MEHR SICHERHEIT FÜR DIE DIGITALE TRANSFORMATION

Warum wir nur gemeinsam die Gesellschaft gegen Angriffe aus dem Netz immunisieren können

JAHRESBERICHT DES WEISENRATS FÜR CYBER-SICHERHEIT 2020

Bonn, 15. Mai 2020

CYBER SECURITY CLUSTER BONN

INHALT

4 — **Grußwort des Cyber Security Cluster Bonn**

6 — **Sicherheit – eine Frage der Einstellung?**
Dirk Backofen, Vorsitzender des Cyber Security Cluster Bonn, über wachsende Gefahren durch Hackerangriffe, leicht zu knackende Passwörter und den neuen Rat der Cyber-Weisen

8 — **Der Weisenrat für Cyber-Sicherheit stellt sich vor**

10 — **Editorial**

12 — **Gefahr für Wirtschaft und Gesellschaft**
Milliardenschäden durch Milliarden Viren: Wie sich Cyber-Angriffe zu einer der größten Bedrohungen unserer Zeit entwickelt haben

14 — **8 Empfehlungen des Weisenrats für Cyber-Sicherheit**
Wie der neu gegründete Weisenrat für Cyber-Sicherheit den Erfolg der digitalen Transformation absichern will

20 — **Bericht des Weisenrats für Cyber-Sicherheit für das Jahr 2020**
Mehr Sicherheit für die digitale Transformation: Warum wir nur gemeinsam die Gesellschaft vor Angriffen aus dem Netz schützen können

32 — **Technologische Souveränität im Cyber-Raum gestalten**
Warum wir „IT Security made in Germany" zum Qualitätssiegel machen müssen

40 — **Digitale und smarte Städte der Zukunft**
Wie wir deren Resilienz und Sicherheit erhöhen und die Privatheit ihrer Bewohner schützen können

48 — **Passwortrichtlinien in deutschen Unternehmen**
Sicherheit muss benutzerfreundlich sein

64 — **Künstliche Intelligenz in der Cyber-Sicherheit**
Warum Deutschland bei der Entwicklung resilienter und sicherer KI eine Vorreiterrolle einnehmen muss

72 — **Kryptoagilität und Post-Quanten-Kryptografie**
Wie wir uns gegen Gefahren von morgen wappnen können

78 — **Alles oder nichts?**
Über die Mittel zum Schutz der Demokratie in einer digitalen Welt

86 — Verzeichnis der Themenverantwortlichen und Impressum

GRUSSWORT

Sehr geehrte Damen und Herren,

rund 71 Millionen Angriffe zählte die Telekom im Januar 2020 auf ihre Hacker-Lockfallen, die sogenannten Honeypots – und das täglich. Ein neuer Spitzenwert, nach 21 Millionen registrierten Attacken im April 2018 und vier Millionen im April 2017. Schier unglaubliche Zahlen, die stetig wachsen und doch nur die Spitze des Eisbergs sind: Schließlich bestätigen aktuelle Studien, dass sieben von zehn deutschen Unternehmen in jüngster Zeit schon Opfer von Netz-Attacken oder Industriespionage wurden. Mit Schäden in Milliardenhöhe. Gerade im Mittelstand findet sich kaum noch ein Unternehmen, das nicht nachweislich oder zumindest mit sehr hoher Wahrscheinlichkeit von einem Hackerangriff betroffen war. Aber auch Behörden, Krankenhäuser oder Universitäten und wir alle als Privatpersonen sind längst ins Visier von Kriminellen geraten. Die mitunter auch darauf aus sind, die öffentliche Meinung zu manipulieren.

Daher müssen wir nun dringend die Voraussetzungen schaffen, um uns wirksam und zuverlässig vor den Attacken aus dem Netz zu wappnen. Eine riesige Aufgabe, die kein Akteur im Alleingang bewältigen kann. Deshalb haben sich Vertreter von unterschiedlichen Organisationen zum Cyber Security Cluster Bonn zusammengeschlossen. Sie alle eint das gemeinsame Verständnis für die entscheidende Bedeutung der Sicherheit im Zeitalter der digitalen Transformation. Das Ziel: Teilen des Sicherheitswissens und Stärkung der Zusammenarbeit auf diesem so relevanten Gebiet. Zu den Partnern gehören unter anderem die Bundesstadt Bonn, das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Kommando Cyber- und Informationsraum der Bundeswehr, die Hochschule Bonn-Rhein-Sieg, die Fraunhofer-Gesellschaft und die Industrie- und Handelskammer Bonn/Rhein-Sieg sowie Unternehmen wie die Deutsche Telekom, SAP, IBM, BWI und die Deutsche Post.

Durch enge Verzahnung aller Stakeholder hat Deutschland nun die Chance, sich als innovativer Anbieter von Sicherheitslösungen zu positionieren. Für uns ist Cyber-Sicherheit ein wesentlicher Standortfaktor. Für Deutschland insgesamt und auch für die lokale Ebene – wie etwa für den Wirtschaftsraum Bonn. Durch ihre Symbiose aus Behörden, Forschungseinrichtungen, Privatwirtschaft und als Standort des neuen Cyber Security Cluster hat die ehemalige Bundeshauptstadt beste Voraussetzungen, zum bundes-, ja europaweiten Magneten für hoch qualifizierte Arbeitskräfte einer sich stark entwickelnden Branche zu werden. Kurz: zum Herz der Cyber-Sicherheit in Europa. Eine Chance, die wir nutzen wollen – und eine Verpflichtung, der wir nachkommen müssen.

Daher begrüßen wir, dass das Cyber Security Cluster den jährlichen Bericht der Cyber-Sicherheitsweisen nicht nur initiiert, sondern auch organisatorisch unterstützt hat. Unser großer Dank gilt aber vor allem den Wissenschaftlern, die diesem neuen Weisenrat für Cyber-Sicherheit angehören. Sie alle leisten mit ihrer Arbeit, mit dem vorliegenden Report sowie ihren konkreten Handlungsempfehlungen einen entscheidenden Beitrag zur Cyber-Immunisierung von Wirtschaft und Gesellschaft.

Bonn, im Mai 2020

Ashok Sridharan
Oberbürgermeister der Stadt Bonn

Arne Schönbohm
Präsident des BSI

Generalleutnant Ludwig Leinhos
Inspekteur Cyber- und Informationsraum

Frank Hoever
Polizeipräsident Bonn

Timotheus Höttges
CEO der Deutschen Telekom AG

Prof. Dr. Peter Martini
Direktor Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)

Prof. Dr. Hartmut Ihne
Präsident der Hochschule Bonn-Rhein-Sieg

Dr. Hubertus Hille
Hauptgeschäftsführer IHK Bonn/Rhein-Sieg

Dirk Lieder
Geschäftsführer CONET Solutions GmbH

Dr. Goodarz Mahbobi
Geschäftsführer der axxessio GmbH

Stephan Wirtz
Geschäftsführer anykey GmbH

CYBER
SECURITY
CLUSTER BONN

SICHERHEIT – EINE FRAGE DER EINSTELLUNG?

Dirk Backofen, Vorsitzender des Cyber Security Cluster Bonn, über wachsende Gefahren durch Hackerangriffe, leicht zu knackende Passwörter und den neuen Weisenrat für Cyber-Sicherheit

Herr Backofen, den Kreis der Wirtschaftsweisen kennt jeder. Warum brauchen wir künftig auch einen Weisenrat für Cyber-Sicherheit?

Dirk Backofen: Weil die Zahl der Angriffe auf IT-Systeme exorbitant wächst, weltweit. Unternehmen aus allen Branchen sowie ganzen Volkswirtschaften entsteht dadurch immenser Schaden. Diesen immer raffinierteren Attacken müssen wir etwas entgegensetzen, sonst gefährden wir die digitale Transformation unserer Unternehmen und Behörden, ja unserer Gesellschaft. Das Cyber Security Cluster Bonn hat sich deshalb eine Immunisierung von Wirtschaft und Gesellschaft gegen IT-Angriffe aller Art zum Ziel gesetzt. Deswegen sind wir sehr froh, dass sich einige der renommiertesten Experten für das Thema Cyber-Sicherheit von unserer Initiative haben inspirieren lassen und sich nun im Weisenrat für Cyber-Sicherheit zusammengefunden haben.

Welche Aufgaben hat der Weisenrat für Cyber-Sicherheit?

Dirk Backofen: Die Wissenschaftler werden jährlich einen Lagebericht zur Cyber-Kriminalität vorlegen – inklusive wissenschaftlich fundierter Empfehlungen und handfester Impulse für Politik und Wirtschaft, mit denen sich die Gefahren aus dem Netz jetzt und in Zukunft entschärfen lassen. Kurz: Mit ihrer geballten Kompetenz erhöhen sie die Schlagkraft unserer „Armee der Guten". Damit meine ich die Allianz all jener, die uns dabei unterstützen, die Immunisierung der Gesellschaft gegen Cyber-Attacken voranzutreiben.

Wo sehen Sie die größten Herausforderungen?

Dirk Backofen: Zum Beispiel darin, dass sich die Bedrohungsszenarien laufend ändern. Aber auch bei der weitverbreiteten Sorglosigkeit im Umgang mit Datensicherheit – etwa bei der Wahl von Passwörtern. Hacker-Angriffe wirksam zu bekämpfen ist nicht nur eine Frage der richtigen Technologie, sondern vor allem der richtigen Einstellung. Und der nötigen rechtlichen Voraussetzungen: Die Politik muss gegen Cyber-Attacken eine angemessene, wirksame Strategie entwickeln und die dafür notwendigen regulatorischen Vorgaben festlegen. Wir dürfen nicht nur das Wissen mehren, wie man den diversen Angriffen trotzt. Wichtiger noch ist mir, dass wir gemeinsam dafür sorgen, dass dieses Wissen auch in der Wirtschaft und bei jedem Bürger ankommt. Wir müssen es künftig allen viel leichter machen, Sicherheit auch umzusetzen.

*„Geballte Kompetenz erhöht unsere **Schlagkraft**."*

Dirk Backofen
ist Vorstandsvorsitzender Cyber Security Cluster Bonn e.V. und Leiter Business Development T-Systems International GmbH

CYBER SECURITY CLUSTER BONN

DER WEISENRAT *FÜR CYBER-SICHERHEIT*

Prof. Dr. Claudia Eckert

Leiterin des Fraunhofer AISEC und des Lehrstuhls für Sicherheit in der Informationstechnik an der TU München

Prof. Dr. Matthias Hollick

Professor für Sicherheit in Mobilen Netzen an der Technischen Universität Darmstadt

Der Weisenrat für Cyber-Sicherheit

Prof. Dr. Norbert Pohlmann

Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco

Prof. Dr. Delphine Reinhardt

Professorin für Computersicherheit und Privatheit an der Georg-August-Universität Göttingen

Prof. Dr. Angela Sasse

Professorin für Human-Centred Security an der Ruhr Universität Bochum

Prof. Dr. Matthew Smith

Professor für Usable Security and Privacy an der Universität Bonn und am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

Sehr geehrte Damen und Herren,

machen wir es Hackern zu einfach? Wie können wir unsere Daten vor ungewolltem Zugriff schützen? Welche Rolle kann Künstliche Intelligenz bei der Entwicklung einer wehrhaften Digitalwirtschaft spielen? Und warum brauchen smarte Städte einen besonderen Schutz?

Fragen wie diese wollen wir auf den folgenden knapp 90 Seiten unseres ersten Reports beantworten und ein Konzept zur Verbesserung der Resilienz unserer Wirtschaft und Gesellschaft gegen Attacken aus dem Netz entwerfen. Wir, das sind sechs WissenschaftlerInnen, die an ihren Lehrstühlen oder Instituten in München, Darmstadt, Gelsenkirchen, Göttingen, Bochum und Bonn oder an den Fraunhofer-Instituten für Angewandte und Integrierte Sicherheit (AISEC) und für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) zu den unterschiedlichen Facetten der Cyber-Sicherheit forschen. Als unabhängige ProfessorInnen haben wir uns auf Initiative des Cyber Security Cluster Bonn zusammengefunden, um das Know-how der deutschen Sicherheitscluster und die Expertise der ihnen angeschlossenen WissenschaftlerInnen zu bündeln.

Wir möchten mit unserem Bericht nicht nur Jahr für Jahr einen unabhängigen Blick auf die digitale Sicherheitslage werfen, sondern vor allem in die Zukunft schauen. Unser Bericht wird Auskunft darüber geben, wie Wirtschaft und Gesellschaft, wie Unternehmen, Organisationen und Individuen den Gefahren im Netz begegnen können – jetzt und künftig. Und wir geben der Politik wie auch allen Stakeholdern konkrete Handlungsempfehlungen.

ZENTRALE FRAGE IM GLOBALEN WETTBEWERB

Warum das so entscheidend ist? Weil Sicherheit im Netz für die Entwicklung von Wirtschaft und Gesellschaft immer relevanter wird. Und weil für Bestand und Weiterentwicklung von Unternehmen aller Größen und Branchen der Kampf gegen Kriminelle längst ebenso überlebenswichtig ist wie für ein modernes Zusammenspiel von Staat und Bürger. Wollen Wirtschaft und Gesellschaft auch künftig von den Vorteilen der digitalen Transformation nachhaltig profitieren, müssen wir wirksame Maßnahmen entwickeln und umsetzen. Nur so können wir unsere Daten als wichtigsten Rohstoff unserer Zeit sichern und unsere Wirtschafts- und Gesellschaftsordnung angemessen schützen.

WIRTSCHAFT UND GESELLSCHAFT BESSER SCHÜTZEN

Die gute Nachricht – trotz aller Hiobsbotschaften von immer raffinierteren, täglich millionenfach ausgelösten Hackerangriffen auf Unternehmen, vom Start-up bis zum Konzern, von der Automobilbranche bis zum Einzelhandel, auf Universitäten, Schulen und Behörden bis hin zum privaten E-Mail-Account: Wir haben die Chance, den Kampf gegen Cyber-Kriminelle zu gewinnen, wenn wir einen dezidierten Immunisierungsplan für Wirtschaft und Gesellschaft entwickeln. Unabdingbare Voraussetzungen für die Sicherheit unserer Daten: technologische Souveränität. Produkte und Services, die Sicherheit zu ihrer DNA machen. Intelligente Authentisierungsmethoden, die Sicherheit und Benutzerfreundlichkeit kombinieren. Resiliente Künstliche Intelligenz, die nicht nur unsere Sicherheit erhöht, sondern große ökonomische Chancen eröffnet. Smarte Städte, die ihre Bewohner schützen und auch im Krisenfall funktionieren. Und ein besserer Schutz unserer Demokratie in der Online-Welt.

Nur so können wir schaffen, was auch die Wirtschaftsweisen in ihrem aktuellen Lagebericht postulieren: den Wandel zu meistern – den sicheren digitalen Wandel.

Bonn, im Mai 2020

Prof. Dr. Claudia Eckert

Prof. Dr. Matthias Hollick

Prof. Dr. Norbert Pohlmann

Prof. Dr. Delphine Reinhardt

Prof. Dr. Angela Sasse

Prof. Dr. Matthew Smith

GEFAHR FÜR WIRTSCHAFT UND GESELLSCHAFT

Milliardenschäden durch Milliarden Viren: Wie sich Cyber-Angriffe zu einer der größten Bedrohungen unserer Zeit entwickelt haben

71 MIO.

Angriffe pro Tag auf die Infrastruktur der Deutschen Telekom (Q1/2020, Peak: 87 Mio.)[1]

2017: **4 Mio.** ▶ 2018: **12 Mio.** ▶ 2019: **42 Mio.**

40 Mio. €

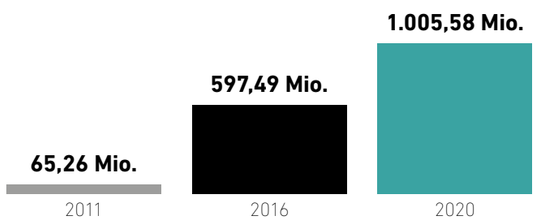
Größter Schadensfall

eines Unternehmens durch Ransomware-Angriff[2]

250

neue Angriffstaktiken entwickeln Hacker pro Monat, um Dax-Infrastrukturen zu schädigen[1]

Die Zahl bekannter Schadsoftware-Varianten ist seit 2011 jedes Jahr um 40 Prozent gestiegen.[3]



1 Milliarde Viren im Umlauf

IM VISIER DER HACKER

Wie viele deutsche Unternehmen 2018 von Datendiebstahl, Industriespionage oder Sabotage betroffen waren.[4]

Ja 75 %

Verdacht 13 %

55 PROZENT

aller deutschen Internetnutzer über 16 Jahre wurden 2019 Opfer von Cyber-Kriminalität. Am häufigsten betroffen waren Malware-Infektionen von Computern und Smartphones.[5]

770.000

Mails mit Schadprogrammen wurden zwischen Mitte 2018 und Mitte 2019 in deutschen Regierungsnetzen abgefangen.[2]

DAS GRÖSSTE UNHEIL DROHT VON ALTEN BEKANNTEN UND NEUEN TÜCKEN.

3 bis 8

neue Angriffsvektoren jeden Tag auf **DAX-Infrastruktur**[6]

32 MRD.

LEAKED ACCOUNT CREDENTIALS[6]

114 MIO.[6]

neue Schadprogrammvarianten

Windows:	MacOS:	Android:	Weitere[7]:
65 Mio.	**0,09 Mio.**	**3,4 Mio.**	**>39 Mio**

9,4 BILLIONEN BOTNET-PAKETE

am Backbone des Fest- und Mobilfunknetzes der Deutschen Telekom innerhalb eines Monats[6]

104 MRD. € SCHADEN

durch Datendiebstahl, Industriespionage oder Sabotage[4]

International:

BIS ZU 220 GBIT/S PEAK DDOS-ANGRIFFEN[6]

National:

135 GBIT/S[6]

252 CYBER-SICHERHEITSVORFÄLLE

auf kritische Infrastrukturen (KRITIS) in Deutschland meldeten deren Betreiber von Mitte 2018 bis Mitte 2019.[6]

11,5 MIO. BERICHTE ÜBER MALWARE-INFEKTIONEN

übermittelte das BSI an deutsche Netzwerkbetreiber.[6]

[1] Deutsche Telekom, 2019
[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2019", Bonn, 2019
[3] AV TEST, „Malware". Zuletzt geprüft: 07.01.2020. [Online]. Verfügbar: https://www.av-test.org/de/statistiken/malware/.
[4] Bitkom, „Wirtschaftsschutz in der digitalen Welt", 06.11.2019. Zuletzt geprüft: 12.01.2019. [Online]. Verfügbar: https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019.pdf
[5] Bitkom, „Mehr als jeder zweite Onliner Opfer von Cyberkriminalität", 07.01.2020. Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://www.bitkom.org/Presse/Presseinformation/Mehr-zweite-Onliner-Opfer-Cyberkriminalitaet
[6] Telekom Security Feb. 2020
[7] Dazu zählen u. a. betriebssystem-unabhängige Scripte, maliziöse Dokumente, Java-Malware usw.

8 EMPFEHLUNGEN

DES WEISENRATS FÜR CYBER-SICHERHEIT

1 Technologie muss sich dem Menschen anpassen, um ihn zu entlasten und zu schützen.

2 Hersteller müssen sich zu regelmäßigen Schwachstellentests und Sicherheitsupdates verpflichten.

3 Digitale Prozesse und Infrastrukturen müssen angriffsresilienter werden.

4 Technologische Souveränität muss erhöht und bewahrt werden.

5 Digitale Infrastrukturen in smarten Städten müssen jederzeit verfügbar, verständlich und beherrschbar bleiben.

6 KI-Systeme müssen transparent und zertifizierbar sein.

7 Langlebige Produkte müssen kryptoagil gestaltet werden.

8 Der Schutz der Demokratie muss online verstärkt werden.

1 Technologie muss sich dem Menschen anpassen, um ihn zu entlasten und zu schützen.

Wir sollten den Menschen nicht mehr als das schwächste Glied in der Cyber-Sicherheit betrachten. Bei Sicherheitsvorfällen dem Nutzer die Schuld zuzuweisen ist keine zielführende Strategie. Falls menschliche Fehler zu Sicherheitsproblemen führen, sollten wir die zugrunde liegenden Technologien kritisch prüfen. Denn wenn Menschen sich nicht an Sicherheitsregeln halten, liegt dies meist daran, dass es oft zeitraubend oder schwierig bis unmöglich ist, sie umzusetzen. Sicherheitsexperten versuchen seit Jahren, diesem Verhalten mit Belehrungen (Security Awareness) gegenzusteuern – vergeblich. Wir benötigen bessere technische Lösungen, die im Gebrauch einfach sind. Ziel muss es sein, die Technologie dem Menschen anzupassen, um ihn zu entlasten und zu schützen. Dies gilt nicht nur für Endnutzer, sondern insbesondere auch für technisch versierte Experten. Fehler, die Administratoren oder Entwickler verursachen, sind oft weitaus gravierender als die Fehler der Endnutzer. Deswegen müssen Systeme für die Experten so entworfen und implementiert werden, dass sie fehlervermeidend und fehlertolerant sind.

