entsprechenden Abteilungen des Bundesamtes für Verfassungsschutz (BfV), des Bundesnachrichtendienstes (BND), des Bundeskriminalamtes (BKA) und der Landespolizeien, das Zentrum für Cybersicherheit der Bundeswehr, die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZiTiS), das Bundesamt für den Digitalfunk für Behörden mit Sicherheitsaufgaben und einige weitere.

Die Aufgabenverteilung ist ebenso divers wie die Behörden selbst. Das BSI als älteste und größte Behörde, dass aus der dem ehemals dem BND angegliederten Zentralstelle für das Chiffrierwesen hervorgegangen ist, hat als prinzipielle Aufgabe den Schutz von Regierungsnetzen sowie sogenannter kritischer Infrastruktur. Zudem unterstützt das BSI auch Wirtschaft und Gesellschaft im Bereich der IT-Sicherheit.

Auch die Normierung von Kryptographieverfahren und die Beratung von Bürger*innen gehört zu der Aufgabenbeschreibung des BSI. Die primäre Aufgabe ist das Abwehren von Cyberattacken. Anders sieht es bei dem BfV, dem BND, der Bundeswehr und dem BKA angegliederten Abteilungen sowie dem ZiTiS aus. Während die Hauptaufgabe des BKA im Bereich der Cybersicherheit bei der Ermittlung der Verantwortlichen für Cyberangriffe liegt, haben die anderen genannten Zentren einen anderen Fokus. So gibt das ZiTiS, eine 2017 neu gegründete Behörde, die „Behörden mit Sicherheitsaufgaben in Ihrer Arbeit unterstützen soll“ seine Aufgabenfelder auf seiner Website an mit Digitaler Forensik, Telekommunikationsüberwachung, Kryptoanalyse und Big Data Analyse an. Der Fokus liegt also klar nicht auf einer Abwehr von Cyberangriffen, sondern auf dem Durchführen solcher, der Entschlüsselung erlangter Daten, sowie der Überwachung, sowie der Auswertung von durch Überwachung erhaltenen Daten. Gleiches ist auch bei den Abteilungen des BND und des BfV zu vermuten, auch wenn Informationen hier rarer sind.

Gerade Behörden wie das ZiTiS stehen seit ihrer Gründung unter großer Kritik, da sie zwar in geografischer Nähe des BND an seinem alten Standort in Pullach angesiedelt wurde, aber diesem offiziell nicht klar zu geordnet wird. Mit Telekommunikationsüberwachung, Kryptoanalyse und Big Data Analyse übernimmt das ZiTiS Aufgaben, die alle einen starken Eingriff in die Freiheitsrechte der Betroffenen darstellen, Dabei wird die ZiTiS nur durch das Bundesinnenministerium kontrolliert, ebenso wie die entsprechenden Zentren von BfV, BND und Bundeswehr nur der Kontrolle ihrer übergeordneten Behörden unterworfen sind. Eine direktere parlamentarische Kontrolle existiert nicht.

Im Bereich der defensiven Behörden stellt sich vor allem das Problem der Zerfaserung der Strukturen. Während das BSI zwar die Hauptbehörde ist, werden gleiche oder ähnliche Aufgaben auch von einer großen Anzahl anderer Behörden, den Polizeien und Nachrichtendiensten übernommen. Dass die Kommunikation zwischen diesen Behörden, die gerade im Fall von Cyberangriffen schnell gehen muss, nicht gegeben ist, lassen Beispiele aus der Vergangenheit erahnen wo es zu Kommunkationspannen und -unwillen zwischen verschiedenen staatlichen Einrichtungen kam.

Die derzeitige Struktur zur Gewährleistung von Cybersicherheit in der Bundesrepublik ist also stark dezentralisiert und demokratisch nur wenig kontrolliert. Sie hat zudem neben der defensiven Ausrichtung auch eine starke offensive Ausrichtung, was weitere Probleme aufwirft.

Behördendurcheinander beenden

Neben den genannten Behörden sind zudem eine Vielzahl weiterer Einrichtungen bei verschiedenen Sicherheitsbehörden auf Länder und Bundesebene entstanden, deren Kompetenzen zudem nicht klar voneinander abgrenzbar sind. Eine effiziente und effektive Sicherheitsstrategie wird dadurch erschwert.

