»Cybersicherheit« – ein Beitrag für einen sicheren digitalen Raum

Diskussionspapier der Arbeitskreise
Kultur, Wissen, Lebensweisen (AK IV)
und Bürger*innenrechte und Demokratie (AK V)

DIE LINKE.
IM BUNDESTAG

Inhalt

DIE LINKE.
IM BUNDESTAG

Fraktion DIE LINKE. im Bundestag
Platz der Republik 1, 11011 Berlin
Telefon: 030/22751170, Fax: 030/22756128
E-Mail: fraktion@linksfraktion.de
V.i.S.d.P.: Arbeitskreis IV und Arbeitskreis V

Autoren: Dr. André Hahn (MdB), Dr. Petra Sitte (MdB), Anke Domscheit-Berg (MdB), Petra Pau (MdB), Dr. Alexander S. Neu (MdB), Martina Renner (MdB), Dirk Burczyk, Dr. Kirsten Jansen, Alexander Reetz, Anne Roth, Dr. Jürgen Scheele, Dr. Simon Weiß

Stand: 4. Juli 2018

Layout/Druck: Fraktionsservice

Mehr Informationen zu unseren parlamentarischen Initiativen finden Sie unter: www.linksfraktion.de

180709

Einleitung

Im Jahr 1983 kam der Film »War Game« in die Kinos und wurde für die nächsten Jahrzehnte bildgebend für die Vorstellung von Hackern und Cyber-War: Ein Schüler dringt in das Netz des Pentagon ein und aktiviert das Atomwaffenarsenal der USA, die Welt steht am Rande der Vernichtung. Nun ist das Pentagon seitdem sicherlich besser gegen Zugriffe geschützt – doch die seit den 90er Jahren rasant zunehmende Anwendung von Computern für alle erdenklichen Anwendungen hat das Risiko, Opfer eines Angriffs auf das eigene System zu werden, omnipräsent gemacht. Nicht zuletzt das Internet der Dinge (IoT/Internet of Things) rückt das Bewusstsein für die Bedrohungen der digitalen Sicherheit ebenso in den Fokus öffentlicher Debatten wie die zunehmende Berichterstattung über Attacken auf die Netze von Regierungen, Parlamenten, Parteien, öffentlichen Verwaltungen, Stiftungen, aber auch sog. Kritische Infrastrukturen (Kritis). Anders als bspw. der Fraktionsvorsitzende der Unionsfraktion Kauder glauben machen möchte, ist die Digitalisierung, und damit verbunden auch die Frage nach deren Sicherheit, nicht erst das »Megathema der kommenden Jahre«,[1] sondern mindestens seit zwei Dekaden Realität.

Durch das IoT geraten Gegenstände des täglichen Gebrauchs in den Fokus potentieller Angreifer. Für Besitzer*innen des viel zitierten smarten Kühlschranks[2] mag es auf den ersten Blick nicht so problematisch sein, wenn sich das Gerät zu einem Botnetz[3] verbindet. Bei einer gehackten smarten Haustür-, Fenstersteuerung oder Heizung und einem damit unmittelbar verbundenen individuellen Schaden mag das schon ganz anders aussehen. Neben Endverbraucher*innen sind aber auch öffentliche Verwaltungen oder Kritische Infrastrukturen (Kritis) Ziel von Attacken. Im letzten Fall mit möglicherweise unabsehbaren Folgen. Dominierten früher Inselnetze, so scheint heute alles miteinander verbunden zu sein.

In vielen Lebensbereichen sorgt die Digitalisierung für erhebliche Erleichterungen. Öffentliche Verwaltungen können im Idealfall schneller und bürger*innenfreundlicher arbeiten. Gleichzeitig führt dies zu einer immer größer werdenden Menge an gespeicherten Daten. Kam es nach quälend langsamen Schritten in diesem Bereich zu Fortschritten, vergaß und vergisst man in dem nun folgenden Rausch der digitalen Glückseligkeit allzu oft die Frage nach der digitalen Sicherheit.

Im Vergleich zur analogen Welt stellt die Frage der Attribution ein ungleich größeres Problem bei Angriffen im digitalen Raum dar. Aggressor*innen können vom einzelnen Nationalstaat über kriminelle Banden bis hin zu Einzeltäter*innen alles sein und von überall aus agieren. Je professioneller die Angreifer*innen vorgehen, umso schwerer wird es herauszufinden, wer die eigentlichen Angreifer*innen sind. Die digitale Forensik bewegt sich zwangsweise in einem Graubereich und kann lediglich Indizien sammeln.

Der Blick auf den Status quo der Ausgestaltung digitaler Sicherheit, bspw. in Form der 2016 novellierten Cybersicherheitsstrategie der Bundesregierung,[4] aber auch die unzähligen Beiträge der Vertreter*innen deutscher Sicherheitsbehörden, zeigt, dass eine klare Zielrichtung fehlt. Vielmehr gibt es ein buntes Durcheinander der Kompetenzen. Ergänzt durch teilweise widerstrebende Interessen: Nicht erst seit der Einführung des Bundestrojaners ist klar, dass es für Geheimdienste, aber auch Strafverfolgungsbehörden wichtig ist, Sicherheitslücken zu kennen, um diese später nutzen zu können. Gleichzeitig werden dieselben Akteure, die auf die Kenntnis von Sicherheitslücken angewiesen sind, als Akteure der gesamtstaatlichen Cybersicherheitsarchitektur eingebunden. Da ist er also wieder, der viel zitierte Bock als Gärtner. Die Verabredungen im Koalitionsvertrag sowie die Kompetenzaufteilungen der Bundesregierung lassen auf wenig Besserung hoffen. Der Koalitionsvertrag enthält lediglich inhaltlich unklare Verabredungen beispielsweise für eine sichere digitale Authentifizierung im Netz, ohne dass eine klare Idee zu ihrer Ausgestaltung erkennbar wäre. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) soll gleichzeitig zur »Cybersicherheitsbehörde« werden und »in seiner Rolle als unabhängige und neutrale Beratungsstelle für IT-Sicherheitsfragen« gestärkt werden.[5] Hinsichtlich einer überfälligen stärkeren Regulierung des IT-Marktes soll es offenbar bei unverbindlichen Standards bleiben – die zudem von den Anbietern selbst entwickelt werden. Wie sich zukünftig Bundesinnenministerium, Bundeswirtschaftsministerium und das Bundeskanzleramt in ihrer Politik der digitalen Sicherheit miteinander abstimmen werden, ist vollkommen offen.

Mit dem vorgelegten Diskussionspapier zeigen die Autor*innen auf, welche (offensichtlichen) Missstände die aktuelle Ausgestaltung der digitalen Sicherheit in Deutschland mit sich bringt und welche Interessenkonflikte hierbei vorherrschen. Darüber hinaus werden Ansätze aufgezeigt, welche es ermöglichen, mehr digitale Sicherheit zu gewährleisten. Mit dem Begriff der »digitalen Sicherheit« soll all das umfasst sein, was unter den Schutzbereich des vom Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung neu aus dem allgemeinen Persönlichkeitsrecht abgeleiteten »digitalen Grundrecht« fällt, dem Recht auf Schutz der Vertrau-

[1] https://www.welt.de/debatte/kommentare/article172922212/Gastbeitrag-Deutschland-braucht-einen-Digitalrat.html

[2] In der Praxis dürften aktuell smarte Fernseher, Smartwatches, Router o.ä. deutlich lebensnäher sein, der beschriebene Effekt bleibt jedoch der gleiche.

[3] Viele Netzwerkgeräte, die durch ein Schadprogramm zusammengeschlossen sind und ferngesteuert zu bestimmten Aktionen missbraucht werden, meist ohne dass die Nutzer*innen etwas davon bemerken.

[4] https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf

[5] Vgl. Koalitionsvertrag von CDU, CSU und SPD für die 19. Wahlperiode, S. 44. https://www.bundesregierung.de/Content/DE/_Anlagen/2018/03/2018-03-14-koalitionsvertrag.pdf;jsessionid=0B7C55E442D27BCF875094B0147514F6.s5t2?__blob=publicationFile&v=5

lichkeit, Integrität und Verfügbarkeit informationstechnischer Systeme und Daten.[6] Im erweiterten Sinne verstehen wir darunter auch jene informationstechnischen Systeme, auf die die Bürger*innen zur Lebensführung in der digitalen Welt angewiesen sind. Der schillernde Begriff »Cyber« bzw. »Cybersicherheit« verunklart aus unserer Sicht mehr, worum es eigentlich geht und was genau als Bedrohung dieser Sicherheit ausgemacht wird. Aus dem hier gebrauchten Begriff der »digitalen Sicherheit« hingegen erhellt beispielsweise unmittelbar, dass davon die Nutzung von Verschlüsselung in der privaten Kommunikation umfasst ist; von den Protagonisten der Cybersicherheit wird Verschlüsselung mal als Bedrohung, mal als wichtiges Instrument begriffen.

Der Begriff der »digitalen Sicherheit« umfasst aus Sicht der Autor*innen natürlich auch private Lebensbereiche und damit die persönliche Sicherheit der Nutzer*innen. Die Bandbreite ist kaum überschaubar und umfasst beispielsweise Identitätsdiebstahl, Mobbing und Kreditkartenbetrug aber auch die Privatisierung des Rechts durch Zuständigkeitsverlagerungen auf Unternehmen. Gerade die Angriffe im digitalen Raum gegen Andersdenkende, -liebende oder -gläubige und insbesondere Mädchen und Frauen haben ein Ausmaß erreicht, dass eine explizite Positionierung in diesem Diskussionspapier den Autor*innen notwendig erscheint.

[6] BVerfGE 129, 274-350.

Behörden der digitalen Sicherheit in Deutschland

In der Bundesrepublik sind unterschiedliche Behörden für Aufgaben der Sicherung von Vertraulichkeit, Integrität und Verfügbarkeit informationstechnischer Systeme und Daten zuständig. Eine passgenaue Zuordnung von Aufgaben ist nur ungefähr möglich und wird einerseits durch vielfache Parallelarbeiten, andererseits durch zahlreiche Kooperationsgremien noch weiter erschwert. In fast allen Behörden mit einer Zuständigkeit für digitale Sicherheit geht es nicht allein um defensive Fähigkeiten, sondern zugleich um die Entwicklung oder den Einsatz eigener offensiver Fähigkeiten. Einzige Ausnahme bildet bislang das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Strafverfolgungsbehörden

Das Bundeskriminalamt (BKA) wie die Landeskriminalämter (LKÄ) haben mit Fragen der digitalen Sicherheit vor allem in Hinsicht auf erfolgte Angriffe mit Ransomware[7], digitale Spionage (insb. Industriespionage) und andere Formen von Angriffen zu tun, bei denen es zu Sicherheitsvorfällen gekommen ist. Bearbeitet werden konkrete Fälle von Cyberkriminalität in der Abteilung Schwere und Organisierte Kriminalität, unterstützt durch die Forschungs- und Beratungsstelle Cybercrime im Kriminalistischen Institut im BKA. Für akute Vorfälle existiert seit 2017 eine »Quick Reaction Force«, die bei Sicherheitsvorfällen mit mutmaßlich kriminellem Hintergrund Beweise sichern soll.

Über entsprechende Analysefähigkeiten verfügt das BKA jedoch zu wenig. Das hat auch mit Prioritätensetzung zu tun: Mit etwa 30 Beschäftigten wurde im Kompetenzzentrum informationstechnische Überwachung über vier Jahre ein Spähprogramm zur Ausleitung verschlüsselter Kommunikation (Quellen-TKÜ/Quellen-Telekommunikationsüberwachung) geschrieben, das zunächst nur sehr begrenzte Einsatzmöglichkeiten hatte. Zugleich wird immer wieder über Defizite in der Strafverfolgung berichtet, weil das BKA (wie auch LKÄ und Staatsanwaltschaften) mit der Auswertung einer immer weiter steigenden Zahl von Datenträgern nicht hinterherkommt. Hier stellt nicht nur die schiere Masse ein Problem dar, sondern auch die Verschlüsselung solcher Datenträger.

