acatech IMPULS

Cybersicherheit

Status quo und zukünftige Herausforderungen

Claudia Eckert, Reinhard Ploss (Hrsg.)

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

acatech IMPULS

Cybersicherheit

Status quo und zukünftige Herausforderungen

Claudia Eckert, Reinhard Ploss (Hrsg.)

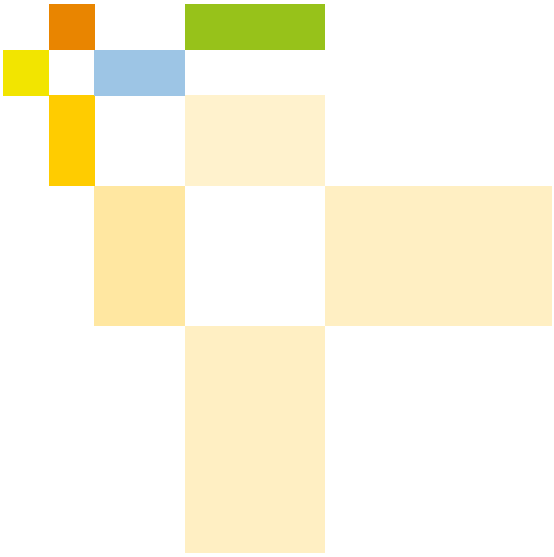
acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

Die Reihe acatech IMPULS

In dieser Reihe erscheinen Debattenbeiträge und Denkanstöße zu technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Sie erörtern Handlungsoptionen, richten sich an Politik, Wissenschaft und Wirtschaft sowie die interessierte Öffentlichkeit. Impulse liegen in der inhaltlichen Verantwortung der jeweiligen Autorinnen und Autoren.

Alle bisher erschienenen acatech Publikationen stehen unter www.acatech.de/publikationen zur Verfügung.

Inhalt



Projekt

Herausgeberin und Herausgeber

- Prof. Dr. Claudia Eckert, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)/Technische Universität München/acatech Präsidiumsmitglied
- Dr.-Ing. Reinhard Ploss, acatech Präsident

Projektleitung

- Prof. Dr. Claudia Eckert, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)/Technische Universität München/acatech Präsidiumsmitglied

Projektgruppe

- Carlos Arglebe, Siemens Healthineers AG
- Prof. Dr. Johannes Alfred Buchmann, Technische Universität Darmstadt/acatech
- Prof. Dr. Claudia Eckert, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)/Technische Universität München/acatech Präsidiumsmitglied
- Alexander von Gernler, genua GmbH
- Prof. Dr. Jörn Müller-Quade, Karlsruher Institut für Technologie (KIT)/acatech
- Raphael Otto, Infineon Technologies AG
- Dr.-Ing. Reinhard Ploss, acatech Präsident
- Prof. Dr. Michael Waidner, Fraunhofer-Institut für Sichere Informationstechnologie (SIT)/Technische Universität Darmstadt/acatech

Weitere Expertinnen und Experten

- Prof. Dr. Christian Reuter, Technische Universität Darmstadt
- Prof. Dr. Haya Shulman, Fraunhofer-Institut für Sichere Informationstechnologie (SIT)/Goethe-Universität Frankfurt am Main
- Dr. Sven Herpig, Stiftung Neue Verantwortung e.V.
- Thomas Schauf, Deutsche Telekom AG
- Dr. Dirk Häger, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Autorin und Autoren

- Prof. Dr. Claudia Eckert, Fraunhofer-Institut für Angewandte
- und Integrierte Sicherheit (AISEC)/Technische Universität
- Dr.-Ing. Reihard Ploss, acatech Präsident
- Simon Litsche, acatech Geschäftsstelle
- Paul Grünke, acatech Geschäftsstelle

Projektlaufzeit

12/2021–11/2022

1 Einleitung und Motivation

Die Digitalisierung in Deutschland schreitet stetig voran. Immer mehr Aufgaben, ob im privaten, beruflichen oder öffentlichen Kontext, werden digital ausgeführt – eine Entwicklung, die sich durch die Covid-19-Pandemie stark beschleunigt hat. Dies ist grundsätzlich als sehr positiv zu bewerten, da die Digitalisierung zahlreiche Potenziale für Gesellschaft und Wirtschaft bietet. Gleichzeitig haben aber auch die Bedrohungen im Cyberraum in den letzten Jahren signifikant zugenommen. Für Unternehmen, öffentliche und staatliche Institutionen sowie für Privatpersonen sind sehr unterschiedliche Bedrohungsszenarien relevant. Unternehmen geraten immer stärker in den Fokus von Cyberkriminellen. Die aktuelle geopolitische Lage hat zudem verdeutlicht, dass auch politisch motivierte Cyberattacken ein erhöhtes Bedrohungspotenzial darstellen können. Eine zentrale Herausforderung der voranschreitenden Digitalisierung stellt das Thema Desinformation dar. Hierbei handelt es sich um eine Problematik, die durch Maßnahmen der Cybersicherheit nicht in vollem Umfang adressierbar ist. Stattdessen sind die Bürgerinnen und Bürger gefragt. Sind sie ausreichend kompetent, um in einer digitalen Welt zu leben?

Desinformation im Kontext neuer, veränderter Kommunikationsformen ist eine eigenständige Herausforderung, die gesondert betrachtet werden muss.

Cybersicherheit (siehe Infobox) ist eine notwendige Voraussetzung für eine erfolgreiche Digitalisierung. Cybersicherheit bedeutet auch, dass Vertrauen aufgebaut wird: Systeme, die es Bürgerinnen und Bürgern, Industrie und Politik erlauben, sich sicher im Netz zu bewegen sowie ihre Geschäfts- und Produktionsprozesse sicher digital zu gestalten, schaffen erhebliche Mehrwertpotenziale für die Zukunft. Eine ambitionierte Cybersicherheitsstrategie muss daher ein Herzstück der deutschen Digitalisierungsstrategie sein. Eng verwoben mit der Cybersicherheit ist der Bedarf, die Digitale Souveränität zu stärken; zusammen bilden sie die Grundlage für selbstbestimmtes und vertrauenswürdiges Handeln im Cyberraum. Um Systeme und Organisationen vor ungewollter Einflussnahme unter anderem über Datenmanipulation, Erpressungsangriffe (Ransomware), Informationsdiebstahl oder Lock-in-Effekte durch Monopolisierung zu schützen, muss sichergestellt werden, dass die in Deutschland eingesetzten digitalen Technologien beherrschbar und die digitalen Systeme ausreichend resilient gestaltet sind. Damit diese beherrschbar sind, ist eine Beurteilungsfähigkeit notwendig, die es ermöglicht, das Risiko einzuschätzen, das mit dem Einsatz von Technologien in Bezug auf den Nutzungszweck verbunden ist. Zudem müssen Alternativen bereitstehen, um eine Risikominimierung selbstbestimmt vornehmen zu können. Es ist essenziell, dass eine Cybersicherheitsstrategie sowohl Maßnahmen zur Erhöhung der Resilienz und der Beurteilungsfähigkeit als auch Wege beinhaltet, auf Cyberangriffe aktiv reagieren zu können. Eine Cybersicherheitsstrategie kann nicht gezielt auf einzelne Bedarfe eingehen, sollte aber konkrete Leitlinien und auch Technologieanforderungen festschreiben, ohne sich auf einzelne Produkte festzulegen.

Digitale Souveränität (siehe Infobox) bedeutet, Wahlmöglichkeiten zu haben.[1] Dies darf aber nicht mit Autarkie und Protektionismus verwechselt werden. Um technologische Abhängigkeiten zu reduzieren und beherrschbarer zu machen, müssen Kernkompetenzen gleichermaßen systematisch auf- und ausgebaut sowie die Entwicklung innovativer, vertrauenswürdiger Schlüsseltechnologien vorangetrieben werden. Das umfasst Fähigkeiten entlang der kompletten Wertschöpfungskette von der Forschung über die Entwicklung von Produkten bis hin zur Beurteilung, zur sicheren Integration und zum sicheren operativen Betrieb von IT-Infrastrukturen. Weitere wichtige Kernkompetenzen sind unter anderem die Risikobeurteilung und die moderne Kryptografie wie etwa die Post-Quantum-Kryptografie oder die homomorphe Verschlüsselung, aber auch digitale Identitäten, die Sicherheit von 6G-Netzen, Threat-Intelligence, vertrauenswürdige Hardware und sicher eingebettete Betriebs-Software. Obwohl Deutschland in den genannten Bereichen in Teilen bereits gut aufgestellt ist, bleibt eine Forcierung der systematischen Weiterentwicklung unerlässlich. Dringender Handlungsbedarf besteht im Hinblick auf Software und IT-Dienstleistungen: Hier gibt es insbesondere im Cloud-Bereich keine relevanten europäischen Alternativen zu den führenden internationalen Hyperscalern wie Google, Amazon oder Microsoft. Deutschland muss seine Digitale Souveränität mit Partnern vorantreiben, die die gleichen demokratischen Werte teilen. Gemeinsame europäische Initiativen wie unter anderem der Chip Act[2], die souveränen Datenräume[3] oder auch die Überarbeitung der eIDAS-Verordnung[4] und der neue Cyber Resiliance Act[5] stellen wichtige Eckpfeiler für die Stärkung der Digitalen Souveränität dar.

1 | Vgl. acatech 2021.
2 | Vgl. Europäische Kommission 2022a.
3 | Vgl. Europäische Kommission 2020.
4 | Vgl. Europäische Kommission 2022b.
5 | Vgl. Europäische Kommission 2022c.

Eine umfassende Cybersicherheitsstrategie muss Antworten auf all diese Herausforderungen finden, um die Digitalisierung erfolgreich voranzutreiben. Dieser IMPULS gibt hierfür Denkanstöße, die zu Maßnahmen und Strategien ausgearbeitet werden können. Zudem wird in der vorliegenden Publikation herausgestellt, dass Cybersicherheit ganzheitlich betrachtet werden muss, weil alle wirtschaftlichen, politischen und gesellschaftlichen Entitäten davon betroffen sind und komplexe Verschränkungen mit verwandten Themen wie dem der Digitalen Souveränität existieren. Darüber hinaus soll veranschaulicht werden, dass eine erfolgreiche Umsetzung nur gelingen kann, wenn das Thema nicht nur von politischen Entscheiderinnen und Entscheidern sowie Unternehmen mit hoher Priorität behandelt wird, sondern wenn auch ein gesellschaftlicher Wandel stattfindet. Dieser IMPULS gibt einen Überblick über den Themenkomplex, tiefergreifende Untersuchungen einzelner hier nur angerissener Teilaspekte werden in kommenden Veröffentlichungen folgen.