Das Nationale Cyber-Abwehrzentrum ist die beim BSI angesiedelte Kooperationsstelle verschiedener Bundesbehörden, wie Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt und der Bundesnachrichtendienst, zur Abwehr von Cyberangriffen. Jedoch haben beispielsweise 13 Bundesländer eigene Cybercrime-Zentren aufgebaut, um Cyberkriminalität zu bekämpfen. Auch BfV und BND versuchen jeweils Cyber-Angriffe auf staatliche und private Einrichtungen abzuwehren und aufzuklären.

Die geschaffenen Strukturen für Cybersicherheit ähneln oder überschneiden sich auch in der Forschung: Die kürzlich vom Bundesministerium des Innern (BMI) und dem Bundesministerium für Verteidigung (BMVg) gegründete Agentur für Innovation in der Cybersicherheit soll Forschungs- und Innovationsvorhaben in der Cybersicherheit anstoßen). Das Forschungsinstitut Cyber Defence (CODE), ebenfalls vom BMVg gegründet, verfolgt ein ähnliches Ziel für die Bundeswehr.

Insgesamt sind in die Cybersicherheitsarchitektur über 50 Akteur*innen und Einrichtungen auf Länder- und Bundesebene involviert. Sich überschneidende Aufgabenbereiche verhindern die effiziente und effektive Umsetzung einer gemeinsamen Cybersicherheitsstrategie.

Verwobene und sich überschneidende Zuständigkeiten verringern die Transparenz der involvierten Stellen. Gerade in einem Bereich, in dem immer wieder die Einschränkung persönlicher Freiheiten zu Gunsten maximaler Sicherheit und Kontrolle gefordert wird, muss die Arbeit der staatlichen Behörden jederzeit überprüfbar sein. Das BSI war bereits bislang eine zentrale Behörde in Bezug auf Cybersicherheit. Deshalb sollen künftig alle Kompetenzen im Bereich der Cybersicherheit dort gebündelt werden. Wir fordern deshalb: Wir fordern daher eine Evaluation der Behördenstrukturen, entsprechende Bündelung von Kompetenzen und ggf. die Auflösung von Einrichtungen. Ziel ist die Federführung des BSI bei Entwicklung und Umsetzung einer gemeinsamen Sicherheitsstrategie, welches als eigene Bundesoberbehörde keinem Bundesministerium mehr unterstehen soll und damit direkt von den Abgeordneten des Bundestages kontrolliert wird. Die Kontrollfunktion obliegt unter anderem den Abgeord-

91neten des Bundestages. Diese Behörde darf nicht beim Verfassungsschutz oder BND angesiedelt sein. Insbesondere müssen dafür angemessene Auskunftspflichten im Auftrag der Einrichtung verankert werden. Die Geheimhaltung der weitergegebenen Informationen muss so gestaltet werden, dass eine normale parlamentarische Arbeit und damit gesellschaftliche Kontrolle möglich wird.

Derzeit besteht eine große Vermischung zwischen Behörden, die sich defensiv beziehungsweise offensiv orientieren. So hat das BSI beispielsweise eine im Großen und Ganzen defensiv angelegte Aufgabenbeschreibung, soll aber nach dem Willen von Innenminister Seehofer weitere offensive Kompetenzen bekommen, zum Beispiel durch sogenanntes „Hack-back“, dem Hacken von mutmaßlichen Hacker*innen zwecks Überführung. Damit verschwimmt die Grenze zwischen Behörden die offensiv und solchen die defensiv arbeiten weiter, eine Linie, die auch derzeit noch nicht klar gezogen ist. So sieht das BfV auch als Teil seines Verantwortungsgebiets Cyberspionage abzuwehren, arbeitet aber gleichzeitig mit offensiven Mitteln, wie Überwachung. Gleiches gilt für die Bundeswehr, die, in einer Überschneidung mit den Kompetenzen des BSI, einerseits den Schutz der eigenen Netze, sowie andererseits das Eindringen in andere Netze betreibt. Diese Vermischung sorgt für eine weitere Undurchschaubarkeit dieses Behördendschungels und erschwert eine demokratische Kontrolle weiter. Der Wunsch der deutschen Geheimdienste auf Augenhöhe mit NSA und GCHQ zu arbeiten und die gleichen weitreichenden Befugnisse zu erhalten, darf nicht Maßstab einer Strategie für Sicherheit im digitalen Raum sein. Stattdessen müssen für die Cybersicherheit bereitstellte Ressourcen vorwiegend für den Ausbau defensiver Maßnahmen verwendet werden. Dazu gehört die grundlegende Verbesserung von