Geheimdienste

Zum Schutz digitaler Sicherheit erklärt sich offensiv auch immer wieder das Bundesamt für Verfassungsschutz (BfV) zuständig. Digitale Angriffe werden in allen Abteilungen, insbesondere in der Spionageabwehr und dem Geheim- und Sabotageschutz beobachtet und ausgewertet. Auch das BfV verfügt über eine »Quick Reaction Force«, die im Falle konkreter Angriffe oder Angriffsversuche ausrückt und Analysen vornimmt – wobei die Abgrenzung zum BKA und zum BSI unklar ist. Während defensive Fähigkeiten in der digitalen Sicherheit über alle Abteilungen verteilt sind, werden offensive Fähigkeiten zur Überwachung von digitaler Kommunikation (von Quellen-TKÜ bis zur Meta-Datenauswertung in sozialen Netzwerken) in einer eigenen Abteilung entwickelt. Auch beim Bundesnachrichtendienst (BND) gibt es eine deutliche Schieflage: Fast eine halbe Milliarde Euro und einige hundert Personalstellen stehen zur Verfügung, um in den kommenden Jahren die Fähigkeiten zur Überwachung des internationalen Internetverkehrs auszuweiten. Von einer ursprünglich mit 130 Planstellen einzurichtenden Abteilung zur Abwehr von Angriffen auf deutsche Verwaltungsstellen vom Ausland aus mithilfe digitaler Werkzeuge ist seit längerem nichts mehr verlautbart. Angesichts der allgemeinen Schwierigkeiten von Behörden in Deutschland, geeignetes Fachpersonal zu finden, ist allerdings davon auszugehen, dass auch hier die angepeilte Personalstärke bei weitem noch nicht erreicht ist.

Zivile Strukturen

Auch wenn Polizei und Geheimdienste sich den Unternehmen im Bereich Cybercrime und digitaler Spionage als staatliche Ansprechpartner andienen – für die Sicherheit ziviler IT-Strukturen sind zunächst die Betreiber*innen von IT-Infrastruktur und im Ernstfall behördlicherseits das BSI zuständig. Es bearbeitet gemeldete Sicherheitsvorfälle aus öffentlichen Verwaltungen und Einrichtungen der Kritischen Infrastruktur (Energie, Wasser, Transport etc.), und entwickelt gemeinsam mit der Industrie Sicherheitsmaßstäbe für IT-Verfahren und -Produkte, die dann Grundlage von Zertifizierungen werden. Die vom BSI veröffentlichten Berichte zur IT-Sicherheitslage weisen Bürger*innen und Unternehmen auf aktuelle Sicherheitsbedrohungen und mögliche Abwehrmaßnahmen hin. Das BSI arbeitet mit Computer Emergency Response Teams (CERT) von Unternehmen und öffentlichen Verwaltungen zusammen und stellt im Notfall auch ein eigenes Team zur Verfügung, um auf Notfälle reagieren zu können.

Für Fürsprecher*innen eines Kurses der digitalen Sicherheit, der in erster Linie auf die Härtung von IT-Infrastrukturen durch sichere Prozesse und Gefahrenbewusstsein bei den Nutzer*innen setzt, könnte das BSI eine wichtige Behörde sein. Dazu wäre es aber notwendig, das BSI aus dem Geschäftsbereich des Bundesinnenministeriums herauszulösen. Wie eine Behörde mit der Aufgabe, die digitale Sicherheit für alle Bürger*innen zu erhöhen und zugleich glaubwürdig Distanz zu staatlichen Überwachungsforderungen zu wahren genau konzipiert und rechtlich verfasst sein soll, ist noch zu klären.

Vernetzung

Behörden mit Zuständigkeiten in der digitalen Sicherheit sind darüber hinaus stark vernetzt, auch wenn das institutionelle Geflecht keine Aussage darüber zulässt,

[7] Schadprogramm, welches die Daten auf einem Computer sperrt. Für die Entsperrung wird von den Geschädigten Geld verlangt.

welcher inhaltlichen Qualität diese Zusammenarbeit ist. Zentral ist das beim BSI seit 2011 angesiedelte »Cyber-Abwehrzentrum« (Cyber-AZ), dem vom Bundesrechnungshof allerdings auch schon bescheinigt wurde, weitgehend ineffizient und überflüssig zu sein. Hier sind neben Polizei, Geheimdiensten und Militär auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe vertreten. Es gibt sowohl einen CERT-Verbund von großen privaten Unternehmen und Verwaltungen als auch einen der Verwaltungen allein, innerhalb dessen ein Austausch über aktuelle Bedrohungen stattfindet. Polizei und Geheimdienste kooperieren darüber hinaus bei der Beobachtung des Internet (Gemeinsames Internetzentrum und Koordinierte Internetauswertung), zumindest mittelbar geht es auch hier darum, aus dem Netz gesteuerte Attacken auf IT-Systeme rechtzeitig zu erkennen und präventiv Maßnahmen ergreifen zu können.

Ressourcenkonflikte

In Bezug auf die digitale Sicherheit gibt es also eine ganze Reihe von Behörden mit unterschiedlichen Aufgabenstellungen und Befugnissen, die vor allem um eine Ressource konkurrieren: IT-Fachkräfte mit hoher Expertise, die über die gefragten Fähigkeiten verfügen. Hiervon gibt es nach Ansicht aller Beteiligten in Deutschland insgesamt zu wenig, was zu hohen Honoraren oder Gehältern bei Großunternehmen führt, mit denen die öffentliche Verwaltung nicht konkurrieren kann.

Hier fehlt es auch an der Ausbildung eigener Fachkräfte. Zwar hat die Bundeswehr-Hochschule nun 11 Professuren für den Bereich IT/Cyber-Warfare ausgeschrieben, in der Ausbildung für die öffentliche Verwaltung an den Landes-Fachhochschulen und an der Hochschule der Verwaltung des Bundes gibt es aber kaum Angebote für die Vermittlung von IT-Fachkenntnissen.

Deutlich wird an diesem Beispiel auch, wie unterschiedlich Ressourcen aufgeteilt werden. Die 11 Professuren an der Bundeswehr-Uni in München sollen zwar auch mithelfen, den Bedarf an IT-Fachkräften in der öffentlichen Verwaltung insgesamt zu befriedigen. Doch selbstverständlich wird hier vor allem die Aneignung offensiver Fähigkeiten im Rahmen des Cyber Warfare im Vordergrund stehen. Im Sinne der Härtung von öffentlicher IT-Infrastruktur gegen Angriffe von außen müsste einerseits die Ausbildung eigener IT-Fachkräfte, die in Rechenzentren etc. für Sicherheit sorgen, sichergestellt werden, andererseits die breite Verankerung von Lerninhalten mit Bezug zur Nutzung von Informationstechnik in der Ausbildung des öffentlichen Dienstes generell eine größere Rolle spielen. Eine breitere Verankerung von IT-Fachwissen in öffentlichen Verwaltungen würde die Abhängigkeit von IT-Unternehmen insgesamt abschwächen. Hierzu sind überzeugende und umsetzbare Konzepte zu entwickeln.

Sicherheitsverlust durch staatliche Aktivitäten

Das vorangegangene Kapitel zeigt kursorisch das Kompetenzgeflecht der eingebundenen Behörden. Jenseits der Frage, ob diese Struktur geeignet ist – was bezweifelt werden darf –, ergibt sich noch ein schwerwiegenderes Problem bei staatlichen Aktivitäten. Staatliche Einrichtungen – sowohl Geheimdienste als auch andere Sicherheitsbehörden – gehören zu den Akteursgruppen, die motiviert und befähigt sind, die Integrität von informationstechnischen System zu verletzen, um daraus Informationen abzuschöpfen. Die damit einhergehende Beeinträchtigung von Grundrechten (die sich insbesondere bei der massenhaften Überwachung von Kommunikationsnetzen durch Geheimdienste als erheblich darstellt) ist nicht das einzige Problem: Aus Sicht der Gewährleistung eines möglichst hohen allgemeinen Schutzniveaus gibt es zwei Bereiche, in denen entsprechende staatliche Bestrebungen Schaden verursachen können.

Hintertüren

Der eine Bereich ist die breit angelegte Schwächung oder gar Verhinderung von Sicherheitsmaßnahmen durch staatliche Vorgaben, etwa durch Einschränkungen der Verwendung von Verschlüsselungstechnologien, einer Pflicht zum Einbau von Hintertüren oder Maßnahmen, die gegen die anonyme Nutzbarkeit des Internets gerichtet sind. Auch wenn derartige Maßnahmen allein auf die Erleichterung des staatlichen Zugriffs gerichtet sind, sind sie zwangsläufig mit einem reduzierten Schutz vor allen Angreifer*innen verbunden. Allerdings werden jedenfalls in Deutschland zwar regelmäßig Forderungen nach derartigen Maßnahmen erhoben (zuletzt durch den ehemaligen Innenminister de Maizière mit dem Wunsch nach verpflichtenden Hintertüren in digitalen Geräten)[8], bislang aber ohne Erfolg; und während beispielsweise die gesetzliche Beschränkung privater Anwendung von Verschlüsselung in den 1990ern noch kontrovers diskutiert wurde, ist davon heute praktisch nicht mehr die Rede. Insbesondere in autoritär regierten Staaten ist die Lage jedoch oft eine andere. Auch in Abwesenheit gesetzlicher Regelungen ist zudem von geheimdienstlichen Aktivitäten in diesem Bereich auszugehen (vergleiche Abschnitt »Investitionen in sichere Infrastrukturen«).

Staatstrojaner

Der andere problematische Bereich ist der staatliche Einsatz von Software, die den direkten Fernzugriff auf Computersysteme erlaubt (Online-Durchsuchung, Staatstrojaner oder euphemistisch Quellen-Telekommunikationsüberwachung). Wiederum besteht hier neben dem tiefgehenden Grundrechtseingriff durch die Maßnahme selbst eine Beeinträchtigung des allgemeinen Schutzniveaus durch den Umstand, dass der wirksame Einsatz derartiger Software nur dann möglich ist, wenn der Staat sich exklusive Kenntnisse über Sicherheitslücken verschafft (sogenannte Zero Day Exploits aufgrund der fehlenden Reaktionszeit auf Bekanntwerden der Lücke) und sie »offenhält«, indem er diese Kenntnisse nicht weitergibt. Mit Blick auf die Gewährleistung eines möglichst hohen Schutzniveaus wäre aber genau das geboten.

Dass es sich hier um mehr als ein hypothetisches Problem handelt, zeigt eindrucksvoll der Fall WannaCry. Der weltweite, bislang schwerwiegendste Angriff seiner Art basierte auf einer Sicherheitslücke, die dem US-Nachrichtendienst NSA bereits seit Jahren bekannt war.[9] Sie hätte also schon längst geschlossen sein können – wäre sie nicht für den Zweck staatlicher Angriffe »gehortet« worden. Ransomware-Angriffe auf Krankenhäuser, die unmittelbar Auswirkungen auf die Abläufe in der Krankenversorgung und sogar auf lebenserhaltende Systeme haben können, zeigen die immensen Gefahren, die damit verbunden sind. Werden zur Terroristenjagd solche Werkzeuge entwickelt, ist ihre Effektivität hinsichtlich der Abwehr terroristischer Gefahren zweifelhaft – die damit verbundenen Risiken sind aber klar erkennbar und real. Dass Befürchtungen, Behörden könnten auch in Deutschland Sicherheitslücken bewusst offenlassen, nicht unbegründet sind, zeigt die Debatte um die Aufgaben der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS). Ihr Chef, der ehemalige Leiter der BND-Abteilung Technische Aufklärung Wilfried Karl, äußerte in einem Interview, es bräuchte einen »Prozess innerhalb der Behörden, wie wir mit Sicherheitslücken in Software verantwortungsvoll umgehen.«[10]

Einsatz in Deutschland

In Deutschland geht der Einsatz von Staatstrojanern durch Sicherheitsbehörden und die öffentliche Diskussion darüber bis in die Mitte der 2000er zurück. Dabei wurde lange darauf verzichtet, eine eigene gesetzliche Grundlage zu schaffen; inzwischen existieren diese im Bund (hier seit 2017 mit sehr weitgehenden Befugnissen)[11] und in zahlreichen Bundesländern. In der Rechtsprechung ist das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 zentral, das ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme herleitet und dem Einsatz von Staatstrojanern enge Grenzen setzt.[12] Der Begriff der »Quellen-Telekommunikationsüberwachung« verweist auf die Verwendung von Staatstrojanern, um auf dem kompromittierten System Telekommunikationsdaten abzugreifen; der Unterschied zur Onlinedurchsuchung besteht also im Einsatzzweck.