2 Hersteller müssen sich zu regelmäßigen Schwachstellentests und Sicherheitsupdates verpflichten.

Hersteller müssen IT-Systeme und -Lösungen bei der Produkt- und Systemeinführung nicht nur einmalig auf Schwachstellen testen, sondern diese Tests kontinuierlich wiederholen. Tests sollten dabei technologisch breit aufgestellt sein. Bei Quellcodetests sollten statische und dynamische Methoden zum Einsatz kommen. Bei Systemtests müssen alle Komponenten berücksichtigt werden. Die Ergebnisse der Tests müssen transparent und überprüfbar sein. Hersteller müssen ihre Geräte, Dienste und Anwendungen über die komplette Lebenszeit mit Sicherheitsupdates versorgen.

3 Digitale Prozesse und Infrastrukturen müssen angriffsresilienter werden.

Zusätzlich zu der Härtung von Systemen gegen Angriffe (siehe Empfehlung 2), sollten Systeme so gebaut und betrieben werden, dass sie in der Lage sind, kompromittierte Systemteile zu tolerieren. Sie müssen auch dann noch verlässlich arbeiten, wenn sie attackiert werden. Die Politik sollte für die Angriffsresilienz Rahmenvorgaben machen, welche Mindestsicherheitsstandards für Systeme festlegen, und sie sollte Anreizsysteme für Unternehmen schaffen, um diese Mindeststandards zu erfüllen. Die Politik muss ferner Rahmenbedingungen schaffen, sodass auch Unternehmen ohne Sicherheitsexpertise in die Lage versetzt werden, die Standards einzuhalten.

4 Technologische Souveränität muss erhöht und bewahrt werden.

Die technologische Souveränität ist ein immer wichtiger werdender Faktor, weil in Zukunft in allen Branchen der Wertschöpfungsanteil von IT und Internet zunehmen wird. Um die Gestaltungsmöglichkeiten unserer Gesellschaft auszuschöpfen, müssen alle Stakeholder, also Hersteller und Anwender von IT-Technologie sowie Wissenschaft, Politik und Verwaltung aus diesem Bereich, gemeinsame Ziele definieren und umsetzen. Erforderlich ist ein gezielter Kompetenzausbau in Schlüsselbereichen, um mögliche Risiken, die durch Abhängigkeiten entstehen (Hersteller, Herkunftsland, Einsatz, Wechselwirkungen) beurteilen zu können. Für kritische Bereiche müssen wir alternative Schlüsseltechnologien entwickeln bzw. bestehende Technologien erweitern, um Abhängigkeiten zu reduzieren und den Einsatz vorhandener Technologien beherrschbar zu gestalten. Regulierungen müssen Vorgaben für den Einsatz von Technologien mit hohem Risikopotenzial für sicherheitskritische Bereiche machen. Es müssen Prüfverfahren und -techniken für eine kontinuierliche Zertifizierung geschaffen werden, um einen beherrschbaren Einsatz sicherheitskritischer Technologien zu ermöglichen. Open-Source-Software als strategisches Instrument sowie eine intensivere Beteiligung an der Entwicklung von internationalen Standards, um frühzeitig mitgestalten zu können, sind weitere wichtige Aspekte, die von der Politik angestoßen und für wichtige Bereiche umgesetzt werden müssen.

5 Digitale Infrastrukturen in smarten Städten müssen jederzeit verfügbar, verständlich und beherrschbar bleiben.

Für digitale Infrastrukturen in smarten Städten müssen wir sicherstellen, dass sie jederzeit verfügbar, verständlich und beherrschbar bleiben. Krisen wie Cyber-Angriffe, Naturereignisse, menschliches und technisches Versagen sowie Gewalt und Terror gefährden den verlässlichen Betrieb von IT-Systemen. Es ist daher notwendig, dass man auch im Krisenfall und bei hohem Vernetzungsgrad einen Betrieb/Notbetrieb kritischer Infrastrukturen in den Sektoren Energie, Verkehr und Logistik, Gesundheit, Ernährung, Wasser, Finanz- und Versicherungswesen sowie Staat und Verwaltung garantieren kann. Ein systematisches Verständnis der Verwundbarkeit von IKT sowie wirksame Maßnahmen zur Erhöhung ihrer Resilienz sind dazu dringend erforderlich. Unsichere oder nicht beherrschbare IT-Systeme dürfen nicht Teil kritischer Infrastrukturen sein und müssen aus digital vernetzten Städten entfernt werden. Gleichzeitig muss eine demokratische Kontrolle über die Daten, die im öffentlichen Raum erhoben werden, gewährleistet sein. Digitalisierte Infrastrukturen in smarten Städten dürfen nicht in eine Überwachung und Kontrolle ihrer Bewohner als Normalzustand münden: Smarte Städte müssen die Rechte des Individuums auf Privatheit schützen.

6 KI-Systeme müssen transparent und zertifizierbar sein.

Maschinelle Lernverfahren und Systeme der Künstlichen Intelligenz werden bereits heute in zahlreichen IT-Infrastrukturen als zentraler Baustein zur Analyse, Prognose und Steuerung eingesetzt. Die Vertrauenswürdigkeit derartiger Systeme ist für Unternehmen aller Branchen, aber auch für staatliche Institutionen von höchster Wichtigkeit. Unternehmerische Entscheidungen werden zunehmend auf Ergebnissen von KI-Systemen basieren. Es entsteht eine gefährliche Abhängigkeit, da die Ergebnisse von maschinellen Lernverfahren meist nicht nachvollziehbar sind und auch die Qualität der Daten, die zum Anlernen genutzt werden, für die Nutzer nicht prüfbar ist. Aufgrund ihres Einsatzes in einer Vielzahl sicherheitskritischer Bereiche werden verlässliche, transparente und zertifizierte KI-Systeme benötigt. Um resiliente KI-Produkte zu entwickeln, sind unterschiedliche Kritikalitäts- und Zertifizierungsstufen für KI-Algorithmen festzulegen. Dafür werden Prüfkataloge sowie technische Richtlinien benötigt. Um branchenspezifischen regulatorischen Anforderungen Rechnung zu tragen, sind zudem branchenspezifische Kataloge und technische Prüfverfahren erforderlich.

7 Langlebige Produkte müssen kryptoagil gestaltet werden.

Kryptografische Verfahren, Schlüssellängen und Zufallszahlengeneratoren, die heute sicher sind, können morgen schon unsicher sein. Entwicklungen im Bereich Quantencomputing werden dazu führen, dass asymmetrische Verschlüsselungsverfahren wie RSA unsicher werden. Deshalb empfehlen wir für IT-Lösungen, die eine lange Lebenszeit haben können, ein kryptoagiles Design als Bestandteil eines Mindeststandards aufzunehmen. Das bedeutet, dass solche Lösungen die Möglichkeit bieten sollten, kryptografische Verfahren und Zufallszahlengeneratoren auszutauschen sowie Schlüssellängen zu erhöhen, ohne ihre eigentliche Funktion zu beeinträchtigen oder Hardware auszuwechseln. Die Fähigkeiten zur Evaluation und Analyse von Post-Quanten-Kryptoverfahren müssen weiter ausgebaut werden. Dies ist eine zentrale Voraussetzung für hochsichere Systeme. Bereits jetzt müssen Migrationsstrategien entwickelt und erprobt werden, die einen einfachen Übergang auf Post-Quanten-Kryptoverfahren ermöglichen.

8 Der Schutz der Demokratie muss online verstärkt werden.

Erfundene und verfälschte Informationen sowie deren gezielte Platzierung in Online-Medien können die Wählermeinung und damit auch politische Entscheidungen beeinflussen. Wahlen sind hierbei nur eines der Missbrauchsziele. Auch der generelle Diskurs im digitalen Raum sowie der faire Umgang mit exponierten Gruppen wie Journalisten, Politikern, Aktivisten sowie mit Minderheiten, Migranten etc. sind in Gefahr. Der Schutz der Ausübung demokratischer Prinzipien in der digitalen Welt ist ein grundlegendes, aber auch ein vielschichtiges Problem. Für dessen komplexe Lösung bedarf es weiterer Anstrengungen. Hierzu ist eine gründlichere Problemanalyse unabdingbar. Nur so können wir die aktuell existierenden isolierten Analysen sowie die vereinzelt vorhandenen technischen Gegenmaßnahmen auf eine breitere Basis stellen. Für neue technische Lösungen, die dieses Problem eindämmen helfen, ist dies eine Grundvoraussetzung. Eine zentrale Rolle kommt hierbei der Berücksichtigung menschlichen Verhaltens und der Benutzbarkeit zu, insbesondere wenn eine enge Interaktion zwischen allen Stakeholdern erfolgt. Gleichzeitig fordern wir eine bessere Untersuchung der möglichen Auswirkungen von technischen Lösungsansätzen über deren rein technische Ebene hinaus und mit besonderem Fokus auf Rechtskonformität, Weiterentwicklung des rechtlichen Rahmens sowie den gesellschaftlichen Auswirkungen.

Bericht des Weisenrats

BERICHT DES WEISENRATS FÜR CYBER-SICHERHEIT 2020

Mehr Sicherheit für die digitale Transformation: Warum wir nur gemeinsam die Gesellschaft vor Angriffen aus dem Netz schützen können

Gestohlene Daten, mit Lösegeldtrojanern infizierte Server, lahmgelegte Fabriken: Privatpersonen, Unternehmen und öffentliche Einrichtungen werden Tag für Tag millionenfach Opfer von Attacken aus dem Netz und erleiden Schäden in Milliardenhöhe. Mit dem Grad der digitalen Vernetzung von Wirtschaft und Gesellschaft entwickelt sich Cyber-Kriminalität zur Gefahr für den Fortschritt der digitalen Transformation und den Bestand unserer Demokratie. Der neu formierte Weisenrat für Cyber-Sicherheit stellt deswegen in seinem ersten Jahresbericht eine Übersicht über ausgewählte wichtige Themen vor und macht acht Empfehlungen, die in der Einschätzung des Rates zu einer Verbesserung der Sicherheitslage von Wirtschaft und Gesellschaft führen werden.

19. Dezember 2019

Bei der Stadt Frankfurt geht nichts mehr. „Aufgrund technischer Probleme sind die städtischen Onlineservices und -Angebote aktuell nicht erreichbar. Wir bitten um Verständnis!", meldet die Stadtverwaltung gegen 16 Uhr – auf Twitter. Der Grund: Unbekannte hatten die hochgefährliche **Schadsoftware Emotet** per E-Mail an einen städtischen Mitarbeiter geschickt. Als der Virenscanner Alarm schlägt, fährt die Stadt ihre IT-Systeme vorsichtshalber herunter. Die Folge: Die Bürgerämter bleiben geschlossen, die Website der Stadt ist 24 Stunden nicht erreichbar. Nur 60 Kilometer entfernt kämpft zur selben Zeit auch die Justus-Liebig-Universität Gießen mit den Folgen einer Netzattacke. Eine unbekannte Schadsoftware zwingt sie **für Wochen in den Offlinemodus.** Tausende Studierende können sich weder Bücher ausleihen noch sich zu Klausuren anmelden.

27. Dezember 2019

Stillstand bei Canyon. Als der Radversender aus Koblenz nach den Weihnachtsfeiertagen um kurz vor 6 Uhr morgens den Betrieb wieder aufnehmen will, sind die IT-Systeme für Montage, Versandlogistik, Telefon und E-Mails nicht funktionsfähig. **Hacker hatten die Server mit Ransomware infiziert** und verschlüsselt, der Betrieb ist tagelang nur eingeschränkt möglich.

07. Januar 2020

Alarm bei der Deutschen Kreditbank (DKB) – Onlinebanking und Website sind für DKB-Kunden nicht erreichbar. **Hacker hatten einen IT-Dienstleister der Bank angegriffen** und den Betrieb mit einer massiven DDoS-Attacke tagelang lahmgelegt.

Copyright: Unsplash/paultrenzel

SICHERHEIT IMMER RELEVANTER FÜR DIE VOLKSWIRTSCHAFT

Nur vier Ereignisse innerhalb weniger Tage, die zeigen: Ob Unternehmen oder Behörden, öffentliche Organisationen oder Privatpersonen – Angriffe aus dem Netz sind längst keine Seltenheit mehr, sie können jeden treffen und sich zur dunklen Seite der Digitalisierung entwickeln. Vom Einschleusen von Schadsoftware über DDoS-Angriffe bis hin zu menschlichem Fehlverhalten: Die Sicherheitslage verschärft sich mit dem Grad der Vernetzung von Wirtschaft und Gesellschaft. Wir leben in einer Zeit, in der Sicherheitsbedrohungen intelligenter und gefährlicher denn je sind. Die digitale Transformation ist nicht nur Quell neuer, innovativer Produkte, Dienstleistungen und Geschäftsmodelle. Mit ihr steigt auch das Maß der Gefährdung. Eine Entwicklung, auf die die Betroffenen möglichst schnell reagieren müssen, um signifikanten Schaden abzuwenden. Wirtschaft, Wissenschaft und Politik, aber auch alle Einzelpersonen, die sich im Netz bewegen, müssen ihre Widerstandskraft erhöhen, um Cyber-Kriminellen Paroli bieten zu können. Nur so lassen sich die großen Chancen nutzen, die die digitale Transformation für Wirtschaft, Staat und Gesellschaft eröffnet. Ohne Sicherheit ist die digitale Transformation zum Scheitern verurteilt. Denn jeder kann Opfer werden – vom privaten Handynutzer bis zum professionellen Programmierer, vom Start-up über den Mittelstand bis zum Großkonzern. Die smarte Stadt bietet genauso potenzielle Angriffsflächen wie die vernetzte Fabrik oder die intelligente Wohnung. Und das überall auf der Welt.

DIE LAGE DER NATION

Das BSI geht in seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2019"[1] davon aus, dass Kriminelle täglich allein 320.000 neue Schadprogramme entwickeln. Aber auch ältere Versionen bleiben gefährlich – und das über Jahre. Die Schadsoftware Wannacry, die im Mai 2017 innerhalb weniger Stunden Hunderttausende Computer weltweit infiziert hatte, soll noch 2019 weltweit für rund jede vierte Ransomware-Attacke verantwortlich gewesen sein[2] und Schäden in Höhe von vier Milliarden US-Dollar verursacht haben.

JÄHRLICH 104 MILLIARDEN EURO SCHADEN IN DEUTSCHLAND

Aber nicht nur Einzeltäter oder organisierte Kriminelle treiben hier ihr Unwesen. Selbst Staaten entwickeln Malware- und Ransomware-Tools, die Hacker im Darknet erwerben können. Die Folge: zunehmende Verunsicherung. 85 Prozent der Chief Information Security Officer sehen laut einer Untersuchung des

[1] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2019", 2019. Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7

[2] J. Ilic, "WannaCry Virus Was the Most Common Crypto Ransomware Attack in 2019", 08.01.2020. Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://www.precisesecurity.com/articles/wannacry-virus-was-the-most-common-crypto-ransomware-attack-in-2019/

IT-Sicherheitsdienstleisters Fortinet in Sicherheitsproblemen die größte Hürde auf dem Weg zur Digitalisierung ihres Unternehmens.[3] Und in einer KPMG-Studie geben 85 Prozent der befragten deutschen Firmen an, dass es ihnen zunehmend schwerer falle, erste Anzeichen von Netzkriminalität zu erkennen.[4] Die Deutsche Telekom zählt allein im Januar 2020 rund 71 Millionen Angriffe auf ihre Honeypots (Hackerlockfallen) – und das täglich. Ein neuer Spitzenwert, nach zwölf Millionen registrierten Attacken im April 2018 und vier Millionen im April 2017.

Mit drastischen Folgen für unsere Wirtschaft: Laut einer Umfrage des Digitalverbands Bitkom verursachen Angriffe auf deutsche Unternehmen jährlich einen Gesamtschaden von knapp 104 Milliarden Euro.[5] Die häufigsten Delikte: Systembeschädigungen oder Computersabotage, Computerbetrug, Datendiebstahl, das Ausspähen oder Abfangen von Daten, Erpressung sowie Manipulation von Konto- und Finanzdaten.

Eine Bedrohung, gegen die sich die Wirtschaft zunehmend zur Wehr setzt: 4,6 Milliarden Euro haben deutsche Unternehmen nach Berechnungen der Marktforscher von IDC und Bitkom 2019 in ihre Cyber-Sicherheit investiert – für Hardware, Software und Services im Bereich IT-Sicherheit. Das sind zehn Prozent mehr als im bisherigen Rekordjahr 2018.[6] Und dennoch ein Klacks gemessen am Bruttosozialprodukt, das schon heute zunehmend von den Erfolgen der digitalen Wirtschaft abhängt. Ganz zu schweigen von dem Potenzial künftiger Wertschöpfung, das für Wirtschaft, Staat und Gesellschaft durch die digitale Transformation in Aussicht steht. Laut BDI[7] kann Europa bis zum Jahr 2025 an die 1,25 Billionen Euro zusätzliche industrielle Wertschöpfung erzielen. Vorausgesetzt, die Unternehmen investieren weiter in die Transformation und schrecken nicht aus Angst vor Datendiebstahl, Sabotage und Spionage vor einem weiteren Engagement zurück.

> „Wie können wir ein **nachhaltiges** Sicherheitsbewusstsein entwickeln?“

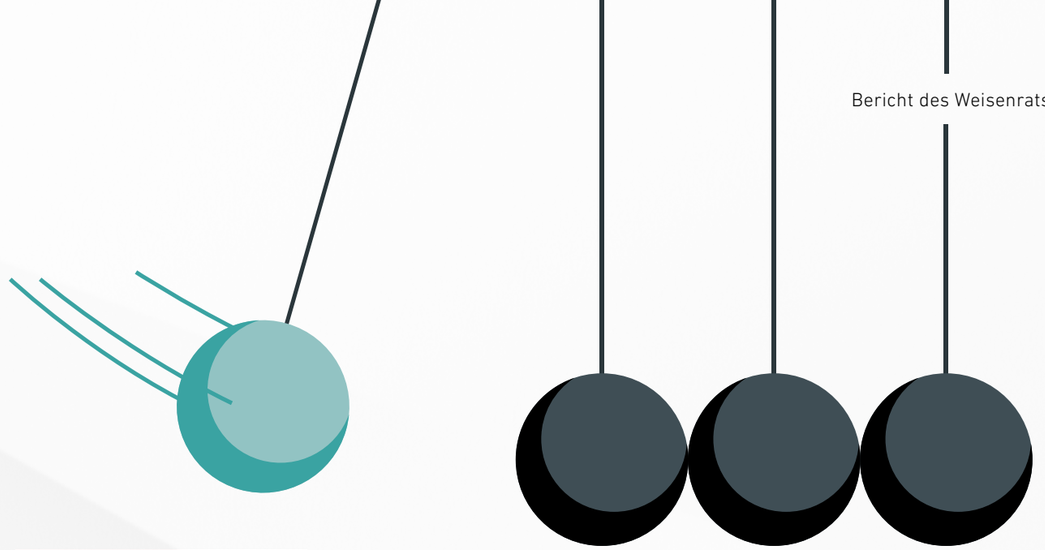
DAS ZIEL: SICHERHEIT UND PRIVATSPHÄRE FÜR DIE GESELLSCHAFT UND IHRE BÜRGER

Die Prognosen legen nahe: Cyber-Sicherheit kommt mittelfristig eine entscheidende Doppelrolle zu – als Gralshüter und Motor des weltweiten Wirtschaftswachstums. Wirksame Schutzsysteme tun also Not: für den einzelnen Bürger oder Kunden genauso wie für Gesellschaft und Volkswirtschaft, für Unternehmen und Behörden, Universitäten und Schulen, Kliniken und Arztpraxen, Parteien wie Verbände, Kommunen und Länder. Denn ohne vernünftige Vorsorge riskieren wir nicht nur ökonomische Schäden gigantischen Ausmaßes – wir gefährden unsere Demokratie und unser Gemeinwesen.

Was wir brauchen, ist ein ganzheitlicher Blick auf IT-Sicherheit und Privatsphäre. Insellösungen, die nur Einzelsysteme schützen oder Lösungen, die den Faktor Mensch nicht berücksichtigen, werden den Angriffen nicht standhalten. Denn Sicherheit von der Gesellschaft bis zum Bürger funktioniert umso besser, je mehr sich alle Akteure ihrer Bedeutung bewusst sind und sich dagegen wappnen. Eine hohe Immunisierungsrate ist für die Sicherheit von Wirtschaft und Gesellschaft im Netz genauso entscheidend wie im Kampf gegen Krankheiten. Denn global vernetzte IT-Strukturen sind nur so stark und widerstandsfähig wie ihre schwächsten Glieder. Doch nur gemeinsam lässt sich angesichts der wachsenden Bedrohung eine angemessene Schlagkraft entwickeln. Allein kann das niemand bewältigen. Notwendig ist ein enger Wissensaustausch von Wirtschaft, Politik und Forschung.