Kapitel 2 Ausgangslage bietet einen Überblick über relevante Akteure und verschiedene Angriffsmethoden sowie eine Definition des Begriffs Cybersicherheit. Im darauffolgenden Kapitel werden zentrale Herausforderungen, die mit einer Erhöhung der Cybersicherheit einhergehen, diskutiert. Dazu zählt eine unzureichende Umsetzung bereits bekannter Konzepte. Des Weiteren werden einzelne relevante Forschungsfelder adressiert – die deutsche Cybersicherheitsforschung ist bereits sehr gut aufgestellt – sowie Hemmnisse für die Forschung aufgedeckt. Zudem werden die Relevanz eines gesellschaftlichen Bewusstseins für Cybersicherheit sowie Hürden bei gesamtgesellschaftlichen Verhaltensanpassungen aufgezeigt. Daran schließt sich eine Betrachtung derjenigen Herausforderungen an, vor die sich die Politik gestellt sieht. Nachfolgend wird analysiert, wie Cybersicherheit durch mangelnde Digitale Souveränität beschränkt wird. Im abschließenden Kapitel 4 Handlungsfelder werden Wege aufgezeigt, wie die bestehenden Aufgaben von den verschiedenen Akteuren angegangen werden können. Um sich dem Thema ganzheitlich zu nähern, wurden Expertinnen und Experten aus verschiedenen Fachrichtungen befragt. Das interdisziplinäre Team konsolidierte die Inhalte in regelmäßigen Abstimmungsrunden.

Definition Cybersicherheit

Cybersicherheit bedeutet, die Nutzung von IT auf eine sichere Art und Weise zu ermöglichen und bildet damit die Grundlage für eine digitalisierte Gesellschaft. Cybersicherheit umfasst einen technischen Kern, der den Schutzzielen der Informationssicherheit entspricht. Die grundlegenden Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit.[6] Zunehmend an Relevanz gewinnt auch das Schutzziel Authentizität, denn Kommunikation und Interaktion erfolgen immer häufiger auf digitalen Wegen. Der wahren Identität einer Person, mit welcher man beispielsweise über E-Mails, Logins oder die Autorenschaft von Updates in Kontakt tritt, kommt somit im wachsenden Maße Bedeutung zu. Darüber hinaus beinhaltet Cybersicherheit auch die politischen, soziokulturellen, rechtlichen und wirtschaftlichen Aspekte, die direkten Bezug zu diesem technischen Kern haben. Das Ziel von Cybersicherheit ist somit einerseits der Schutz von Daten und Informationen sowie andererseits auch der Schutz aller Kommunikations- und Informationssysteme, die zur Verarbeitung und Übertragung dieser Daten und Informationen genutzt werden und der sie umgebenden physischen Systeme. Nachdem ein kompletter Schutz beziehungsweise das vollständige Erreichen der Schutzziele nicht garantiert werden kann, muss immer abgewogen werden, wie ein angemessener Grad an Zielerreichung mit angemessenem Aufwand erlangt werden soll. Was Angemessenheit im jeweiligen Kontext bedeutet, bedarf eines gesellschaftlichen Diskurses.

6 | Vertraulichkeit: Aufrechterhaltung autorisierter Zugangs- und Offenlegungsbeschränkungen von Informationen einschließlich entsprechender Mittel zum Schutz der Privatsphäre sowie geschützter Informationen. Integrität: Schutz vor unsachgemäßer Änderung oder Zerstörung von Informationen einschließlich der Gewährleistung der Unleugbarkeit und Authentizität von Informationen. Verfügbarkeit: Gewährleistung eines rechtzeitigen und zuverlässigen Zugangs zu Informationen sowie deren Nutzung. Weitere Schutzziele der Informationssicherheit sind beispielsweise Datensicherheit, Authentizität, Nichtabstreitbarkeit, Verbindlichkeit und Zuverlässigkeit.

2 Ausgangslage

Trotz der Anstrengungen, die Cybersicherheit zu erhöhen, nahmen Cyberangriffe in den letzten Jahren deutlich zu. 2021 haben bei einer Befragung durch den Branchenverband Bitkom[7] 86 Prozent der befragten deutschen Unternehmen angegeben, dass Cyberangriffe Schäden versucht haben. 2019 waren es noch 70 Prozent. Die Schadenssumme hat sich innerhalb dieser zwei Jahre verdoppelt. Einem Bericht des BKA[8] zufolge gab es 2021 in Deutschland fast 150.000 Cybercrime-Delikte – ein Zuwachs von über 12 Prozent im Vergleich zum Vorjahr. Der dadurch entstandene Schaden beläuft sich auf etwa 223,5 Milliarden Euro. Auch international sind Cyberangriffe ein wachsendes Problem. Der Schaden, der weltweit durch Cyberkriminalität entsteht, wird für 2021 auf etwa sechs Billionen US-Dollar geschätzt und übertrifft damit den Umsatz etwa des weltweiten Drogenhandels.

Cyberangreifer lassen sich grob vier – auch hinsichtlich der Motivation – unterschiedlichen Kategorien zuordnen: Cyberkriminelle, staatlich geförderte Akteure, „Access-as-a-Service"-Unternehmen (AaaS) und Hacktivisten. Während die Motivation von Cyberkriminellen meist finanzieller Natur ist, liegen den Angriffen staatlich geförderter Akteure üblicherweise die Interessen der Staaten zugrunde, für die sie agieren. Mögliche Ziele sind beispielsweise die Beschaffung von Informationen durch Spionage, die Vorbereitung und Durchführung von Sabotageaktionen, die Manipulation von Wahlergebnissen beziehungsweise der öffentlichen Meinung und Wahrnehmung. Legale AaaS-Unternehmen bieten in einem nur teilweise regulierten Markt offensive Cyberdienstleistungen an und agieren im Sinne ihrer Auftraggeber.[9] Hacktivisten, die Cyberangriffe aus ideologisch-politischen Motiven durchführen, spielen mittlerweile nur noch eine untergeordnete Rolle.[10] Als problematisch erweist sich bei dieser Einteilung die Attribution, also die Zuordnung einer

Abbildung 1: ENISA-Bedrohungslage 2021 – Primäre Bedrohungen (Quelle: ENISA 2021)

7 | Vgl. Bitkom 2021.
8 | Vgl. BKA 2022.
9 | Vgl. Atlantic Council 2021a.
10 | Vgl. Security Intelligence 2019.

Angriffsaktion zu einem dedizierten Angreifer. Denn die Grenzen zwischen den einzelnen Akteuren können nicht trennscharf gezogen werden und Motive können sich überlagern. Es ist evident, dass Cyberkriminelle beispielsweise regelmäßig mit staatlich geförderten Akteuren zusammenarbeiten und staatlich geförderte Gruppierungen teilweise auch aus finanziellen Motiven handeln.[11,12] Zudem ist oft nicht klar, ob die Angriffe der persönlichen Bereicherung, der Devisenbeschaffung oder der Verschleierung anderer Motive dienen.[13] Darüber hinaus besteht die Möglichkeit, dass Angreifer die bestehenden Infrastrukturen anderer Gruppierungen nutzen, um ihre Spuren zu verschleiern. AaaS-Unternehmen erschweren die Attribution zusätzlich, da ihre Auftraggeber üblicherweise nicht identifiziert werden können.[14]

Mögliche Ziele von Cyberattacken stellen Privatpersonen, staatliche und öffentliche Organe sowie Einrichtungen und Unternehmen dar. In diesem Zusammenhang sind insbesondere Unternehmen hervorzuheben, die der kritischen Infrastruktur angehören (KRITIS)[15]. Angriffe auf sie können besonders schwerwiegende Konsequenzen haben. Wenn zum Beispiel Krankenhäuser angegriffen werden, geraten Menschenleben direkt in Gefahr.[16] Aber auch eine mangelnde Versorgung mit wichtigen Gütern hat gravierende Folgen, wie der Angriff auf den Pipeline-Betreiber „Colonial Pipeline" zeigte. Infolge des Angriffs wurde Benzin in Teilen der USA knapp, was zu Panikkäufen und deutlichen Preissteigerungen führte.[17] In Bezug auf den Angriff fällt die Attribution schwer, da offenkundig zwar monetäre Interessen verfolgt wurden, zugleich aber die Vermutung bestand, dass es sich bei dem Angriff in Wahrheit um eine staatlich geförderte Verschleierungsaktion handelte.[18]

Cyberkriminelle professionalisieren sich zunehmend, was sich daran zeigt, dass sich ihr Fokus immer mehr auf Ziele verschiebt, die hohe Einnahmen versprechen.[19] Ihre Angriffe richten sich daher aktuell weniger gegen Privatpersonen oder kleine und mittlere Unternehmen (KMU), sondern zunehmend gegen größere Unternehmen und staatliche Organe.[20,21] Beispielsweise wurde die Verwaltung des Landkreises Anhalt-Bitterfeld angegriffen und lahmgelegt. Die Dateien auf der IT-Infrastruktur des Landkreises wurden gestohlen und verschlüsselt, um Geld zu erpressen. Infolge des Angriffs konnten unter anderem keine Sozialleistungen mehr ausgezahlt werden. Der Schaden für den Landkreis betrug etwa zwei Millionen Euro.[22]

Die Möglichkeiten, Cyberangriffe durchzuführen, sind mannigfaltig. Abbildung 1 gibt einen Überblick über die von der Agentur der Europäischen Union für Cybersicherheit (ENISA) identifizierten Hauptbedrohungen. Von den neun abgebildeten Kategorien sieht die ENISA in „Ransomware" aktuell die größte Bedrohung.[23]

Die Methoden, mit denen Cyberangriffe durchgeführt werden, sowie die Bedrohungsszenarien verändern sich im Laufe der Zeit. Um dauerhaft geschützt zu sein, ist es daher wichtig, dass Deutschland resilient wird. Die Infrastrukturen und die Architekturen der IT-Systeme müssen folglich so aufgesetzt werden, dass es in der Lage ist, auch neuartigen Cyberangriffen zu begegnen. Dafür müssen alle Entitäten einer Gesellschaft – Unternehmen, staatliche Organe, Privatpersonen sowie die Forschung – ihren Beitrag leisten. Die jüngsten geopolitischen Entwicklungen lassen deutlich erkennen, dass es im Cyberraum keine nationalen Grenzen gibt. Zu Beginn des Kriegs in der Ukraine erfolgte zum Beispiel ein Cyberangriff auf das Satellitennetzwerk KA-SAT, der zum Ausfall der Kommunikationsdienste des Landes führte. Als Kollateralschaden wurde auch die Fernwartung von Windkraftwerken in ganz Mitteleuropa gestört.[24] Deutschland muss sich daher beim Thema Cybersicherheit international aufstellen und die grenzüberschreitende Zusammenarbeit fördern. Dazu gehört insbesondere auch, sich stärker in den Prozess der internationalen Standardisierung einzubringen und die Entwicklung international geltender Standards voranzutreiben.

11 | Vgl. Intel471 2020.
12 | Vgl. Mandiant 2019.
13 | Vgl. Accenture 2020.
14 | Vgl. PwC 2020.
15 | Zur Übersicht der Sektoren, die zu KRITIS zählen, vgl. BBK.
16 | Vgl. Handelsblatt 2020.
17 | Vgl. Washington Post 2021.
18 | Vgl. Atlantic Council 2021b.
19 | Vgl. CrowdStrike 2021a.
20 | Vgl. Flashpoint 2021.
21 | Vgl. Europol 2019.
22 | Vgl. Süddeutsche Zeitung 2022.
23 | Vgl. ENISA 2021.
24 | Vgl. Tagesspiegel Background Cybersecurity 2022.