[8] http://www.rnd-news.de/Exklusive-News/Meldungen/November-2017/De-Maiziere-will-Ausspaehen-von-Privat-Autos-Computern-und-Smart-TVs-ermoeglichen

[9] https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.e534b94b9925

[10] https://www.welt.de/politik/deutschland/article178035350/Neue-Cyber-Behoerde-Zitis-Es-geht-nur-um-legale-Ueberwachung.html

[11] http://dipbt.bundestag.de/doc/btd/18/127/1812785.pdf

[12] http://www.bverfg.de/e/rs20160420_1bvr096609.html

Eine technische Gewährleistung der Beschränkung auf laufende Kommunikationsdaten wird für kaum möglich gehalten.[13] DIE LINKE hat sich vor allem aufgrund des erheblichen Grundrechtseingriffs wiederholt klar gegen jedweden Einsatz von Staatstrojanern ausgesprochen.

Für das BKA ist derzeit der (geplante) Einsatz von zwei verschiedenen Softwarelösungen bekannt: Die selbstprogrammierte Remote Communication Interception Software (RCIS), die in einer ersten Version auf die Überwachung von Skype für Windows auf Desktopsysteme (RCIS 1.0) begrenzt ist und in einer zweiten Version auch mobile Geräte wie Smartphones und Tablets infizieren und abhören können soll (RCIS 2.0), und das Produkt FinSpy der Firma FinFisher.[14] Beide Produkte werden wegen ihrer begrenzten Anwendungsreichweite bislang nur in Einzelfällen sowohl im Bereich der Gefahrenabwehr und der Strafverfolgung eingesetzt.

Handel mit Sicherheitslücken und Überwachungstechnik

Um Sicherheitslücken für solche Zwecke zu verwenden, muss der Staat zunächst einmal Kenntnis davon erlangen. Ressourcen, um Lücken selbständig zu identifizieren, haben deutsche staatliche Stellen nur begrenzt, selbst wenn sie wie im Fall des BKA eigene Staatstrojaner programmieren. Welche Rolle die neue Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) hier in Zukunft spielen wird, ist unklar.

Der Einsatz von Staatstrojanern bringt es demnach mit sich, dass der Staat Sicherheitslücken – wenn nicht gleich ganze Softwarelösungen – ankauft. Damit fördert er den bestehenden Markt rund um derartige Lücken und erhöht indirekt die Anreize für Dritte, gefundene Sicherheitslücken zu verkaufen, statt sie in verantwortungsvoller Weise bekannt zu machen. Es existiert eine ganze Industrie, die Überwachungssoftware an staatliche Behörden in aller Welt verkauft. Ein berüchtigtes Beispiel von vielen ist die in München ansässige Firma FinFisher, deren Produkte nicht nur von deutschen Sicherheitsbehörden gekauft werden, sondern auch autoritären Regimen als Werkzeug dienen, um gegen Oppositionelle vorzugehen.[15]

Vor diesem Hintergrund wird seit einiger Zeit über Exportkontrollen von Überwachungssoftware diskutiert. Seit 2015 wird auf europäischer Ebene Überwachungstechnologie in Übereinstimmung mit dem »Wassenaar-Abkommen für Exportkontrollen von konventionellen Waffen und doppelverwendungsfähigen Gütern und Technologien« von der Dual-Use-Verordnung erfasst, was bis jetzt jedoch keine erheblichen Einschränkungen in der Praxis mit sich gebracht hat.[16] Eine Überarbeitung der Verordnung, die in diesem Bereich strengere Regeln beinhalten könnte, ist zurzeit im Entwurfsstadium.[17] DIE LINKE fordert in ihrem Wahlprogramm zur Bundestagswahl 2017 ein generelles Exportverbot für Überwachungstechnologien.[18] Diese Forderung steht jedoch vor zwei zentralen Herausforderungen. So sind vom Wassenaar-Abkommen zunächst auch solche Programme (Intrusionsoftware) erfasst, die für Penetrationstests verwendet werden und gerade der Härtung von IT-Systemen dienen sollen – aber eben auch für das Eindringen in fremde Systeme gebraucht werden können. Mit der Aufnahme dieser Dual-Use-Software in die Exportkontrolle soll sichergestellt sein, dass sie nur an solche Staaten exportiert wird, die Gewähr für einen bestimmungsgemäßen Einsatz bieten. Ein generelles Exportverbot ließe auch das nicht mehr zu.

Hackbacks

Es werden in jüngster Zeit vermehrt Forderungen laut, staatliche Stellen zu ermächtigen, im Fall von Angriffen auch durch Gegenangriffe reagieren zu können, um so z. B. Server auszuschalten oder abgegriffene Daten zu löschen. Entsprechend äußerten sich insbesondere Anfang des Jahres 2017 Verfassungsschutzpräsident Maaßen und der ehemalige Innenminister de Maizière.[19] Hierfür wurde zuletzt sogar eine Änderung des Grundgesetzes ins Spiel gebracht.[20]

Unklar ist, wer über eine solche Ermächtigung verfügen könnte. In der Diskussion genannt werden u.a. die Strafverfolgungsbehörden von Bund und Ländern, der Verfassungsschutz, die Bundeswehr im Rahmen ihres neuen Kommandos Cyber- und Informationsraum oder das BSI. In den Vereinigten Staaten wird sogar die Forderung diskutiert, derartige Maßnahmen auch zivilen Opfern eines Angriffs selbst zu erlauben.[21]

Da die Durchführung solcher Angriffe das unbefugte Eindringen in informationstechnische Systeme voraussetzt, sind sie mit dem gleichen grundsätzlichen Problem verbunden, das bereits für den Einsatz von Staatstrojanern angeführt wurde: Der Staat muss sich über geeignete Kanäle Kenntnis von Sicherheitslücken verschaffen, ohne sie zu schließen, und beeinträchtigt somit das allgemeine Sicherheitsniveau globaler digitaler Netze.

Ein zusätzliches Problem entsteht als Folge des allgemeinen Attributionsproblems: Da Angriffe üblicherweise nicht direkt erfolgen, sondern über Systeme von Dritten ohne deren Einverständnis oder Wissen, kann Kollateralschaden nicht ausgeschlossen wer-

[13] https://ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf
[14] https://netzpolitik.org/2017/geheimes-dokument-das-bka-will-schon-dieses-jahr-messenger-apps-wie-whatsapp-hacken/; https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/
[15] http://www.spiegel.de/netzwelt/netzpolitik/gamma-gruppe-hacker-kopieren-finfisher-unterlagen-a-985098.html
[16] https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153
[17] https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Internetfreiheit/20170209_Stellungnahme_ROG_BMWi_Dual_Use_Richtlinie.pdf
[18] https://www.die-linke.de/fileadmin/download/wahlen2017/wahlprogramm2017/die_linke_wahlprogramm_2017.pdf (S. 124).
[19] http://www.spiegel.de/netzwelt/netzpolitik/bundesamt-fuer-verfassungsschutz-plant-cyber-gegenangriffe-a-1129273.html
[20] https://www.berliner-zeitung.de/politik/gesetzaenderung-effektiver-gegen-cyberkriminalitaet-aus-dem-ausland-vorgehen-28943184?dmcid=sm_fb
[21] https://tomgraves.house.gov/uploadedfiles/discussion_draft_acdc_act.pdf

den. Schlimmstenfalls könnte dieser von Angreifern nicht nur in Kauf genommen werden, sondern sogar provoziert, indem etwa bewusst kritische Systeme für Angriffe zweckentfremdet werden oder False-Flag-Operationen durchgeführt werden. Betroffene Dritte könnten sich ebenfalls zu einer Reaktion veranlasst sehen, womit die Gefahr einer Eskalation verbunden ist.[22]

Ein System, in dem Sicherheitslücken als Währung zur Steigerung der Sicherheit von IT-Systemen begriffen werden, ist zum Scheitern verurteilt. Es muss daher ein anderer Ansatz gefunden werden.

[22] Für eine ausführlichere Darstellung dieser und weiterer Problemfelder beim Einsatz von Hackbacks vgl. https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf (S. 9ff.).

Erfassung und Meldung von Vorfällen und Sicherheitslücken

Bei der Frage nach verpflichtenden oder freiwilligen Meldungen im Bereich der IT-Sicherheit müssen zwei verschiedene Bereiche unterschieden werden: Die Meldung von sicherheitsrelevanten Vorfällen, auf die sich bislang gesetzgeberische Aktivität konzentriert hat; und die Meldung von Sicherheitslücken, für die keine entsprechenden Regelungen existieren.

Meldung von sicherheitsrelevanten Vorfällen

Seit 2015 besteht durch das IT-Sicherheitsgesetz ein rechtlich vorgeschriebenes Verfahren zur Meldung erheblicher Störungen von informationstechnischen Systemen für die Betreiber*innen sogenannter Kritis an das BSI. Daneben besteht mit der »Allianz für Cyber-Sicherheit« bereits seit 2012 eine vom BSI in Kooperation mit der Wirtschaft eingerichtete Stelle für freiwillige Meldungen.[23] 2016 wurden durch die sogenannte NIS-Richtlinie (2016/1148) vergleichbare Regelungen auf europäischer Ebene vorgegeben, in deren Folge 2017 auch die deutschen Regelungen noch einmal angepasst wurden, insbesondere durch eine Erweiterung auf Dienste wie Suchmaschinen und Cloud-Computing-Dienste.

DIE LINKE hat in den parlamentarischen Beratungen den Ansatz eines IT-Sicherheitsgesetzes grundsätzlich begrüßt, aber Kritik an den unklaren Begriffsdefinitionen und der schwierigen Rolle des einerseits hier zuständigen, andererseits nicht vom Innenministerium – und damit den potentiell entgegenlaufenden Interessen von Sicherheitsbehörden – unabhängigen BSI geübt.[24]

Was genau dem Bereich der Kritischen Infrastruktur zuzuordnen ist, wurde 2016 mit der BSI-Kritis-Verordnung[25] zunächst für die die Bereiche Energie, Wasser, Ernährung und IKT festgelegt, 2017 erweitert um Festlegungen für Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr.

Meldung von Sicherheitslücken

Keine allgemeine gesetzliche Regelung besteht für die Meldung von Sicherheitslücken als solche. Auch das BSI ist lediglich nach §§ 4 und 8b des BSI-Gesetzes grundsätzlich verpflichtet, Bundesbehörden und Betreiber*innen Kritischer Infrastrukturen über sie betreffende Informationen zu Sicherheitslücken zu unterrichten; nach § 7 darf es Warnungen über Sicherheitslücken auch in anderen Fällen Betroffenen oder der Öffentlichkeit bekanntmachen.[26]

Verschiedentlich wird gefordert, eine allgemeine Melde- bzw. Veröffentlichungspflicht für Sicherheitslücken analog zu Vorfällen einzuführen, so etwa 2013 von einem Arbeitskreis der Gesellschaft für Informatik,[27] vom Forum Informatiker*innen für Frieden und gesellschaftliche Verantwortung (FIfF)[28] und 2017 vor dem Hintergrund von WannaCry von Telekom-Chef Höttges.[29] Eine solche Pflicht würde, wenn sie auch staatliche Stellen trifft, den Einsatz von Staatstrojanern und anderer Überwachungssoftware auf Basis von Zero Day Exploits ausschließen. In jedem Fall wäre damit Firmen, die mit derartiger Software handeln, die Geschäftsgrundlage entzogen. Zu beachten ist allerdings, dass auch eine öffentlich bekannte bzw. durch Updates bereits adressierte Sicherheitslücke in der Praxis noch vorhanden und ausnutzbar sein kann.

Ein verantwortlicher Umgang mit derart identifizierten Sicherheitslücken wird allgemein darin gesehen, zuerst diejenigen darüber zu informieren, die in der Position sind, sie zu schließen, nach einer dafür geeigneten Frist aber öffentlich zu machen.

---

[23] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html

[24] https://dipbt.bundestag.de/doc/btp/18/18110.pdf (S. 10572); http://dipbt.bundestag.de/doc/btp/18/18221.pdf (S. 22295f.).

[25] https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

[26] http://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[27] http://pak-datenschutz.gi.de/nc/stellungnahmen/detailansicht/article/eu-meldepflicht-fuer-cyberattacken-greift-zu-kurz-sicherheitsluecken-veroeffentlichen.html

[28] https://cyberpeace.fiff.de/Kampagne/Forderung10

[29] http://www.faz.net/aktuell/wirtschaft/unternehmen/telekom-chef-hoettges-wir-kommen-dann-zwischen-zehn-und-zwoelf-15035218.html

Produkthaftung, Produktsicherheit, Produktlebensdauer

Neben der Einhegung des staatlichen Geschäfts mit Sicherheitslücken ist es für die Schaffung einer effektiven Sicherheit von IT-Systemen aller Art ebenso notwendig, die IT-Produkte selbst respektive deren Hersteller*innen in die Verantwortung zu nehmen. Da sichere Produkte in den meisten Fällen aktuell kein Wert an sich sind, sondern zuallererst Zusatzkosten für die Produzent*innen erzeugen, muss an dieser Stelle ein Ansatzpunkt gefunden werden.