SICHERHEIT IST AUCH STAATSAUFGABE

Wie können Organisationen Kriminalität im Netz schneller aufspüren? Wie darauf reagieren? Welche



„Jährlich 104 Milliarden Euro Schaden in Deutschland“

Rolle muss der Staat im Kampf gegen die Kriminellen spielen? Auf welchen Handlungsfeldern sollte unser Fokus liegen? Wie können wir ein nachhaltiges Sicherheitsbewusstsein entwickeln? Und wie weit dürfen und müssen Sicherheitsmaßnahmen gehen, um Bevölkerung, Unternehmen und kritische Infrastrukturen zu schützen, ohne dabei die Freiheit einzelner Personen und Organisationen zu beschneiden? Fragen und Handlungsfelder wie diese stehen im Mittelpunkt des diesjährigen, des ersten Berichts. Der Report zeigt, wie wir diesen Kraftakt im Schulterschluss von Wirtschaft, Wissenschaft und Gesellschaft gemeinsam bewältigen können. Dabei ist es wichtig, den verschiedenen menschlichen Akteuren gerecht zu werden. „Der Mensch sollte nicht mehr als das schwächste Glied in der Cyber-Sicherheit gesehen werden. […] Ziel muss es sein, die Technologie dem Menschen anzupassen, um ihn zu entlasten und zu schützen“, heißt es in der ersten von acht Empfehlungen der Cyber-Sicherheitsweisen (siehe Seite 14). Das Zusammenspiel der Akteure spielt ebenfalls eine wichtige Rolle. Die Politik sollte für die Angriffsresilienz Rahmenvorgaben machen, die Mindestsicherheitsstandards für Systeme festlegen, und sie sollte Anreizsysteme für Unternehmen schaffen, um diese Mindeststandards zu erfüllen (siehe Empfehlung 3 auf Seite 14). Sicherheit muss ferner bei jeder Neu- oder Weiterentwicklung eines Produkts oder einer Dienstleistung von Beginn an mitgedacht und in der DNA eines Produkts oder Services verankert werden.

IT SECURITY MADE IN GERMANY

Selbstverständlich betrifft das Thema Cyber-Sicherheit nicht nur uns in Deutschland. Bedeutet: Gelingen Deutschland auf diesem Feld dank einer konzertierten Aktion entscheidende Fortschritte, dann positionieren wir uns als Vorreiter auf einem globalen Markt. Die deutsche Sicherheitsindustrie ist zwar stark fragmentiert,

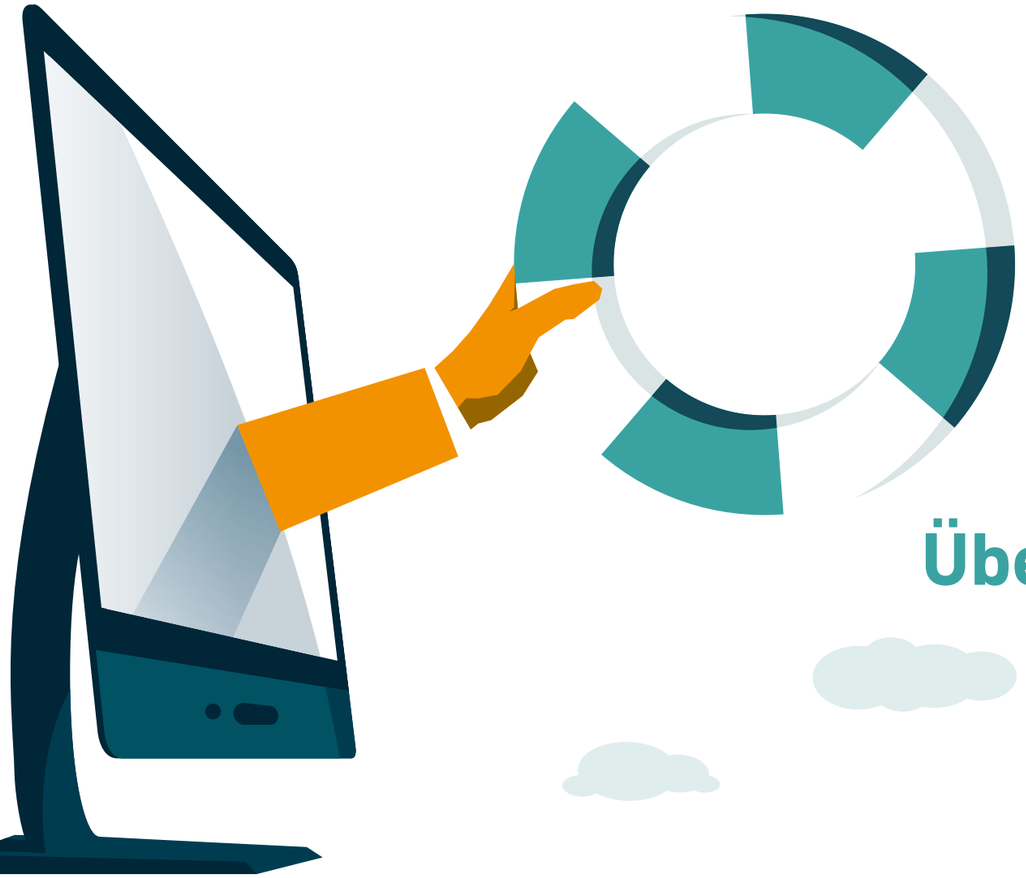
[3] C. Müller-Dott und P. Schmitz, „Die Paradoxa der Security im Zeitalter der Digitalisierung“, 27.05.2019. Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://www.security-insider.de/die-paradoxa-der-security-im-zeitalter-der-digitalisierung-a-831230/
[4] KPMG, „Computerkriminalität in der deutschen Wirtschaft 2019: e-Crime wird unterschätzt“, 10.07.2019. Zuletzt geprüft:13.01.2020. [Online]. Verfügbar: https://home.kpmg/de/de/home/themen/2019/07/e-crime-in-der-deutschen-wirtschaft-2019.html
[5] Bitkom, „Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr“, 06.11.2019. Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr
[6] Bitkom, „Rekordjahr im Markt für IT-Sicherheit“, 08.10.2019. Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://www.bitkom.org/Presse/Presseinformation/Rekordjahr-Markt-fuer-IT-Sicherheit
[7] Bundesverband der Deutschen Industrie e.V., „Cybersicherheit bildet das Rückgrat der Digitalisierung“, 19.11.2019. Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://bdi.eu/artikel/news/cybersicherheit-bildet-das-rueckgrat-der-digitalisierung/

bietet aber im Vergleich zu anderen Ländern höherwertige Cyber-Sicherheitslösungen wie Verschlüsselung, Public-Key-Infrastrukturen in der Kryptologie, aktive Cyber-Sicherheitssysteme und Hardware-Sicherheitsmodule. Auch mit seinen Sicherheitsexperten im Hochschul-, Forschungs- und Industriebereich spielt unser Land an der Spitze mit. Heißt: „Made in Germany" ist mit Blick auf den Bereich der IT-Sicherheit schon jetzt ein wichtiges Qualitätssiegel – und das lässt sich weiter ausbauen.

TECHNOLOGISCHE SOUVERÄNITÄT

Wie aber lässt sich die gewünschte Sicherung von Wirtschaft und Gesellschaft erreichen? Sie setzt immer ein gewisses Maß an technologischer Souveränität voraus – also das selbstbestimmte Entscheiden und Handeln von Personen, Betrieben und anderen Institutionen im Bei der Cloud oder bei proprietärer Hard- und Software ist die Marktdominanz außereuropäischer Anbieter unbestritten. Aber um selbstbestimmt und unabhängig agieren zu können, müssen Unternehmen hierzulande die unterschiedlichen Technologien bewerten können. Nur dann können sie souverän entscheiden, welche Abwehrstrategie sie wählen oder wem sie ihre Daten anvertrauen. Selbstverständlich sollten sie auch die Risiken, die sich aus möglichen Abhängigkeiten ergeben, beurteilen können. Um ihre Wirtschaft erfolgreich zu gestalten, müssen moderne Gesellschaften daher wichtige Schlüsseltechnologien für die Wirtschaft beherrschen und weiterentwickeln können, sodass eine störende Fremdbestimmtheit durch andere Staaten oder dominierende Hersteller verhindert wird (siehe Seite 32 bis 39).

Das gilt in besonderem Maße für Künstliche Intelligenz. Sie ist die Schlüsseltechnologie der Zukunft und spielt gerade in jenen Bereichen, in denen Deutschland traditionell stark ist, beispielsweise in der Automobilbranche und der Industrie, eine immer wichtigere Rolle. Um hier nicht in immer stärkere Abhängigkeiten zu geraten, sollten wir unsere Daten zunehmend in Deutschland oder Europa speichern und verarbeiten. Mit der europäischen Cloud GAIA-X etwa ließe sich eine solche vertrauenswürdige und sichere Dateninfrastruktur etablieren. Genauso entscheidend ist der Aufbau einer leistungsstarken KI-Infrastruktur und von KI-Kompetenzzentren, die den Mittelstand fördern. Denn nur wer technologisch souverän ist, kann Zukunftstechnologien aktiv mitgestalten und kontrollieren.



Kein Platz für Überwachungsstädte

MEHR SCHUTZ FÜR DIE SMARTE STADT

Zukunftstechnologien verändern nicht nur Unternehmen oder machen das Leben von Individuen komfortabler. Auch Staaten und Gesellschaften digitalisieren sich zunehmend und müssen die persönliche Integrität ihrer Mitglieder und deren materiellen Besitz vor Angriffen bewahren. Gelingt ihnen dies nur unzureichend, sind Demokratie und Freiheit in Gefahr. Das lässt sich am Beispiel der smarten Stadt verdeutlichen (siehe Seite 40 bis 47). Nach Schätzungen der Vereinten Nationen werden im Jahr 2050 rund zwei Drittel der Weltbevölkerung in Städten leben. Um dieses Wachstum professionell zu begleiten, nutzen Städte zunehmend digitale Infrastrukturen in allen relevanten Bereichen – Energie, Verkehr und Logistik, Gesundheit, Ernährung und Wasser sowie Verwaltung. Sie wandeln sich Stück für Stück zu Smart Citys, deren Infrastrukturen gleich mehrfach abgesichert werden müssen: gegen Naturkatastrophen, menschliches oder technisches Versagen sowie gegen Kriminalität und Terror. Aber auch gegen die Versuchung, die Smart City in eine Überwachungsstadt zu verwandeln, was sich mit unserer freiheitlichen und demokratischen Grundordnung nicht vereinbaren ließe und nicht das Ziel sein darf.

RESILIENZ WIRD ZUR DNA JEDES PRODUKTS

Noch aber fehlt nicht nur ein systematisches Verständnis für die Verwundbarkeit digitaler Städte. Es mangelt auch an wirksamen Maßnahmen, welche die Resilienz und Sicherheit in diesen Lebensräumen erhöhen und die Privatheit ihrer Bewohner schützen können. Technische Lösungen – und dies gilt nicht nur für die smarte Stadt – müssen künftig von Grund auf resilient und sicher konzipiert sowie in der Lage sein, die Privatheit ihrer Bürger und Institutionen zu schützen. Denn generell gilt: Sicherheit ist keine Eigenschaft, mit der sich ein bereits fertiges Produkt oder ein Service nachträglich veredeln ließe. Sie muss bei jeder Neu- oder Weiterentwicklung von Beginn an mitgedacht werden und zur DNA eines jeden Produkts oder Services gehören.

DER FAKTOR MENSCH

Zwar schützen 63 Prozent der deutschen Internetnutzer ihre Daten und Geräte mit einem Passwort[8] – haben jedoch teils große Mühe dabei sichere Passwörter zu benutzen. Passwörter wie „123456" und „hallo123" sind von Angreifern schnell geknackt – dennoch gehören beide zu den zehn beliebtesten Passwörtern. Damit sind Einfallstore für potenzielle Angreifer vielerorts weit geöffnet (siehe Seite 48 bis 63).

Die technischen Maßnahmen, solche Passwörter per Richtlinie zu verhindern, schaffen jedoch oft Benutzbarkeitsprobleme. Interne Passwortrichtlinien geben Einblicke in das Sicherheitsbewusstsein deutscher Unternehmen. Ein weitverbreiteter und verständ-

[8] Statista: „Welche Authentifizierungsverfahren nutzen Sie selber zum Schutz Ihrer Daten und Geräte?", 2019. Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://de.statista.com/prognosen/952951/umfrage-in-deutschland-zu-authentifizierungsverfahren-zum-schutz-von-daten

licher Irrglaube ist es, dass strengere Richtlinien die Qualität der Passwörter steigern. Dies lässt sich jedoch nicht pauschal sagen und es gibt Situationen, in denen strengere Regeln die Qualität der gewählten Passwörter mitunter sogar verschlechtern, weil sich die Nutzer gezwungen sehen, Bewältigungsstrategien zu finden. Diese sind jedoch den Angreifern ebenfalls bekannt und somit anfällig. Von Menschen zu verlangen, sich immer mehr und immer kompliziertere Passwörter zu merken, ist kein gangbarer Weg. Es ist daher anzuraten, den Menschen bei dieser Aufgabe technisch zu unterstützen.

> „Passwortmanager und Zwei-Faktor-Authentisierung zum **Standard** machen.“

Passwortmanager und Zwei-Faktor-Authentisierung sollten daher zum Standard werden, sowohl für Unternehmen wie auch für Einzelpersonen. Passwortmanager sind für viele Anwendungsbereiche und gegen eine große Anzahl von einfachen Angriffen eine effektive und benutzerfreundliche Lösung. Noch mehr Sicherheit kann mit einem zweiten Faktor erzielt werden. Auf die Eingabe des richtigen Passworts folgt eine weitere Schranke, die sich nur mithilfe des zweiten Faktors öffnet: etwa durch einen Bestätigungscode auf dem Smartphone, einen Fingerabdruck auf einem Sensor oder über eine Chipkarte. Entscheidend ist, dass die beiden Sicherheitskomponenten auf zwei getrennten Geräten angesiedelt sind.

RESILIENTE KI ALS WACHSTUMSCHANCE

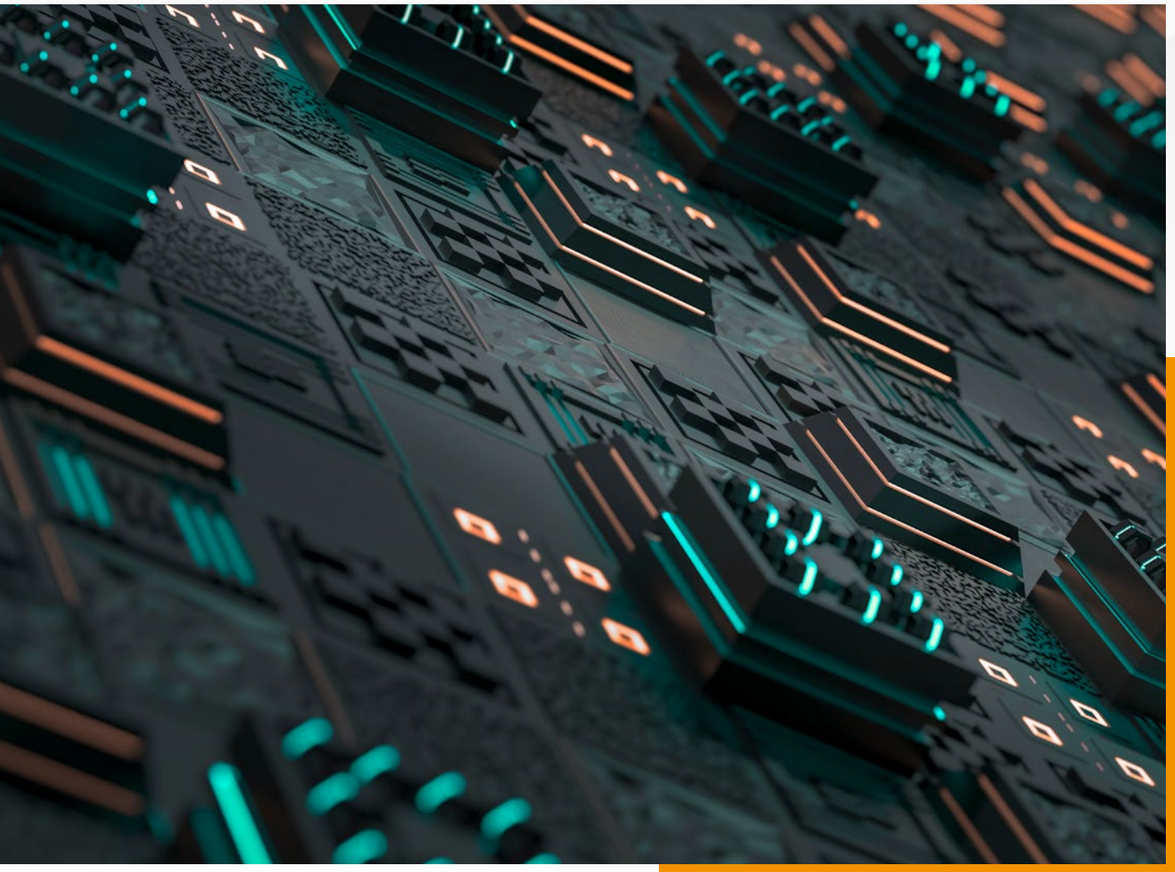
Die Sicherheit im Netz lässt sich mit KI-Systemen substanziell verbessern (siehe Seite 64 bis 71). Schon heute können KI-basierte Algorithmen Angriffe früher und schneller erkennen als ein menschlicher Analyst. Aber auch Künstliche Intelligenz ist verwundbar – durch Angriffe von außen genauso wie aufgrund fehlerhaften Trainings der Algorithmen. Wenn es uns daher gelingt, eine vertrauenswürdige und resiliente KI zu entwickeln, deren Entscheidungen für den Menschen nachvollziehbar und transparent sind, erfüllen wir eine zentrale Zukunftsaufgabe. Die Voraussetzungen dafür sind gerade hierzulande ausgesprochen gut: Deutschland verfügt über ausgezeichnete Kompetenzen in den Bereichen der Zertifizierung, der KI und der IT-Sicherheit. Zudem gehört der faire und vertrauenswürdige Umgang mit sensitiven Daten zu den Grundwerten unseres Demokratieverständnisses.

Damit aber die Unternehmen KI sicher nutzen können, brauchen wir nun dringend Methoden zu deren Zertifizierung. Denn an solchen Zertifikaten ließe sich der Resilienzgrad der jeweiligen KI leicht ablesen und vergleichbar machen. Voraussetzung dafür sind jedoch entsprechende Prüfkataloge, die einerseits auf die unternehmerischen Prozesse und Governance-Regeln, andererseits aber auch auf die technische Qualität und Sicherheit der Anwendungen abzielen. Wie sich Deutschland zum europäischen Leader für resiliente KI im Sicherheitsbereich entwickeln kann? Indem es in einem ersten Schritt einen solchen Prüfkatalog (Common Criteria Catalogue) entwickelt und parallel dazu eine staatlich geförderte Infra- und Wissensstruktur zum Thema KI im Cyber-Sicherheitsbereich aufbaut. Das wäre ein gutes Instrument, um gleichzeitig den Anschluss an die internationale Entwicklung im Bereich KI zu halten beziehungsweise künftig eine größere Rolle zu spielen.