108Softwarequalität sowie die an öffentlichen Hochschulen entwickelten Technologien für die Sicherheit von informationstechnischen Systemen schnellstmöglich auch in die Praxis zu bringen. Wir fordern daher

die Auflösung aller ausschließlich offensiv arbeitenden Behörden. Defensiv arbeitende Behörden dürfen keine offensiven Befugnisse erhalten und sind in einer zentralen Bundesbehörde zu bündeln

Kompetenzen einer zentralen Behörde Verschweigen von Sicherheitslücken

Ein hoher Grad an Cybersicherheit lässt sich nur dann erreichen, wenn Informationen über bekannte IT-Sicherheitslücken weitergegeben werden, sodass diese durch verantwortliche Stellen und Akteur*innen beseitigt werden können. Bisher unbekannte Schwachstellen in Computersoftware, sogenannte Zero-Day Schwachstellen, können zur Überwachung und Infiltration genutzt werden, solange diese nicht geschlossen oder beseitigt wurden. Um Spionagesoftware wie Staatstrojaner erfolgreich einsetzen zu können, bedarf es eingebauter Hintertüren oder aber bislang nicht geschlossener Sicherheitslücken. Offene Schwachstellen können jedoch auch von Dritten wie Kriminelle und Geheimdienste für deren Ziele genutzt werden und stellen deshalb für alle Betroffenen eine Gefahr dar. Wissen über Software-Sicherheitslücken darf deshalb nicht von staatlicher wie unternehmerischer Seite zurückgehalten werden, um diese für eigene Zwecke zu missbrauchen. Die fatalen Auswirkungen einer solchen Politik, zeigten z. B. die Trojaner WannaCry und NotPetya, die weltweit den Betrieb kritischer Infrastruktur (wie z. B. Bahnanlagen, Krankenhäuser, etc.) zum Erliegen brachten. Basis dieser Trojaner war die Ausnutzung einer als ETERNALBLUE bezeichneten Sicherheitslücke in Microsoft Windows. Dem amerikanische Geheimdienst NSA war diese Sicherheitslücke zum Zeitpunkt der Angriffe seit über einem Jahrzehnt bekannt, um vermeintliche Offensivkapazitäten zu erhalten, wurde jedoch keine Meldung an den Hersteller veranlasst. Daher fordern wir

Eine umfassende und augenblickliche Information über Sicherheitslücken in Software an geeignete Stellen.

Koordiniertes Verfahren zur Behebung von Schwachstellen

Es existiert derzeit kein einheitliches Verfahren für den Umgang mit gefundenen Sicherheitslücken. So kommt es in der Praxis vor, dass Nutzer*innen Sicherheitslücken an Hersteller*innen melden, diese jedoch keine zeitnahen Gegenmaßnahmen ergreifen. Ein jüngerer bekannter Fall ist die grob unsicher konzipierte Gesundheitsdatenapplikation Vivy. Der Hacker Martin Tschirsich meldete diverse, von ihm gefundene Sicherheitslücken an den Hersteller. Anstatt diese zu beseitigen, wurde ihm mit Klage gedroht. Deshalb fordern wir ein durch das BSI koordiniertes Verfahren zur zügigen Meldung und Beseitigung von kritischen Sicherheitslücken. Auch die Information der Industrie und Zivilbevölkerung über die gefundenen Sicherheitslücken muss Teil dieses Prozesses sein.