Die Ausweitung der Produkthaftung auf IT-Hersteller*innen kann mittel- und langfristig zur Härtung von IT-Systemen beitragen, indem die Hersteller*innen zu mehr Sorgfalt in der Entwicklung von Hard- und Software bewegt werden. Die Etablierung von verbindlichen Vorgaben zur Produktsicherheit setzt überdies einen Schritt früher an, indem von vornherein Mindeststandards für mit dem Internet verbundene IT-Systeme vorgegeben werden. Regelungen zur Produktlebensdauer dienen ferner der Aufrechterhaltung einer sicherheitskonformen Funktionalität von insbesondere in der Betriebsverantwortung von privaten Endanwender*innen sich befindenden IT-Systemen, indem verbindliche Vorgaben zur erwartbaren Lebensdauer gemacht und für diesen Zeitraum beispielweise Software- und Sicherheitsupdates bereitzustellen sind. Alle drei Vorgaben bedeuteten eine beträchtliche Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit auf Seiten der Verantwortlichkeit der IT-Hersteller*innen. Ein Blick auf die bestehenden Gesetzesregelungen zeigt jedoch, dass diese nicht auf die spezifischen Sicherheitsbedingungen von mit dem Internet verbundenen IT-Systemen ausgerichtet sind.

IT-Produkthaftung

Nach der EU-Produkthaftungsrichtlinie (85/374/EWG**),** umgesetzt in nationales Recht durch das Gesetz über die Haftung für fehlerhafte Produkte (ProdHaftG), werden unter dem Produktbegriff bewegliche Sachen einschließlich Elektrizität erfasst. Grundsätzlich unterliegen somit Hard- und Software dem verschuldensunabhängigen Haftungsrecht und müssen somit für den Zweck, für den sie entwickelt wurden, die erforderliche Sicherheit aufweisen.[30] Allerdings ist die Haftung für Entwicklungsrisiken, wie sie sich insbesondere in Form von IT-Sicherheitslücken darstellen, ausgeschlossen. Gehaftet wird nicht, wenn der Fehler nach dem Stand der Wissenschaft und Technik beim Inverkehrbringen nicht erkannt werden konnte (§ 1 Abs. 2 Nr. 5 ProdHaftG).

Diese Norm folgt der EU-Produkthaftungsrichtlinie unmittelbar. Letztere sieht zwar die Möglichkeit zu einer Ausnahmeregelung vor (Art. 15 Abs. 1 lit. b 85/374/EWG): Demnach können die Mitgliedstaaten Rechtsvorschriften erlassen, nach denen ein Hersteller auch dann haftet, wenn der Fehler nach dem Stand der Wissenschaft und Technik beim Inverkehrbringen nicht erkannt werden konnte. Doch wirkte eine solche Ausnahmereglung nur bedingt, da der Schadensbegriff aus der verschuldensunabhängigen Haftung auf Personenschäden und Schäden auf privat genutzte Sachen (Beschädigung oder Zerstörung einer anderen Sache als des fehlerhaften Produkts, die zum privaten Ge- oder Verbrauch bestimmt ist) beschränkt ist (Art. 9 85/374/EWG, §1 Abs. 1 ProdHaftG). Ohne Änderungen im Schadensbegriff des europäischen Sekundärrechts könnten Produktfehler, wie sie in IT-Sicherheitslücken hervortreten, allenfalls für Branchen mit latent hohem Schadensrisiko für Personen wie etwa Krankenhäuser oder Flugsicherung dem verschuldensunabhängigen Haftungsrecht unterworfen werden.

IT-Produktsicherheit

Das Produktsicherheitsgesetz, es folgt ebenfalls europäischen Vorgaben aus einer Vielzahl von EU-Richtlinien, ist ähnlich wie das ProdHaftG auf die Sicherheit und Gesundheit von Personen oder allgemein Körperschäden beschränkt (§ 3 ProdSG). Vermögens- und Eigentumsschäden, aber auch Schäden an Daten und Datenbeständen werden nicht erfasst. In den Sicherheitsanforderungen zu technischen Arbeitsmitteln und Verbraucherprodukten, konkretisiert noch in mehreren Ausführungsbestimmungen wie etwa der Verordnung über elektrische Betriebsmittel (1. ProdSV), finden sich zudem keinerlei Produktsicherheitsnormen, die auf mit dem Internet verbundene IT-Systeme und entsprechende IT-Sicherheitsvorfälle beziehbar wären oder anwendbar sind.

IT-Produktlebensdauer

Bislang bestehen Vorgaben zu einer garantierten Produktlebensdauer lediglich im Rahmen der europäischen Ökodesign-Richtlinie (2009/125/EG), und das für zwei Produktgruppen: Leuchtmittel und Staubsauger. Für die letztgenannte Produktgruppe beispielsweise wurde eine Motorlebensdauer von mindestens 500 Stunden festgelegt.[31] Ziel der Ökodesign-Richtlinie ist es, die Umweltverträglichkeit energieverbrauchsrelevanter Produkte unter Einbeziehung ihres gesamten Lebensweges mittels Vorgabe von Ökodesign-Anforderungen zu verbessern und EU-weit zu vereinheitlichen, um zu verhindern, dass solche nationalstaatlich unterlaufen

[30] Im Falle von Software, insbesondere von online übertragener Software, ist die Produkteigenschaft allerdings teilweise streitig. Vgl. Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler, Universität Göttingen. BSI, 2007. S. 85-87. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2

[31] Verordnung (EU) Nr. 666/2013 der Kommission vom 8. Juli 2013 zur Durchführung der Richtlinie 2009/125/EG des Europäischen Parlaments und des Rates im Hinblick auf die Festlegung von Anforderungen an die umweltgerechte Gestaltung von Staubsaugern. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0214+0+DOC+XML+V0//DE

und zu Handelshemmnissen werden können. Indikatoren für die Produktlebensdauer sind laut Anhang I der Richtlinie die garantierte Mindestlebensdauer, der Mindestzeitraum der Lieferbarkeit von Ersatzteilen, die Modularität, die Nachrüstbarkeit sowie die Reparierbarkeit. Als energieverbrauchsrelevante Produkte werden unter dem Regelungsniveau der EU-Ökodesign-Richtlinie grundsätzlich auch IT-Systeme und –Komponenten erfasst, obgleich diese in der Bewertungspraxis vorrangig noch als Stand-Alone-Systeme betrachtet werden und bislang keinerlei Regelungen für eine zu garantierende Mindestlebensdauer für solche erlassen wurden. Mit dem Internet verbundene IT-Systeme wie Smartphones oder IoT-Produkte wurden ferner bislang noch überhaupt nicht erfasst.

Vorschlag zu einer Cyber-Design-Verordnung

Eine Cyber-Design-Verordnung für informationstechnische Systeme (Hard oder Software oder beides) bietet zahlreiche Vorteile. Vorgaben zur Produkthaftung, Produktsicherheit und Produktlebensdauer für mit dem Internet verbundene IT-Systeme können separat, unabhängig von der Änderung einer Vielzahl von EU-Richtlinien und der durch sie spezifizierten Produkteigenschaften etabliert werden. In Form eines gesonderten Rechtsakts setzt jene auf bestehende Regelungen obenauf und bleiben letztere unberührt. Als Verordnung gilt sie zudem unmittelbar und etabliert einheitliche Schutzmaßnahmen in allen Mitgliedstaaten, ohne dass es eines nationalen Umsetzungsaktes bedarf. Indem – ähnlich wie nach der Ökodesign-Richtlinie – produktspezifische Durchführungsmaßnahmen erlassen werden, kann überdies in Fragen der Produkthaftung für Hard- und Softwarehersteller nach der Sicherheitssensitivität internetfähiger IT-Systeme differenziert werden und entsprechend den durchaus unterschiedlichen Belangen von Großunternehmen, kleinen und mittleren Unternehmen (KMU) sowie Kleinstunternehmen entgegengekommen werden. Insbesondere letztgenannten ist es heute in den meisten Fällen wirtschaftlich nicht möglich und auch künftig weiterhin nicht erforderlich, sich pauschal gegen Schadensfälle abzusichern, während der Abschluss von Cyber-Versicherungen zur Risikominimierung und zum Risikoausgleich den beiden erstgenannten unbenommen bleibt. Schließlich wird erstmals eine garantierte Mindestlebensdauer für solche IT-Systeme möglich, die sich – wie Smartphones oder IoT-Produkte – in der Betriebsverantwortung von privaten Endanwender*innen befinden und über die in der Praxis Cyberangriffe geführt werden, ohne dass deren Besitzer*innen es bemerken. Dazu ist die Produktlebensdauer, einschließlich des Vorhaltens von Software- und Sicherheits-Updates, entsprechender Geräte erheblich gegenüber dem Ist-Stand – die Funktionsfähigkeit von Smartphones beispielsweise ist nach Angaben des Umweltausschusses des Europäischen Parlaments heute bereits nach ein bis zwei Jahren nicht mehr ausreichend gewährleistet –[32] zu verlängern. Da der Europäische Binnenmarkt nicht zuletzt den größten gemeinsamen Markt weltweit darstellt, können sich gemeinschaftlich erlassene Schutzmaßnahmen und Sicherheitsstandards über eine Verbreitung der hier zulässigen Produkte außerhalb des EU-Binnenmarktes mittelbar auch jenseits der Gemeinschaftsgrenzen etablieren.

Zertifizierung, Security by Design und by Default

Außerhalb des Bereichs Kritischer Infrastrukturen, bei denen Sicherheitsstandards auf Basis der Kritis-Verordnung durch verantwortliche Unternehmen eingehalten werden müssen, fehlen ansonsten verbindliche Sicherheitsstandards für IT-Produkte, insbesondere solche mit Verbindung ins Internet. Sowohl das IT-Sicherheitsgesetz als auch die derzeit im Gesetzgebungsverfahren befindliche Verordnung der EU über die Einrichtung einer EU-Sicherheitsagentur (ENISA) und eines Sicherheitszertifizierungssystems sehen lediglich eine marktkonforme Form der Regulierung vor: Demnach sollen dem ursprünglichen Kommissionsvorschlag zufolge von öffentlicher Seite nur Vorgaben für Sicherheitszertifizierungen gemacht werden, deren Einhaltung dann von privaten Unternehmen überprüft und entsprechend zertifiziert wird. Das Zertifikat ist dabei keineswegs verbindlich vorgeschrieben, um ein Produkt überhaupt auf den Markt zu bringen. Es soll lediglich den Kund*innen bei ihrer Kaufentscheidung helfen.

Dies ist aus unserer Sicht nicht ausreichend und wurde vom Bundesrat auch bereits kritisiert (Bundesratsdrucksache BR 680/17). Vielmehr ist zu diskutieren, wie weit eine solche Sicherheitszertifizierung obligatorisch für die Marktzulassung werden sollte und aus pragmatischer Sicht werden kann. Hier ist auf die Zertifizierungspflicht der EU-Datenschutzgrundverordnung für Produkte, die den Anforderungen von Privacy by Design und Privacy by Default entsprechen müssen, als Vorbild zu verweisen (Art. 42 i.V.m. Art. 25 Verordnung (EU) 2016/679, Amtsblatt der EU L 119/1 vom 4.5.2016). Eine solche Regelung hinsichtlich Security by Design und Security by Default für IT-Produkte wäre im Rahmen einer abgestimmten Politik der EU sogar geboten, weil Fragen des Datenschutzes in Zeiten der Digitalisierung unmittelbar mit Fragen der Datensicherheit verknüpft sind. Security by Design würde dabei das Sicherheitsniveau auf dem Stand der Technik erfassen (Minimierung von Zugriffsmöglichkeiten), Security by Default beträfe beispielsweise den Umgang mit Zugangspasswörtern. Es müsste dann für jedes Produkt ein voreingestelltes, individuelles Passwort geben, statt solcher voreingestellter Passwörter wie »admin« oder »1234«. Der damit für die Hersteller verbundene Mehraufwand ist durch die Gefahren, die hinsichtlich der Möglichkeit des Aufbaus von Botnetzen im IoT bestehen, gerechtfertigt. Zudem sollten Hersteller*innen verpflichtet werden, Nutzer*innen eindeutig und verständlich darauf hinzu-

[32] Stellungnahme des Ausschusses für Umweltfragen, öffentliche Gesundheit und Lebensmittelsicherheit (11.4.2017) für den Ausschuss für Binnenmarkt und Verbraucherschutz zu dem Thema »Längere Lebensdauer für Produkte: Vorteile für Verbraucher und Unternehmen« (2016/2272(INI)). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0214+0+DOC+XML+V0//DE

weisen, welche Geräte und Anwendungen einen Zugang zum Internet haben und welche Gefahren damit möglicherweise einhergehen.