HOCHSICHERHEITSRISIKO QUANTENCOMPUTER

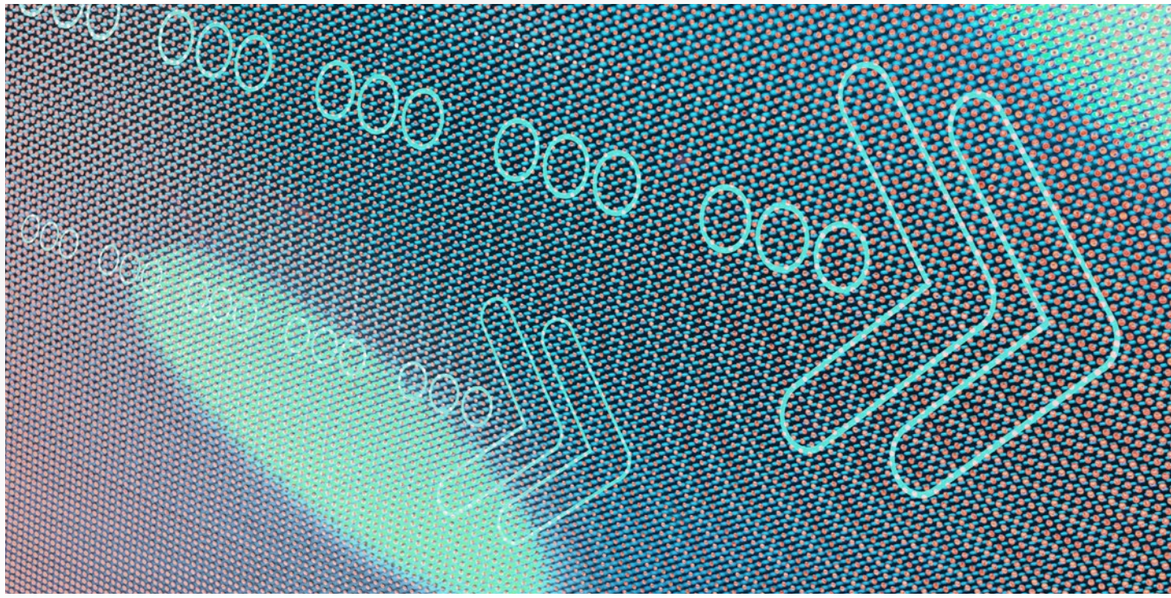
Wie aber wappnet man sich gegen Gefahren, die heute noch gar nicht existieren? Wie schützt man Daten, die momentan sicher verschlüsselt sind, vor der Gefahr, in absehbarer Zeit geknackt zu werden? Wie lassen sich langlebige Produkte und Services aus dem Internet der Dinge so entwickeln, dass sie über ihren gesamten Lebenszyklus sicher bleiben? Klar ist: Auf künftige Bedrohungen müssen wir uns schon heute vorbereiten

(siehe Seite 72 bis 77). Zwar werden leistungsstarke und kostengünstige Quantencomputer erst in einigen Jahren verfügbar sein. Doch schon jetzt ist abzusehen, dass sie mit ihrer enormen Rechenleistung zu erheblichen Sicherheitsrisiken führen werden. Sie können aktuelle Verschlüsselungsalgorithmen ganz einfach außer Gefecht setzen. Deshalb muss die Politik darauf dringen, dass Sicherheitszertifizierungen nicht nur den aktuellen Sicherheitszustand des Systems untersuchen. Sondern auch berücksichtigen, ob die Hersteller das Thema Kryptoagilität umgesetzt haben, ihre Produkte also auch künftige Bedrohungen abwehren können. „Da die meisten digitalen Lösungen gar keine Sicherheitszertifizierungen anstreben, brauchen wir als Alternative die Produkthaftung", sagt Dr. Eckert. „Der Staat muss Hersteller also dazu verpflichten, ihre Geräte, Dienste und Anwendungen über die komplette Lebenszeit mit Sicherheitsupdates zu versorgen."



Künftige Bedrohung: Quantencomputer

Quantencomputer werden mit ihrer enormen Rechenleistung zum Sicherheitsrisiko – denn sie können die herkömmlichen Verschlüsselungsmethoden außer Kraft setzen.



DEMOKRATISCHE GRUNDORDNUNG IM VISIER

Sicherheit ist ein wichtiger Bestandteil unserer Demokratie – und sie gerät zunehmend in Gefahr (siehe Seite 78 bis 85). Zahlreiche Angreifer sind nicht in erster Linie von finanziellen Interessen, sondern von politischen Absichten getrieben. Heißt unter anderem: Autokraten wollen Demokratien destabilisieren – mithilfe von Spionage, Cyber-Kriminalität, Onlinetrollen und Desinformation. So gab es bei den Wahlkämpfen in den USA und Frankreich oder beim Brexit-Referendum gezielte Versuche, mit gefälschten Informationen die Wahlentscheidungen zu beeinflussen. Top-Entscheider aus Wirtschaft und Politik haben im vergangenen Jahr die Manipulation der öffentlichen Meinung durch Fake News erstmals als höchstes Sicherheitsrisiko für die Bevölkerung eingestuft.[9] Die Gefahren spitzen sich mit Deepfakes weiter zu. Darunter versteht man täuschend echt wirkende Bilder und Videos, die sich mittels Künstlicher Intelligenz herstellen lassen. Die Software dazu gibt es kostenlos im Netz. Vor allem öffentliche Personen, von denen es viele Bild- und Videoaufzeichnungen gibt, werden Opfer solcher Deepfakes. Das Problem: Mit derart manipulierten Bildern und Videos wird es immer schwieriger, gefälschte von echten Inhalten zu unterscheiden.

Besonders manipulativ: Social Bots. Computerprogramme also, die in den sozialen Netzwerken selbstständig und gezielt bestimmte Meinungen oder Informationen verbreiten und damit den öffentlichen Diskurs beeinflussen. Viele der von solchen Bots verbreiteten Informationen sind falsch, gleichzeitig wird es immer schwieriger, zu erkennen, ob eine Meinungsäußerung von einem Menschen oder einer Maschine kommt. Wie aber lassen sich Authentizität sowie Integrität der Informationen gewährleisten? Wir fordern eine bessere Untersuchung der möglichen Auswirkungen von technischen Lösungsansätzen über deren rein technische Ebene hinaus und mit besonderem Fokus auf Rechtskonformität, Weiterentwicklung des rechtlichen Rahmens sowie den gesellschaftlichen Auswirkungen.

[9] Deloitte, „Fake News, Datendiebstahl & Co. – der Deloitte Cyber Security Report 2019". Zuletzt geprüft: 13.01.2020. [Online]. Verfügbar: https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html

TECHNOLOGISCHE SOUVERÄNITÄT IM CYBER-RAUM GESTALTEN

Warum wir „IT Security made in Germany“ zum Qualitätssiegel machen müssen

Die Digitalisierung ist der Motor und die Basis für das Wohlergehen unserer modernen und globalen Gesellschaft. Da die Digitalisierung global ist, wird sie auch technologisch von globalen Herstellern und Dienste-anbietern beeinflusst. Der Digitalisierungsprozess wird auf allen Ebenen immer schneller und damit beschleunigen sich auch die Veränderungen in unseren Lebensräumen. Das bedeutet aber auch, dass die notwendigen Technologien einen zunehmend kürzeren Innovationszyklus haben und damit rascher austauschbar sind, was für die Schaffung einer höheren technologischen Souveränität eine sehr gute Voraussetzung darstellt.

Technologische Souveränität kann dazu beitragen, eigenständig, selbstbestimmt und unabhängig Wirtschaft und Gesellschaft zu gestalten. Da eine vollständige technologische Souveränität finanziell nicht umgesetzt werden kann, sollten zumindest wichtige Schlüsseltechnologien beherrscht und weiterentwickelt werden können. Damit lassen sich technologische Abhängigkeiten reduzieren und stärken. Technologische Souveränität eröffnet Wirtschaft und Gesellschaft Gestaltungsmöglichkeiten.

Für den Cyber-Raum sind sämtliche mit dem globalen Internet verbundene IT und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen, Wissen und Intelligenzen zu berücksichtigen.

In Abgrenzung von der technologischen Souveränität zielt eine digitale Souveränität mehr auf den Bürger ab, der digitale Medien mit den verwendeten Daten kompetent, sicher, vielfältig und frei nutzen will.

Ein weiterer wichtiger Aspekt der technologischen Souveränität ist die Festlegung der Gesellschaft, in der sie wirken soll: sei es ein Unternehmen, eine Branche, Deutschland, Europa oder aber auch die internationale Staatengemeinschaft. Die Vor- und Nachteile dieser Festlegung sind vielfältig und betreffen insbesondere die Gesamtkosten, Abhängigkeiten und die Innovationsgeschwindigkeit der entsprechenden Technologien.

1. SITUATION DER TECHNOLOGISCHEN SOUVERÄNITÄT IN DEUTSCHLAND

Im Folgenden wird für einige Bereiche die Situation der technologischen Souveränität für Deutschland aufgezeigt.

Software
Die meisten Marktführer kommen aus den USA, zum Beispiel Google, Microsoft, Apple, IBM, Oracle, VMware, Salesforce, Adobe oder Symantec. Ausnahmen in den Top Ten der größten Softwarehersteller sind SAP aus Deutschland und HCL aus Indien.

Hardware
Die Marktführer kommen in der Regel aus Asien.

Plattformökonomie
Die Marktführer stammen aus den USA und Asien, darunter Google, Facebook, Airbnb, Uber, Netflix, WeChat, Tencent QQ oder Q-Zone.

Betriebssysteme
Zu den wichtigesten Vertretern im Bereich der Betriebssysteme gehören: Windows (Microsoft), Mac OS X/iOS (Apple), Android/Chrome OS (Google) und Linux (Open Source).

Technologische Souveränität im Cyber-Raum gestalten

Cloud-Lösungen
Viele Marktführer im Bereich IT wie Amazon, Microsoft, Google, IBM oder Oracle haben Cloud-Lösungen entwickelt und bieten verschiedenste Cloud Services weltweit sehr erfolgreich an. Durch diesen Trend steigt die Abhängigkeit von Cloud-Service-Anbietern und ihren Technologien, da diese nur zentral angeboten und auch die eigenen Daten zentral gespeichert werden. Die Leistungsfähigkeit bei diesen Cloud-Lösungen ist in erster Linie wegen Hyperscalern aus den USA und Asien besonders groß.

Cyber-Sicherheitsanbieter
Die Marktführer im Bereich der Massenprodukte, beispielsweise Anti-Malware, Authentifizierungslösungen, Firewall, VPN usw. im Bereich Cyber-Sicherheit kommen aus den USA und Israel.

Die deutsche Cyber-Sicherheitsindustrie ist stark fragmentiert, bietet aber hochwertige und aus deutscher Sicht vertrauenswürdigere Cyber-Sicherheitslösungen wie Verschlüsselung, PKIs, proaktive Cyber-Sicherheitssysteme und Hardware-Sicherheitsmodule an.

Deutsche Cyber-Sicherheitsexperten im Hochschul-, Forschungs- und Industriebereich spielen bereits an der internationalen Spitze mit. Dadurch hat Deutschland ideale Voraussetzungen, um sich in der Cyber-Sicherheit international erfolgreich zu positionieren und Marktführer zu werden. Um den Ruf, die Vertrauenswürdigkeit und das Marktpotenzial nicht zu schädigen, ist es jedoch wichtig, dass deutsche Geheimdienste Sicherheitsstandards und Sicherheitsprodukte nicht unterwandern und damit die Marke „Sicherheit made in Germany“ nachhaltig schädigen.

2. GENERELLE ASPEKTE FÜR DIE AUFRECHTERHALTUNG DER EIGENSTÄNDIGEN WETTBEWERBSFÄHIGKEIT

Bei der technologischen Souveränität spielt eigenständige Wettbewerbsfähigkeit eine tragende Rolle. Da in Zukunft in allen Branchen der Wertschöpfungsanteil von IT und Internet immer größer wird, werden auch alle Branchen davon abhängig.

Aus diesem Grund sollten die folgenden generellen Aspekte bezüglich der eigenständigen Wettbewerbsfähigkeit besonders beachtet und umgesetzt werden.

2.1. UNABHÄNGIGKEIT VON WICHTIGEN TECHNOLOGIEN HERSTELLEN

Neben der Daseinsvorsorge und der öffentlichen Sicherheit ist es für die Gesellschaft sowie ihre Leitindustrie und -märkte von entscheidender Bedeutung, bei kritischen Technologien eigenständig und gestaltungsfähig zu bleiben bzw. zu werden. Dafür müssen wichtige Technologiebereiche gemeinsam mit allen Stakeholdern identifiziert und entsprechende Maßnahmen umgesetzt werden, die technologische Innovations-, Entwicklungs- und Herstellungsfähigkeiten und darauf aufbauendes wirtschaftliches Wachstum fördern.

2.2. REGELN FÜR WICHTIGE TECHNOLOGIEBEREICHE DEFINIEREN UND UMSETZEN

Technologische Souveränität sollte auch mit Regeln gestaltet werden. Dazu müssen Abhängigkeiten bewertet und dann reduziert werden. Die folgenden Aspekte spielen dabei zum Beispiel eine besondere Rolle:

- Festlegung der Länder, von denen wichtige Hardware genutzt werden darf, weil die Abhängigkeiten und Risiken vertretbar bleiben.
- Festlegung, wo wichtige digitale Werte gespeichert werden dürfen (Cloud etc.).
- Förderung von technologischen Standards und Regeln für technologische Standards, um Abhängigkeiten abzubauen. Beispielsweise müsste dabei der Hersteller einer Technologie ab einem bestimmten Marktanteil verpflichtend einem Standard genügen, damit die jeweilige Technologie ausgetauscht werden kann, wenn Probleme auftauchen.
- Umsetzung von Gesetzen wie eIDAS, EU-DSGVO, NIS, PSD2 oder Cybersecurity Act, um wichtige Sicherheits- und Wertestandards erfüllen zu können und einige prinzipielle Abhängigkeiten zu reduzieren.

2.3. VERTRAUENSWÜRDIGKEIT DER TECHNOLOGIEPARTNER UND URSPRUNGSLÄNDER ÜBERPRÜFEN

In einer globalen Gesellschaft spielen globale Märkte und globale Technologieanbieter eine besondere Rolle. Daher müssen verwendete Technologien über Gütesiegel, Zertifizierungen und weitere Verifizierungsmöglichkeiten auf die Vertrauenswürdigkeit hin überprüft werden, bevor sie strategisch zum Einsatz kommen. Außerdem muss eine Bewertung der Abhängigkeit vom entsprechenden Ursprungsland vorgenommen und berücksichtigt werden.

2.4. DEFINITION UND NUTZUNG VON OPEN-SOURCE-SOFTWARE

Eine weitere, sehr gute Möglichkeit für die internationale Staatengemeinschaft, eine gemeinsame und kostenoptimierte technologische Souveränität zu erreichen, sind die Definition und Nutzung von Open-Source-Software. Wichtig ist dabei auch, dass sich Konsortien bilden, welche die unabhängige Entwicklung und Verifizierung von Open-Source-Software fördern und aktiv mitgestalten.

3. HANDLUNGSEMPFEHLUNGEN FÜR DIE TECHNOLOGISCHE SOUVERÄNITÄT IN DEUTSCHLAND

Um eine technologische Souveränität für Deutschland zu erreichen, müssen alle wichtigen und relevanten Stakeholder aus unterschiedlichen Bereichen aktiv und verantwortungsvoll zusammenarbeiten: Anbieterwirtschaft (Hersteller von IT-Technologien, Anbieter von IT-Diensten etc.), Anwenderwirtschaft (Nutzung von IT-Technologien, IT-Diensten etc.) sowie Vertreter von Politik, Staat und Wissenschaft im Bereich der IT-Technologien.

Die wichtigen Stakeholder sollten gemeinsam konkrete, messbare Ziele für die technologische Souveränität formulieren, deren Umsetzung beschließen und mit vereinten Kräften durchführen.

Im Folgenden werden exemplarisch einige maßgebliche Schlüsseltechnologien im Cyber-Raum diskutiert.

> *„KI ist eine Schlüsseltechnologie für das **zukünftige** Wirtschaftswachstum.“*

3.1. KI-FÄHIGKEIT FÖRDERN UND AUFBAUEN

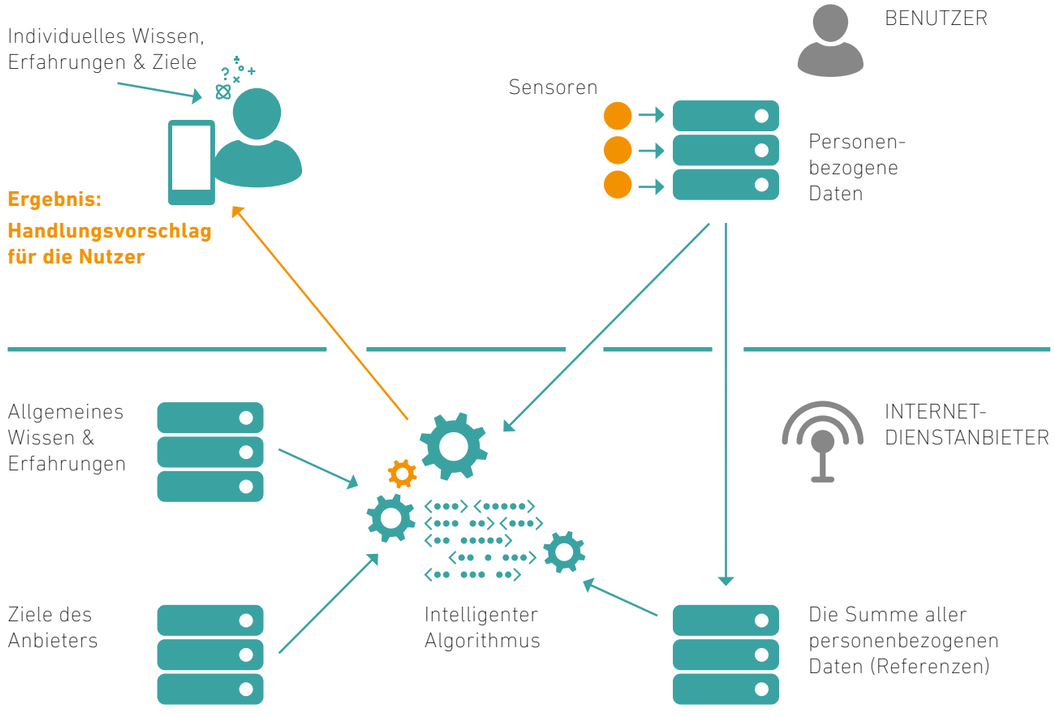
Wir brauchen eine leistungsfähige und unabhängige KI-Infrastruktur. KI ist eine Schlüsseltechnologie für das zukünftige Wirtschaftswachstum in allen Branchen und Wirtschaftsbereichen und muss deswegen geschützt werden. Dabei ist die Datenhoheit ein entscheidender Faktor bei der Verwendung von KI-getriebenen Technologien. Eine weitere wesentliche Bedeutung kommt der Verfügbarkeit von leistungsstarken KI-Infrastrukturen zu, um die KI-Anwendungen erfolgreich, sicher, qualitativ und souverän umsetzen zu können. Aber auch die Motivation eines KI-Ökosystems durch KMU/Start-up-Unterstützung/Förderung, Ausbildungsinitiativen, Internationalisierungskampagnen etc. ist maßgebend. Wichtig ist darüber hinaus, zu verstehen, dass KI zunehmend in Bereichen verwendet wird, in denen Deutschland traditionell sehr erfolgreich und souverän ist, zum Beispiel in der Automobilindustrie und in der Industrie-4.0-Branche. Als Querschnitts- und Schlüsseltechnologie kommt dem Bereich der KI eine elementare Funktion zur Erlangung und Aufrechterhaltung von technologischer Souveränität zu. Um diese erfolgreiche und vorhandene Souveränität in bedeutenden Branchen aufrechtzuerhalten, sollten mit der KI keine neuen Abhängigkeiten in den vorhandenen und erfolgreichen Branchen geschaffen werden.

Empfehlungen für den KI-Bereich:

1. Verfügbarkeit der Daten sicherstellen

Es muss dafür gesorgt werden, dass die erhobenen Daten zunehmend im deutschen/europäischen Raum gespeichert und verarbeitet werden, sodass die aktuelle und existenzgefährdende Abhängigkeit der eigenen Daten von außereuropäischen Unternehmen auf ein vertretbares Maß reduziert wird.

Hier empfiehlt es sich, Konzepte zu entwickeln, die besonders kritische Daten identifizierbar machen, welche ihrerseits nicht nur dezentral an europäischen Standorten gespeichert, sondern auch zusätzlich von öffentlichen Stellen vorgehalten werden. Damit kann sichergestellt werden, dass eine Verweigerung der Herausgabe der in anderen Hoheitsgebieten gespeicherten Daten als Druckmittel verwendet werden kann.



Nur so lassen sich die Verfügbarkeit der Daten und die Rechte unabhängig von der politischen und wirtschaftlichen Lage gewährleisten.

2. Leistungsstarke KI-Infrastruktur aufbauen
Außerdem muss der Aufbau einer leistungsstarken KI-Infrastruktur zur Berechnung von Wissen aus Daten mit KI-Algorithmen gefördert werden, um souverän das Wirtschaftswachstum in allen Branchen und Bereichen zu ermöglichen und voranzutreiben. Eine Lösung kann in der Förderung wie auch dem Aufbau von realen und virtuellen Hyperscaler-Infra-strukturen bestehen, sodass zukunftsweisende KI-Lösungen eigenständig und unabhängig für Innovationen entwickelt werden können. Dann sind wir auch in der Lage, KI als Schlüsseltechnologie sicher und qualitativ für den zukünftigen Erfolg unserer Gesellschaft zu nutzen.

3. Unterstützung des Mittelstands
Wir brauchen Förderungen für den Mittelstand, damit dieser KI optimal, qualitativ und souverän nutzen kann, um den zukünftigen Erfolg zu garantieren. Dazu sollten geeignete KI-Kompetenzzentren mit leistungsfähigen KI-Infrastrukturen und qualitativ hochwertigen Daten etabliert werden.