3 Herausforderungen

3.1 Mangelnde Umsetzung bekannter Konzepte

Cyberkriminelle beschränken sich oft darauf, einfache Ziele anzugreifen. Unsicher konfigurierte IT-Systeme (Hardware und Software), Systeme mit schwachen Kontrollen oder Systeme mit nicht behobenen Sicherheitsschwachstellen werden daher häufig das Opfer eines erfolgreichen Cyberangriffs. Daher ist es wichtig, dass vergleichsweise einfache Maßnahmen der „Cyberhygiene" konsequent angewandt werden, wozu beispielsweise zählt, die Software auf dem aktuellen Stand zu halten. Für alle Sicherheitsmaßnahmen ist es essenziell, diese als Prozess zu verstehen und zu verankern. Da Cybersicherheit nicht statisch ist, müssen alle Sicherheitsmaßnahmen kontinuierlich überprüft und umgesetzt werden.

Langfristig muss Cybersicherheit schon beim Design von Systemen konsequenter mitgedacht werden. Konzepte wie „Security by Design" existieren bereits, werden aber bislang selten implementiert. Ein neues Konzept für das sichere Design von Systemen mit vielen Teilnehmern ist die sogenannte „Zero-Trust-Architektur" (siehe Infobox, sowie Abbildung 2). Gerade kleineren und mittleren Unternehmen sowie Kommunen fehlen jedoch oft die Ressourcen und das Wissen, um dieses Konzept selbstständig umzusetzen. Aber auch Behörden auf Bundesebene sowie viele größere Unternehmen implementieren die „Zero-Trust-Architektur" selten, sodass das Konzept hierzulande bislang kaum Anwendung findet.

Um nicht ins Visier von Cyberkriminellen zu geraten, ist es in der Regel ausreichend, wenn der Aufwand den potenziellen Nutzen eines Angriffs übersteigt. Unabhängig von den ergriffenen Maßnahmen ist es jedoch unmöglich, sich vollständig gegen Cyberangriffe abzusichern. Ziel sollte es daher sein, Kostenaufwand und Schutzniveau gegenüber dem Schadenspotenzial abzuwägen und das Maßnahmenpaket dementsprechend auszugestalten. Zudem sollten zusätzlich Maßnahmen zur Erhöhung der Resilienz ergriffen werden. Neben angemessenen Schutzmaßnahmen werden daher auch Pläne und Kompetenzen zum „Incident Response" benötigt, um Angriffen standhalten sowie nach einem Angriff effizient wieder zu einem Normalbetrieb zurückkehren zu können. Solche Notfallpläne sind insbesondere für Institutionen und Unternehmen relevant, die zur kritischen Infrastruktur (KRITIS) zählen, da ein Ausfall hier enormes gesamtgesellschaftliches Schadenspotenzial birgt. Die Pläne sollten aber nicht auf KRITIS beschränkt sein, da viele Institutionen und Unternehmen, die aktuell unter der KRITIS-Schwelle liegen, für Teilsysteme essenziell sind und vor allem bei längeren Ausfallzeiten signifikanter Schaden entstehen würde.

„Zero-Trust-Architektur"

„Zero-Trust" beschreibt ein Konzept für den Aufbau einer Cybersicherheitsstrategie, die sich deutlich von der bis dato gängigen Herangehensweise unterscheidet. Bislang war es üblich, einen Unternehmenskontext zu definieren, innerhalb dessen implizit allen Teilnehmenden vertraut wird („Trusted Network"), und diesen Kontext, diese Domäne nach außen zu schützen.

„Zero Trust" gibt die Idee eines per se vertrauenswürdigen Bereichs auf und verfolgt stattdessen einen datenzentrierten Ansatz. Anstatt jeder Nutzerin und jedem Nutzer zu vertrauen, die/der in der Domäne agiert (zum Beispiel, weil der Zugriff über ein Endgerät einer/eines Mitarbeitenden erfolgt), müssen sich alle Nutzerinnen und Nutzer, die auf Unternehmensdaten zugreifen wollen, authentifizieren („Never trust, always verify"). In einem zweiten Schritt wird die Sicherheit des verwendeten Endgeräts validiert. Die Anforderungen an die Authentifikation und Validierung können dabei dynamisch und abhängig von der Sensibilität der Daten, auf die zugegriffen werden soll, gestaltet werden. Zudem gilt hierbei das Prinzip „Least-privileged access", das jeder Nutzerin beziehungsweise jedem Nutzer nur so viele Rechte und Zugriffsmöglichkeiten einräumt, wie für die jeweilige Tätigkeit notwendig sind. Dabei ist das Vertrauen in die Instrumente und Systeme, die diesen Prozess ermöglichen, eine entscheidende Voraussetzung für den Erfolg der „Zero-Trust-Architektur".[25] Für eine grafische Darstellung der „Zero-Trust-Architektur" siehe Abbildung 2.

3.2 Forschungsbedarfe und Forschungsförderung

Zwischen Cyberangreifern und -verteidigern findet ein permanenter, dynamischer Wettkampf statt. Aufgabe der Forschung ist

25 | Vgl. CrowdStrike 2021b.

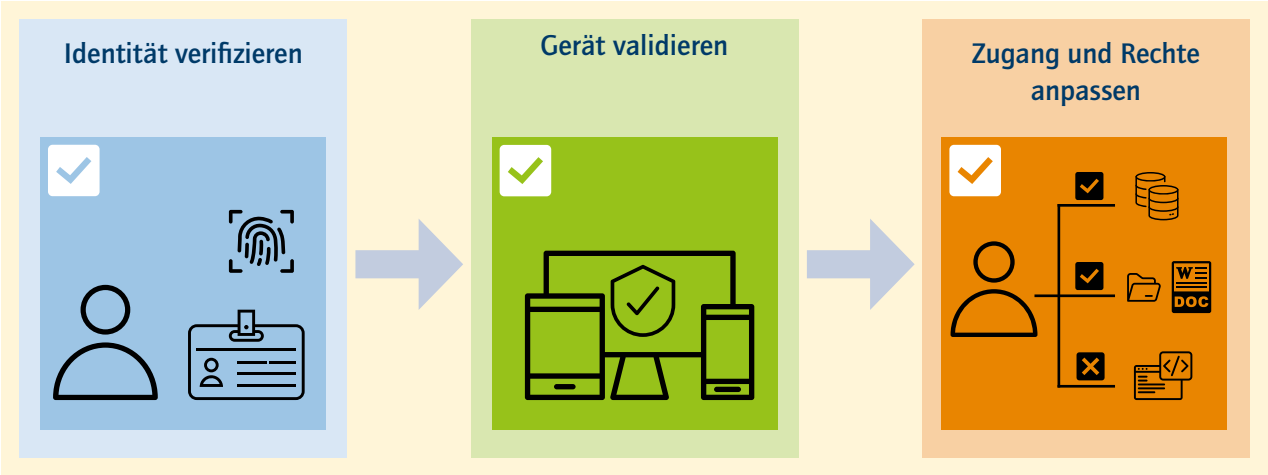


Abbildung 2: Zero-Trust-Architektur (Quelle: eigene Darstellung unter Verwendung von Icons von Noun)

es, Methoden weiterzuentwickeln, um den Schutzbedarf zu beurteilen, aber auch neue Architekturen, Sicherheitslösungen sowie Werkzeuge und Methoden zu entwickeln, um Bestandsysteme systematisch resilienter gegen Angriffe auszugestalten. Gleichzeitig müssen Wege gesucht werden, wie komplexe Verfahren vereinfacht werden können, sodass möglichst viele Nutzerinnen und Nutzer profitieren und diese auch vertrauensvoll nutzen. Wenngleich Deutschland in vielen Forschungsfeldern im Bereich Cybersicherheit führend ist, muss die Forschung weiterhin konsequent gefördert werden, um diese Spitzenposition halten zu können.

Zentrale Forschungsfelder in diesem Bereich sind aktuell etwa Verschlüsselungsmethoden und Methoden zur Quantifizierung von Risiken, Verfahren zur automatisierten und kontinuierlichen Beurteilung der Resilienz von Systemen gegen Angriffe, Konzepte zur Umsetzung des Zero-Trust-Prinzips und dessen automatisierte Überprüfung und Aktualisierung, aber auch neue Methoden und Werkzeuge zur Bewertung der Vertrauenswürdigkeit von KI-Verfahren und Machine-Learning-Algorithmen. Der Einsatz von Quantencomputern könnte dazu führen, dass bestehende Verschlüsselungsmethoden unsicher werden. Das macht eine Umstellung auf neue Methoden notwendig und erfordert neue Verfahren wie zum Beispiel Post-Quanten-Kryptografie und deren nahtlose Integration in existierende Systemlandschaften. Weitere wichtige Forschungsfelder sind unter anderem die Weiterentwicklung von Methoden zum Entwurf, aber insbesondere auch zum sicheren Betrieb von Systemen über deren gesamte Lebenszeit. Außerdem entscheidend ist die Weiterentwicklung von praktisch anwendbaren Testverfahren, mit denen eine automatisierte Prüfung und Verifikation komplexer Software- und Hardwareartefakte – unter anderem auf Korrektheit sowie Abwesenheit von bekannten Schwachstellen – durchgeführt werden kann. Die Forschungslandschaft in Deutschland ist in diesen Bereichen gut aufgestellt, es mangelt jedoch an einem effizienten Transfer der Forschungsergebnisse in die praktische Anwendung.

Eine zentrale Hürde für die angewandte IT-Sicherheitsforschung ist die weiterhin unsichere Rechtslage. Um Systeme auf Schwachstellen zu prüfen, bedienen sich IT-Sicherheitsforschende der gleichen Methoden, wie sie üblicherweise bei Cyberangriffen verwendet werden. Da das aktuelle IT-Strafrecht nicht nach der Intention des Angreifers unterscheidet, besteht für Forschende daher die Gefahr, sich strafbar zu machen. Dieser Umstand befördert eine Situation, in der eher Cyberkriminelle als Forschende Schwachstellen aufdecken, sodass Schwachstellen oft ausgenutzt, anstatt geschlossen zu werden. Hier ist die Politik gefragt, einen eindeutigen Handlungsrahmen für die Forschung zu schaffen und betreffende gesetzliche Regelungen so anzupassen, dass Forschung zur IT-Sicherheit hierzulande ohne die Gefahr rechtlicher Konsequenzen möglich ist.

Ein weiteres Hemmnis für die Forschung ist die mangelnde Datenverfügbarkeit. Zum einen werden nicht alle Angriffe registriert, da die Verantwortlichen in der Regel versuchen, ihre Spuren zu verwischen. Zum anderen werden Angriffe häufig nicht gemeldet oder Sicherheitsforschenden zugänglich gemacht, etwa aus Angst vor einem Imageschaden für das betroffene Unternehmen oder aus Datenschutzgründen. Daher müssen Möglichkeiten und Verfahren entwickelt werden, wie die relevanten Daten von

geeigneten Personen oder Instanzen zu Analysezwecken unter Wahrung der Datenschutzrichtlinien untersucht werden können.