Die EU-Datenschutzgrundverordnung könnte zugleich hinsichtlich des Sanktionsregimes bei vorsätzlicher Verletzung der Prinzipien Security by Design/Security by Default und der oben genannten Meldepflichten für festgestellte Sicherheitslücken als Vorbild dienen. Für Datenschutzverstöße sind dort bis zu vier Prozent des Welt-Jahresumsatzes als Sanktion vorgesehen.

Investitionen in sichere Infrastrukturen

Jenseits einer fehlenden Haftung für Entwicklungsrisiken bestehen weitere Gründe, dass Hardware und Software nicht immer von Anfang an als sicher gelten können. Hervorzuheben sind im hiesigen Kontext insbesondere zwei.

Erstens: Mandatierte Sicherheitslücken in zentralen Netzkomponenten, mit denen staatliche Zugriffe durch Geheimdienste bspw. auf Netzwerkrouter ermöglicht werden, ohne dass die entsprechenden Hersteller*innen diese öffentlich machen dürfen. Weltweit wird der Markt für Switch- und Router-Technologien von Firmen aus den USA und China dominiert, sodass auch in Europa die Betreiber*innen von Netzinfrastrukturen mehr oder minder zwangsläufig diese Komponenten nutzen. Zudem bestätigte sich im Rahmen der Snowden-Enthüllungen ausdrücklich, dass die NSA Sicherheitslücken in diesbezüglichen Systemen von US-Hersteller*innen mandatierte und damit einhergehende Manipulationsmöglichkeiten nutzte. Umgekehrt geht die US-Regierung zugleich davon aus, dass ähnliche Hintertüren auch in chinesischen Produkten bestehen, sodass diese in den USA nicht in Hochsicherheitsbereichen eingesetzt werden dürfen.[33]

Zweitens: Betriebssysteme und andere Softwareapplikationen, die in ständiger Verbindung mit dem Internet stehen, um personenbezogene Daten auf den Clientsystemen zu erheben und auszuleiten. Hier ist unter anderem auf die Marktmacht von Microsoft und die Abhängigkeit von Behörden in Deutschland von dessen Produkten zu verweisen. Im Falle des Betriebssystems Windows 10 etwa kann, wie die Bundesbeauftragte für den Datenschutz (BfDI) konstatiert, selbst bei optimaler Konfiguration aller Datenschutzeinstellungen die Übertragung und Verarbeitung von personenbezogenen Daten auf Serversysteme in den USA nicht verhindert werden, können zudem die ausgelesenen Daten nicht geprüft werden, da sie verschlüsselt ausgeleitet werden.[34] Neben dem generellen Dilemma der Vulnerabilität von Microsoft-Produkten gegenüber Angriffen auf IT-Infrastrukturen kann dem Grundsatz, dass in Behörden eingesetzte Windows-Rechner von diesen uneingeschränkt kontrollierbar sein sollen, (gegenwärtig) nicht entsprochen werden.[35]

Es bedarf daher in Deutschland und Europa einer Rückgewinnung an technologischer Souveränität in Form von erheblichen Investitionen in Forschung und Entwicklung sicherer Infrastrukturen. Als Gegenmodell zur amerikanischen, partiell aber auch chinesischen Dominanz ist eine europäische Open-Source-Infrastruktur mit offenen und transparent entwickelten Standards zu etablieren. Die bereits für die IT-Forschung bspw. im Rahmen von »Horizont 2020« bereitgestellten Mittel müssen von der Förderung kommerzieller Produktentwicklungen zur Förderung von Open-Source-Software umgelenkt werden. Es soll nicht darum gehen, wie in der herrschenden Digitalwirtschaftspolitik konkurrenzfähige Unternehmen zu den USA und China aufzubauen, sondern IT-Produkte mit hohen Sicherheitsstandards für alle zugänglich zu machen. Zwar sind Open-Source-Software und Open-Source-Hardwarekomponenten nicht grundsätzlich fehlerfrei, doch lassen sie jederzeit eine Überprüfung zu. Auch können Open-Source-Anwendungen durch öffentlich ausgelobte Auditierungen oder bedingungslos ausgelobte Geldpreise für das Auffinden kritischer Sicherheitslücken (Bug-Bounty-Programme)[36] in ihrer Qualität erhöht und in ihrer potentiellen Kritikalität umgekehrt beständig verbessert werden. Durch offene Verfahren und das Prinzip vieler Augen können die Weichen in Richtung sicherer Open-Source-Infrastrukturen im Hinblick auf Software, Hardware und Dienste gestellt werden. Darüber hinaus lässt sich mit einer solchen Förderung von Open-Source-Technologien auch die Entwicklung von Privacy by Design-Standards verbinden, eine stärkere Verknüpfung mit der sozial- und geisteswissenschaftlichen Begleitung der Entwicklung und Einführung neuer Innovationen herstellen und die Einhaltung von ethischen Standards (Responsible Research) durchsetzen.

[33] https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf (S. 15).
[34] BfDI: 26. Tätigkeitsbericht zum Datenschutz 2015–2016. Erscheinungsdatum: 30.05.2017. S. 125f. https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/26TB_15_16.pdf?__blob=publicationFile&v=3

[35] https://www.heise.de/newsticker/meldung/Behoerden-ignorieren-Sicherheitsbedenken-gegenueber-Windows-10-3971133.html
[36] Gerade hinsichtlich der Missbrauchsmöglichkeiten solcher Programme, zunächst selbst für Sicherheitslücke zu sorgen, die dann später gemeldet werden können, kommt der Transparenz hinsichtlich der Mitwirkung an der Entwicklung von Open-Source-Produkten eine hohe Bedeutung zu.

Schwachstelle Mensch

Neben den Fragen der technisch zu lösenden Probleme der IT-Sicherheit liegt eine weitere bei den Anwender*innen von Technologie. Wie nicht zuletzt der Angriff auf die Netze des Bundes gezeigt hat, der im Frühjahr 2018 bekannt wurde, gibt es in der konkreten Nutzung eine Reihe möglicher Schwachstellen, die auch vielfach ausgenutzt werden: Zu den bekannteren gehören etwa Anhänge von E-Mails oder per Mail verschickte Links, die, wenn sie angeklickt werden, Schadsoftware auf dem Rechner bzw. im Netzwerk der Adressat*innen ausführen. Was bringt Nutzer*innen dazu? Links oder Anhänge sind meist mit einem mehr oder weniger überzeugenden Begleittext versehen, der vortäuscht, bei der Mail handele es sich um eine zu zahlende Rechnung, eine spannende Einladung oder sogar ein Sicherheitsproblem, bei dem Eile geboten ist.

Diese als Phishing bekannte Methode ist eine Variante des Social Engineering (sinngemäß: soziale Manipulation), bei dem durch Interaktion mit den Nutzer*innen Vertrauen aufgebaut wird, das dann zu sicherheitsgefährdendem Verhalten führt. Dazu gehört etwa auch die Weitergabe von USB-Sticks, die nach Verbindung mit einem Rechner dort Schadsoftware installieren: Die Infektion von Rechnern im Bundeskanzleramt durch die Spionage-Software Regin im Jahr 2014 wurde so durchgeführt.

Letztlich basiert fast jede Interaktion mit technischen Geräten, die nicht dem originär eigenen technischen Verständnis der genutzten Hard- und Software entspringt, darauf, dass anderen Vertrauen entgegen gebracht wird – nämlich, dass sie wissen, was sie tun, dass sie das Richtige empfehlen und dabei sowohl die Sicherheit als auch die dem angestrebten Ziel angemessene Benutzbarkeit der eingesetzten Technologie im Blick behalten.

Sowohl für die Nutzer*innen als auch für die Administrator*innen von IT-Infrastruktur stellt sich oft die Frage, ob die jeweilige Arbeitsumgebung komfortabel, also auch mit viel Freiheit in der Nutzung von Hard- und Software gestaltet sein soll, oder aber ob sie aus Perspektive der IT-Sicherheit möglichst sicher und damit sehr restriktiv sein soll. Mehr Bequemlichkeit für die Nutzer*innen bringt eine größere Zahl möglicher Schwachstellen mit sich und erfordert sowohl mehr Fähigkeiten bei den Nutzer*innen selbst, Risiken einzuschätzen und zu vermeiden als auch mehr Ressourcen für die Administration der Infrastruktur, sowie letztlich die Bereitschaft, bestimmte Gefährdungen in Kauf zu nehmen.

Ständige Weiterbildung

Der gut informierte und damit möglichst sichere Umgang mit Computern und technischer Kommunikation ist in einer sich technisch ständig wandelnden Welt eine große Herausforderung. Es wird erwartet, dass sich Menschen neben ihrem Alltag und den Erfordernissen ihres Berufs ständig technisch weiterbilden und zwar sowohl in der Anwendung (nicht mehr so) neuer Medien und Technologien als auch in der Abwehr von Gefahren.

In den vielen beruflichen Situationen gibt eine mehr oder weniger stark ausgeprägte Bedrohung durch wirtschaftliche wie durch politische Spionage.

Auch im privaten Alltag sind wir ständig mit IT-Sicherheitsthemen umgeben: Gefahren beim Online-Banking, Profilbildung in Sozialen Medien und die Nutzung dieser Daten durch Dritte wie bspw. bei Facebook durch Cambridge Analytica, Fake News und die Frage, welche Informationen eigentlich stimmen.

Der frühere Präsident des Bundesnachrichtendienstes, August Hanning, sagte als Zeuge im NSA-Untersuchungsausschuss lapidar: »Wir sind ein Land mit relativ niedriger Sicherheitskultur. In Deutschland werden viele Dinge über offene Leitungen miteinander ausgetauscht, wo ich als ehemaliger BND-Chef immer gesagt habe: Wie kann das eigentlich nur sein?«[37]

Dies bezog sich auf Kommunikation in der Politik aus der Perspektive der Spionageabwehr. Es lohnt sich aber, die Frage allgemein zu stellen: Warum wird individuell mit der Frage der IT-Sicherheit oft so unbesorgt umgegangen? Neben der verbreiteten Haltung: »Ich habe nichts zu verbergen«, die bei privaten Finanzen oder Fotos sowie bei beruflichen Unterlagen offensichtlich nicht zutrifft, findet sich die Antwort oft darin, dass viele zu wenig darüber wissen und darüber hinaus auch gar nicht, wen sie fragen könnten.

Ein wesentlicher Beitrag zu mehr Sicherheit ist eine Umgebung, die allen neben ihren sonstigen Tätigkeiten ermöglicht, sich mit relativ wenig Aufwand regelmäßig weiterzubilden und dazu ermutigt, Fragen zu stellen.

Diese Weiterbildung sollte nicht unterschätzt werden, insbesondere nicht in sicherheitsrelevanten Bereichen. Allein die Bereitstellung von guter Verschlüsselungssoftware hilft wenig, wenn die Anwendung ein Rätsel darstellt und ggf. lieber deaktiviert wird, um bestimmte Fristen einhalten zu können. Mobile Geräte erweitern beständig den Rahmen, innerhalb dessen kommuniziert und gearbeitet wird und mit ihnen ändert sich die Software häufig, die dafür benutzt wird.

Der Erfolg jeder Weiterbildung schließlich hängt von der Motivation der Lernenden ab, das Gelernte zu verstehen und anzuwenden. Im Bereich der IT-Sicherheit – wie überall sonst – hat positive Motivation mehr Erfolg als negative. Das bedeutet, dass Erfolgserlebnisse nachhaltigere Effekte haben als das Erzeugen von Schreckensszenarien.

[37] Dr. August Hanning, Protokoll Nr. 65 I des 1. Untersuchungsausschusses der 18. Wahlperiode des Bundestages, S. 20.

Statt also ausführlich zu erläutern, was bei der Nutzung von Verschlüsselung alles schief gehen kann, ist es weitaus zielführender, sich damit zu beschäftigen, wie bestimmte neue Routinen in den Alltag eingebaut werden können, die mit kleinen Schritten die Sicherheit verbessern und möglicherweise sogar Spaß machen, oder doch jedenfalls das Erfolgserlebnis erzeugen, etwas selbständig anwenden zu können.