4. Die Selbstbestimmung und Autonomie der Nutzer sollten berücksichtigt werden.
Immer mehr Internetdienste machen Handlungsvorschläge für die Nutzer auf der Basis verschiedener Arten von Sensoren, wie Wearables oder Smartphones. Intelligente Algorithmen nutzen diese vielen privaten Sensordaten, bewerten sie und vergleichen sie mit privaten Daten anderer Nutzer. Zudem verwenden sie allgemeines Wissen und Erfahrungen, um Handlungsempfehlungen zu berechnen.

Das kann sehr nützlich sein, da KI viele Daten sehr schnell und intelligent auswerten kann. Der individuelle Mensch mit seinem persönlichen Wissen, seinen Erfahrungen und seiner Intuition sowie intelligente Algorithmen mit sehr vielen Daten und fast unbegrenzter Rechnerpower sind eine optimale Kombination.

Wenn die Internetdienste dies transparent und vertrauenswürdig leisten, bieten gut berechnete Handlungsempfehlungen einen hohen Nutzen.

Verdienen die Internetdienste aber mit solchen Serviceleistungen indirekt Geld, wird die berechnete Handlungsempfehlung eher im Interesse des Internetdienstes und dessen Kunden liegen als im Interesse der Nutzer. Jeder Nutzer wird zwangsläufig zum Produkt. Dadurch könnten Menschen ihre Selbstbestimmung verlieren. Das kann nicht im Sinne einer modernen Gesellschaft sein. Es sind Transparenz und Vertrauenswürdigkeit notwendig, die regulatorisch motiviert werden müssen.

3.2. CLOUD-DIENSTE FÖRDERN UND AUFBAUEN

Eine vollständige Cloudifizierung im Gegensatz zur heutigen nur teilweisen Nutzung von Cloud-Diensten wird sich durchsetzen. Es ist keine Frage von „ob in die Cloud", sondern lediglich, „wann".

Neben der KI-Fähigkeit sollten wir auch eigene Cloud-Dienste fördern, die unsere Sicherheits- und Wertestandards berücksichtigen, um für die normalen IT-Dienste wie Officeanwendungen, Kommunikationsdienste (E-Mail, Chat, Video etc.) usw. technologische Souveränität zu erreichen und damit die wirtschaftliche Leistungsfähigkeit insbesondere der KMUs und der Gesellschaft insgesamt aufrechtzuerhalten und zu stärken.

Das Projekt GAIA-X ist der richtige Ansatz, weil hier in Europa mit europäischen Anbietern „virtuelle Hyperscaler", eine Alternative zu den monolithischen Hyperscalern der außereuropäischen Marktführer, geschaffen werden sollen. Diese unterstützen dann auch hohe Cyber-Sicherheits-, ethische und Datenschutzstandards und die Portabilität der Daten. Wichtig ist, dass diese Idee konsequent und erfolgreich umgesetzt wird.

3.3. TECHNOLOGISCHE CYBER-SICHERHEIT ZUM SCHUTZ DER BÜRGER, WIRTSCHAFT UND GESELLSCHAFT

Die Cyber-Sicherheitsherausforderungen sind groß. Im Folgenden werden einige beschrieben und Handlungsempfehlungen aufgezeigt:

Wirtschaftsspionage
Laut dem Verein Deutscher Ingenieure (VDI) entstehen jährlich 100 Milliarden Euro Schaden durch Wirtschaftsspionage. Die Schäden beinhalten insbesondere Umsatzeinbußen von 23 Milliarden Euro durch Plagiate, Kosten von 18,8 Milliarden Euro durch Patentrechtsverletzungen und Verluste in Höhe von 13 Milliarden Euro durch Ausfall, Diebstahl oder Beeinträchtigung von IT-Systemen sowie Produktions- und Betriebsabläufen.

Die Angreifbarkeit der IT und des Internets wird immer größer und Werte, die als Bits und Bytes zur Verfügung stehen, werden zunehmend zum Risikofaktor für die einzelnen Unternehmen, die Bürger und den Staat. Experten aus der Cyber-Sicherheit, Wirtschaft und Politik müssen aktiv werden und mit den unterschiedlichen Stakeholdern geeignete Cyber-Sicherheitsmaßnahmen einleiten, um das Know-how deutlich wirkungsvoller zu schützen, damit die Digitalisierung risikoärmer und dadurch erfolgreicher umgesetzt werden kann.

Die Cyber-Sicherheitsmaßnahmen zur Prävention müssen deutlich mehr dem Stand der Technik genügen, um auch den stetig intelligenter werdenden Angriffen wirksam begegnen zu können.

Die verbleibenden Risiken müssen durch immer besser werdende Detektionsmaßnahmen identifiziert und Schäden mit passenden schnellen Reaktionen beherrschbar gemacht werden.

Cyber-War
Eine weitere und in wachsendem Maße bedeutsame Herausforderung ist Cyber-War. Angriffe auf kritische Infrastrukturen wie die Energieversorgung stellen eine prinzipiell höhere Verwundbarkeit der Gesellschaft dar und erreichen eine neue Qualität der existenziellen Bedrohung. Stuxnet hat seinerzeit dokumentiert, dass mit einem Kostenaufwand von rund 9 Millionen US-Dollar für eine intelligente Malware politische Ziele einfach und sehr erfolgreich umgesetzt werden können. Mit der intelligenten Malware Stuxnet konnten die Amerikaner und Israelis zusammen die Uranaufbereitung im Iran erfolgreich um zwei Jahre verzögern. Die Alternative zur Erreichung dieses politischen Ziels wäre gewesen, dass mehrere Hunderttausend Soldaten in den Iran einmarschiert wären, was nicht nur Kosten von mehreren Milliarden US-Dollar verursacht, sondern auch Menschenleben aufs Spiel gesetzt hätte.

Ein weiteres Risiko in diesem Bereich ist der „Kill Switch", also die Idee, dass andere Staaten die Technologie durch ihre Marktführer ausschalten lassen, zum Beispiel Betriebssysteme, Kommunikationstechnologie, Officelösungen, Datenbanken, Businessanwendungen, autonome Autos etc. Auf diese neue Wirklichkeit von Cyber-War muss professionell reagiert werden.

Dazu müssen passende und unabhängige Cyber-Sicherheitstechnologien entwickelt und genutzt werden. Außerdem sind die wichtigen Technologien auf ihre Vertrauenswürdigkeit aktiv und nachhaltig zu überprüfen.

Sicherstellung von IT-Sicherheitsinfrastrukturen und deren Diensten

IT-Sicherheitsinfrastrukturen und deren Dienste wie zum Beispiel für VPN, E-Mail-Verschlüsselung, elektronische Identitäten für Nutzer und IT-Geräte (IoT, Industrie 4.0, Autos etc.), Domänenzertifikate usw. sollten hinsichtlich der Herkunft von Technologien und Produkten in europäischer Verantwortung liegen und den Stand der Technik erfüllen.

In der Digitalisierung werden immer mehr Vertrauensdienste auf der Basis von PKI- und Blockchain-Technologien aufgebaut. Diese sind notwendig, um auf der einen Seite kritische Daten und Werte sicher und vertrauenswürdig ablegen und auf der anderen Seite die Verifikationen von Rechten, Abschlüssen, Besitzverhältnissen, Urhebern, Auslösern von Geschäften und weiteren Attributen umsetzen zu können.

Damit solche Technologien langfristig in der Lage sind, erfolgreich die Vertrauensdienste anzubieten und zu nutzen, sollte auch in die Kryptoagilität investiert werden. Deutschland muss es gelingen, sichere kryptografische Algorithmen eigenständig und unabhängig zu nutzen. Dazu gehört auch die Post-Quanten-Kryptografie.

Vorrangiges Ziel ist es, die eigene Souveränität von IT-Sicherheitsinfrastrukturen zu bewahren und – falls notwendig – wiederzuerlangen. Die technologische Souveränität ist ein essenzieller Baustein der digitalen Selbstbestimmung, insbesondere der IT-Sicherheitsinfrastrukturen.

3.4. DEFINITION, ENTWICKLUNG, NUTZUNG UND EVALUIERUNG VON OPEN-SOURCE-SOFTWARE

Die Entwicklungsparadigmen Security by Design, Privacy by Design sowie nachvollziehbare Qualitätssicherung müssen für alle IT-Lösungen bedingungslos definiert und umgesetzt werden, um mehr Sicherheit und Vertrauenswürdigkeit in der Digitalisierung zu erzielen.

Transparenz ist eine wichtige Voraussetzung für Vertrauen. Offene Systeme, IT-Architekturen und IT-Produkte erlauben es, Sicherheit und Vertrauenswürdigkeit zu überprüfen. Ein Großteil unserer Gesellschaft funktioniert zurzeit mit und dank Open-Source-Software.

Die Qualität und die Prozesse rund um die Entwicklung der quelloffenen Software bergen zurzeit großes Verbesserungspotenzial bezüglich Sicherheit und Vertrauenswürdigkeit in der IT. Das Verbesserungspotenzial für sichere und vertrauenswürdigere Software, insbesondere Open-Source-Software, muss gemeinsam erfolgreich gefördert, gefordert und genutzt werden.

> „Es ist keine Frage von **‚ob in die Cloud'**, sondern lediglich, **‚wann'** und wie sicher."

Eine (Mit-)Verantwortung aller nutzenden Firmen für wichtige Open-Source-Komponenten muss übernommen werden.

Der gemeinsame Aufbau eines Fonds, um finanzielle Mittel für die Verbesserung der Softwarequalität von wichtigen Open-Source-Komponenten zur Verfügung zu stellen, könnte ein geeigneter Ansatz sein, um die Sicherheit und Vertrauenswürdigkeit sowie die technologische Souveränität zu steigern.

Neben der Durchführung regelmäßiger Sicherheitsassessments weitverbreiteter und gemeinsam genutzter Software sollten die Formulierung und Förderung von wünschenswerten, kollektiv nutzbaren Open-Source-Technologien aktiv von allen Stakeholdern vorangetrieben werden.

Diese Entwicklung kann und sollte auch mit der internationalen Staatengemeinschaft gemeinsam umgesetzt werden, um internationale Interoperabilität zu gewährleisten sowie preisgünstige und notwendige Innovation in Gang zu bringen. Wir sollten uns im Schwerpunkt auf die Verifizierung der Open-Source-Technologien konzentrieren, um die Sicherheits- und Wertestandards gewährleisten zu können. Auch sollte sichergestellt werden, dass eine eigene Weiterentwicklung personell und finanziell möglich ist.

Langfristig signifikante Softwarebereiche, in denen Open-Source-Technologien für die technologische Souveränität besonders wichtig sein können, sind Officeanwendungen, Datenbanken, Router, IoT-Frameworks, KI-Technologien, Cyber-Sicherheitslösungen usw.

ABSTRACT

Deutschland spielt zurzeit im Bereich der IT und des Internets keine besondere Rolle bei Technologien, Diensten und Plattformen. Die technologische Souveränität ist ein immer wichtiger werdender Faktor für die gesamte Volkswirtschaft und Wettbewerbsfähigkeit Deutschlands, insbesondere weil in Zukunft in allen Branchen der Wertschöpfungsanteil von IT und Internet zunehmen wird. Technologische Souveränität eröffnet Wirtschaft, Politik und Gesellschaft Gestaltungsmöglichkeiten. Um diese Möglichkeiten auszuschöpfen und zu gestalten, müssen mit allen Stakeholdern, also Herstellern und Anwendern von IT-Technologie, sowie Wissenschaft, Politik und Verwaltung gemeinsame Ziele definiert und umgesetzt werden. Besonders wichtig sind dabei die folgenden Aspekte:

- Die technologische Fähigkeit im Bereich der Künstlichen Intelligenz fördern und aufbauen.
- Cloud-Dienste fördern und aufbauen, um in den Bereichen Officeanwendungen, Kommunikationsdienste wie E-Mail, Chat, Video usw. souverän zu bleiben.
- Technologische Cyber-Sicherheit zum Schutz der Bürger, Wirtschaft und Gesellschaft fördern und ausbauen.
- Open-Source-Software als strategisches Instrument motivieren und erfolgreich für wichtige Bereiche umsetzen und dabei den besonderen Schwerpunkt auf die Verifizierung der Softwarequalität, Sicherheit und Vertrauenswürdigkeit legen.
- Die Evaluierung- und Zertifizierung von IT-Technologien und -Diensten insbesondere von außereuropäischen Anbietern sicherstellen.
- Mehr international standardisieren, um frühzeitig mitgestalten zu können.

Literatur

- C. Eckert: „Impuls: Technologische Souveränität: Voraussetzung für mehr Cyber-Sicherheit", 2020
- N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2019
- Bundesverband IT-Sicherheit – TeleTrusT: Handreichung zum „Stand der Technik", Berlin 2020 https://www.teletrust.de/publikationen/broschueren/stand-der-technik/
- N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit – Unausgegoren aber notwendig", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019

DIGITALE UND SMARTE STÄDTE DER ZUKUNFT

Wie wir deren Resilienz und Sicherheit erhöhen und die Privatheit ihrer Bewohner schützen können

Die Entstehung von Städten in den vergangenen Jahrhunderten war gekennzeichnet durch das Schaffen von vorteilhaften Rahmenbedingungen für eine Vielzahl von Interessengruppen. Ihre Infrastrukturen und Umgebungsbedingungen ermöglichten den Bewohnern ein sicheres und angenehmes Leben. Regeln und Gesetze erlaubten es, Dienste bereitzustellen und zu konsumieren, Handel und Austausch mit anderen Städten führten zu einer ständigen Erneuerung und Weiterentwicklung. Physische Transportinfrastrukturen waren eine wichtige Voraussetzung dafür: Straßen, Eisenbahnen und öffentlicher Verkehr beschleunigten den Austausch von Waren und die Mobilität von Menschen – und damit den Austausch von Wissen. Diese jahrhundertelange Entwicklung gewann in den letzten Dekaden massiv an Fahrt: 1930 lebten rund 30 Prozent der Weltbevölkerung in Städten, 2010 etwa 50 Prozent. Prognosen zufolge werden 2050 rund zwei Drittel der Weltbevölkerung in Städten leben.[1] Dieser Urbanisierungstrend wird durch anpassungsfähige und effiziente kritische Infrastrukturen in den Sektoren Energie, Verkehr und Logistik, Gesundheit, Ernährung, Wasser, Finanz- und Versicherungswesen sowie Staat und Verwaltung angefacht.

Seit einigen Jahren ist die Transformation von über Jahrhunderte gewachsenen Städten hin zu smarten Städten zu beobachten, während gleichzeitig neue, von Grund auf digital konzipierte Städte entstehen. Informations- und Kommunikationstechnologie (IKT) stellt den digitalen Widerpart zu den genannten physischen Transportinfrastrukturen dar und wir sehen – quasi im Zeitraffer – vergleichbare Entwicklungen. Der digitale Raum zieht eine zunehmende Anzahl von Menschen an und schafft vorteilhafte Bedingungen für Handel, Wissensaustausch etc. Gleichzeitig ist die Bevölkerung bisher noch nicht so tief in der digitalen Welt verwurzelt wie in der physischen Welt.

Unter einer digitalen, smarten Stadt verstehen wir das komplex vernetzte cyberphysische System, das die physischen Funktionen und Aktivitäten in der Stadt durch einen mittels moderner IKT geschaffenen digitalen Raum erweitert sowie eine Vielzahl von neuen und verbesserten Diensten ermöglicht.[2,3,4] Der Anspruch an diese Dienste muss ähnlich sein wie der Anspruch an bestehende physische Dienste und Infrastrukturen: Die ständige Verfügbarkeit von Wasser-, Energie-, Verkehrs- oder IKT-Dienstleistungen ist in vielen Ländern zur Selbstverständlichkeit geworden. Der störungsfreie und nahtlose Betrieb von Infrastruktursystemen repräsentiert das Selbstverständnis und den Zustand der technischen, sozialen und politischen Stabilität hoch technisierter Gesellschaften. Heute maßgeblich für die Anpassungsfähigkeit und Effizienz dieser Infrastrukturen ist der ubiquitäre Einsatz von Informations- und Kommunikationstechnologie.[5] In der digitalen Stadt schaffen mit IKT durchsetzte soziotechnische Systeme die Grundlage für eine optimierte Zirkulation von Personen, Gütern, Stoffen und Informationen. Gleichzeitig werden nicht öffentliche Bereiche von Städten wie Privathaushalte, Individualverkehr und Wirtschaft verstärkt von IKT durchdrungen. Somit ergeben sich erhebliche Abhängigkeiten von IKT-Systemen, die mit steigender Vernetzung weiter zunehmen.

In solchen digital vernetzten Städten ist die Funktionsfähigkeit der IKT-gestützten Infrastrukturen durch Naturereignisse, menschliches und technisches Versagen sowie Gewalt und Terror gefährdet. Ein systematisches Verständnis der Verwundbarkeit digitaler Städte und wirksame Maßnahmen zur Erhöhung ihrer Resilienz und Sicherheit sowie der Privatheit ihrer Bewohner sind dringend erforderlich, fehlen aber bisher.

1. RESILIENZ, SICHERHEIT UND PRIVATHEIT – DEFINITIONEN

Resilienz, Sicherheit und Privatheit in digitalen, smarten Städten müssen stets gemeinsam für die physischen und digitalen Aspekte betrachtet werden und gehen daher über bisherige isolierte Betrachtungen in nur einer dieser Domänen hinaus.[6,7] Unter Resilienz, Sicherheit und Privatheit verstehen wir:

Resilienz. Signifikante Systemschwankungen, Schock- oder Krisenereignisse (nachfolgend zusammengefasst als „Krisen" bezeichnet) stellen den angestrebten Normalzustand von digitalen, smarten Städten infrage, indem sie die Verfügbarkeit der kritischen IKT-Infrastrukturen beeinträchtigen. Urbane Resilienz[8] als Gegenpol bezeichnet die Fähigkeit der Stadt, Krisen und Gefahrensituationen zu bewältigen, sich mit Widerstandskraft zeitnah und nachhaltig von den Auswirkungen zu erholen und die notwendigen Grundstrukturen wiederherzustellen. In smarten Städten rückt damit IKT-Resilienz – das betrifft vor allem die Eigenschaften Widerstands-, Anpassungs- und Wandlungsfähigkeit – in das Zentrum der Aufmerksamkeit, um die Funktionsfähigkeit der Städte möglichst jederzeit zu gewährleisten.[9] Ein besonderes Augenmerk liegt hierbei auf kritischen Infrastrukturen.[10]

Sicherheit. Der Begriff „Sicherheit" umfasst im Deutschen sowohl Schutzaspekte (engl. „security") als auch Aspekte der Abwesenheit von Gefahr oder Betriebssicherheit (engl. „safety"). Für cyberphysische Systeme und damit für digitale Städte sind beide Aspekte gleichermaßen relevant. Klassische Schutzziele umfassen die Vertraulichkeit, die Integrität sowie die Verfügbarkeit. Betriebssicherheit beinhaltet insbesondere die Abwesenheit von Gefahren für den Nutzer durch Ausfälle von Komponenten oder (Teil-)Systemen ohne Fremdeinwirkung. Sicherheitsherausforderungen für smarte Städte wurden bisher nur unzureichend untersucht.[11] Die IKT von Städten besitzt eine inhärent große Angriffsfläche durch die hohe Anzahl langlebiger kritischer und vernetzter Systeme. Die Vernetzung und gegenseitige Abhängigkeiten führen im Angriffsfall zu Kaskadeneffekten, die Langlebigkeit der Systeme überfordert die heutige Herangehensweise an Betrieb und Wartung von IKT-Systemen.[12] Besondere Aufmerksamkeit kommt der gemeinsamen Betrachtung von Schutz und Gefahrlosigkeit zu, da beide Aspekte interagieren: erfolgreiche Cyber-Angriffe (unzureichender Schutz) auf kritische Infrastrukturen können zur Gefahr für Leib und Leben der Bevölkerung führen.