Abwehr von Cyberangriffen:

Die Abwehr von Angriffen ist essentieller Teil einer Sicherheitsstrategie. So muss im Falle eines Cyberangriffs dieser schnell erkannt und wirksame Gegenmaßnahmen ergriffen werden können. Solche Gegenmaßnahmen können zum Beispiel das Blockieren von Netzwerkverkehr einer oder mehrere Netzwerkverbindungen sein. Dazu sollen umfassende staatliche Vorgaben, etabliert und in Zusammenarbeit mit den Telekommunikationsunternehmen erarbeitet werden. Auch die schnelle Bereitstellung von Patches, um Sicherheitslücken zu schließen und ggf. Infektionen sind wichtige Gegenmaßnahmen. Dazu ist weiterhin eine enge Zusammenarbeit mit Hersteller*innen anzustreben.

Zudem fordern wir verstärkte Investitionen in die Forschung im Bereich der Cyberabwehr. Die Auswirkungen der Ransomware WannaCry blieben, trotz des entstandenen Schadens, weit hinter dem möglichen Schadenspotential zurück, da Sicherheitsexpert*innen innerhalb kürzester Zeit, durch Analyse des Schädlings, eine Funktionalität fanden, die dazu genutzt werden konnte, die weitere Ausbreitung zu verhindern.

Die vom Staat vielfach geforderte Kapazität, auf Cyberangriffen mit Gegenmaßnahmen zu reagieren, ist nicht zielführend sondern kontraproduktiv. Die oft als „Hack-Back“ oder auch „aktive Abwehr“ benannte Strategie ist eine Offensivreaktion und keine Abwehrmaßnahme, bei der der*die vermeintliche Angreifer*in attackiert wird. Ein Hack-Back verbietet sich schon aufgrund der unzureichenden Identifikation des Angreifers/der Angreiferin: Nur selten kann die Quelle des Angriffs zweifelsfrei einem”r bestimmten Akteur*in zugewiesen werden. Es gibt verschiedene Methoden, um die eigenen Spuren im Netz zu verschleiern. Angreifer*innen können ihre IP-Adresse fälschen oder das TOR-Netzwerk nutzen, Staaten können Angriffe durch nicht-staatliche Akteure*innen ausüben lassen, Hacker*innen-Gruppen können „False-Flag“-Attacken ausführen, etwa indem sie ihre Aktivitäten über Server in mehreren Ländern lenken.

Ein prominentes Beispiel ist die Schadsoftware Stuxnet, die darauf programmiert war, Kernkraft-Zentrifugen im Iran lahmzulegen. Da das Computersystem nicht mit dem Internet verbunden war, wurde zunächst nicht von einem Cyber-Angriff ausgegangen. Erst Wochen später wurden vermehrt Anzeichen für einen Cyberangriff gefunden. Für die Attacke wurden die USA und Israel verantwortlich gemacht, jedoch konnte deren Ursprung nie zweifelsfrei geklärt werden. Dieses Beispiel verdeutlicht erstens, wie schwierig es ist, die Herkunft von Cyberangriffen zu klären und zweitens, dass es dafür nicht zwingend einer Internet-Verbindung bedarf.

Ein Gegenschlag nach einem Hacker*innenangriff kann ebenfalls Unbeteiligte treffen. Wird beispielsweise ein von Hackern infiltrierter Computer eines Energieversorgers in einem anderen Land durch einen Hack-Back beschädigt, wären Stromausfälle eine denkbare Konsequenz. Solche Kollateralschäden müssen jedoch vermieden werden. Auch eine Eskalation als Folge eines Hack-Backs kann nicht ausgeschlossen werden. Geschädigte Dritte könnten in den Konflikt eingreifen oder aber der Hack-Back zu weiteren, stärkeren Attacken des*der identifizierten Angreifer*in führen und im schlimmsten Fall in einer Aggressionsspirale enden.

153

Auch als Ultima Ratio in Notsituationen, wie ein folgenschwerer Angriff auf die kritische Infrastruktur eines Landes, ist Hack-Back keine wirksame Strategie. Gerade destruktive Angriffe erfordern gute Kenntnisse über Hard- und Software der Attackierenden sowie über deren Intention und Vorgehensweise. Dieses Wissen aufzubauen ist zeit- und kostenintensiv, eine zeitlich verzögerte Gegenmaßnahme ist jedoch keine Notwehrmaßnahme. Nach internationalem Völkerrecht muss ein Akt der Selbstverteidigung unmittelbar als Reaktion auf einen Angriff erfolgen. Offensive Angriffe auf ausländische Computersysteme können als aggressiven Akt verstanden werden und sind laut Grundgesetz verfassungswidrig. Hack-Backs sind folglich kein geeignetes Mittel gegen Cyberangriffe. Wir fordern daher:

Eine Evaluation der Hack-Backs und deren Einsatz nur als letzte Option, die verschiedensten Auflagen unterliegt. Desweiteren muss die Forschung im Bereich Hack-Backs ausgebaut werden.