Genauso notwendig ist die Produktion von Software, die einfach und verständlich funktioniert und dabei die Sicherheit verbessert.

Sensibilisierung

Ein wichtiger erster Schritt zur Verbesserung der eigenen Sicherheit und damit auch der von anderen, mit denen wir kommunizieren, über Netzwerke verbunden sind oder sonst Daten teilen ist es, mögliche Gefahren zu verstehen, erkennen und einordnen zu können.

Nicht alle sind gleichermaßen bedroht: Es gibt Unterschiede der Sensibilität von Daten, der Angreifbarkeit der verwendeten Hard- und Software, und nicht alle sind von denselben Angreifern bedroht. Entsprechend ist nicht nötig, dass alle das gleiche Schutzniveau anstreben. Was aber wichtig ist, ist sich darüber klar zu werden, wem warum welche Gefahr drohen kann und auf welche Risiken besser verzichtet würde.

Dazu ist bspw. auch ein Verständnis dafür nötig, wie Inhalts- und Metadaten von anderen verwendet werden (können), wie leicht scheinbar anonyme Daten wieder personenbeziehbar werden und was die Konsequenzen von Big Data und maschinellem Lernen sind – im positiven wie im negativen Sinn. Die Weitergabe der Daten von 50 Millionen Facebook-Nutzer*innen an die Firma Cambridge Analytica, die im März 2018 bekannt wurde, hat gezeigt, dass es ein erhebliches öffentliches Interesse für genau diese Fragen gibt – wenn sie verständlich und mit den möglichen Konsequenzen für die Nutzer*innen thematisiert werden.

Es wäre andererseits fatal, in Informationstechnik lediglich mögliche Gefahren zu sehen, ohne den gesellschaftlichen – und individuellen – Nutzen zu erkennen. Im Gegenteil ist das Interesse und die Möglichkeit, sich regelmäßig weiterzubilden die nötige Grundlage für den informierten Umgang mit sich ständig wandelnden Daten, Hard- und Software.

Bildung

Bildung kann und sollte überall stattfinden. In einer Welt, in der die Digitalisierung nicht mehr wegzudenken ist, ist das Erlernen der technischen Voraussetzungen, ebenso wie die Vermittlung einer generellen Medienkompetenz dringend geboten. Sie ist ein lebensbegleitender Prozess und muss in Bildungsangebote für alle gesellschaftlichen Gruppen und Altersstufen integriert werden. Medienkompetenz beschränkt sich dabei nicht nur auf die kritische Aneignung von digitalen und analogen Medieninhalten, technischen Funktionsweisen und die Auseinandersetzung mit den möglichen Gefahren, sondern soll auch zur eigenverantwortlichen Mediengestaltung befähigen.

Inhaltlich muss sie ein breites Spektrum an Themen umfassen: Sobald Kinder in Kontakt mit digitalisierten Inhalten kommen, sollte dies medienpädagogisch begleitet werden. Nicht nur das Fach Informatik muss in allen Schulformen selbstverständlich zum Fächerkanon dazugehören, vielmehr muss die Aneignung von Medienkompetenz fächerübergreifend stärker berücksichtigt werden: Online-Quellen erleichtern Hausaufgaben und Präsentationen, aber für den sinnvollen Umgang gehört das kritische Hinterfragen von digitalen Quellen und Informationen genauso dazu wie in der analogen Welt. Rechtliche und technische Fragen des Datenschutzes betreffen uns, sobald wir Adressdatenbanken pflegen, aber oft auch schon bei der Nutzung sozialer Medien, wie der aktuelle Facebook-Skandal deutlich vor Augen führt.

Je mehr sich Nutzer*innen im Netz bewegen, desto mehr digitale Spuren hinterlassen sie auch (z. B. durch Cookies). So wird es möglich, dass Profile über sie angelegt werden oder die so erhobenen Daten (über Einkäufe, besuchte Webseiten oder allgemeines Surfverhalten) für ungewollte Werbung oder gar zur Überwachung genutzt werden können.

Bildung im digitalen Bereich sollte immer verschiedene Perspektiven beinhalten – die Technik selbst, das Verhältnis zwischen Technologie und Gesellschaft und dessen kulturellen Auswirkungen und schließlich die Frage der Anwendungen: Wie und warum sie sich unterscheiden und welche die jeweils sinnvollsten sind.

Um all das leisten zu können, sind ständige Aus-und Weiterbildung von Erzieher*innen, Lehrer*innen und Dozent*innen erforderlich, dazu kommen die technischen Ausstattungen der pädagogischen Einrichtungen und deren Wartung.

Digitale Bildung endet nicht mit Schule und Ausbildung, sondern geht über in lebenslanges Lernen: Dafür muss es überall Möglichkeiten zur Weiterbildung geben. Dies ist für die Bewältigung vieler beruflicher Anforderungen so notwendig wie für die Gewährleistung von IT-Sicherheit.

Handhabbare Verschlüsselung

Ein wichtiger Bestandteil sicherer Kommunikation und IT-Infrastrukturen ist stabile Verschlüsselung. Im Idealfall findet sie im Hintergrund statt und erfordert keine Eingabe von komplizierten Passwörtern, die schnell vergessen oder unsicher auf Zetteln unter der Tastatur aufgeschrieben werden. Leider ist es aber so, dass die Realität viel zu oft anders aussieht. Noch vor einigen Jahren war die Absicherung bspw. von Daten, die über Web-Formulare eingegeben wurden (Webmail, Accounts bei Web-Anbietern aller Art) völlig ungenügend. Mit der Verbreitung von offenen WLANs stieg und steigt die Gefährdung privater und geschäftlicher Daten in dem Maß, wie die Verbindung mit dem Netz unverschlüsselt stattfindet.

Spätestens seit den Snowden-Enthüllungen hat sich die Erkenntnis durchgesetzt, dass E-Mails, Kurznachrichten und auch Telefonate genauso vor dem Mitlesen und –hören geschützt werden sollten, wie wir Geschäftsbriefe, vertrauliche Papiere und private Nachrichten nicht ohne Briefumschlag per Post verschicken. Bis heute ist allerdings die Verschlüsselung von E-Mails ein weitgehend ungelöstes Problem. Zwar hat sich die Handhabbarkeit der Ende-zu-Ende-Verschlüsselung mit PGP und später GnuPG deutlich verbessert, aber für die meisten Anwender*innen bleibt sie bis heute zu kompliziert.

Dringend erforderlich sind hier langfristige Fördermodelle für freie Software, denn elementare Grundlage für sichere Verschlüsselung ist, dass sie offenen und damit überprüfbaren Quellcode hat und seriös auditiert wird. Diese Förderung muss auch die fortdauernde Weiterentwicklung umfassen. Genauso wichtig ist aber die Usability, also die leicht verständliche und intuitive Benutzbarkeit der Anwendungen.

Digitale Gewalt

Die Digitalisierung aller Lebensbereiche betrifft auch den Alltag der Menschen, ihre zwischenmenschlichen Beziehungen und viele Formen der Kommunikation. Soziale Interaktionen haben sich verändert und viele Möglichkeiten geschaffen. Dies hat positive, aber auch negative Konsequenzen bis hin zu Veränderungen von Formen geschlechtsspezifischer Gewalt.

Was ist Digitale Gewalt?

Der Begriff »Digitale Gewalt« bezeichnet alle Formen von Gewalt, die sich technischer Hilfsmittel oder digitaler Medien bedienen, sowie Gewalt, die im digitalen Raum stattfindet, also bspw. im Rahmen von Online-Portalen oder sozialen Plattformen. Der Bundesverband Frauenberatungsstellen und Frauennotrufe/Frauen gegen Gewalt e.V. (bff) geht »davon aus, dass digitale Gewalt nicht getrennt von ‚analoger Gewalt' funktioniert, sondern meist eine Fortsetzung oder Ergänzung von Gewaltverhältnissen und -dynamiken darstellt«,[38] also als eine Form häuslicher Gewalt gesehen werden sollte. Dabei gibt es Angriffe einerseits im öffentlichen digitalen Raum und andererseits im sozialen Nahfeld.

Die Phänomene Digitaler Gewalt lassen sich in folgenden Gruppen zusammenfassen:

Gewalt im Rahmen von sozialen Beziehungen, Täter*innen sind hier häufig aktuelle oder ehemalige Beziehungspartner*innen, zum Beispiel

- Stalking in der Partnerschaft, während oder nach der Trennung, z. B. durch das Verschicken von SMS, Messages oder E-Mails;

- Kontrolle und in der Folge Einschüchterung und Bedrohungen durch

    · das Installieren von Spy-Apps, die es ermöglichen, den Aufenthalt festzustellen, Gesprächs- und Suchverläufe zu verfolgen, Kamera und Mikrofon von Mobilgeräten anzusteuern und einzuschalten,

    · den Zugriff auf Mobilgeräte durch Kenntnis von Passwörtern,

    · das Mitlesen von E-Mails und Social-Media-Accounts,

    · heimliches Filmen durch Kameras, die in privaten Räumen installiert wurden,

    · heimliches Abhören von Gesprächen;

- Revenge Porn, also Verbreiten von oder Erpressen durch die Ankündigung der Verbreitung intimer Fotos oder Videos.

Gewalt durch Fremd- und bekannte Täter*innen, zum Beispiel

- Identitätsdiebstahl, also das Verbreiten von Inhalten und Informationen im Namen der Betroffenen mit dem Ziel der Diffamierung, Einschüchterung und der sozialen Isolierung der Betroffenen, etwa wenn das in ihrem sozialen Umfeld wie z. B. in Firmen-Intranets geschieht;

- das Erstellen von falschen Profilen für Dating-Seiten, soziale Netzwerke, Porno-Seiten, die dann unerwünschte Kontaktaufnahmen, Belästigungen und weitere sexualisierte Gewalt zur Folge haben;

- das Erstellen und Verbreiten von Aufnahmen, die ohne Wissen oder Einwilligung der Betroffenen erstellt wurden, auch unter Verwendung von Betäubungsmitteln;

- sog. Doxing, also das Sammeln und Veröffentlichen von personenbezogenen Daten im Internet.

Gewalt im öffentlichen digitalen Raum, bei der sich Angreifer und Angegriffene nicht kennen, zum Beispiel

- gezielte verbale Angriffe gegen exponierte Personen wie Journalist*innen, Politiker*innen und Menschen, die sich politisch positionieren;

- gezielte verbale Angriffe gegen Angehörige von Minderheiten;

- Verwendung von Hatespeech;

- verbale Angriffe, bei denen verschiedene Diskriminierungsformen verschränkt sind, also bspw. Rassismus gekoppelt mit sexualisierten Beleidigungen; betroffen sind besonders Frauen, Women of Color, Geflüchtete, Migrant*innen, LGBTIQ.

Gewalt, die primär Jugendliche und Kinder betrifft

- das sog. Cyber-Mobbing oder Bullying, also das systematische Schikanieren und Quälen über einen längeren Zeitraum unter Jugendlichen etwa in Chatgruppen;

- Cyber-Grooming: Die gezielte sexuelle Belästigung von Kindern und Jugendlichen im Internet, bis hin zu sexualisierter Gewalt bei realen Treffen.