Privatheit. Das Konzept der Privatheit hat sich in der westlichen Kultur über Jahrhunderte etabliert – auch einhergehend mit der Entwicklung von Städten. Ein wichtiger Aspekt der Privatheit umfasst das Recht der Selbstbestimmung, welche Daten anderen Nutzern verfügbar gemacht werden sollen. Konzepte in Bezug auf Datensparsamkeit bzw. auf die Kontrolle der Datenweitergabe sollen helfen, diese informationelle Selbstbestimmung umzusetzen. Die großflächige und ständige Erhebung, Speicherung und Verarbeitung von Daten in digital vernetzten Städten stehen der Privatheit des einzelnen Nutzers entgegen. Zielkonflikte zwischen Nutzern und Diensteanbietern sind damit vorprogrammiert. Alltagsnutzer erleben das Netz als immer undurchsichtiger, sich selbst im Netz aber als immer durchsichtiger bzw. gläserner. Transparenz der IKT-Systeme sowie Vertrauen in angebotene Dienste können helfen, diese Schieflage zu korrigieren.[13]

Städte befinden sich international im Wettbewerb um die kreativsten und klügsten Köpfe. Dabei spielt Digitalisierung eine wichtige Rolle. Welche Bedeutung haben dabei die Faktoren Resilienz, Sicherheit und Privatheit? Die nachfolgende Tabelle gibt eine Übersicht über ausgewählte digitale, smarte Städte sowie deren Selbstverständnis in Bezug auf Resilienz, Sicherheit und Privatheit.[14]

[1] United Nations, World Urbanization Prospects: The 2018 Revision, 2018.
[2] A. Cocchia, „Smart and Digital City: A Systematic Literature Review", in, Smart City. Progress in IS, R. Dameri, C. Rosenthal-Sabroux, C. (Hrsg.), Cham, 2014.
[3] I. Schieferdecker, L. Bruns, S. Cuno, M. Flügge, K. Isakovic, J. Klessmann, P. Lämmel, D. Stadtkewitz, N. Tcholtchev. C. Lange, B. T. Imbusch, L. Strauß, A Vastag, F. Flocke, V. Kraft, Urbane Datenräume – Möglichkeiten von Datenaustausch und Zusammenarbeit im urbanen Raum, Fraunhofer Fokus, Berlin, 2018.
[4] C. Harrison, B. Eckmann, R. Hamilton, P. Hartswick, J. Kalagnanam, P. Williams, "Foundations for Smarter Cities", in IBM Journal of Research and Development Bd. 54, 2010, Nr. 4, S. 1–16.
[5] A. Caragliu, C. del Bo, P. Nijkamp, „Smart cities in Europe", in Journal of Urban Technology, Bd. 18, 2011, Nr. 2, S. 65–82.
[6] T. Braun, B.C.M. Fung, F. Iqbal, B. Shah, „Security and privacy challenges in smart cities", in Sustainable cities and society, Bd. 39, Elsevier, 2018, S. 499–507.
[7] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, X.S. Shen, „Security and Privacy in Smart City Applications: Challenges and Solutions", in IEEE Communications Magazine Bd. 55 (2017), Nr. 1, S. 122–129.
[8] Definition nach United Nations Office for Disaster Risk Reduction. URL: www.unisdr.org/we/inform/terminology
[9] M. Hollick, A. Hofmeister, J. I. Engels, B. Freisleben, G. Hornung, A. Klein, M. Knodt, I. Lorenz, M. Mühlhäuser, P. Pelz, A. Rudolph-Cleff, R. Steinmetz, F. Steinke, O. von Stryk. „The Emergency Responsive Digital City". in World Congress on Resilience, Reliability and Asset Management, WCRRAM, 2019.
[10] M. Hollick, S. Katzenbeisser, „Resilient Critical Infrastructures", in Information Technology for Peace and Security, Ch. Reuter, Springer Fachmedien, Wiesbaden, 2019, S. 305–318.
[11] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler,A.A. Kountouris, D. Barthel, „Security and Privacy in your Smart City" in Proceedings of the Barcelona smart cities congress, Bd. 292, 2011, S. 1–6.
[12] R. Kitchin, M. Dodge, „The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention", in: Journal of Urban Technology, Bd. 26, 2019, Nr. 2, S. 47–65.
[13] Vgl. https://www.informatik.tu-darmstadt.de/privacy-trust/privacy_and_trust/index.en.jsp
[14] Eigene Recherche auf Basis der offiziellen Webseiten der genannten Städte sowie städtischer Initiativen zur Digitalisierung, Stand 01.11.2019.

AUSGEWÄHLTE DIGITALE, SMARTE STÄDTE UND DEREN SELBSTVERSTÄNDNIS

STADT, LÄNDERKÜRZEL	SELBSTVERSTÄNDNIS UND BEZUG ZU RESILIENZ, SICHERHEIT, PRIVATHEIT
Amsterdam, NL	**Nachhaltigkeit, Datensicherheit und -schutz explizit genannt.** Amsterdam Smart City (Public Private Partnership); Digitalisierung mit Fokus auf Gesundheit, nachhaltige Mobilität, Bürgernähe, soziale Probleme, Müllreduzierung; Verweis auf Datensicherheit und Privatheit.
Barcelona, ES	**Starker Fokus auf Resilienz und Privatheit.** Sehr fortschrittlich, mit Strategiedokumenten und Maßnahmenpaketen belegt; hat ein „Department of Urban Resilience" (Fokus Ökologie, Nachhaltigkeit), ein „Urban Resilience Model" (Fokus Naturkatastrophen) und ein Konzept für „Barcelona as a Digital City" mit expliziter Nennung von Datensouveränität, Ethik und Privatheit; Mitbegründung eines Städtenetzwerks zum Schutz digitaler Rechte; Kooperationen mit UN-Habitat, „City Resilience Profiling Programme"; UNISDR, „Making Cities Resilient"-Kampagne.
Berlin, DE	**Keine gesonderte Betrachtung von Resilienz, Sicherheit, Privatheitsschutz.** Smart-City-Strategie Berlin 2015, Fokus Klimaschutz, Energieeinsparung, Wirtschaftsförderung, demografischer Wandel, Handlungsfelder: Verwaltung und Stadtgesellschaft, Wohnen, Wirtschaft, Mobilität, Infrastrukturen und öffentliche Sicherheit; Nennung von Resilienz nur im Hinblick auf Klimaanpassung.
Boston, US	**Kein Fokus auf Sicherheit, Datenschutz oder IKT-Resilienz.** Resilienz mit Fokus auf Klimaschutz, aber auch soziale Ungleichheit (als langsam wirkende Katastrophe); Smart City vor allem mit Fokus auf Straßenüberwachung und Verkehrssicherheit (hier Hinweis auf Datenschutz).
Chicago, US	**Resilienz kritischer Infrastrukturen explizit genannt.** Resilienzstrategie, Fokus: Klimaschutz, soziale Ungleichheit (als chronische Katastrophe), Kriminalität, Bereitstellung kritischer Infrastrukturen, Vorbereitung und Beteiligung der Bevölkerung, Gesundheitsschutz; Smart City, Fokus auf E-Government und Wirtschaftsförderung.
Darmstadt, DE	**Fokus auf IT-Sicherheit, Datenschutz und IKT-Resilienz.** Sicherheit, Privatheit und Resilienz sind Handlungsfelder der Stadt und werden gemeinsam mit den Forschungszentren emergenCITY (Resilienz) und ATHENE (Sicherheit und Privatheit) entwickelt. Wurde vom Branchenverband Bitkom zur Digitalstadt gekürt; Green Smart City (Kooperation mit House of IT).
Dubai, AE	**Nachhaltigkeit, Sicherheit und Resilienz explizit genannt.** Smart Dubai 2021, Fokus: Glück, Kosteneinsparung, Sicherheit (von Personen und Informationen), nachhaltige und resiliente Infrastrukturen; sehr umfassend; Office of Smart City Impact Management.
Kopenhagen, DK	**Starker Fokus auf Nachhaltigkeit ohne dedizierte Hervorhebung von IKT-Aspekten.** Nachhaltigkeit, Verkehr; Smart City umfasst zwei Labs im Stadtraum (Solutions Lab und Energy Lab) sowie Smart Parking, Fokus auf Folgen des Bevölkerungswachstums; Sicherheit nur als öffentliche Sicherheit.
Melbourne, AU	**Explizite Nennung von Resilienz und IT-Sicherheit.** Umfassende Resilienzstrategie, Fokus auf alle Krisenphasen, Berücksichtigung chronischer Belastungen (Klimawandel, soziale Ungleichheit, Arbeitslosigkeit, Bevölkerungswachstum) und akute Schocks (Umweltkatastrophen, [Cyber-] Angriffe, Seuchen, Infrastrukturnotfälle), Lernen aus vergangenen Krisen (historische Perspektive); Smart-City-Konzept, Fokus auf Mobilität, Lebensqualität, Nachhaltigkeit.
Shanghai, CN	**Sicherheit und Privatheit entsprechen einer Überwachungsstadt.** Gesichtserkennung ist weit verbreitet, soziales Fehlverhalten wird digital erfasst und sanktioniert. Resilienz v. a. im Hinblick auf Klimawandel und Naturkatastrophen.
Singapur, SG	**IT-Sicherheit und Datenschutz als Voraussetzung für smarte Entwicklung genannt.** „Smart Nation Singapore" ist eine der sichtbarsten smarten Städte. Fokus auf Digital Economy und Digital Government, Mobilität; Privacy und Cyber-Security als Voraussetzungen für smarte Entwicklung.
Tokio, JP	**Nachhaltigkeit explizit genannt. Keine Nennung von IKT-Resilienz, Sicherheit und Privatheit.** Smart City mit Fokus auf Klimaschutz, Energieeinsparung, nachhaltige Entwicklung, Wirtschaftsförderung; Resilienz mit Fokus auf Naturkatastrophen; oft Verweis auf Olympische Spiele.
Toronto, CA	**Keine explizite Nennung von IKT-Resilienz. Sicherheit und Privatheit durch privates Betreibermodell gegeben.** Digitales Gründerviertel: Die Sidewalk Labs (Google) beabsichtigen, den Prototyp einer digital vernetzten Stadt der Zukunft zu erschaffen. Private Anbieter dominieren die Daten und es besteht Uneinigkeit über die Frage der Privatheit. Für Toronto gesamt: „Resilience Strategy" und „Resiliene Office", Fokus vor allem auf Naturkatastrophen, Klimawandel, Ungerechtigkeit, Wohnungsnot, demografischer Wandel; sozialer Zusammenhalt als Voraussetzung für Resilienz, Smart-City-Konzept v. a. im Hinblick auf Mobilität, E-Government, Wirtschaftswachstum, gleichberechtigter Zugang.
Wien, AT	**Keine explizite Nennung von IKT-Resilienz, Sicherheit oder Privatheit.** Umfassende Smart-City-Strategie, Fokus auf Lebensqualität, Klimaschutz, Ressourcenschonung und Versorgung/Infrastruktur in den Bereichen Energie, Gebäude, Mobilität, Infrastruktur, Informationstechnologien.

Digitale und smarte Städte der Zukunft

2. HERAUSFORDERUNG

Im Folgenden betrachten wir ausgewählte wichtige Herausforderungen smarter Städte, die in direktem Bezug zu IKT-Resilienz, Sicherheit und Privatheit stehen.

2.1. Technologische Treiber und Hürden

Die Entwicklung digitaler Städte profitiert einerseits von der rasanten Entwicklung des Internets der Dinge sowie dem damit einhergehenden Preisverfall von IKT. Andererseits wird über das Ausbringen von IKT in kritische städtische Infrastrukturen deren Angriffsfläche und damit die Verwundbarkeit der gesamten Stadt signifikant erhöht. Beispielhaft seien millionenfach ausgebrachte Sensoren wie Kameras im öffentlichen Raum genannt – aber auch private Endsysteme wie Smartphones, Smartwatches und Smartspeaker, die uns im Alltag begleiten und fortwährend Daten erheben. Gemeinsam mit den Berechnungsfähigkeiten in der Cloud sind sie die Basis für smarte Städte.

Allerdings sorgen der Kostendruck sowie der Fokus auf Funktionalität vor Sicherheit dafür, dass der Stand der IT-Sicherheit für die genannten vernetzten Geräte

Copyright: Unsplash/hughhan

in weiten Teilen in einem schlechten Zustand ist. Eine kontinuierliche Pflege der Systeme ist nicht sichergestellt, Softwareupdates stehen nur für kurze Zeiträume bereit. Dies steht in direktem Gegensatz zu den langlebigen und häufig über Jahrzehnte in Betrieb befindlichen städtischen Infrastrukturen.

2.2. Neue Schutzziele und Schutzziele mit neuem Fokus

In klassischen IKT-Systemen stehen meist die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit an erster Stelle. In der jüngeren Vergangenheit werden zunehmend Fragen zur Privatheit thematisiert.[15] Mit dem Übergang hin zu digitalen Städten bekommen klassische Schutzziele durch die Vernetzung von physischer und digitaler Welt einen neuen Fokus. Integrität und Verfügbarkeit werden wichtiger, wenn Leben an der IKT hängen.[16] Für die Zielerreichung sind klassische risikobasierte Ansätze nicht mehr ausreichend. Resilienzbasierte Ansätze stellen eine vielversprechende Option dar, um die Funktionsfähigkeit der Städte möglichst jederzeit zu gewährleisten.

2.3. Smarte Entscheidungen – Menschen im Fokus, aber ohne eigene Stimme

Der Charme digital vernetzter Städte wird nicht zuletzt von dem Mythos gespeist, dass die Verfügbarkeit umfassender Sensordaten in Kombination mit Künstlicher Intelligenz automatisch zu smarten Städten führt. Die Definition und Ausgestaltung entsprechender Systeme erfolgen aktuell allerdings überwiegend durch Wirtschaftsunternehmen mit dem Ziel der Profitmaximierung. Die Rolle der Bevölkerung kann bisher als ungeklärt gelten und spielt sich zwischen unmündigen Empfängern der Vorgaben von Unternehmens-KI sowie freiheitlichen Gestaltern ihrer eigenen digitalen Zukunft ab. Die Gewährleistung der Privatheit der Nutzer bei gleichzeitiger Ermöglichung von smarten Entscheidungen ist bisher nur unzureichend erforscht.

3. LÖSUNGSANSÄTZE

In einer Stadt mit fragiler IKT kann diese auch nicht zur urbanen Resilienz beitragen. Kritische Infrastrukturen können in einer Stadt mit unsicherer IKT nicht zuverlässig betrieben werden. Eine Stadt, die Privatheitsschutz nicht erzwingt, kann ihren BürgerInnen nicht die Wahl lassen, was mit privatheitskritischen Daten geschehen soll. Technische Lösungen müssen daher von Grund auf resilient, sicher und privatheitserhaltend konzipiert werden („Resiliency by Design", „Security by Design" und „Privacy by Design").

Resiliente IKT erlaubt der digitalen Stadt, durch Vernetzungsaspekte hervorgerufene kaskadierende Ausfälle zu minimieren und die Dysfunktion der digitalen Stadt zu vermeiden. Gleichzeitig ermöglicht sie der digitalen Stadt, in einen Notbetrieb zu gehen und schrittweise überlebenswichtige sowie zur Krisenbewältigung hilfreiche Dienste anzubieten. Dies gestattet der Bevölkerung, mit IKT-Unterstützung eine effektive Selbsthilfe zu organisieren und die Interaktion mit Rettungskräften zu optimieren. Behörden und Rettungskräfte können – unter Mithilfe der Bevölkerung – die Situation in der Stadt erfassen, analysieren und im Rahmen ihrer Krisenreaktion beeinflussen. Auf Basis der vor und während der Krise gesammelten Daten kann Wissen zur Stärkung der digitalen Stadt und zur künftigen Krisenprävention gewonnen werden, was den Umgang mit künftigen Krisen vereinfacht. Schlussendlich kann resiliente IKT auch im Normalbetrieb dafür sorgen, dass signifikante Systemschwankungen und Schocks in der digitalen Stadt besser absorbiert werden bzw. eine Adaption oder ein Übergang in einen wünschenswerten Betriebszustand erfolgen kann.

Gleichermaßen steigt die Bedeutung der IT-Sicherheit sowie des Privatheitsschutzes. Die Wichtigkeit der Schutzziele Integrität und Verfügbarkeit nimmt zu, wenn IKT in kritischen Umgebungen zum Einsatz kommt. Sicherheitsplattformen können die Hürde und die Kosten für den Einsatz von angemessener Sicherheitstechnologie dramatisch senken.[17] Gleichzeitig besteht Forschungs- und Innovationsbedarf. Privatheit ist von herausragender Bedeutung, wenn die Interessen der Bürger berücksichtigt werden. Digitalisierung erfolgt bisher stark profitgetrieben und daher meist mit dem Menschen als „Datenlieferanten" und nicht als „Souverän". Die Stärkung der Rechte der Bürger ist technisch möglich, erfordert aber weitreichende Regulierung und eine Abkehr von bestehenden Nutzungsmodellen.

4. HANDLUNGSEMPFEHLUNGEN

4.1. Gemeinsam: Bürger, Politik, Wirtschaft, Wissenschaft

Die Digitalisierung von Städten geht Hand in Hand mit der Digitalisierung aller Lebensbereiche und der Digitalisierung ihrer Bewohner. Menschen haben traditionell die Rolle von Sensoren („Fühle ich mich sicher?", „Brauche ich einen Regenschirm?", „Sieht das Restaurant appetitlich aus?") und gleichzeitig Entscheidern/Aktoren eingenommen („Ich nehme den Bus, um nicht nass zu werden!", „Ich entscheide mich für dieses Restaurant!"). Smarte Städte sollen dem Bürger zur Seite stehen und ihn bei diesen Prozessen unterstützen. Die heutige Realität ist eine andere: Nutzer sind Datenlieferanten in einem für sie intransparenten Entscheidungsprozess. Ihre Daten werden ohne Rückfrage vermarktet, sie werden geflutet von Werbung und verlieren zunehmend die Möglichkeit, einer ständigen Überwachung zu entgehen.

> *„Nutzer sind Datenlieferanten in einem für sie **intransparenten** Entscheidungsprozess."*

Zielkonflikt: Unterschiedliche Stakeholder haben unterschiedliche Ansprüche und Interessen. Bürger wollen bestmögliche Dienste unter Wahrung ihrer Privatheit (Bürger als Datensouverän), Firmen streben vollständiges Wissen an, um ihren Gewinn zu maximieren (Bürger als Datenlieferant). Demokratische wie autoritäre Regierungen streben Kontrolle an (Bürger als Staatsbürger/Bürger als Teil der Stadtgesellschaft).

[15] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, X.S. Shen, „Security and Privacy in Smart City Applications: Challenges and Solutions", in: IEEE Communications Magazine, Bd. 55 (2017), Nr. 1, S. 122–129.
[16] T. Braun, TB. C. M. Fung, F. Iqbal, B. Shah, „Security and privacy challenges in smart cities", in Sustainable cities and society, Bd. 39, Elsevier, 2018, S. 499–507.
[17] DIN SPEC 91357:2017-12. Reference Architecture Model Open Urban Platform (OUP). https://dx.doi.org/10.31030/2780217

Empfehlung: Um im städtischen Raum eine demokratische Kontrolle über die Daten zu erhalten, müssen entsprechende Vorgaben gemacht werden. Kritische städtische Infrastruktur sollte bevorzugt in öffentlicher Hand liegen, oder, falls dies nicht möglich ist, durch geeignete Betreibermodelle so betrieben werden, dass die Anforderungen der Bevölkerung als wichtigstem Stakeholder erfüllt werden.

4.2. Sicherheit ohne Wenn und Aber

In digitalen, smarten Städten können unsichere IKT-Systeme Leib und Leben gefährden. Daher müssen Schutz (Security) und Gefahrlosigkeit/Betriebssicherheit (Safety) durchgängig und langfristig gewährleistet sein. Im Bereich der Verbraucherelektronik haben wir in den letzten Jahrzehnten ein nur durchschnittliches Sicherheitsniveau hingenommen, da die Auswirkungen nur selten dramatisch waren. Die gleichen Systeme werden künftig Teil von smarten Städten oder können auf die Systeme der Stadt einwirken.

Zielkonflikt: Digitalisierung verspricht Effizienz und Kostenreduktion. Sicherheit ist ein kontinuierlicher Prozess, der von der Entwicklung über die Produktion bis hin zum Betrieb Mehraufwand und -kosten verursacht. Allerdings werden aktuell die Marktteilnehmer bevorzugt, die den schnellen Aufbau eines Kundestamms durch die Fokussierung auf neue Funktionalität – und dabei häufig auf Kosten der Sicherheit – durchführen.

Empfehlung: Sicherheit muss eine verpflichtende Systemeigenschaft werden („Security by Design") und unsichere IKT muss aus digital vernetzten Städten verbannt werden, denn sie kann kritische Infrastrukturen beeinträchtigen und damit Menschenleben kosten. Hersteller müssen verpflichtet werden, ihre Geräte, Dienste und Anwendungen über die komplette Lebenszeit mit Sicherheitsupdates zu versorgen.

4.3. Privatheit ohne Wenn und Aber

In einer smarten Stadt wird die Bevölkerung jederzeit und überall überwacht, um die Daten und Informationen zu sammeln, die die Stadt für smarte Entscheidungen benötigt. Bürger haben aktuell keine Möglichkeit des „Opt-out" und es ist nicht regulär möglich, in die Datenerhebung/-nutzung einzuwilligen bzw. diese Einwilligung zu widerrufen.