3.3 Digitalkompetenzen der Gesellschaft

Um das gesamtgesellschaftliche Cybersicherheitsniveau zu heben, muss das Thema Cybersicherheit fest in der breiten Gesellschaft verankert sein. Grundlage dafür sind Verhaltensanpassungen, die nur erreicht werden können, wenn einfache Migrationswege, adäquate Alternativangebote sowie unkomplizierte und bequeme Cybersicherheitslösungen vorhanden sind. Entscheidend ist, dass die Technologien für die Anwenderinnen und Anwender – insbesondere aus dem privaten Bereich – verständlich und leicht zu nutzen sind. Benutzerfreundlichkeit muss hier im Fokus stehen, denn Sicherheitsmaßnahmen, die zu komplex sind, werden selten genutzt, was dazu führt, dass Systeme häufig unsicher und angreifbar bleiben. Sicherheit sollte daher idealerweise implizit – also ohne weiteres Zutun – in Produkten und Dienstleistungen für Privatanwenderinnen und -anwender implementiert sein. Hier sind Unternehmen und Forschung gefragt, unterstützt durch staatliche Förderung und Anreizsetzung, Lösungen zu entwickeln, die diesen Anforderungen gerecht werden.

Die zentrale Aufgabe der Bürgerinnen und Bürger ist es, ihre eigenen Endgeräte und privaten Infrastrukturen, beispielsweise im Rahmen von Smart-Home-Szenarien, zu sichern. Da sie auf die Sicherheit der installierten Anwendungen, die Sicherheit der Cloud-Plattformen, die in der Regel eingebunden werden, aber auch auf die Sicherheit der Apps und Webdienste keinen direkten Einfluss nehmen können, ist hier der Staat gefragt, die entsprechenden Rahmenbedingungen zu definieren. Dazu zählt etwa eine sichere Internetinfrastruktur, die möglichst viele Cyberbedrohungen abwehrt. Darüber hinaus ist eine einfach zu benutzende und zuverlässige Methode wichtig, um Identitäten im digitalen Raum sicherzustellen. Ein weiterer Aspekt, der von Privatpersonen kaum geleistet werden kann, ist das Abwägen von Sicherheit und Risiko einzelner Komponenten und verschiedener Technologien. Endverbraucherinnen und Endverbraucher müssen auf einfache und transparente Weise Informationen über die Sicherheit von Geräten und die Dauer von Unterstützung durch Softwareupdates erlangen können. Hier können Sicherheitsbeurteilungen einzelner Soft- und Hardwareprodukte sowie digitaler Dienstleistungen (wie etwa Software-as-a-Service), beispielsweise durch offizielle Zertifizierungen oder durch freiwillige beziehungsweise verpflichtende Herstellerangaben, unterstützen. Um die gewünschte Wirkung zu entfalten, müssen offizielle Zertifizierungen allerdings durch eine geeignete und adäquat ausgestattete, unabhängige Institution ausgestellt werden. Herstellerangaben müssen ebenfalls durch eine unabhängige Institution zumindest stichprobenartig verifiziert werden – wobei politische Richtlinien sicherstellen sollten, dass ein Betrug bei den Herstellerangaben unattraktiv ist. Auf diese Weise können Aspekte der Cybersicherheit einen größeren Einfluss auf die Kaufentscheidung von Soft- und Hardwareprodukten sowie digitalen Dienstleistungen entfalten und zum Differenzierungsmerkmal gegenüber konkurrierenden Anbietern werden. So bekommt Sicherheit auch für die herstellenden Firmen einen finanziellen Wert. Durch die Zertifizierung und Kennzeichnung von Technologien mit dem IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurde bereits ein Schritt in diese Richtung unternommen, allerdings beschränkt sich das Kennzeichen bislang auf einige wenige Produktgruppen.[26]

Um Verhaltensänderungen herbeizuführen, muss neben einfacher Anwendbarkeit das entsprechende Wissen in der gesamten Gesellschaft vorhanden sein. Auch wenn das Bewusstsein für das Thema Cybersicherheit zuletzt deutlich zugenommen hat, fehlt es häufig noch an profunden IT-Kompetenzen. Es ist von entscheidender Bedeutung, die Bevölkerung zu mehr Cybersicherheit zu befähigen, etwa durch die Stärkung von Bildungsangeboten. Diese sollten möglichst alle gesellschaftlichen Schichten erreichen – beginnend mit Schülerinnen und Schülern über Studierende bis hin zu Berufstätigen aller Qualifikationsstufen. Das Ziel sollte sein, dass ein sicherer Umgang mit Digitaltechnologien und deren Risiken ebenso selbstverständlich wird wie der Umgang mit Gefahren im Straßenverkehr. Ein wichtiger Eckpfeiler hierfür ist die konsequente Umsetzung der „Cyberhygiene", deren Maßnahmen allen Bürgerinnen und Bürgern vertraut sein sollten. Mehr Digitalkompetenz hilft den Menschen zudem dabei, die zunehmenden, demokratiefeindlichen Desinformationskampagnen zu erkennen und diese adäquat bewerten zu können. Darüber hinaus müssen die Bildungsangebote auch darauf ausgerichtet sein, mehr Fachkräfte im Bereich Cybersicherheit auszubilden.

3.4 Herausforderungen für die Politik

Die Politik spielt eine entscheidende Rolle beim Ziel, die Cybersicherheit in Deutschland zu erhöhen. In den Zuständigkeitsbereich der Politik fällt es, die entsprechenden gesetzlichen Rahmenbedingungen zu schaffen, aber auch Bildungsangebote

26 | Vgl. BSI.

bereitzustellen. Die Cybersicherheitsstrategie in dritter Fassung[27] sowie die in Vorbereitung auf die vierte Fassung der Strategie vorgelegte Cybersicherheitsagenda[28] zeigen, dass sich die Politik intensiv mit dem Thema Cybersicherheit in Deutschland auseinandersetzt. Dennoch gibt es aktuell viele Aspekte von Cybersicherheit, die noch unzureichend berücksichtigt oder umgesetzt wurden. Beispielsweise besitzt Deutschland eine weit entwickelte Behördenarchitektur, die Zuständigkeiten beim Thema Cybersicherheit haben[29]. Das ist zwar grundsätzlich als positiv zu bewerten, allerdings muss diese Struktur grundlegend konsolidiert werden, um Zuständigkeiten klarerer zu verteilen und die Kommunikation zwischen den einzelnen Behörden zu verbessern. Trotz der zahlreichen Einrichtungen auf Bundes- und Länderebene gibt es aktuell beispielsweise keine Regelungen, wie eine aktive Cyberabwehr umgesetzt werden kann. Solche Regelungen sind nicht zu verwechseln mit Gegenschlägen nach einer Cyberattacke, den sogenannten Hackbacks. Da staatliche Einrichtungen auch Anwender von Technologien sind, sollten sie anstreben, eine Voreiterrolle bei der Erhöhung von Cybersicherheit einzunehmen und innovative Ansätze sowie Technologien einzusetzen, um für andere Anwender als gutes Beispiel zu fungieren. Zu diesem Zweck sollte der Staat sichere Open-Source-Lösungen für die Verwaltung fördern und Wege finden, wie diese institutionell – beispielsweise durch Foundations – betrieben werden können. Diese Lösungen können dann wiederum für Anwender aus Wirtschaft und Gesellschaft als kostengünstige und sichere Alternativen zur Verfügung gestellt werden. Andere Staaten sind hier deutlich weiter.

Die Strategie Singapurs beispielsweise basiert darauf, dass der Staat seine hoheitlichen Aufgaben konsequent vorantreibt und gleichzeitig die Gesellschaft einbindet, indem für Bürgerinnen und Bürger Möglichkeiten aufgezeigt werden, wie jede und jeder Einzelne einen Mehrwert für die Cybersicherheit Singapurs schaffen kann.[30] Die USA haben sehr konkrete und ambitionierte Maßnahmen festgelegt, wie Cybersicherheit von allen staatlichen Stellen umgesetzt werden soll und diese auch mit eindeutigen Verantwortlichkeiten, Prozessen und Deadlines hinterlegt. Beispielsweise müssen alle US-Bundesbehörden bis 2024 eine „Zero-Trust-Architektur" implementieren.[31]

Auch für Deutschland ist ein derartiges Vorgehen sinnvoll, da sich auf diese Weise das allgemeine Sicherheitsniveau deutlich anheben ließe. Wichtig dabei ist, dass die vorgeschriebenen Architekturen und Maßnahmen möglichst konkret und ambitioniert, dem aktuellen Stand der Technik nach aber auch umsetzbar sind. Regelmäßige Überprüfungen und Anpassungen dieser Vorgaben sollten daher fest eingeplant werden. Neben staatlichen Organen sollten diese Vorgaben auch für die zumeist privaten Betreiber kritischer Infrastrukturen gelten. Hierbei ist auch eine Unterstützung der Unternehmen bei der Umsetzung der Richtlinien denkbar, da ein hohes Sicherheitsniveau bei der kritischen Infrastruktur ein originäres Ziel staatlichen Handelns sein sollte. Perspektivisch können auch öffentliche Einrichtungen auf kommunaler Ebene einbezogen werden. Für eine konsequente Umsetzung wäre es notwendig, dass im Zuge öffentlicher Ausschreibungen nur noch Anbieter berücksichtigt werden, die diese Vorgaben erfüllen können. Dadurch würde das Angebot an entsprechenden Produkten und Dienstleistungen steigen, was wiederum zu sinkenden Kosten führt. Dies eröffnet zunehmend mehr Nutzerinnen und Nutzern einen kostengünstigeren Zugang zu Produkten und Dienstleistungen mit diesen höheren Sicherheitsstandards. Die Cybersicherheitsagenda fordert zwar einen Ausschluss nicht vertrauenswürdiger Hersteller beim Infrastrukturausbau, doch ist dieser nur möglich, wenn entsprechende alternative Angebote vorhanden sind.

3.5 Herausforderung Digitale Souveränität

Digitale Souveränität (siehe Infobox) darf nicht mit Autarkie gleichgesetzt werden. Im Sinne der Digitalen Souveränität muss die Maßgabe sein, über mindestens eine gute Alternative zu verfügen, sodass man den Instrumenten und Systemen, die der Sicherstellung von Cybersicherheit dienen und die diesen Prozess ermöglichen, vertrauen kann. Dies erfordert, dass das eigene Innovationsökosystem zusammen mit Partnern gestärkt und internationale Standards und Normen den europäischen Vorstellungen entsprechend mitgestaltet werden. Zur Digitalen Souveränität gehört auch das bewusste Eingehen sowie die Diversifizierung von Abhängigkeitsverhältnissen bei denjenigen Themen, bei denen ein eigenes europäisches Innovationsökosystem (noch) nicht möglich ist.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt im Zusammenhang mit dem Ukrainekonflikt die aus

27 | Vgl. BMI 2021.
28 | Vgl. BMI 2022.
29 | Vgl. Stiftung Neue Verantwortung 2022.
30 | Vgl. Cyber Security Agency of Singapore 2021.
31 | Vgl. The White House 2021.