Schutz von Betroffenen ohne deren Wissen

Eine weitere Frage, die sich stellt, ist, ob es dem Staat gestattet sein sollte in die Geräte von Privatpersonen ohne deren Wissen, unter Ausnutzung bekannter und in neueren Softwareversionen geschlossenen Sicherheitslücken, einzugreifen, um Sicherheitslücken zu schließen oder Angriffe zu verhindern oder zu minimieren. Insbesondere von Bedeutung ist diese Frage bei sogenannten Bot-Nets. Bot-Nets sind ein Zusammenschluss von teils mehreren zehntausend Computern, der ohne das Wissen der Computerbesitzer*innen durch Schadsoftware geschieht. Die durch diese Zusammenschlüsse entstehende hohe Rechenleistung wird dann von den Angreifer*innen zur Zerstörung oder Unschädlichmachung der Zielserver verwendet.

Zur Verhinderung eines solchen Angriff ist es notwendig, die Schadsoftware von jedem einzelnen Computer eines Bot-Nets' zu entfernen und entsprechende Sicherheitslücken zu schließen. Aufgrund der schieren Anzahl der Computer, ist es praktisch unmöglich die Zustimmung aller betroffenen Nutzer*innen in einem sinnvollen Zeitraum über diese Maßnahmen einzuholen.

Deshalb ist zu überlegen, ob es dem Staat erlaubt sein sollte, entsprechende Maßnahmen ohne die Zustimmung der Nutzer*innen einzuleiten, sofern dies dem Schutz der betroffenen Server, zu Beispiel dem des Bundestages dient. Diese Maßnahme - das Eingreifen in die elektronischen Endgeräte von Personen, die sich keinerlei Straftat schuldigt gemacht haben, noch nicht einmal einer verdächtigt sind - bereitet den Boden für zu viele Möglichkeiten des Missbrauchs. Das Argument "die Allgemeineit zu schützen" könnte, wenn mit ihm ein solch starker Eingriff in die Privatssphäre gerechtfertigt würde, für einen starken Ausbau von Überwachung und Eingriffsmöglichkeiten in die Privatssphäre von Seiten des Staates verwendet werden. Daher fordern wir:

Insbesondere höchstpersönliche Daten sind für uns Jusos besonders schützenswert. Einschränkungen und Eingriffe in die persönlichen Sphären dürfen deshalb niemals flächendeckend und pauschal erfolgen, sondern allein als Ausnahmen unter strengen Auflagen weiterhin bestehen. Hierbei müssen Grundrechte wie die Unschuldsvermutung und das Recht auf informationelle Selbstbestimmung gewahrt werden. Dem folgend ist ein staatliches Eingreifen in die elektronischen Endgeräte von Privatpersonen nur in absoluten Härtefällen zu gestatten. Dabei muss gewährleistet sein, dass die Datenschutzrichtlinien für die privaten Verbraucher*innen eingehalten werden.

Standards für Security bei Design und Verschlüsselung

Durch Verschlüsselung von Kommunikation kann bereits ein sehr hoher Sicherheitsstandard gewährleistet werden. Es gibt derzeit einige Verschlüsselungsprotokolle, die bei ausreichenden Schlüssellänge eine fast vollständige Sicherheit der Daten gewährleisten. So können diese Daten zwar durch Cyberangriffe weiterhin abgefangen werden, sind jedoch für die sie Abgreifenden wertlos. Durch leicht nutzbare Software ist das Verschlüsseln von persönlichen Daten auch für wenig technikaffine Privatnutzer*innen problemlos möglich. Gleiches gilt insbesondere für Regierungsnetzwerke. Wichtiger aber ist noch das sogenannte „Security by Design". Es gibt verschiedene Arten und Weisen bereits die Hardware, als das Gerät selbst, so zu bauen, dass ein Hacken sehr schwierig bis unmöglich ist. Hierfür braucht es jedoch verbindliche Standards, die von der Bundesbehörde zu entwickeln sind. Wir fordern:

Die Setzung verbindlicher Standards für den Bau von Geräten, die die Prinzipien des „Security by Design" beherzigen. Den Einsatz der Bundesregierung auf europäischer Ebene für einheitliche „Security by Design"-Standards und Regelungskompetenzen der Aufsichtsbehörde, um diese Standards durchzusetzen und mangelhafte Produkte aus dem Verkehr zu ziehen. Gegebenenfalls wird dies jedoch auf nationaler Ebene primär umgesetzt.

Naming/Blaming von Angriffen

Das sogenannte Naming/Blaming von Angriffen bezeichnet das Offenlegen von Angriffen, sowie der angreifenden Gruppen. Im Rahmen dieser Methode kann insbesondere auf infizierte Websites, sowie derzeit aktuelle Angriffsmaschen hingewiesen werden. Einige Institutionen, wie etwa der Verbraucher*innenschutz NRW betreibt bereits ein sogenanntes Phishing Radar, dass besonders häufig vorkommende Betrugsversuche und Schadsoftware listet. Gleiches geschieht auf der Seite des BSI. Da die Informationslage des Ersteren jedoch nicht vollständig und die Seite des Zweiteren kaum bekannt ist, wissen nur wenige Menschen um diese Informationsquelle. Diese Informationen müssen niedrigschwellig zur Verfügung stehen. Deswegen fordern wir:

Einen Ausbau der Informationen über Cyberangriffe und Betrugsmethoden, die einer großen Anzahl an Menschen niedrigschwellig zur Verfügung stehen.

Die Einführung einer neuen Meldepflicht für alle Unternehmen für erkannte IT-Schwachstellen ihrer Produkte. Hier soll das Verursacher*innenprinzip gelten: wer Schwachstellen in ihren*seinen Produkten verschweigt, muss hierfür zur Verantwortung gezogen werden wenn der*die Hersteller*in nicht binnen einer vom BSI zu setzenden Frist Abhilfe schafft. Bei Nutzung von offenem oder offengelegtem Quelltext muss keine Meldung erfolgen. Einhergehend mit diesem Aufgabenzuwachs müssen die Stellen bei den zuständigen Abteilungen des BSI erweitert werden.

Die Wichtigkeit des privaten Schutzes vermitteln

Es gibt viele Möglichkeiten wie sich Nutzer*innen privat schützen können und so das Netz auch insgesamt für alle sicherer machen können. Ähnlich wie beim Impfen lässt sich auch hier der Schaden den ein Virus anrichten kann und das Ausmaß an Abzug persönlicher Daten nicht wirksam bekämpfen, wenn nur ein Teil aller elektronischer Endgeräte wirksam geschützt ist. Deswegen ist der Schutz des eigenen Gerätes zu gleich auch ein Schutz der anderen. Viele Menschen wissen weder um die Gefahren, noch um die Möglichkeit des Schutzes von technischen Geräten, obgleich einige dieser Möglichkeiten, wie das Verschlüsseln von E Mails, das Wählen sicherer Passwörter und das Nutzen sicherer Messenger-Dienste, relativ einfach zu handhaben sind. Technische Geräte haben einen immer größeren Anteil an unserem Alltag. Mit ihnen sicher umzugehen wird immer wichtiger. Die nötigen Kenntnisse für einen sichereren Umgang mit Informationstechnik sind unverzichtbarer Bestandteil der informationstechnischen Grundausbildung (ITG). In Berlin ist ITG bereits Lehrinhalt der Sekundarstufe I. Der Lehrplan muss dahingehend erweitert werden, so dass sicherer Umgang mit IT und grundlegende Verhaltensregeln gelehrt werden, ITG muss Teil der schulischen Bildung in allen Bundesländern werden.