Zielkonflikt: Die erhobenen Daten haben einen immensen Wert – für den Nutzer, für Firmen, für die Stadt sowie für Regierungen allgemein. Das Missbrauchspotenzial ist hoch: Firmen und Regierungen können NutzerInnen umfassend überwachen. Das einmal gewonnene Wissen kann auch gegen die Interessen von Individuen und der Bevölkerung als Ganzes eingesetzt werden.

Empfehlung: Daten- und Privatheitsschutz muss verbindlich und von Beginn an im kompletten IKT-System verankert sein („Privacy by Design"). Unsere digitalen, smarten Städte dürfen sich nicht zu Überwachungsstädten verwandeln, die unserer freiheitlichen, demokratischen Grundordnung diametral gegenüberstehen. Um im städtischen Raum eine demokratische Kontrolle über die Daten zu erhalten, müssen entsprechende Vorgaben gemacht und Anreize geschaffen werden.

4.4. Resilienz als Systemeigenschaft

Kritische Infrastrukturen können in einer Stadt mit unsicherer IKT nicht zuverlässig betrieben werden. Heutige technische Lösungen fokussieren meist auf Effizienz und Kosteneinsparung, ohne der stetig zunehmenden Kritikalität und Vulnerabilität durch immer komplexere vernetzte Infrastrukturen ausreichend Rechnung zu tragen.

Zielkonflikt: Die zunehmende Komplexität digitaler Städte erschwert, dass deren IKT-gestützte Funktionen und Prozesse verfügbar, verständlich und beherrschbar bleiben. Ein systematisches Verständnis der Verwundbarkeit von IKT sowie wirksame Maßnahmen zur Erhöhung ihrer Resilienz fehlen bisher. Dabei müssen sowohl der effiziente Normalbetrieb als auch ein Betrieb/Notbetrieb im Krisenfall für kritische Infrastrukturen in den Sektoren Energie, Verkehr und Logistik, Gesundheit, Ernährung, Wasser, Finanz- und Versicherungswesen sowie Staat und Verwaltung garantiert werden.

Empfehlung: Resilienz für und durch IKT muss zum Leitziel werden. Resilienz für IKT erlaubt in einem ersten Schritt, diese IKT auch in kritischen Anwendungsdomänen langfristig sicher einzusetzen. In einem zweiten Schritt können dann sämtliche Prozesse durch IKT unterstützt werden und dabei an Verfügbarkeit und Sicherheit gewinnen.

5. AUSBLICK

Ist es möglich, digitale, smarte Städte zu konzipieren, die freiheitlich und demokratisch sind und dafür in ihrer DNA die notwendigen Gene für Resilienz, Sicherheit und Privatheit tragen?
Das folgende Gedankenexperiment soll zeigen, dass die heute vorherrschenden Realisierungen technischer Systeme nicht eins zu eins auf künftige digitale Städte übertragen werden müssen und die Antwort auf die Eingangsfrage „Ja!" lauten kann. Können Sie sich vorstellen, dass Ihr Smartphone Informationen über nahegelegene gute Restaurants geben kann, ohne dass Ihr Standort kontinuierlich an den Kartenanbieter gesendet wird? Können Sie sich vorstellen, dass es Geschäftsmodelle für digitale Dienste geben kann, ohne dass Werbetreibende wissen, welche Geschäfte Sie besuchen und was Sie dort wann kaufen? Würden Sie sich wünschen, dass Ihre digitalen Assistenten Ihnen eine unvoreingenommene Auswahl von Diensten anbieten, anstatt Dienste, die von Werbenden mit dem größten Budget an die Spitze der Trefferliste platziert werden? Und glauben Sie, dass in Ihrer Stadt im Krisenfall ein IKT-Notbetrieb die Rückkehr zur Normalität beschleunigt?

Aus technischer Sicht ist die Antwort klar: Ja, all das Genannte ist (in weiten Teilen selbst mit heutiger Technologie) machbar, wenn auch nicht ohne zusätzlichen technischen und regulatorischen Aufwand. Was fehlt, sind jederzeit verfügbare, verständliche und beherrschbare digitale (kritische) Infrastrukturen für smarte Städte, mündige, weil aufgeklärte BürgerInnen, ein gesellschaftlicher Konsens, wie wir Digitalisierung leben wollen, sowie ein regulatorischer Rahmen, der Gestaltungsvorgaben macht, die einen funktionierenden Markt zulassen. Deutschland kann damit zum Vorreiter für resiliente, sichere, aber gleichzeitig auch freie und demokratische Städte werden, die ihrer Bevölkerung dienen.

ABSTRACT

Seit einigen Jahren ist die Transformation von über Jahrhunderte gewachsenen Städten hin zu smarten Städten zu beobachten, während gleichzeitig neue, von Grund auf digital konzipierte Städte entstehen. In solchen digital vernetzten Städten ist die Funktionsfähigkeit der IKT-gestützten Infrastrukturen durch Naturereignisse, menschliches und technisches Versagen sowie Gewalt und Terror gefährdet. Für digitale Infrastrukturen in smarten Städten müssen wir sicherstellen, dass sie jederzeit verfügbar, verständlich und beherrschbar bleiben. Es ist daher notwendig, dass man auch im Krisenfall und bei hohem Vernetzungsgrad einen Betrieb/Notbetrieb kritischer Infrastrukturen in den Sektoren Energie, Verkehr und Logistik, Gesundheit, Ernährung, Wasser, Finanz- und Versicherungswesen sowie Staat und Verwaltung garantieren kann. Ein systematisches Verständnis der Verwundbarkeit von IKT sowie wirksame Maßnahmen zur Erhöhung ihrer Resilienz sind dazu dringend erforderlich. Unsichere oder nicht beherrschbare IT-Systeme dürfen nicht Teil kritischer Infrastrukturen sein und müssen aus digital vernetzten Städten entfernt werden. Gleichzeitig muss eine demokratische Kontrolle über die Daten, die im öffentlichen Raum erhoben werden, gewährleistet sein. Digitalisierte Infrastrukturen in smarten Städten dürfen nicht in eine Überwachung und Kontrolle ihrer Bewohner als Normalzustand münden: Smarte Städte müssen die Rechte des Individuums auf Privatheit schützen.

PASSWORTRICHTLINIEN IN DEUTSCHEN UNTERNEHMEN

Sicherheit muss benutzerfreundlich sein

Trotz vieler Probleme sind Passwörter weiterhin der am weitesten verbreitete Authentisierungsmechanismus. In diesem Bericht werden die Ergebnisse von zwei Studien zu Passwortrichtlinien vorgestellt. Darauf basierend werden Vorschläge zur Verbesserung gemacht.

Viele Benutzer wählen unsichere Passwörter. Das ist hinlänglich bekannt. Das Hasso-Plattner-Institut hat, basierend auf einer halben Million Passwörter aus seinem Identity Leak Checker, die von .de-E-Mail-Adressen am häufigsten genutzten Passwörter analysiert:

1.	**123456**	6.	**hallo123**
2.	**12345**	7.	**hallo**
3.	**123456789**	8.	**123**
4.	**ficken**	9.	**passwort**
5.	**12345678**	10.	**master**

Die in Deutschland meistgenutzten Passwörter 2018.[1]

Solch leicht zu erratende Passwörter stellen ein beliebtes Einfallstor für Angreifer dar. Um zu verhindern, dass Benutzer solche Passwörter auswählen, werden Passwortrichtlinien eingesetzt. Diese sollen Benutzer zwingen, komplexere und somit schwerer zu erratende Passwörter zu wählen. Wie komplex ein Passwort sein muss, um als sicher zu gelten, kommt auf die Angriffsformen an, gegen die man sich schützen möchte.

1. GEFAHREN UND HERAUSFORDERUNGEN DURCH ONLINE- UND OFFLINEANGRIFFE

Man muss dabei zwischen Online- und Offlineangriffen unterscheiden. Bei Onlineangriffen hat der Angreifer Zugriff auf einen offiziellen Log-in-Mechanismus, zum Beispiel eine Website oder das Keyboard des Arbeitsplatzrechners. Bei solchen Angriffen ist es möglich, die Anzahl der Rateversuche zu limitieren. Dies kann entweder durch ein hartes Limit oder ein sogenanntes Exponential-Back-off-Verfahren geschehen. Bei einem harten Limit wird etwa nach drei Fehlversuchen der Account gesperrt. Beim Exponential-Back-off-Verfahren wird die Wartezeit nach einem Fehlversuch exponentiell verlängert, um den Angriff zu verlangsamen. Aus der Perspektive eines einzelnen Accounts sind, bei entsprechender Limitierung der Ratemöglichkeiten, die Komplexitätsanforderung an Passwörter nicht sonderlich hoch. Es reicht, wenn das Passwort komplex genug ist, dass ein Angreifer ein paar Tausend Rateversuche bräuchte. Wenn der Angreifer jedoch nicht einen bestimmten Account angreifen möchte, sondern einen beliebigen von vielen, schützen diese Mechanismen nicht und dem Angreifer reicht ein einziges unsicheres Passwort, um Zugriff zu erlangen.

Noch kritischer sieht es bei Offlineangriffen aus. Hier hat der Angreifer sich Zugriff auf die Datenbank verschafft, in der die Passwörter gespeichert sind. Best Practices schreiben vor, dass Passwörter in diesen Datenbanken kryptografisch geschützt sein müssen. Dies sollte mittels kryptografischer Hashfunktionen umgesetzt werden. In der gestohlenen Datenbank stehen somit die Passwörter nicht im Klartext, sondern als kryptografischer Hash, der nicht reversibel ist. Allerdings sind die Hashverfahren öffentlich bekannt und Angreifer können somit probieren, die Passwörter durch Erraten und Vergleich der Hashwerte zu knacken. Da die Datenbank im Besitz des Angreifers ist, kann der Angreifer beliebig oft raten.

Angreifer haben üblicherweise Listen von allen bisher bekannt gewordenen Passwörtern und probieren als Erstes diese an allen Accounts in der Datenbank aus. Solche Passwörter werden dann innerhalb von Sekunden geknackt. Bei gezielten Angriffen gegen einzelne Accounts können Angreifer auch mehr Rechenleistung einsetzen und so unbekannte Passwörter durch Ausprobieren erraten. Je länger und komplexer Passwörter sind, desto schwieriger ist es für Angreifer, sie durch diese Methode zu knacken.

Diese Art, Passwörter zu knacken, wird dadurch verstärkt, dass Angriffe gegen Hashfunktionen immer mächtiger werden und Hashfunktionen, die einst als sicher galten, nicht mehr sicher sind. Entwickler müssen somit in regelmäßigen Abständen ihre Software aktualisieren und unsichere Mechanismen durch aktuelle und sichere ersetzen. Studien der Universität Bonn und des Fraunhofer FKIE zeigen jedoch, dass viele Entwickler dabei große Schwierigkeiten haben und viele Passwortdatenbanken nicht ausreichend geschützt werden.[2,3,4] Dies wird auch durch die vielen Passwortleaks deutlich belegt.[5,6,7]

Um diese Offlineangriffe abzuschwächen, sind die Anforderungen an die Komplexität von Passwörtern deutlich höher. Mit Passwortrichtlinien können Unternehmen versuchen zu verhindern, dass Benutzer leicht zu erratende Passwörter wählen. Sie können beispielsweise festlegen, dass Passwörter eine definierte Mindestlänge haben müssen, bestimmte Zeichen oder Wörter nicht enthalten dürfen und nach einer gewissen Zeit geändert werden müssen.

Studien haben jedoch ergeben, dass zu strenge Vorgaben die Qualität der Passwörter nicht zwangsläufig steigern, da zum Beispiel Sonderzeichen an ein einfaches Passwort angehängt werden und so ein vorhersehbares Muster geschaffen wird.[8] Gleichzeitig reduzieren zu strenge Vorgaben die Produktivität der Nutzer und damit einhergehend der Unternehmen.[9] Daher stellen Passwortrichtlinien immer einen Kompromiss zwischen Sicherheit und Benutzerfreundlichkeit dar.

[1] Hasso Plattner Institut, „Die Top Ten deutscher Passwörter", 18.12.2018.Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://hpi.de/pressemitteilungen/2018/die-top-ten-deutscher-passwoerter.html
[2] A. Naiakshina et al., „Why do developers get password storage wrong?: A qualitative usability study", in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017.
[3] A. Naiakshina et al., „Deception task design in developer password studies: exploring a student sample", in Fourteenth Symposium on Usable Privacy and Security, 2018.
[4] A. Naiakshina, Alena et al., „If you want, I can store the encrypted password: A Password-Storage Field Study with Freelance Developers" in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019.
[5] Heise Online, „Passwort-Sammlung mit 773 Millionen Online-Konten im Netz aufgetaucht", 17.01.2019. Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://www.heise.de/security/meldung/Passwort-Sammlung-mit-773-Millionen-Online-Konten-im-Netz-aufgetaucht-4279375.html
[6] Have I been Pwnd, „Pwnd websites. Breached websites that have been loaded into Have I been Pwned". Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://haveibeenpwned.com/PwnedWebsites
[7] Hasso Plattner Institut, „Erfasste veröffentlichte Leaks der letzten Monate". Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://sec.hpi.de/ilc/statistics
[8] B. Ur et al., „I Added'!at the End to Make It Secure: Observing Password Creation in the Lab." in: Eleventh Symposium On Usable Privacy and Security, 2015.
[9] P. G. Inglesant, M. A. Sasse, The true cost of unusable password policies: password use in the wild, 2010.

2. PASSWORTRICHTLINIEN IN DER DEUTSCHEN INDUSTRIE – BEFRAGUNG

Um einen Einblick zu bekommen, wie es um Passwortrichtlinien in der deutschen Industrie steht, wurde eine Befragung von Unternehmen durchgeführt. Zu der Umfrage wurde über die Newsletter des BSI, des Bitkom und des Cyber Security Cluster sowie über persönliche Kontakte zu CISOs und CTOs eingeladen. Die Rekrutierung war somit nicht zufällig und hat vornehmlich sicherheitsinteressierte Unternehmen angesprochen. Der im Weiteren beschriebene Überblick über die Passwortrichtlinien stellt deshalb wahrscheinlich eine positive Obergrenze dar.

Um eine Einschätzung der Benutzerfreundlichkeit der Richtlinien zu bekommen, wurde zusätzlich ein Fragebogen über Clickworker an 200 Endnutzer geschickt. In diesem Fragebogen wurden Teilnehmer gebeten, einzelne Elemente von Passwortrichtlinien sowie ausgewählte Richtlinien zu bewerten.

Insgesamt haben 110 Unternehmen an der Umfrage teilgenommen. Dabei wurden 83 vollständige und valide Datensätze gesammelt. Die Größe der Unternehmen reicht dabei von Kleinstunternehmen bis zu Unternehmen mit über 1.000 Mitarbeitern. Genauere Informationen finden sich in Abbildung 1. Abbildung 2 gibt eine Übersicht über die Anzahl der Mitarbeiter, die in den befragten Unternehmen in Vollzeit an IT-Sicherheitsthemen arbeiten.

Um die Passwortrichtlinien vergleichbar und den Kontext interpretierbar zu machen, wurden die Teilnehmer gefragt, ob sie einen Mitarbeiteraccount betreiben, mit dem sich ein Mitarbeiter zum Beispiel auf dem Arbeitsrechner und bei anderen Diensten einloggen kann. Der Großteil unserer Teilnehmer (67) gab an, einen solchen Mitarbeiteraccount zu benutzen. Die Accounts konnten beispielsweise zusätzlich für E-Mails oder VPN genutzt werden. Bei den Unternehmen ohne einen solchen zentralen Account haben wir die Passwortrichtlinien für ihre E-Mail-Accounts erhoben.

Der Fragebogen war an den Mitarbeiter gerichtet, der für diesen Account zuständig ist. Da Passwortrichtlinien zum Teil über längere Zeiträume bestehen, wurde erfragt, von wem die Richtlinien erstellt wurden (Abbildung 3).

Diejenigen Teilnehmer, die selbst für die Erstellung der Richtlinie verantwortlich waren, wurden gefragt, welche Quellen sie genutzt haben (Abbildung 4). Mehrfachnennungen waren möglich. Die Mehrzahl der Teilnehmer gab an, sich auf eigenes Wissen zu stützen. An zweiter Stelle folgen Empfehlungen für Passwortrichtlinien des BSI. Auch der Austausch mit anderen Unternehmen und Expertenforen sind beliebte Quellen. Die Organisationen OWASP und NIST haben ebenfalls Empfehlungen für Passwortrichtlinien veröffentlicht.

ABBILDUNG 1: **ANZAHL MITARBEITER & ANZAHL BETREUTE CLIENTS**

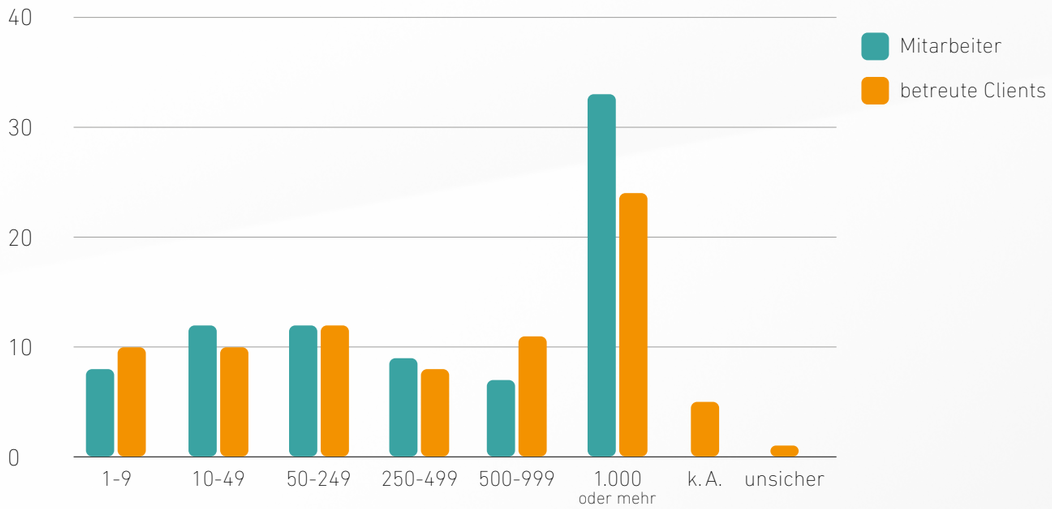


ABBILDUNG 2: **ANZAHL DER MITARBEITER, DIE IN DEN BEFRAGTEN UNTERNEHMEN VOLLZEIT AN IT-SICHERHEITSTHEMEN ARBEITEN**

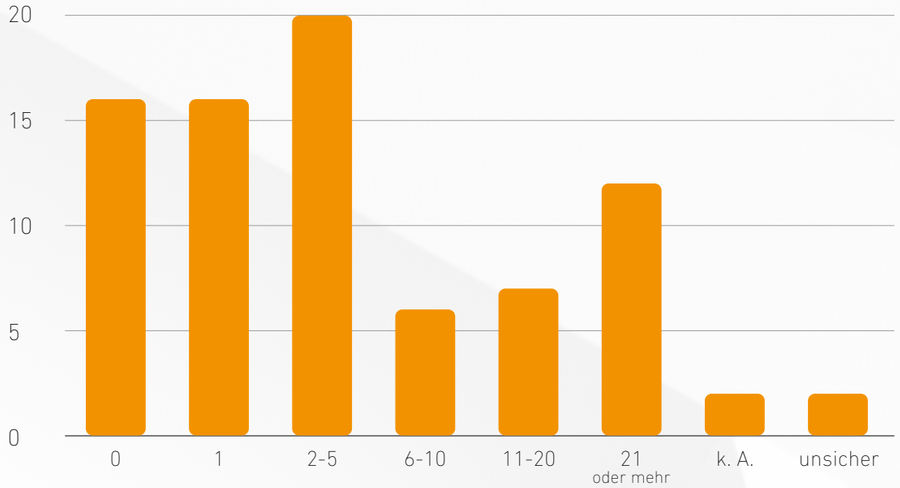


ABBILDUNG 3: **WER HAT DIE PASSWORT-RICHTLINIEN ERSTELLT?**

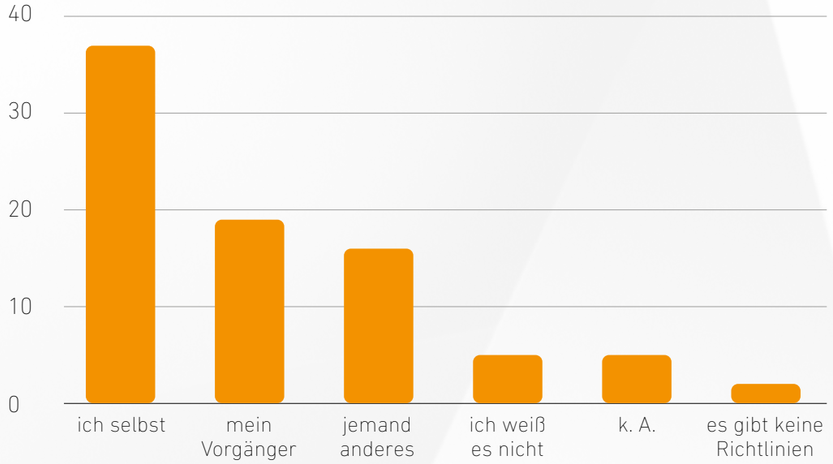
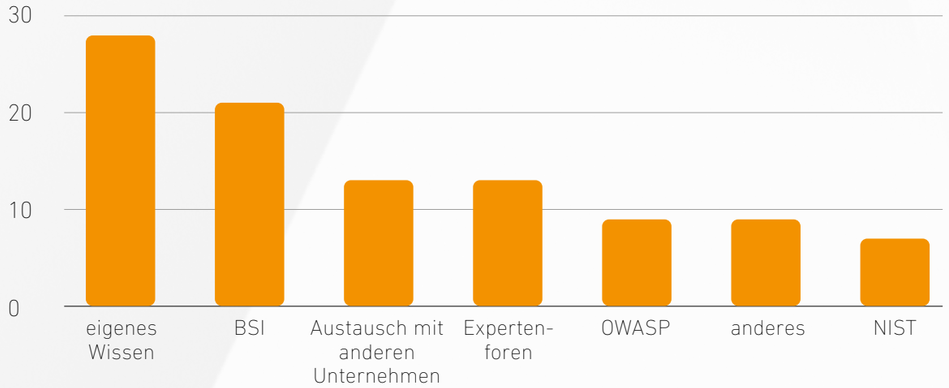


ABBILDUNG 4: **INFORMATIONSQUELLEN**



3. BSI-, OWASP- UND NIST-RICHTLINIEN

Um Unternehmen die Wahl der Passwortrichtlinien zu erleichtern, haben verschiedenste Institutionen Vorschläge und Orientierungshilfen veröffentlicht. Die nachfolgende Tabelle gibt eine Übersicht über die konkreten Vorschläge von BSI[10], NIST[11] und OWASP, die zu der Zeit der Umfrage galten. Das BSI hat im Februar 2020 seine Richtlinien überarbeitet. Im Folgenden bezeichnen wir die Richtlinien vor Februar 2020 als die alten BSI-Richtlinien und die aktuellen als die neuen BSI-Richtlinien.