Russland stammende Antivirensoftware der Firma Kaspersky als nicht vertrauenswürdig ein.[32] Dies unterstreicht, wie wichtig es ist, dass verschiedene alternative Angebote vorhanden sind. Denn es kann nicht angenommen werden, dass die politische Stabilität von Partnerländern dauerhaft und allzeit gegeben ist. Da im oben genannten Marktsegment für Antivirensoftware genügend Alternativen verfügbar sind, blieb die Einschätzung des BSI ohne weitreichende Konsequenzen. In anderen Bereichen aber, insbesondere in dem der IT-Dienstleistungen, Software und Chipproduktion, sind kaum Alternativen vorhanden, weshalb die Schaffung alternativer Angebote eine zentrale Zielsetzung darstellen sollte. Wenn die Abwägung aller Faktoren ergibt, dass das Sicherheitsniveau nicht ausreicht und eine sicherere Alternative gewählt werden sollte, müssen zuerst Alternativen auf allen Ebenen (siehe Abbildung 3) verfügbar sein. Zumindest das zugrunde liegende Know-how muss vorhanden sein. Der Fokus hierbei sollte auf zentralen Schlüsseltechnologien beziehungsweise grundlegenden Basiskomponenten[33] liegen. Denn dadurch eröffnet sich die Möglichkeit, zum Beispiel Hardware nach eigenen, konkreten Vorgaben herstellen zu lassen, um so den Grad an Sicherheit zu erhöhen, etwa indem dem Einbau von Hardware-Backdoors vorgebeugt wird. Darüber hinaus kann dadurch die Beurteilungsfähigkeit – also das Verständnis über die Systemwirkungen einzelner Bausteine – erweitert werden. Denn zunehmend größere und komplexere Systeme sowie die sich daraus ergebenden, kaskadierenden Effekte erschweren die Sicherheitseinschätzung der betrachteten Systeme. Dazu kommt, dass vor allem Software häufig nicht von einem einzelnen Hersteller entwickelt wird, sondern – analog zu physischen Produkten – ganze Lieferketten beziehungsweise -netzwerke an der Entstehung beteiligt sind. Die Sicherheitseinschätzung bezieht sich also immer auch implizit auf die enthaltenen Vorprodukte. Bei der Entwicklung stehen allerdings Sicherheitsaspekte oftmals nicht im Vordergrund. Proprietäre Software ist überdies häufig intransparent, was die Beurteilung zusätzlich erschwert. Außerdem fehlen Steuerungsmöglichkeiten, um einer möglichen Manipulation der Software vorzubeugen. Aber auch Open-Source-Software mit einsehbarem Quellcode ist nicht automatisch sicher. Denn aufgrund der hohen Komplexität des Quellcodes aktueller Softwareprodukte kann eine fundierte Sicherheitseinschätzung selbst von Expertinnen und Experten nicht mehr manuell, sondern nur noch durch umfassende Analysen mithilfe entsprechender Werkzeuge vorgenommen werden. Problematisch in diesem Zusammenhang ist außerdem, dass die Open-Source-Lösungen aktuell oft von Einzelpersonen oder kleinen Gruppen entwickelt werden. Um die Souveränität voranzutreiben, sollten hier (internationale) institutionelle Organisationsformen aufgebaut werden, um mehr Transparenz, Vertrauenswürdigkeit und Unabhängigkeit zu gewährleisten.

Definition Digitale Souveränität

Digitale Souveränität bedeutet, dass Personen, Unternehmen und Politik in der Lage sind, unabhängig zu entscheiden, auf welche Weise und mit welcher Zielsetzung der digitale Wandel gestaltet werden soll. Es geht hierbei sowohl um Wettbewerbsfähigkeit als auch um politische Selbstbestimmtheit. Digitale Souveränität europäischer Prägung will allen Entitäten die Wahlfreiheit bei der Digitalisierung ermöglichen, sie muss europäischen Rechts- und Wertevorstellungen folgen, weltoffen sein und fairen Wettbewerb fördern. Um die Komplexität der Digitalen Souveränität abzubilden, hat acatech ein Schichtenmodell mit acht aufeinander aufbauenden Ebenen entwickelt.[34]

In Ermangelung alternativer Angebote ist es für viele Anwenderinnen und Anwender am einfachsten und kostengünstigsten, auf die Services von Hyperscalern wie Microsoft, Amazon oder Google zurückzugreifen. Deren Angebote sind grundsätzlich gut gegenüber Cyberangriffen abgesichert und in der Anwendung einfach. Problematisch kann hier jedoch die Einhaltung des Schutzziels Vertraulichkeit sein, da es keine Möglichkeiten gibt zu kontrollieren, wie sicher die eigenen Daten bei einem Hosting-Anbieter sind. Die Kundinnen und Kunden sind darauf angewiesen, dem Anbieter zu vertrauen. Dies birgt insbesondere deshalb Risiken, da aktuell alle Hyperscaler im außereuropäischen Ausland angesiedelt sind und somit auch der jeweiligen Gesetzgebung dort unterliegen. Der PATRIOT Act und der CLOUD Act beispielsweise räumen den US-Behörden weitreichende Befugnisse für den Zugriff auf Daten ein, die von Cloudanbietern gehostet werden.

32 | Vgl. BSI 2022.

33 | Als Basiskomponenten sind in diesem Zusammenhang alle grundlegenden Elemente gemeint, die für das Funktionieren von IT-Systemen und cyberphysischen Systemen benötigt werden, wie beispielsweise Chip- und Halbleitertechnik sowie Fertigungsverfahren, Betriebssysteme und Firmware für Internet-of-Things(IoT)-Geräte sowie die dazugehörige Managementsoftware.

34 | Vgl. acatech 2021.

Es gibt verschiedene Ansätze, wie europäische Alternativen aufgebaut werden können. Entscheidend ist, damit die Grundlagen für ein florierendes und innovatives Ökosystem zu schaffen. In zentralen, bereits besetzten Technologiefeldern sollte zumindest so viel Know-how aufgebaut werden, dass eine ausreichende Beurteilungsfähigkeit gegeben ist. Noch wichtiger ist es aber, hinreichend Innovationskraft zu entwickeln, um zukünftige Trends frühzeitig erkennen und mitgestalten zu können. Das Ziel muss dabei immer sein, Produkte und Dienstleistungen zu entwickeln, die mit den führenden internationalen Angeboten konkurrenzfähig sind. Der Aufbau alternativer Angebote könnte etwa durch die Förderung von Innovationen, Start-ups oder Open-Source-Technologien erfolgen. Dies kann aber nur durch ein gemeinsames Vorgehen von Partnern aus Wirtschaft und Politik auf europäischer Ebene gelingen.

Eine weitere Möglichkeit der Einflussnahme stellen internationale Gremien dar, die Standards und Normen festlegen. Es ist kritisch zu bewerten, dass chinesische Unternehmen sich hier zuletzt verstärkt eingebracht haben, während das europäische Engagement stagnierte oder sogar zurückging. Ursächlich dürfte ein Mangel an Anreizen für Forschende sowie Unternehmen sein, sich in zeitintensiven und arbeitsaufwendigen Standardisierungs- und Normierungsprozessen zu engagieren. Doch selbst wenn es Europa gelingt, internationale Standards wieder stärker zu prägen, werden weiterhin Technologien aus Ländern zum Einsatz kommen müssen, die nicht den europäischen Werten entsprechen. Daher müssen Lösungen gefunden werden, wie der Einsatz solcher Technologien gelingen kann, ohne einen kritischen Effekt auf die Systemsicherheit zu entfalten.

Abbildung 3: Ebenen der Digitalen Souveränität gemäß dem acatech Schichtenmodell (Quelle: eigene Darstellung)

4 Handlungsfelder

Eine stetige und konsequente Weiterentwicklung der Cybersicherheit ist notwendig, um Deutschland dauerhaft vor Angriffen aus dem virtuellen Raum zu schützen. Damit eng verknüpft ist das strategische Ziel, die Digitale Souveränität auszubauen. Beide Ziele bedingen einander: Ohne adäquate Cybersicherheit kann Digitale Souveränität nicht gewährleistet werden und je mehr Digitale Souveränität besteht, desto höher ist das erreichbare Niveau an Cybersicherheit. Dass die Politik die Dringlichkeit des Themas erkannt hat, zeigt die im Juli 2022 vom Bundesministerium des Innern und für Heimat (BMI) veröffentlichte Cybersicherheitsagenda.[35] Sie kann als Weiterentwicklung der Cybersicherheitsstrategie aus dem Jahr 2021 verstanden werden und deutet bereits an, welchen Weg die für das Jahr 2023 geplante Novelle der Cybersicherheitsstrategie einschlagen wird. Viele Maßnahmen und Ansätze der Cybersicherheitsagenda gehen in die richtige Richtung, sind jedoch noch nicht ausreichend konkretisiert worden. Die neue Cybersicherheitsstrategie sollte sich an dem konkreten und ambitionierten Maßnahmenkatalog orientieren, der unlängst in den USA veröffentlicht wurde.[36] Kritisch zu bewerten ist der offensichtliche Interessenskonflikt in der Cybersicherheitsagenda zwischen einer Erhöhung der Cybersicherheit und den verbesserten Möglichkeiten der Strafverfolgung. So wird etwa von einem „Schwachstellenmanagement" gesprochen, was die Vermutung nahelegt, dass nicht alle bekannten Schwachstellen geschlossen werden sollen. Darüber hinaus wird beispielsweise von dem „Ausbau" und der „Modernisierung der Ermittlungsfähigkeiten und -instrumente" und einer stärkeren Kontrolle von Inhalten in sozialen Medien gesprochen. Auch wenn diese Maßnahmen für sich genommen sinnvoll sind, dienen sie nicht der Erhöhung der Cybersicherheit und sollten daher nicht Gegenstand der Cybersicherheitsdebatte sein.

Im Nachfolgenden werden verschiedene Handlungsfelder zur Erhöhung der Cybersicherheit adressiert und an geeigneter Stelle mit der Cybersicherheitsagenda gespiegelt. Die Handlungsfelder stellen keinen konkreten Maßnahmenkatalog dar, sondern sollen dazu anregen, diese Felder tiefergreifend zu untersuchen und detaillierter auszuarbeiten.

Handlungsfelder für politische Entscheidungsträgerinnen und Entscheidungsträger

Es ist Aufgabe der Politik, gesetzliche Rahmenbedingungen zu schaffen, um die Cybersicherheit Deutschlands voranzutreiben. Gleichzeitig sind staatliche Organe wie etwa Ministerien auch Anwender von Technologien. Diese staatlichen Organe sollten anstreben, hier eine Vorreiterrolle mit dem Ziel einzunehmen, durch staatliche Nachfrage nach sichereren Technologien Angebote in diesem Bereich zu fördern, sodass der Markt dafür im Laufe der Zeit wächst und sichere Alternativen einfacher verfügbar werden.