Wer ist betroffen

Es gibt nur wenige Studien, die sich mit Digitaler Gewalt oder einzelnen ihrer Phänomene befassen. Amnesty International hat im November 2017 die Ergebnisse einer Umfrage veröffentlicht, bei der je 500 Frauen zwischen 18 und 55 Jahren in sechs EU-Staaten, Neuseeland und den USA zu Digitaler Gewalt im Internet oder durch Soziale Medien befragt wurden. Knapp ein Viertel (23 Prozent) hatte online Digitale Gewalt erlebt, von diesen fühlten sich 41 Prozent in der Folge auch in

[38] bff: Fachberatungsstellen und die Digitalisierung geschlechtsspezifischer Gewalt, Oktober 2017, S. 2.

ihrer physischen Sicherheit bedroht. 55 Prozent erlebten Panikattacken oder Angstzustände. Bedeutend ist außerdem, dass mehr als drei Viertel der Frauen Verhaltensänderungen bei sich im Alltag und im Umgang mit der digitalen Welt feststellen.[39]

Der bff hat 2017 eine Umfrage unter Frauenberatungsstellen und Frauennotrufen zu ihren Erfahrungen mit Digitaler Gewalt in der Beratungstätigkeit durchgeführt, an der sich 60 Beratungsstellen beteiligten. Zu den Ergebnissen gehört, dass ein Großteil der Beratungsstellen angab, dass die Beratungsanfragen zum Thema Digitale Gewalt in den letzten drei Jahren angestiegen war. Vor allem bei Stalking werde mittlerweile in »nahezu allen Fällen das Internet oder digitale Medien dazu genutzt, Stalking-Handlungen auszuüben«. Weiterhin spielten Spy-Apps, die auf Smartphones installiert werden, eine »große Rolle im Kontext von Beziehungsgewalt«.[40]

Ein weiteres Ergebnis der Umfrage war, dass es für die Beratungsstellen oft schwierig ist, kompetente Ansprechpartner*innen bei der Polizei zu finden: »Teilweise sei es schwer, die Zuständigen für Fälle digitaler Gewalt bei der Polizei in Erfahrung zu bringen. Oft ist das Wissen der Polizei über digitale Gewalt gegen Frauen marginal, die Betroffenen werden nicht immer ernst genommen und äußerst selten gibt es (zuständige) IT-Spezialist*innen.«

Im Juni 2017 veröffentliche das Europäische Institut für Gleichstellungsfragen (EIGE) den Bericht »Gewalt im Internet gegen Frauen und Mädchen« und nahm darin auch Bezug auf die knappe Datenlage. So gehe eine 2014 vom der Agentur der Europäischen Union für Grundrechte (FRA) erstellte Studie zu Gewalt gegen Frauen, die auch Fragen zu Online-Stalking und Belästigung im Internet enthielt, davon aus, dass 10 Prozent der Frauen ab 15 Jahren bereits mindestens eine Form Digitaler Gewalt erfahren haben.[41] Die Autor*innen weisen außerdem darauf hin, dass Digitale Gewalt nicht losgelöst von sonstigen Gewalterfahrungen betrachtet werden sollte. Online-Stalking steht häufig in Verbindung mit realem Stalking, Frauen, die Digitale Gewalt im sozialen Nahfeld erleben, haben auch oft bereits unter häuslicher Gewalt gelitten.[42]

Männer und Frauen

Nicht nur Frauen und Mädchen sind von Digitaler Gewalt betroffen. Insbesondere mit internetbasierten, öffentlichen Formen Digitaler Gewalt sind auch oft Männer konfrontiert: Insbesondere Hatespeech oder Online-Mobbing. Der EIGE-Bericht kommt allerdings zu dem Ergebnis, dass die verfügbaren Studien vermuten lassen, »dass Frauen im Verhältnis zu Männern überproportional zum Ziel bestimmter Formen von Gewalt im Internet werden. So waren beispielsweise in einer Umfrage mit 9000 deutschen Internetnutzer*innen im Alter von 10 bis 50 Jahren Frauen deutlich häufiger Opfer von sexueller Belästigung über das Internet und Cyber-Stalking, und die Auswirkungen dieser Formen der Gewalt waren für die Opfer traumatischer.[43] Frauen sind insgesamt auch deutlich häufiger von Stalking betroffen als Männer. In Deutschland werden 17 Prozent aller Frauen und 4 Prozent aller Männer im Laufe ihres Lebens Opfer von Stalkern.[44]

Eine Umfrage des US-amerikanischen Pew Research Center stellte 2014 fest, dass Männer zwar häufiger weniger gravierende Formen Digitaler Gewalt erleben, aber vor allem jüngere Frauen deutlich häufiger von Stalking, sexualisierter Bedrohung und fortgesetzter Belästigung betroffen sind.[45]

Handlungsbedarf

Die Befassung mit dem Thema Digitaler Gewalt und die Suche nach Lösungen bewegt sich in einem Teufelskreis: Es gibt zu wenig Daten als Grundlage für die Diskussion und damit formal wenig Anlass, gesetzgeberisch tätig zu werden. Für viele der bekannten Phänomene gibt es keine klare gesetzliche Regelung, insbesondere nicht für Fälle, bei denen es zu Häufungen von Übergriffen gegen eine Person durch einen Täter (seltener: eine Täterin) kommt, die der Digitalen Gewalt zuzurechnen sind. Die einzelnen Taten jeweils für sich betrachtet werden kaum verfolgt oder Ermittlungen bald eingestellt. Zwar gibt es Straftatbestände wie Beleidigung (§ 185 StGB), Bedrohung (§ 241 StGB), Körperverletzung (§ 223 StGB), Nötigung (§ 240 StGB), Nachstellung/Stalking (§ 238 StGB). »Doch diese Straftatbestände werden bislang nicht zur Bekämpfung digitaler Gewalt mobilisiert. Ein Grund dürfte sein, dass digitale Gewalt verharmlost und ihre strafrechtliche Relevanz nicht erkannt wird: «nur Worte». Zudem wird oft bestritten, dass die Tatbestandsvoraussetzungen der jeweiligen Norm vorliegen.«[46]

Da geeignete gesetzliche Grundlagen fehlen, fehlen meist auch Sachkenntnis bei Polizei und Justiz, und zwar bei Staatsanwält*innen und Richter*innen wie im übrigen auch bei den Strafverteidiger*innen. Für die Identifizierung und Einordnung der Folgen der Verwendung von Spy-Apps oder anderen Formen der Verfolgung, Einschüchterung und Bedrohung fehlen häufig das technische Verständnis sowie die nötige technischen Ausstattung.

[39] Amnesty reveals alarming impact of online abuse against women, 20.10.2017. https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/
[40] bff: Fachberatungsstellen und die Digitalisierung geschlechtsspezifischer Gewalt, Oktober 2017, S. 8.
[41] Agentur der Europäischen Union für Grundrechte (FRA 2014). Violence against women: an EU-wide survey. Main results report. Luxemburg: Amt für Veröffentlichungen der Europäischen Union, S. 104. http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report
[42] Europäisches Institut für Gleichstellungsfragen (EIGE): Gewalt im Internet gegen Frauen und Mädchen, 2017, S. 4.
[43] Ebd., S. 3.
[44] bff: Stalking. Was ist das? https://www.frauen-gegen-gewalt.de/was-ist-das-362.html
[45] Pew Research Center, Online Harassment, 22.10.2014. http://www.pewinternet.org/2014/10/22/online-harassment/
[46] Ulrike Lembke: Kollektive Rechtsmobilisierung gegen digitale Gewalt, e-Paper der Heinrich-Böll-Stiftung, Dez. 2017, S. 9.

Auch weil es oft nicht zu strafrechtlicher Verfolgung oder gar Urteilen kommt, fehlen Daten zur Einschätzung der Bedeutung des Problems.

Es gibt also Handlungs- und politischen Regelungsbedarf auf folgenden Ebenen:

- Weiterbildung, mehr finanzielle Ressourcen und bessere Ausstattung – auch technisch – zum Thema Digitale Gewalt für Beratungsstellen. Dabei darf nicht unterschätzt werden, dass sich die technischen Methoden ständig verändern. Jeder Fall einer Frau, die in einem Frauenhaus Zuflucht findet und unbemerkt über ihr Smartphone von ihrem Angreifer geortet wird, bringt auch andere Frauen in Gefahr.

- Weiterbildung für Polizei und Justiz. Polizeibehörden müssen Fälle Digitaler Gewalt verstehen und ernst nehmen, und sie müssen technisch in der Lage sein, Ermittlungen durchzuführen.

- Leicht verständliche, gut erreichbare und regelmäßig aktualisierte Informationen für Betroffene.

- Bessere Daten über das Ausmaß und Formen Digitaler Gewalt, über Täter*innen und Betroffene: Es fehlen aussagekräftige und repräsentative Studien. Die letzte repräsentative Studie zu Gewalt gegen Frauen in Deutschland wurde vor 14 Jahren veröffentlicht.[47]

- Detailliertere Erfassung durch polizeiliche Statistiken.

- Es muss geprüft werden, inwieweit die verhältnismäßig neuen Formen der Digitalen Gewalt von geltenden Gesetzen überhaupt angemessen erfasst werden.

Zur Umsetzung fast aller dieser Punkte ist Deutschland im Übrigen durch die Ratifizierung der Istanbul-Konvention im Februar 2018 verpflichtet.[48]

[47] Bundesministerium für Familie, Senioren, Frauen und Jugend: Studie: Lebenssituation, Sicherheit und Gesundheit von Frauen in Deutschland, Januar 2005. https://www.bmfsfj.de/bmfsfj/studie--lebenssituation--sicherheit-und-gesundheit-von-frauen-in-deutschland/80694

[48] Die sogenannte Istanbul-Konvention ist das »Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt« und in Deutschland zum 1. Februar 2018 als rechtlich bindendes Menschenrechtsinstrument in Kraft getreten. https://www.coe.int/en/web/istanbul-convention/text-of-the-convention

Cyber Warfare – Fragestellungen aus friedens- und sicherheitspolitischer Sicht

Im sicherheits- und rüstungspolitischen Diskurs des Bundesverteidigungsministeriums steht Cyber War insbesondere seit Beginn der Dekade sehr hoch im Kurs. Das Rüstungsressort weist auf die immens gestiegenen Risiken hin, bietet anderen Ressorts (Amts-)Hilfe an und baut seine eigenen »Cyberkrieger«-Kapazitäten personell und finanziell aus. Die Sicherheit Deutschlands soll – so die Diktion des Bundesministeriums der Verteidigung (BMVg) – künftig auch im Cyberraum verteidigt werden.

In den letzten zwei Haushaltsjahren hat das BMVg sich seinen Etat für den IT-Bereich deutlich aufstocken lassen. Der IT- und Cyber-Bereich wurde auch strukturell und personell verstärkt, u. a. durch den Aufbau des eigenständigen Kommandos Cyber- und Informationsraum (CIR), das neben den traditionellen Teilstreitkräften Heer, Luftwaffe und Marine nun zu einer eigenen Waffengattung gegliedert wird, sowie durch die Einstellung/Rekrutierung zusätzlicher Fachleute für diesen Bereich. Die Bundeswehr und das BMVg argumentieren – auch in diesem Bereich – so gut wie ausschließlich mit der Intention, Angriffe abzuwehren.

Die wirksamste nicht-eskalierende Strategie hierfür wäre, effektiv in einen Schutz nach außen zu investieren, d. h. eine Sicherung und Abschottung der eigenen Waffensysteme, Netze und der dafür nötigen Infrastruktur. Das würde bedeuten, sich auf Entnetzung, Härtung und systemische Begrenzungen innerhalb des Netzes zu konzentrieren. Ein wesentlicher Aspekt eines solchen Ansatzes wäre ein Fokus auf Security by Design: Eine weitgehende Produkt- und Systemkontrolle auf allen Produktions- und Nutzungsstufen, beginnend beim Entwickeln und Testen von Hard- und Software, dem Patchen von Schwachstellen und dem Einbau und der Verwendung neuer Komponenten durch Entwickler*innen oder Nutzer*innen.

Stattdessen setzt das BMVg aber zur Kostenminderung und Beschleunigung der Beschaffungsprozesse weiträumig auf Einkäufe off the shelf (also: von der Stange) bei kommerziellen Anbietern (was mit Blick auf die explodierenden Kosten all der Rüstungsentwicklungsprojekte, die nicht richtig ans Laufen kommen, fast beruhigend ist – leider aber nicht für die Sicherheit der genutzten Systeme spricht).

Auch der Problemlösungsansatz ist offensichtlich nicht auf Defensive und Erhöhung des Schutzniveaus orientiert, sondern auf das Etablieren und Üben von Fähigkeiten, die zwar helfen können, Angriffe abzuwehren, zu hemmen, vereiteln oder in ihren Auswirkungen zu reduzieren, aber ebenso gut für eigene Angriffe eingesetzt werden können:

Die Bundeswehr fokussiert auf das Trainieren der (aktiven) Abwehr von Angriffen in den Netzen. Das führt zwangsläufig zur Ausbildung offensiver Fähigkeiten. Denn das Testen der Netze und das Üben der Abwehr von Angriffen bedeutet spiegelbildlich das Entwickeln und Üben eigener Angriffsfähigkeiten, also den Erwerb der für offensive Einsätze benötigten Fähigkeiten.

Wirklich »effektiv« ist dieser Ansatz im Übrigen nur, wenn zugleich die Infiltration anderer Netze aktiv trainiert wird. Der Übergang vom Eindringen in fremde Netze, über das Analysieren der vorgefundenen Strukturen und Eingriffs-/Angriffsmöglichkeiten, zum aktiven (und im Ergebnis offensiven) »Wirken« zur Durchführung eigener Angriffe oder dem Stoppen fremder Angriffe (Hackback) ist fließend.