Forschung ausbauen

Kein Wirtschaftlicher Bereich entwickelt sich derzeit so rasant wie das der IT. Durchschnittlich 230 Schadsoftwaren werden pro Minute neu entwickelt. Mit sich ständig ändernden Geräten und einem Ansteigen der Rechenleistung verändern sich auch die Angriffe, die auf diese Geräte möglich sind. Um weiterhin eine relative Cybersicherheit garantieren zu können, müssen also auch die Verfahren zu Abwehr und Schutz fortlaufend weiterentwickelt werden. Während jedoch ganze Masterstudiengänge in Cybersicherheit und Kryptographie in anderen europäischen Ländern Gang und Gäbe ist, sieht es in der Bundesrepublik wesentlich schlechter aus. Hier handelt es sich meistens um einzelne Spezialisierungsrichtungen in allgemeinen Informatik-Masterstudiengängen oder um Angebote privater Träger*innen. So gibt es auch nur wenige Institute, die sich explizit mit Cybersicherheit beschäftigen. Wie bei vielen anderen Themen rund um die technische Seite der Digitalisierung, zum Beispiel künstliche Intelligenz und Machine Learning, scheint dieses Thema in der deutschen Hochschullandschaft noch nicht angekommen zu sein. So gibt es im gesamten Raum Berlin-Brandenburg nur an der Brandenburgisch-Technischen Hochschule einen Master in Cybersicherheit. Bundesweit sieht es nicht besser aus. Die meisten der deutschen Sicherheitsbehörden, wie etwa der BND und die Bundeswehr bilden daher ihre Fachkräfte in eigenen Studiengängen aus. Auch betreiben Behörden wie ZiTiS, das BSI und die Bundeswehr Forschung in diesem Bereich, öffentlich finanziert, aber nicht der Öffentlichkeit zugänglich gemacht und publiziert wird. Wir fordern daher:

Einen Ausbau der Lehre und Forschung im Bereich der Kryptographie, Cybersicherheit, IT Security und IT Forensik

Öffentlich geförderte Forschung muss sofern möglich der Öffentlichkeit zugänglich gemacht werden. Das Gros der Forschung im Bereich Cybersicherheit soll daher an öffentlichen Hochschuen und außeruniversitären Instituten stattfinden. Alle Forschung zu dem Thema ist nach den geltenden Verfahren im Wissenschaftsbetrieb zu publizieren.

Kritische Infrastruktur unter demokratischer Kontrolle stellen

Die für die Internetnutzung benötigte Infrastruktur besteht im Wesentlichen aus zwei Komponenten: Netze, die eine schnelle und sichere Datenübertragung ermöglichen, sowie Server auf denen die Daten aller Websites, Shops und Anwendungen liegen.

Bei letzterem finden virtualisierte Hardware-Ressourcen im Rahmen von Cloud Computing immer mehr Verwendung („Infrastructure as a Service“). Die größten Anbieter sind Amazon (ca. 49% Marktanteil) und Microsoft Azure (ca. 16% Marktanteil). Auch deutsche Behörden nutzen die Infrastruktur dieser Unternehmen, so verwendet die Bundespolizei Amazon Services zur Speicherung und Auswertung von Bodycam-Videos. Die Anbieter verfügen über eine immense

Marktmacht und agieren in keinem Maße transparent für demokratisch legitimierte deutsche oder europäische Institutionen. Es ist nicht hinnehmbar, dass bei dieser auch zukünftig kritischen Infrastruktur eine komplette Abhängigkeit von privaten Unternehmen herrscht.

Wie begrüßen daher die Bestrebungen eine öffentliche, europäische Alternative zu diesen Cloud-Diensten zu schaffen, die Prinzipien wie Transparenz, Interoperabilität, Dezentralität und Datensouveränität in den Fokus stellt. Es muss selbstverständlich sein, dass alle sensiblen und staatlich erhobenen Daten bei solch einem öffentlichen Service gespeichert werden.

Mit fortschreitender Durchdringung der Digitalisierung wird die Nutzung digitaler Infrastruktur immer wichtiger für die Teilhabe am kulturellen Leben. Digitale Teilhabe muss dabei für alle Menschen möglich sein und darf nicht vom Geldbeutel abhängen. Diese Aufgabe betrachten wir als Teil der Daseinsvorsorge.