- **Ambitionierte Cybersicherheitsstrategie:** Deutschland braucht eine umfassende und ambitionierte Cybersicherheitsstrategie. Diese darf nicht für sich alleinstehen, sondern muss in eine umfassende und kohärente Digitalisierungsstrategie eingebettet werden. Cybersicherheit ist kein Selbstzweck, sondern bildet die Basis für eine sichere und vertrauenswürdige Digitalisierung. Die Cybersicherheitsstrategie kann zwar nicht gezielt auf einzelne Bedarfe eingehen, sollte aber konkrete Leitlinien und auch Technologieanforderungen festschreiben, ohne sich auf einzelne Produkte festzulegen.
- **Zero Trust implementieren:** In der Cybersicherheitsagenda werden wichtige Grundsätze, wie etwa Sicherheit „by design" und „by default" in der Bundesverwaltung, genannt. Noch wichtiger ist jedoch eine konsequente und ambitionierte Umsetzung des Zero-Trust-Prinzips, wie dies auch durch die US-amerikanische Regierung vorangetrieben wird. In der für Anfang 2023 geplanten Cybersicherheitsstrategie muss daher ein konkreter, ambitionierter Zeit- und Maßnahmenplan für die Institutionen der öffentlichen Hand enthalten sein.
- **Sichere Infrastruktur:** Es ist die Aufgabe der Politik, den Aufbau einer funktionierenden und möglichst sicheren Infrastruktur voranzutreiben. Beispielsweise kann die Regierung zusammen mit den Internetdienstleistern die nationale Internetinfrastruktur besser absichern, indem das DNSSEC-Protokoll (Domain Name System Security Extension) in allen lokalen Internetdomänen implementiert wird. Dadurch können viele Angriffe bereits abgewehrt werden, bevor sie Endnutzerinnen und -nutzer überhaupt erreichen.
- **Konsolidierung der Behördenarchitektur:** Derzeit existieren allein auf Bundesebene 75 verschiedene Behörden, Gremien und Initiativen mit Zuständigkeiten im Bereich Cybersicherheit.[37] Der Ansatz aus der Cyberagenda, einzelne Ein-

35 | Vgl. BMI 2022.
36 | Vgl. The White House 2021.
37 | Vgl. Stiftung Neue Verantwortung 2022.

richtungen aufzuwerten, geht daher in die richtige Richtung. Um Zuständigkeiten klarer zu verteilen und die Abstimmung zwischen den einzelnen Einrichtungen zu verbessern, ist jedoch eine umfassende Konsolidierung dieser Strukturen unumgänglich. Dabei sollten einzelnen Behörden eine klare Mission und eindeutige Zuständigkeiten zugeordnet werden. Die befragten Expertinnen und Experten unterstützen insbesondere die Aufwertung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und empfehlen, es vom Bundesministerium des Innern und für Heimat (BMI) loszulösen, um Interessenskonflikten vorzubeugen.

- **Modernisierung und Standardisierung der behördlichen Infrastruktur:** Teil des oben genannten Zeit- und Maßnahmenplans sollte auch die Modernisierung der behördlichen Infrastruktur sein. In diesem Zusammenhang sollte eine Standardisierung der verwendeten Soft- und Hardwarelösungen angestrebt werden. Dies erleichtert unter anderem den Datenaustausch zwischen den verschiedenen staatlichen Organen. Darüber hinaus erhöht der Einsatz standardisierter Technologien die Sicherheit, da so Ressourcen für umfassendere Sicherheitsüberprüfungen gebündelt werden können. Vorschläge aus der Cybersicherheitsagenda, wie etwa die Einführung eines zentralen Videokonferenzsystems oder Investitionen in Quantencomputing und Post-Quanten-Kryptografie sowie die Weiterentwicklung des Informationssicherheitsmanagements des Bundes, unterstützen die befragten Expertinnen und Experten.
- **Leitlinienfunktion der behördlichen IT-Infrastruktur:** Es ist anzustreben, im Zuge der Modernisierung und Standardisierung der behördlichen Infrastruktur ein System aufzusetzen, das als Leitlinie für Anwenderinnen und Anwender außerhalb dienen kann. Damit Unternehmen sowie Privatpersonen sich hieran orientieren können, muss eine hohe Benutzerfreundlichkeit im Fokus stehen. Ein Beispiel dafür ist die Einführung eines einheitlichen, sicheren und einfach zu nutzenden Verfahrens zur Verifikation digitaler Identitäten bei gleichzeitiger Wahrung bestehender Datenschutzrichtlinien.
- **Zertifizierung kritischer Technologien:** Ebenfalls im Rahmen der Modernisierung und Standardisierung der behördlichen Infrastruktur sollten relevante Technologien (insbesondere kritische Komponenten) hinsichtlich ihrer Sicherheit, Integrität sowie der Möglichkeit politischer Einflussnahme umfassend geprüft und zertifiziert werden. Dies gilt auch für die Vorprodukte und Lieferketten. Technologien, die den strengen Anforderungen entsprechen, können in einer Permit List gesammelt werden, die regelmäßig aktualisiert und gegebenenfalls revidiert werden muss. Basierend darauf kann eine Freigabe und Empfehlung für alle Verwaltungseinrichtungen gegeben werden. Dieses Vorgehen trägt zur Erhöhung der allgemeinen Cybersicherheit bei, denn Unternehmen und Privatpersonen können sich ebenfalls an der Permit List orientieren, was wiederum einen Anreiz für Hersteller und Entwickler schafft, die Kriterien der Permit List zu erfüllen. Dieser Ansatz erweitert den Vorschlag aus der Cybersicherheitsagenda, die Prüfmöglichkeiten des BSI hinsichtlich der Vertrauenswürdigkeit von Herstellern auszubauen, denn hier beschränkt man sich auf die Betreiber kritischer Infrastrukturen.
- **Open Source für die Verwaltung:** Der Bund sollte die Entwicklung von sicheren, verifizierten Open-Source-Lösungen für staatliche Organe vorantreiben, weil hierdurch eine Nachfrage nach diesen Open-Source-Lösungen und somit deren Entwicklung gefördert wird. Da bei Open-Source-Technologien die Beitragenden üblicherweise nicht identifiziert sind, muss sichergestellt werden, dass kein versteckter Schadcode enthalten ist (siehe Handlungsfeld Digitale Souveränität). Nach entsprechend eingehenden Prüfungen können diese Lösungen ebenfalls in die Permit List übernommen werden. Sie stehen damit als kostengünstige Option für alle Bereiche des deutschen Verwaltungsapparats zur Verfügung. Die Vorarbeit auf Bundesebene erleichtert Ländern, Gemeinden und Kommunen die Umsetzung komplexer Cybersicherheitsverfahren, ohne die Kosten für sie in die Höhe zu treiben. Die Cybersicherheitsagenda nimmt keine Stellung zu diesem relevanten Thema, was in der Ausarbeitung der Cybersicherheitsstrategie nachgeholt werden muss.
- **Aktive Verteidigung:** Die aktive Verteidigung ist im Falle massiver Cyberangriffe von zentraler Bedeutung. Es ist wichtig, diesen Ansatz von Hackbacks zu unterscheiden. In der kommenden Cybersicherheitsstrategie sollte auf eine klare Kommunikation sowie einheitliche und klare Nomenklatur geachtet werden. Damit im Ernstfall schnell reagiert werden kann, müssen die noch immer zahlreichen bestehenden Hürden auf dem Weg zur Umsetzung einer aktiven Cyberabwehr zeitnah überwunden werden. Noch ungeklärt sind etwa Fragen rund um die Zuständigkeiten, wie eine angemessen kurze Reaktionszeit bei adäquater Kosten-Nutzen-Abwägung sichergestellt werden kann und wie mit etwaigen Kollateralschäden umgegangen werden soll.

Handlungsfelder Unternehmen

Unternehmen sind auf der einen Seite Anwender digitaler Technologien, auf der anderen Seite entwickeln sie aber auch (Vor-)Produkte und Dienstleistungen verschiedenster Art. Es ist es wichtig, dass Unternehmen die Bedeutung von Cybersicherheit verstehen und entsprechend handeln. Zahlreiche Unternehmen haben dies bereits erkannt und entsprechende Maßnahmen

umgesetzt. Unternehmen, die zur kritischen Infrastruktur zählen, nehmen aufgrund ihrer Bedeutung für das Funktionieren der Gesellschaft eine Sonderstellung ein. Dementsprechend muss der angestrebte Grad an Sicherheit hier (noch) höher sein.

- **Usability (Benutzerfreundlichkeit):** Bei allen digitalen (Vor-) Produkten und Dienstleistungen muss es das Ziel sein, benutzerfreundliche Cybersicherheit von Anfang an im Fokus zu haben und als Teil des Konzepts zu begreifen. Denn nur einfach anwendbare Cybersicherheitslösungen werden konsequent genutzt und nur, wenn Sicherheit von Anfang an mitgedacht wird, lassen sich komplexe Maßnahmen (wie etwa Security-by-Design) umfassend implementieren. Ein wachsendes Bewusstsein der Anwenderinnen und Anwender sowie staatliche Mindeststandards lassen hieraus auch einen wirtschaftlichen Wettbewerbsvorteil erwachsen.
- **Lieferkettensicherheit bei Softwareprodukten:** Softwarehersteller müssen sicherstellen, dass die in ihrer Software enthaltenen Vorprodukte sicher sind. Dazu zählt auch eine Analyse der politischen Rahmenbedingungen, unter denen ein Vorprodukt entwickelt wurde.
- **Resilienz steigern:** Die Covid-19-Pandemie hat gezeigt, wie anfällig unser komplexes Wirtschaftssystem ist. Daher ist es wichtig, einen stärkeren Fokus auf Resilienz[38] zu legen – insbesondere für Unternehmen, die zur kritischen Infrastruktur zählen. Im Kontext von Cybersicherheit heißt das konkret, dass nicht nur in Maßnahmen zur Erhöhung der Sicherheit investiert wird, sondern auch Pläne und Maßnahmen für den Fall eines erfolgreichen Angriffes vorbereitet werden sollten. Dazu zählen etwa Fähigkeiten, einen Notfallbetrieb aufrechtzuerhalten („Graceful Degradation") und schnell wiederherstellen zu können. Dort, wo es möglich und sinnvoll ist, sollten analoge Schutzmechanismen implementiert werden. So kann etwa ein mechanisches Überdruckventil das Explodieren einer Gaspipeline verhindern, auch wenn das gesamte IT-System des Anbieters von Hackern übernommen wurde.

Handlungsfelder Forschung

Die dynamische Entwicklung im Bereich Cybersicherheit führt zu einem Wettkampf zwischen Angreifern und Verteidigern, wobei die Verteidiger immer in Vorleistung gehen müssen. In diesem Wettkampf kommt der Forschung die zentrale Aufgabe zu, immer neue Methoden und Werkzeuge zu entwickeln, die zur Erhöhung der Sicherheit und der einfachen Nutzbarkeit sicherer Lösungen beitragen.