Schon mit der Infiltration anderer Netze, ohne dass darüber hinausgehende Manipulationen oder sogar ein Angriff erfolgen, begibt die Bundeswehr sich mindestens in eine völkerrechtliche Grauzone. Ähnlich wie Spionage stellt das Eindringen in fremde Netze – auch, wenn es nicht unmittelbar einem Angriff dient – einen Bruch des völkerrechtlichen Souveränitätsgrundsatzes dar. Selbst wenn dabei kein Schaden im Bereich eines anderen Staates verursacht wird, verstößt der Eingriff also gegen das Interventionsverbot.

Digitale Waffen haben ein hohes Proliferationsrisiko, weil sie in kürzester Zeit entdeckt, analysiert und umgeschrieben werden können. Darüber hinaus ist das Trainieren der Abwehr und Durchführung von Hacker-Angriffen im militärischen Bereich selbstverständlich ebenso wie beim Einsatz von Behörden im Inland in der Praxis verknüpft mit dem Finden, Ausnutzen und Offenlassen von Schwachstellen, und damit der Schwächung von digitaler Sicherheit.

Immens ist schließlich die mit einer starken Fokussierung auf Cyber Warfare und IT-Waffen verbundene Eskalationsgefahr: Die Bedrohungs- und Angriffsspirale kann sich leicht hochschaukeln zu einem mit »richtigen« Waffen ausgetragenen konventionellen militärischen Konflikt.

Verschärft wird dieses Risiko einer Eskalation von IT-Angriffen zu konventionellen militärischen Auseinandersetzungen durch die Missbrauchsmöglichkeiten, die sich aus der Schwierigkeit der präzisen Attribution von Angriffen ergeben: Tatsächlich durchgeführte Angriffe lassen sich nicht sicher zuordnen, es können falsche Fährten gelegt werden. Andererseits könnten – faktisch kaum widerlegbar – Angriffe anderer Staaten, die tatsächlich gar nicht stattgefunden haben oder tatsächlich andere Urheber hatten, fingiert/behauptet werden und (wenn sie verbunden sind mit einer Verursachung physischer Schäden, die einem »bewaffneten Angriff« im Sinne von Art. 51 UN Charta gleichkommen) sogar zur Grundlage eines (konventionellen) militärischen (Selbstverteidigungs-) Angriffs gemacht werden.

Auf dem Weg in diese Richtung befinden wir uns bereits mit sich in den letzten Jahren häufenden, kaum überprüfbaren oder widerlegbaren, Vorwürfen der sog. Hybriden Kriegführung (und die Bundesregierung gehört mit zu den Akteur*innen, die »Hybrid« und »Cyber War« nahezu synonym nutzen).

Völkerrechtlich interessant sind vor allem die folgenden Aspekte: Die Frage, ob die geltenden völkerrechtlichen Regeln anwendbar sind – das dürfte grundsätzlich der Fall sein. Die Frage nach der Erheblichkeitsschwelle, d. h. ob/wann ein digitaler Angriff vorliegt, der hinsichtlich Umfang und Wirkung so intensiv ist, dass er einem Einsatz von Waffengewalt gleichkommt, der eine Selbstverteidigungssituation im Sinne von Art. 51 UN Charta oder Art. 5 NATO-Vertrag auslöst bzw. die Berufung darauf ermöglicht. Damit eng verknüpft sind wiederum Fragen der sicheren Attribution von Angriffen – eine »Selbstverteidigung auf Verdacht« gegen einen Staat, dem der Angriff zugeschrieben wird, ist völkerrechtlich nicht zulässig.

Das Unterscheidungsgebot des Humanitären Völkerrechts ist zu beachten: Militärische Angriffe dürfen nur gegen militärische Ziele, nicht auf zivile Objekte oder Zivilpersonen gerichtet werden. Cyber-Attacken können oder werden nahezu zwangsläufig Auswirkungen auf zivile Infrastruktur und die Bevölkerung haben, bis hin zu nicht absehbar hohen Zahlen an gravierend Verletzten oder Toten. Im Fall von Angriffen auf Kritische Infrastrukturen wie z. B. Krankenhäuser, Transportinfrastruktur, Energieversorgungseinrichtungen/Kraftwerke ist das überdeutlich. Im Fall der Übernahme der Steuerungsgewalt über Waffensysteme kann es aber auch dazu kommen, dass diese Waffensysteme gegen die Bevölkerung gerichtet werden oder dort zumindest Opfer verursachen (z. B.: Absturz eines gekaperten Kampfjets über bewohntem Gebiet).

Fürs deutsche Recht relevant ist schließlich auch der Parlamentsvorbehalt: Wie soll das Parlament informiert und seine Zustimmung eingeholt werden? Ab welchem Zeitpunkt und welcher Eingriffsstufe/Intensität? Und vor allem, mit Blick darauf, dass Cyber-Angriffe heimlich/verdeckt und ohne Vorwarnung erfolgen müssen, wenn sie Wirkung entfallen sollen: Wie kann der Parlamentsvorbehalt wirksam aufrechterhalten bzw. seine Aushebelung verhindert werden?

Die aufgeworfenen völker- und verfassungsrechtlichen Probleme sind eigentlich so gravierend, dass es allenfalls einen geringen Anwendungsbereich für legale militärische Hacker-Attacken geben kann. Zweifelhaft ist allerdings, inwieweit Regierungen sich dieser rechtlichen Bindung tatsächlich auch unterwerfen. Aktivitäten in Richtung einer Anpassung des Kriegsvölkerrechts sind schon im Gange: Auf Initiative der NATO sind von 2009 bis 2012 bereits Völkerrechtler zusammengekommen, um ein Regelungssystem zu skizzieren; herausgekommen dabei ist das 2013 erschienene »Tallin Manual on the International Law Applicable to Cyber Warfare«.

Die Bundeswehr hat ihren (soweit bekannt) ersten eigenen Hacker-Einsatz in fremden Netzen schon seit einiger Zeit hinter sich, ohne dass das Parlament vorher oder auch nur nach Abschluss darüber informiert wurde: CNO[49]-Kräfte hackten sich ins IT-System eines afghanischen Mobiltelefonbetreibers und lieferten die Positionsdaten der Entführer einer deutschen Entwicklungshelferin in Kabul. Verbrämt wurde das als »Geiselbefreiung«, obwohl die Entführte aufgrund einer Lösegeldübergabe freigelassen wurde – vermutlich um die Behauptung, der Einsatz sei vom Bundestagsmandat abgedeckt, überzeugender wirken zu lassen.[50]

Zwei Tendenzen dürften auszumachen sein: Ebenso wie andere staatliche Stellen fokussiert die Bundeswehr weniger darauf, eigene Strukturen wirksam zu schützen, als darauf, Angriffe aktiv/offensiv abwehren und selbst ausführen zu können. Gegenläufig ist zu befürchten, dass, (auch) zur Behebung von Attributionsproblemen und der Erleichterung eigener Infiltrationsaktivitäten, seitens der Bundesregierung und nachgeordneter Stellen darauf hingearbeitet werden könnte, größere staatliche Kontrolle über IT-Aktivitäten der Bevölkerung/Nutzer zu erlangen, also weitere Regelungen zur erleichterten Nachverfolgbarkeit von Datenaustausch zu implementieren.

Daraus leiten sich folgende Forderungen an die Bundeswehr und Bundesregierung ab: Strikte Bindung an das Verfassungs- und Völkerrecht. Die Bundeswehr muss auf eine effektive Sicherung ihrer eigenen Waffensysteme, Netze und der dafür benötigten Infrastruktur beschränkt bleiben, primär durch Entnetzung, Abschottung, systematische Begrenzungen sowie weitreichende Produkt- und Systemkontrolle auf allen Produktions- und Nutzungsstufen. Schon das derzeit praktizierte »Üben« trägt zur Unsicherheit der IT-Infrastruktur bei (Zero-Day-Exploit-Problematik) und leitet über zur Vorbereitung eigenen aktiven, offensiven Agierens, verbunden mit dem aufgezeigten Eskalations- und Proliferationsrisiko.

Und Einsätze der Bundeswehr im Inneren zum Schutz kritischer Infrastrukturen sind in »Friedens«-zeiten natürlich genauso abzulehnen wie jeder andere Inlandseinsatz.[51]

[49] Computer-Netzwerk-Operationen.

[50] http://www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html

[51] Nur ausnahmsweise, und auch nur im »wirklichen« Verteidigungsfall gegen militärische Angriffe von außen (also nicht im Rahmen der aktuell praktizierten, nur prolongierten/gewillkürten Landes- bzw. Bündnisverteidigung durch Auslandseinsätze im NATO-/EU-Rahmen) könnte die Aufgabenstellung für die Bundeswehr sich auf den Schutz kritischer ziviler Infrastrukturen gegen von Menschen ausgehende Eingriffe erstrecken.

Fazit und Forderungen

Die getroffenen Regelungen, Ausgestaltungen und Maßnahmen des Sicherheitsmanagements unterlaufen einander teilweise selbst. Gut gemeinte Ansätze werden durch gegenläufige Interessen unterminiert und durch vielfache Doppelzuständigkeiten verkompliziert. Solange der Widerspruch zwischen der scheinbaren Notwendigkeit des Besitzes von Sicherheitslücken einerseits und dem Willen, IT-Systeme durch die Schließung von Sicherheitslücken zu härten, nicht aufgelöst ist, werden die eigenen Anstrengungen stets konterkariert. Nach Auffassung der Autor*innen kann nur eine umfassende Meldepflicht von Sicherheitslücken zu einem Mehr an IT-Sicherheit führen. Darüber hinaus braucht es eine unabhängige Einrichtung, deren Interesse allein der IT-Sicherheit gilt – indem sie als Servicedienstleister für digital souveräne Bürger*innen agiert und Schutzstandards für Unternehmen und Kritis setzt. Eine solche Funktion könnte das BSI übernehmen, wenngleich es dafür vom BMI entbunden werden müsste. Neben grundsätzlichen Änderungen im Bereich staatlicher Zuständigkeiten ist es ebenso notwendig, die Hersteller der Produkte in Haftung zu nehmen. Durch die Schaffung einer Cyber-Design-Verordnung kann es gelingen, auch im Bereich der Produkte selbst einen notwendigen Sicherheitsgewinn zu erzielen.

Folgende Kernforderungen lassen sich aus dem vorangegangenen Text ableiten:

1. Das BSI soll eine Behörde werden, deren Kernaufgabe die Erhöhung der digitalen Sicherheit für alle Bürger*innen ist. Dafür muss das BSI aus der Zuständigkeit des BMI entlassen werden und als eigenständige Behörde aufgebaut werden.

2. Einführung einer generellen Meldepflicht für Sicherheitslücken. Die Meldung soll in einem abgestuften Verfahren (erst Verantwortliche, dann Öffentlichkeit) erfolgen.

3. Ausweitung der Produkthaftung auf IT-Hersteller sowie Einführung einer Cyber-Design-Verordnung.

4. Eine deutliche Erhöhung der Investitionen in Open-Source-Software und in Open-Source-basierte IT-Sicherheitstechnologien sowie ihr Einsatz in den Behörden.

5. Für Gefahrenabwehr und Strafverfolgung im Bereich von Cybercrime, IT-gestützter Spionage und Angriffen auf die digitale Infrastruktur sind allein die Polizeibehörden zuständig. Geheimdienste, zu deren Aufgaben Infiltration und Spionage gehören, sind für die Schließung von Sicherheitslücken ungeeignet.

6. Verbot des Einsatzes von Staatstrojanern, keine Nutzung oder Anschaffung von Zero Day Exploits oder eingebauter Backdoors.

7. Exportverbot für Überwachungssoftware.

8. Keine Hackbacks durch staatliche Institutionen.

9. Für regelmäßige Weiterbildung zu Fragen der IT-Sicherheit müssen in allen Bereichen des privaten und beruflichen Alltags Zeit und Ressourcen zur Verfügung stehen.

10. Digitale Gewalt muss als eigenständiges Phänomen begriffen werden, für das eigene Statistiken, gesonderte, besonders geschulte Bereiche in den Behörden der Strafverfolgung und mehr Ressourcen für die Beratungsstellen erforderlich sind.

11. Kein Ausbau der Cyberfähigkeiten der Bundeswehr und kein Einsatz der Bundeswehr zum Schutz kritischer Infrastrukturen im Inland.

Notizen

Notizen

www.linksfraktion.de