- **Forschungsförderung:** Die in der Cybersicherheitsagenda vorgeschlagene Förderung der Forschung ist ein zentraler Pfeiler sowohl zur Erhöhung der Cybersicherheit als auch der Digitalen Souveränität. Dafür ist es neben monetären Investments in Forschungsprojekte wichtig, die passenden Rahmenbedingungen aufzubauen. Gefördert werden sollte vor allem die Forschung in Schlüsseltechnologien, wie etwa Risikobewertung, Beurteilungsfähigkeiten, Kryptografie, Digitale Identitäten, Netzwerksicherheit, Threat-Intelligence, vertrauenswürdige Hardware, Quantifizierung und Engineering sicherer Software. Die Cybersicherheitsstrategie der Bundesregierung muss diese und weitere relevante Forschungsfelder konkret identifizieren und vorantreiben.
- **Transfer und Requirement Engineering:** Damit Forschungsergebnisse dazu beitragen können, die Cybersicherheit zu erhöhen, ist der Transfer in die Anwendung zentral. Daher sollten Migrationswege schon zu Beginn von Forschungsvorhaben mitgedacht werden. Angewandte Forschung sollte sich darüber hinaus an den Bedürfnissen der späteren Anwenderinnen und Anwender orientieren und sicherstellen, dass nicht am bestehenden Bedarf vorbeientwickelt wird.
- **(Automatisierte) Test- und Verifikationsverfahren:** Ein elementarer Baustein zur Erhöhung von Cybersicherheit ist die Weiterentwicklung von Methoden und praktisch anwendbarer Test- und Verifikationsverfahren zur automatisierten Prüfung komplexer Software- und Hardwareartefakte auf Korrektheit sowie Abwesenheit von bekannten Schwachstellen. Diese Verfahren unterstützen die Erstellung von Permit Lists mit geprüfter Hard- und Software und die Überprüfung der Sicherheit von Open-Source-Lösungen.
- **Datenverfügbarkeit:** Forschende müssen einen Zugang zu Daten strukturierter Cyberangriffe auf Unternehmen erhalten, um daraus Erkenntnisse ableiten zu können. Diese Daten liegen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zwar bereits vor, sie dürfen aktuell jedoch nicht genutzt werden, da hierfür eine Neuauslegung der Datenschutz-Grundverordnung (DSGVO) notwendig wäre. Eine Möglichkeit, um die vorhandenen Daten nutzen zu können, bietet die Schaffung eines sicheren Datenraums für verifizierte Forschende. Eine Verschwiegenheitsvereinbarung beispielsweise kann die Identität der betroffenen Unternehmen schützen. Die Cybersicherheitsstrategie muss hierfür eine passende Lösung finden.
- **Handlungsräume klar definieren:** Es ist wichtig, Rechtssicherheit für die Forschung zu schaffen. Beispielsweise müssen Forschende bei der Suche nach Schwachstellen vom Gesetzgeber geschützt werden. Aktuell können derartige Aktivitäten noch als Hacking klassifiziert und daher strafrechtlich

38 | Vgl. acatech 2022.

geahndet werden. Dieser Punkt wird in der Cybersicherheitsagenda leider nicht beachtet.

Handlungsfelder Gesellschaft

Um langfristige, nachhaltige Veränderungen zu erzielen, muss sich das gesellschaftliche Bewusstsein für Cybersicherheit nachhaltig wandeln. Ein Schlüssel hierzu stellt Bildung dar. Bildungsaufgaben werden in erster Linie von staatlicher Seite wahrgenommen, aber auch gesellschaftliche Einrichtungen können diese Aufgabe übernehmen. Genauso wichtig ist es aber, dass die Gesellschaft durch die Bereitstellung einfach zu nutzender Werkzeuge unterstützt wird. Die Cybersicherheitsagenda stellt allerdings die Bekämpfung strafbarer Inhalte und nicht die gesellschaftliche Befähigung in den Fokus, weshalb folgende Punkte in der nächsten Fassung der Cybersicherheitsstrategie Beachtung finden sollten:

- **Usability (Benutzerfreundlichkeit) und Interoperabilität:** Ein wichtiger Punkt, um private Nutzerinnen und Nutzer bei der Erhöhung ihrer Cybersicherheit zu unterstützen, ist das Vorhandensein einfach zu nutzender Sicherheitslösungen. Viele Methoden zur Erhöhung der Cybersicherheit sind für Privatanwenderinnen und -anwender aktuell noch zu komplex in der Umsetzung – hier sind Forschung und Unternehmen gefragt, einfachere Umsetzungsmöglichkeiten zu entwickeln. Idealerweise sollte Cybersicherheit implizit („by default") vorhanden sein und nicht erst nachträglich konfiguriert werden müssen. Messenger-Dienste beispielsweise bieten dies – im Unterschied zu E-Mails – zwar an, ihre Geschäftsmodelle basieren aber auf einem Lock-in der Nutzerinnen und Nutzer. Um hier Abhilfe zu schaffen, müssen der Staat beziehungsweise die Europäische Union Interoperabilität vorschreiben.
- **Digitalkompetenzen:** Neben Medienkompetenz brauchen digital kompetente Bürgerinnen und Bürger ein grundlegendes Verständnis für digitale Technologien, Prozesse und Abläufe. Um dieses Verständnis auf- und auszubauen, sollten die Lehrpläne für Schülerinnen und Schüler aller Altersstufen digitale Kompetenzen deutlich stärker in den Fokus nehmen. Darüber hinaus werden entsprechende, niederschwellige Weiterbildungsangebote für Berufstätige benötigt. Ziel muss sein, dass ein souveränes Handeln in der digitalen Welt selbstverständlich wird.
- **Gezielte Desinformation:** Gezielte Desinformationen stellen für demokratische Staaten ein großes Problem dar. Die Funktionsweisen der Algorithmen sozialer Medien tragen zur Bildung von Informationsblasen bei. Frei verfügbare Technologien zur Erstellung realitätsnaher Deep Fakes verschärfen das Problem zusätzlich. Um gezielten Desinformationskampagnen und Deep Fakes entgegenzuwirken, ist die Einführung eines einheitlichen, sicheren und einfach zu nutzenden Verfahrens zur Verifikation digitaler Identitäten wichtig. Dadurch können Bürgerinnen und Bürger leichter die Authentizität des Urhebers feststellen, gleichzeitig können Behörden die Urheberinnen und Urheber strafbarer Inhalte identifizieren und entsprechende Schritte einleiten. Darüber hinaus ist die digitale Kompetenz der Bürgerinnen und Bürger gefragt. Auf europäischer Ebene müssen Social-Media-Plattformen in die Pflicht genommen werden, Falschmeldungen zu löschen, ohne dabei zu zensieren.
- **Zertifizierungen:** Offizielle Zertifizierungen respektive freiwillige oder verpflichtende Herstellerlabels helfen Privatpersonen dabei, schneller und einfacher die Sicherheit von Produkten, Anwendungen oder Dienstleistungen einzuschätzen. So kann Sicherheit zu einem Wettbewerbsvorteil für Unternehmen werden und gleichzeitig das Vertrauen in Technologien gestärkt werden. Mit der Einführung des IT-Sicherheitskennzeichens hat das BSI diesbezüglich bereits erste Schritte unternommen, jedoch ist es aktuell auf zu wenige Produktgruppen beschränkt, um eine starke Wirkung zu entfalten.

Handlungsfelder Digitale Souveränität

Das Vorhandensein Digitaler Souveränität ist eine Grundvoraussetzung für Cybersicherheit. Gleichzeitig führt ein höheres Cybersicherheitsniveau auch zu mehr Digitaler Souveränität. Die nachfolgenden Maßnahmen helfen dabei, beide Zielsetzungen parallel voranzutreiben. Dies kann nur durch ein gemeinsames Vorgehen von Partnern aus Wirtschaft und Politik auf europäischer Ebene gelingen.

- **Alternative Angebote:** Das Angebot für Hard- und Softwarelösungen weist oftmals oligopolistische Marktstrukturen auf. Daher ist es für Anwenderinnen und Anwender selten möglich, auszuweichen, wenn beispielsweise Sicherheitsbedenken bei einer bestimmten Lösung bestehen. Aus diesem Grund ist es wichtig, sichere alternative Angebote zu schaffen. Auch die Cybersicherheitsagenda versucht sicherzustellen, dass nicht vertrauenswürdige Hersteller vom Ausbau der für die voranschreitende Digitalisierung benötigten Infrastruktur ausgeschlossen werden. Entscheidende Voraussetzung hierfür jedoch ist, dass entsprechende alternative Angebote existieren. Um deren Entstehung zu ermöglichen, müssen verschiedene Ansätze kombiniert werden, wie beispielsweise eine umfassendere Unterstützung von Open-Source-Projekten, bessere Förderungen von Start-ups sowie eine europäische Chipproduktion. Dies gewährleistet auch eine bessere

Verfügbarkeit von Hardware. Darüber hinaus sollte das Vergaberecht so angepasst werden, dass junge europäische Unternehmen und Open-Source-Ansätze bei Ausschreibungen bevorzugt zum Zuge kommen. So kann die ohnehin vorhandene staatliche Nachfrage effizient eingesetzt werden. Gleichzeitig müssen (angewandte) Forschungsprojekte initiiert und vorangetrieben werden. Gemeinsame europäische Initiativen wie etwa der Chip Act,[39] der Aufbau souveräner Datenräume,[40] die Überarbeitung der eIDAS-Verordnung[41] oder auch der neue Cyber Resiliance Act[42] sind gute Ansätze zur Stärkung der Digitalen Souveränität.

- **Kompetenzen in Schlüsseltechnologien:** Eng verknüpft mit der Schaffung alternativer Angebote ist der Aufbau von Kompetenzen in Schlüsseltechnologien,[43] denn ohne das entsprechende Know-how können keine alternativen Angebote entwickelt werden. Darüber hinaus bildet die Beurteilungsfähigkeit das Fundament, um die Sicherheit von Technologien zu evaluieren. Entsprechendes Know-how kann wiederum in internationalen Gremien zur Standardisierung und Normierung eingebracht werden, um damit auf die zukünftige Richtung, in die sich Technologien entwickeln, Einfluss zu nehmen.
- **Vertrauenswürdige Open-Source-Software:** Open-Source-Lösungen können aufgrund ihres hohen Innovationspotenzials dazu beitragen, sichere Alternativen zu schaffen. Dafür muss Open-Source-Software jedoch umfassend getestet, aktuell gehalten und gewartet sowie ihre Sicherheit (einschließlich der Lieferketten) verifiziert werden. Konzepte zur systematischen und weitestgehend automatisierten Integritätsprüfung könnten hier hilfreich sein. Sowohl für den Betrieb als auch für die Nachfrage nach Open-Source-Software ist Planungssicherheit entscheidend. Wichtig ist es, die internationale Open-Source-Gemeinschaft einzubeziehen und die Community lebendig zu halten, damit der Quellcode dauerhaft aktualisiert wird und Sicherheitslücken, sobald sie bekannt werden, geschlossen werden können. Open Source muss auf Dauer vertrauenswürdig sein, um effizient und in allen Bereichen nutzbar zu sein. Dafür ist es wichtig, dass die Entwicklung nicht nur in den Händen einzelner Personen beziehungsweise kleiner Gruppen liegt, sondern möglichst institutionelle Organisationen (etwa Foundations) die Weiterentwicklung übernehmen. Diese Instanzen können dann aus der großen Menge an Open-Source-Angeboten eine Vorauswahl treffen und dieser Auswahl durch ausführliches Testing sowie durch das Angebot von Wartung der Software ein erhöhtes Sicherheitsniveau verleihen. Verifizierte Kuratoren, die beispielsweise von Public-Private-Partnerships oder Foundations bezahlt werden, können die Prüfung und Wartung übernehmen. Derartige Instanzen sollten auch den Betrieb der Open-Source-Lösungen übernehmen.

39 | Vgl. Europäische Kommission 2022a.
40 | Vgl. Europäische Kommission 2020.
41 | Vgl. Europäische Kommission 2022b.
42 | Vgl. Europäische Kommission 2022c.
43 | Dazu zählen unter anderem Risikobewertung, Kryptografie, digitale Identitäten, Netzwerksicherheit, Threat-Intelligence und vertrauenswürdige Hardware.

Literatur

acatech 2022
acatech (Hrsg.): *Sicherheit, Resilienz und Nachhaltigkeit* (acatech IMPULS), München 2022.

acatech 2021
acatech (Hrsg.): *Digitale Souveränität. Status quo und Handlungsfelder* (acatech IMPULS), München 2021.

Accenture 2020
Accenture (Hrsg.): *2020 Cyber Threatscape Report*, 2020. URL: www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf [Stand: 27.09.2022].

Atlantic Council 2021a
Atlantic Council (Hrsg.): *Countering Cyber Proliferation – Zeroing in on Access-as-a-Service*, 2021. URL: www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf [Stand: 27.09.2022].

Atlantic Council 2021b
Atlantic Council (Hrsg.): A*ssessing Russia's Role and Responsibility in the Colonial Pipeline Attack*, 2021. URL: www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/ [Stand: 27.09.2022]

BBK
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: *Sektoren und Branchen KRITIS*. URL: www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.htm [Stand: 27.09.2022].

Bitkom 2021
Bitkom (Hrsg.): *Wirtschaftsschutz 2021*, 2021. URL: www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf [Stand: 27.09.2022].

BKA 2022
Bundeskriminalamt: *Cybercrime*, Bundeslagebild 2021, Wiesbaden 2022.

BMI 2022
Bundesministerium des Innern und für Heimat: *Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode*, Berlin 2022. URL: www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4 [Stand: 27.09.2022].

BMI 2021
Bundesministerium des Inneren, für Bau und Heimat: *Cybersicherheitsstrategie für Deutschland 2021*, Berlin 2021. URL: www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=9AA3AE7DC92A8FF6770FDE6EC5DCEB35.2_cid332?__blob=publicationFile&v=2 [Stand: 27.09.2022].

BSI 2022
Bundesamt für Sicherheit in der Informationstechnik: „BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten" (Pressemitteilung vom 15.03.2022). URL: www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/Presse-Archiv/220315_Kaspersky-Warnung.html [Stand: 27.09.2022].

BSI
Bundesamt für Informationssicherheit: *IT-Sicherheitskennzeichen*, 2022. URL: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html [Stand: 27.09.2022].

CrowdStrike 2021a
CrowdStrike (Hrsg.): *2021. Global Threat Report*, 2021. URL: go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf [Stand: 27.09.2022].

CrowdStrike 2021b
CrowdStrike (Hrsg.): *Zero Trust Security Explained: Principles of the Zero Trust Mode*l, 2021. URL: www.crowdstrike.com/cybersecurity-101/zero-trust-security/ [Stand: 27.09.2022].

Cyber Security Agency of Singapore 2021
Cyber Security Agency of Singapore: *The Singapore Cybersecurity Strategy 2021*, 2021. URL: www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021 [Stand: 27.09.2022].

ENISA 2021
European Union Agency for Cybersecurity (ENISA): *ENISA Threat Landscape 2021*, 2021. URL: www.enisa.europa.eu/publications/enisa-threat-landscape-2021 [Stand: 04.11.2022].

Europäische Kommission 2022a
Europäische Kommission: *Europäisches Chip-Gesetz, 2022*. URL: ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_de [Stand: 27.09.2022].

Europäische Kommission 2022b
Europäische Kommission: *eIDAS Regulation*, 2022. URL: digital-strategy.ec.europa.eu/en/policies/eidas-regulation [Stand: 27.09.2022].

Europäische Kommission 2022c
Europäische Kommission: *Cyber Resilience Act, 2022*. URL: digital-strategy.ec.europa.eu/en/library/cyber-resilience-act [Stand: 27.09.2022].

Europäische Kommission 2020
Europäische Kommission: *Europäische Datenstrategie, 2020*. URL: ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de [Stand: 27.09.2022].

Europol 2019
European Union Agency for Law Enforcement Cooperation Europol: *IOCTA. Internet Organised Crime Threat Assessment*, 2019. URL: www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf [Stand: 27.09.2022].

Flashpoint 2021
Flashpoint (Hrsg.): *Facing Five Types of Ransomware and Cyber Extortion*, 2021. URL: www.flashpoint-intel.com/blog/facing-five-types-of-ransomware-and-cyber-extortion/ [Stand: 27.09.2022].

Handelsblatt 2020
Handelsblatt (Hrsg.): *Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf*, 2020. URL: www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html [Stand: 27.09.2022].

Security Intelligence 2019
Security Intelligence (Hrsg.): *The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015*, 2019. URL: securityintelligence.com/posts/the-decline-of-hacktivism-attacks-drop-95-percent-since-2015/ [Stand: 27.09.2022].

Intel471 2020
Intel471 (Hrsg.): *Partners in Crime: North Koreans and Elite Russian-speaking Cybercriminals*, 2020. URL: intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals [Stand: 27.09.2022].

Mandiant 2019
Mandiant (Hrsg.): *APT41: A Dual Espionage and Cyber Crime Operation*, 2019. URL: www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation [Stand: 27.09.2022].

Noun
Noun Projekt. URL: https://thenounproject.com [Stand: 17.12.2021].

PwC 2020
PwC (Hrsg.): *Cyber Threats 2020: A Year in Retrospect*, 2020. URL: www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf [Stand: 27.09.2022].

Süddeutsche Zeitung 2022
Süddeutsche Zeitung (Hrsg.): *Ein Jahr nach Cyberangriff: Anhalt-Bitterfeld spürt Folgen,* 2022. URL: www.sueddeutsche.de/wirtschaft/internet-koethen-anhalt-ein-jahr-nach-cyberangriff-anhalt-bitterfeld-spuert-folgen-dpa.urn-newsml-dpa-com-20090101-220705-99-910444 [Stand: 27.09.2022].

Stiftung Neue Verantwortung 2022
Stiftung Neue Verantwortung (Hrsg.): *Deutschlands staatliche Cybersicherheitsarchitektur,* 8. Auflage, 2022. URL: www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur_achteauflage0422.pdf [Stand: 27.09.2022].

Tagesspiegel Background Cybersecurity 2022
Tagesspiegel Background Cybersecurity (Hrsg.): *Attacke auf Viasat – eine gezielte Cyberaktion*, 2022. URL: background.tagesspiegel.de/cybersecurity/attacke-auf-viasat-eine-gezielte-cyberaktion [Stand: 27.09.2022].

The White House 2021
The White House: *Executive Order 14028: Improving the Nation's Cybersecurity*, 2021. URL: www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ [Stand: 27.09.2022].

Washington Post 2021
Washington Post (Hrsg.): *Panic Buying Strikes Southeastern United States as Shuttered Pipeline Resumes Operation*s, 2021. URL: www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/ [Stand: 27.09.2022].

Über acatech – Deutsche Akademie der Technikwissenschaften

acatech berät Politik und Gesellschaft, unterstützt die innovationspolitische Willensbildung und vertritt die Technikwissenschaften international. Ihren von Bund und Ländern erteilten Beratungsauftrag erfüllt die Akademie unabhängig, wissenschaftsbasiert und gemeinwohlorientiert. acatech verdeutlicht Chancen und Risiken technologischer Entwicklungen und setzt sich dafür ein, dass aus Ideen Innovationen und aus Innovationen Wohlstand, Wohlfahrt und Lebensqualität erwachsen. acatech bringt Wissenschaft und Wirtschaft zusammen. Die Mitglieder der Akademie sind herausragende Wissenschaftlerinnen und Wissenschaftler aus den Ingenieur- und den Naturwissenschaften, der Medizin sowie aus den Geistes- und Sozialwissenschaften. Die Senatorinnen und Senatoren sind Persönlichkeiten aus technologieorientierten Unternehmen und Vereinigungen sowie den großen Wissenschaftsorganisationen. Neben dem acatech FORUM in München als Hauptsitz unterhält acatech Büros in Berlin und Brüssel.

Weitere Informationen unter www.acatech.de.

Herausgeberin und Herausgeber:

Claudia Eckert
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit
Lichtenbergstraße 11
85748 Garching bei München

Reinhard Ploss
acatech – Deutsche Akademie der Technikwissenschaften
Karolinenplatz 4
80333 München

Reihenherausgeber:
acatech – Deutsche Akademie der Technikwissenschaften, 2022

Geschäftsstelle
Karolinenplatz 4
80333 München
T +49 (0)89/52 03 09-0
F +49 (0)89/52 03 09-900

Hauptstadtbüro
Pariser Platz 4a
10117 Berlin
T +49 (0)30/2 06 30 96-0
F +49 (0)30/2 06 30 96-11

Brüssel-Büro
Rue d'Egmont/Egmontstraat 13
1000 Brüssel (Belgien)
T +32 (0)2/2 13 81-80
F +32 (0)2/2 13 81-89

info@acatech.de
www.acatech.de

Empfohlene Zitierweise:
Eckert, C./Ploss, R. (Hrsg.): *Cybersicherheit. Status quo und zukünftige Herausforderungen* (acatech IMPULS), München 2022.
DOI: https://doi.org/10.48669/aca_2022-7

ISSN 2702-7627

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Koordination: Dr. Anna Frey, Paul Grünke, Simon Litsche
Redaktion: Alrun Straudi
Lektorat: Lektorat Berlin
Layout-Konzeption, Konvertierung und Satz: Groothuis, Hamburg
Titelfoto: © shutterstock/Khakimullin Aleksandr

Die Originalfassung der Publikation ist verfügbar auf www.acatech.de.

Professionelle Cyberangriffe von organisierten Kriminellen und politisch motivierten Akteuren stellen eine zunehmend größer werdende Bedrohung für Deutschland und den gesamten europäischen Raum dar. Cybersicherheit, also die Fähigkeit, diesen Gefahren zu begegnen, ist ein entscheidender Eckpfeiler für eine erfolgreiche Digitalisierung. Sie schafft Vertrauen in die digitalen Systeme, mit denen täglich gearbeitet wird. Eng verwoben mit Cybersicherheit ist das Themenfeld Digitale Souveränität. Zusammen bilden sie die Grundlage für selbstbestimmtes und vertrauenswürdiges Handeln im Cyberraum.

Cybersicherheit sollte als gesamtgesellschaftliche Aufgabe verstanden werden: Politik, Wirtschaft, Wissenschaft sowie Bürgerinnen und Bürger sind alle betroffen. Der vorliegende IMPULS gibt einen Überblick über das Themenfeld sowie Anregungen, wie alle involvierten Akteure zur Erhöhung der Cybersicherheit beitragen können. Das Herzstück muss dabei eine von der Politik konzipierte, ambitionierte Cybersicherheitsstrategie bilden.