Sowohl die alten wie auch die neuen BSI-Richtlinien wurden bewusst abstrakt gehalten. In den alten Richtlinien wurde zum Beispiel darauf hingewiesen, dass eine „ausreichende" Mindestlänge gesetzt werden soll. Ebenfalls wurde empfohlen, „ausreichend" viele Zeichenklassen und in „angemessenen Zeitabständen" einen Passwortwechsel zu erzwingen. Was ausreichend und angemessen ist, bleibt der Einschätzung der Administratoren überlassen. Auf persönliche Anfrage beim BSI können inoffizielle Beispiele erfragt werden und es wird darauf verwiesen, dass es BSI-zertifizierte Berater gibt, die Unternehmen beim Entwurf einer Richtlinie unterstützen. Die neuen BSI-Richtlinien fassen die Komplexitätsanforderungen zusammen und empfehlen, dass Passwörter eine geeignete Qualität haben und so komplex sein sollen, dass sie nicht leicht zu erraten, aber noch gut zu behalten sind. Von dem zeitlich gesteuerten Passwortwechsel wird in den neuen Richtlinien abgeraten.

NIST und OWASP geben deutlich konkretere Empfehlungen. Der 2017 von NIST veröffentlichte Standard 800-63B stellt einen deutlichen Bruch mit bisherigen Richtlinien dar. Typische Elemente wie das Erzwingen von mehreren Zeichenklassen (groß, klein, Zahlen und Sonderzeichen) wurden nicht nur entfernt, sondern es wird explizit davon abgeraten. Auch von der Vorschrift, regelmäßig das Passwort zu ändern, wird explizit abgeraten. Es werden weiterhin konkrete Empfehlungen für minimale Passwortlänge und erlaubte Zeichensätze gegeben. Zudem wird eine minimale Maximallänge spezifiziert. Konkret schlägt das NIST vor, dass Passwörter mindestens acht Zeichen lang sein sollen und mindestens 64 Zeichen erlaubt sind. Dies ist insbesondere für die Nutzung von Passwortmanagern relevant, da sie lange Passwörter generieren. Die große Umgestaltung der NIST-Richtlinien wurde vollzogen, um sowohl die Benutzerfreundlichkeit als auch die Sicherheit zu verbessern. NIST hat dabei einen evidenzbasierten Ansatz gewählt. Denn wissenschaftliche Studien haben belegt, dass zu komplexe Richtlinien Benutzer zu unsicheren Praktiken verleiten, um einfache Passwörter zu finden, die trotzdem den Richtlinien entsprechen. Der OWASP Application Security Verification Standard 4.0 (ASVS) lehnt sich stark an den NIST 800-63B Standard an und möchte explizit kompatibel sein. Interessanterweise gibt es zusätzlich zum OWASP ASVS noch den OWASP Authentication Cheat Sheet, der auf dem ASVS basiert – allerdings in einigen Punkten davon abweicht.

[10] Bundesamt für Sicherheit in der Informationstechnik, „ORP4.A8 Regelung des Passwortgebrauchs". Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html - Zugriff: 27.10.19
[11] National Institue of Standards and Technology, „NIST Special Publication 800-63B - 5.1.1.2 Memorized Secret Verifiers". Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://doi.org/10.6028/NIST.SP.800-63b

TABELLE 1: ÜBERSICHT ÜBER PASSWORTRICHTLINIEN

	BSI[12] (alt)	BSI (neu)	NIST[13]	OWASP Cheat Sheet	OWASP ASVS 4
Mindestlänge	ausreichend		8	8	12
Minimale Maximallänge			64	ausreichend (typisch: 128)	64
Komplexität Anforderungen (min. Anzahl der Zeichenklassen groß/klein/Zahlen/ Sonderzeichen)	ausreichend		wird von abgeraten	wird von abgeraten	wird von abgeraten
Qualität		geeignet			
Erzwungenes Änderungsintervall	angemessene Zeitabstände	wird von abgeraten	wird von abgeraten	wird von abgeraten	wird von abgeraten
Erlaubte Zeichen			alle ASCII-Zeichen, alle Unicode-Zeichen	alle ASCII-Zeichen, alle Unicode-Zeichen	alle ASCII-Zeichen, alle Unicode-Zeichen
Verbotene Passwörter		leicht zu erratende Passwörter häufige Passwörter mehrfach genutzte Passwörter	mindestens: geleakte Passwörter Wörter aus dem Wörterbuch sich wiederholende Zeichenfolgen (z. B. „aaaaa", „abc1234") kontextsensitive Wörter (z. B. Name vom Service, Username und Ableitungen davon)	häufige Passwörter geleakte Passwörter	geleakte Passwörter

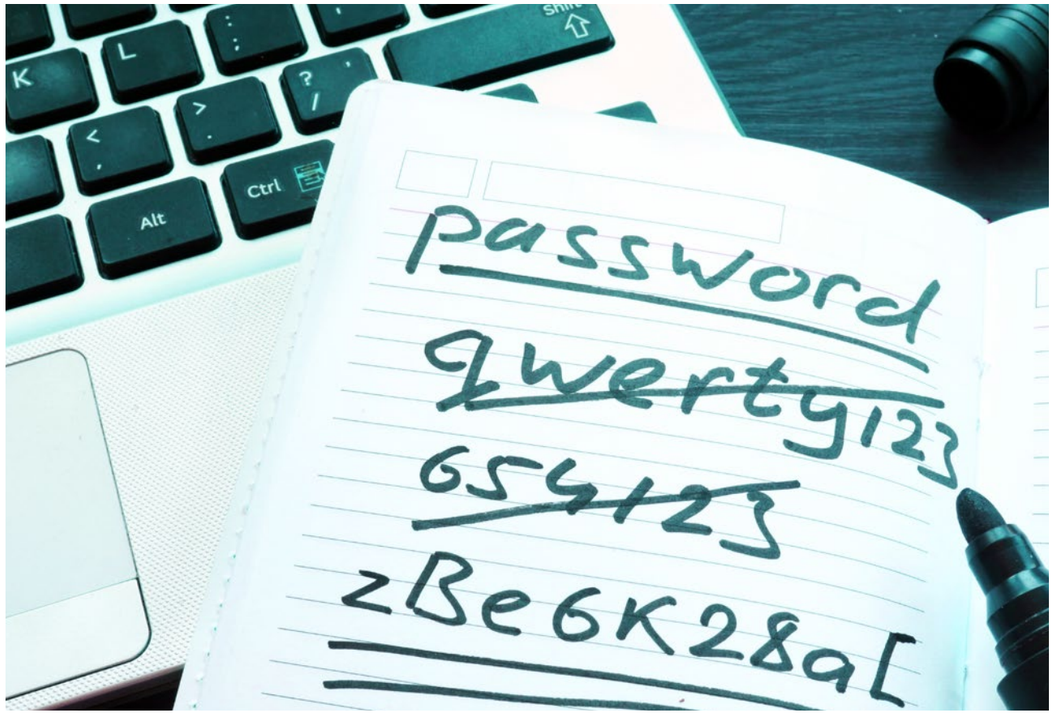
[12] Bundesamt für Sicherheit in der Informationstechnik, „ORP4.A8 Regelung des Passwortgebrauchs". Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html - Zugriff: 27.10.19
[13] National Institue of Standards and Technology, „NIST Special Publication 800-63B - 5.1.1.2 Memorized Secret Verifiers". Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://doi.org/10.6028/NIST.SP.800-63b

Passwortrichtlinien in deutschen Unternehmen

TABELLE 2: EINZELBEWERTUNG DER ELEMENTE AUS DEN RICHTLINIEN

Das Vorkommen ist folgendermaßen codiert:
nie: 0 Vorkommen; selten: 1–2 Vorkommen; gelegentlich: 3–10 Vorkommen; oft: 20–40 Vorkommen.
Zahlen in Klammern: Die Regel wird durch andere Regeln indirekt erfüllt.

Regel	Vorkommen	Erfülle ich sowieso	Stört		
			nicht	etwas	sehr
Verwendung von mind. zwei verschiedenen Zeichengruppen	gelegentlich	99	35	10	4
Eine Mindestlänge von acht Zeichen	oft	92	44	9	3
Passwort darf nicht in einer Leakdatenbank sein	nie	77	53	13	5
Ihre E-Mail-Adresse	selten	88	29	17	14
Ihr Accountname	gelegentlich	82	37	17	12
Ihre Telefonnummer	selten	88	28	15	17
Tastaturfolgen wie „123“ oder „asdf“	selten	80	39	17	12
Ihr Geburtsdatum	gelegentlich	79	41	15	13
Ihr Vor- bzw. Nachname	gelegentlich	80	38	15	15
Im Kontext einfach zu erraten (z. B. Firmen- oder Dienstname)	gelegentlich	76	40	22	10
Ihr Kfz-Kennzeichen	selten	80	33	21	14
Verwendung von mind. drei verschiedenen Zeichengruppen	oft	68	47	27	6
Ihre ID-Nummer (z. B. Ihre Personalnummer)	selten	79	36	15	18
Zahlen wie den aktuellen Monat oder das Jahr	selten	60	57	24	7
Das Passwort darf kein Wort sein, das man in einem Wörterbuch findet (z. B. „Blume“ oder „Sonnenschein“ sind verboten; in Kombination sind jedoch Wörter erlaubt, z. B. „Blume762“ oder „DieBlumeistschön“)	selten	66	46	25	11
Leerzeichen	selten	62	49	22	15
Mehr als zwei aufeinanderfolgende gleiche Zeichen (z. B. „aaa“ oder „!!!“)	gelegentlich	52	55	24	17
Mehr als zwei Zeichen, die in Folge auch in Ihrem Namen vorkommen	selten	36	58	40	14
Bestimmte Sonderzeichen, wie Umlaute oder „ß“	selten	36	54	45	13
Das Passwort muss sofort geändert werden, wenn es den Verdacht gibt, dass ein anderer in den Besitz gelangt ist	gelegentlich	N/A	115	24	9
Sonderzeichen als letztes Zeichen	selten	31	60	39	18
Das Passwort darf kein Wort enthalten, das man in einem Wörterbuch findet (z. B. „Blume“, „Blume761“ oder „DieBlumeistschön“ sind verboten)	selten	50	26	43	29
Verwendung von allen vier Zeichengruppen	oft	36	39	45	28
Das neue Passwort darf nicht genau das gleiche sein wie das letzte Passwort	nie (oft)	N/A	98	34	16
Das Kennwort muss einmal im Jahr geändert werden	gelegentlich	N/A	90	49	9
Eine Maximallänge von 20 Zeichen	selten	34	47	26	41
Eine Mindestlänge von zwölf Zeichen	gelegentlich	22	43	60	23
Der Account wird nach ein paar Fehlversuchen gesperrt (z. B. fünf fehlerhafte Eingaben)	gelegentlich	N/A	81	46	21
Eine feste Passwortlänge von genau acht Zeichen	gelegentlich	22	40	46	40
Das neue Passwort darf nicht genau das gleiche sein wie alle bisher verwendeten Passwörter	nie	N/A	74	44	30
Das neue Passwort muss sich deutlich unterscheiden von dem letzten Passwort (einzelne Buchstaben ändern oder Sonderzeichen anhängen reicht nicht aus)	selten	N/A	41	70	37
Das Kennwort muss alle 90 Tage geändert werden	oft	N/A	46	58	44
Das neue Passwort muss sich deutlich unterscheiden von allen bisher verwendeten Passwörtern (einzelne Buchstaben ändern oder Sonderzeichen anhängen reicht nicht aus)	nie	N/A	33	67	48
Eine Mindestlänge von 16 oder mehr Zeichen	gelegentlich	14	20	50	64
Das Kennwort muss alle 42 Tage geändert werden	selten	N/A	24	50	74



4. ANALYSE DER PASSWORTRICHTLINIEN DER TEILNEHMER

In dem Fragebogen wurden Teilnehmer darum gebeten, die Passwortrichtlinien des zentralen Betriebsaccounts oder, falls nicht vorhanden, des Einzelaccounts anzugeben. Aus den 83 gültigen Datensätzen konnten 81 Passwortrichtlinien analysiert werden. Die abweichende Zahl ergibt sich dadurch, dass vier Teilnehmer mehrere Richtlinien und sechs Teilnehmer keine Richtlinien oder nicht verständliche Richtlinien angegeben haben. Bei der Analyse muss bedacht werden, dass es keine Garantie bezüglich der Vollständigkeit gibt, da gegebenenfalls gewisse Elemente vergessen oder ungenau spezifiziert wurden.

Aus den Richtlinien wurden die einzelnen Bestandselemente extrahiert, zum Beispiel Mindestlänge oder Zeicheneinschränkungen, und in Tabelle 2 aufgeführt. Die zweite Spalte gibt an, wie häufig das Element von den Befragten genutzt wird. Um eine Schätzung zu bekommen, wie sehr die einzelnen Elemente den Benutzer stören, wurden mit einem zweiten Fragebogen diese Elemente mittels Clickworker 200 Personen gezeigt. Die Teilnehmer sollten dabei bewerten, ob sie von den Elementen betroffen wären und ob oder wie sehr diese Elemente sie beim Erstellen von Passwörtern stören. Dabei konnten Teilnehmer zwischen folgenden Antwortmöglichkeiten auswählen:

Erfülle ich sowieso: Die Art, wie ich meine Passwörter erstelle, erfüllt die Bedingung sowieso schon.

Stört mich nicht/etwas/sehr: Die Regel zwingt den Mitarbeiter, seine Passwörter in einer anderen Weise als bisher zu erstellen. In diesem Fall wählt er aus, wie sehr ihn diese Regel stört.

Tabelle 2 zeigt die Ergebnisse der Umfrage. Dabei wurden die Elemente von „am wenigsten störend" bis „am meisten störend" sortiert. Das heißt, oben stehen diejenigen Elemente, welche die Benutzer schon verinnerlicht haben und die deswegen nicht mehr stören oder, selbst wenn sie eine Änderung erzwingen, als weniger störend wahrgenommen werden. Unten stehen im Gegensatz Regelelemente, die viele Benutzer betreffen und diese mehr stören. Dabei werden Regeln, die Benutzer unabhängig von ihren eigenen Präferenzen betreffen, mit N/A markiert, zum Beispiel Passwörter müssen nach 42 Tagen gewechselt werden.

Im Folgenden werden einige wichtige Gruppierungen der Elemente analysiert. Als Basis werden die NIST-Richtlinien genutzt, da die BSI-Richtlinien keine konkreten Vorgaben machen und die OWASP-Richtlinien auf den NIST-Richtlinien beruhen. Weiterhin wird die Benutzbarkeitseinschätzung aus Tabelle 2 einbezogen.

4.1. PASSWORTALTER UND REGELMÄSSIGES ÄNDERN VON PASSWÖRTERN

Den deutlichsten Handlungsbedarf sehen wir in Deutschland hinsichtlich des Passwortalters. 54 unserer Teilnehmer geben an, eine regelmäßige Änderung des Passworts zu erzwingen. Abbildung 5 zeigt die Verteilung der Änderungszeiträume.

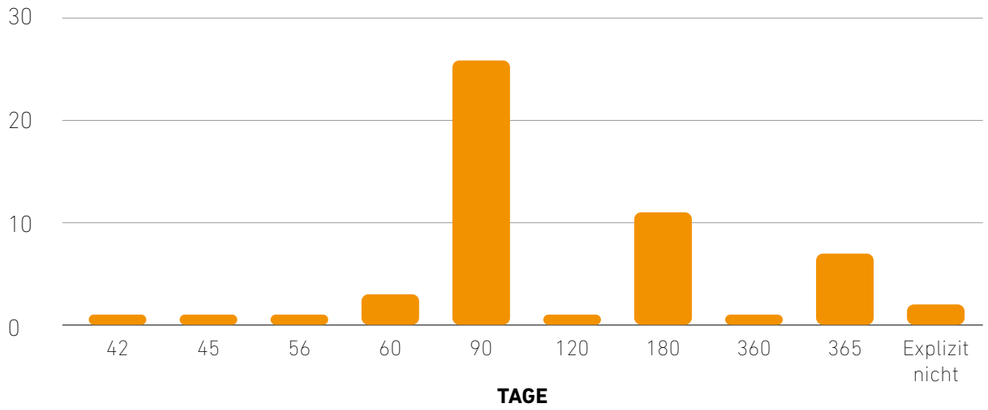
NIST rät schon seit längerem davon ab, Nutzer regelmäßig zu einer Änderung der Passwärter zu zwingen. Die Organisation empfiehlt stattdessen, nur dann Änderungen zu verlangen, wenn es einen Hinweis gibt, dass Passwörter kompromittiert wurden. Eine Reihe von Untersuchungen legen nahe, dass eine erzwungene Änderung nicht den gewünschten Mehrwert für die Sicherheit bietet.[14] Die neuen BSI-Richtlinien vertreten ebenfalls diese Position. Zur Zeit der Umfrage empfohlen die Richtlinien jedoch, die Passwörter in „angemessenen" Zeitabständen zu ändern. Was „angemessen" dabei bedeutet, war im Einzelfall zu entscheiden. Angemessen kann somit auch sein, keine Änderung zu erzwingen. Die Mehrzahl der Befragten hat sich jedoch dafür entschieden, einen regelmäßigen Wechsel zu erzwingen.

Die Benutzbarkeitsevaluierung zeigt deutlich, dass das erzwungene Ändern von Passwörtern und die damit verbundenen zusätzlichen Regeln als besonders störend empfunden werden. Von den sechs unbeliebtesten Regeln fallen fünf in diese Kategorie. Zudem sind weitere Regeln nötig, um sicherzustellen, dass die neuen Passwörter nicht den alten ähneln und den Sicherheitsgewinn zunichtemachen. Deswegen sind die neuen BSI-Richtlinien sehr zu begrüßen.

4.2. PASSWORTHISTORIE UND ZÄHLERREGEL

Viele Nutzer haben Strategien entwickelt, um sich den Passwortwechsel möglichst einfach zu machen. Sie nutzen beispielsweise abwechselnd zwei oder mehrere verschiedene Passwörter. Das hilft zwar dem Benutzer, sich die neuen Passwörter zu merken, reduziert jedoch den erhofften Sicherheitsgewinn erheblich. Um den Wechsel zwischen einigen wenigen Passwörtern zu verhindern, setzen viele Unternehmen auf Passworthistorien, die dazu führen, dass Nutzer eine bestimmte Anzahl ihrer letzten Passwörter nicht

ABBILDUNG 5: **MAXIMALALTER DER PASSWÖRTER**



[14] Yinqian Zhang et al., „The security of modern password expiration: an algorithmic framework and empirical analysis", CCS 2010, https://dl.acm.org/citation.cfm?doid=1866307.1866328

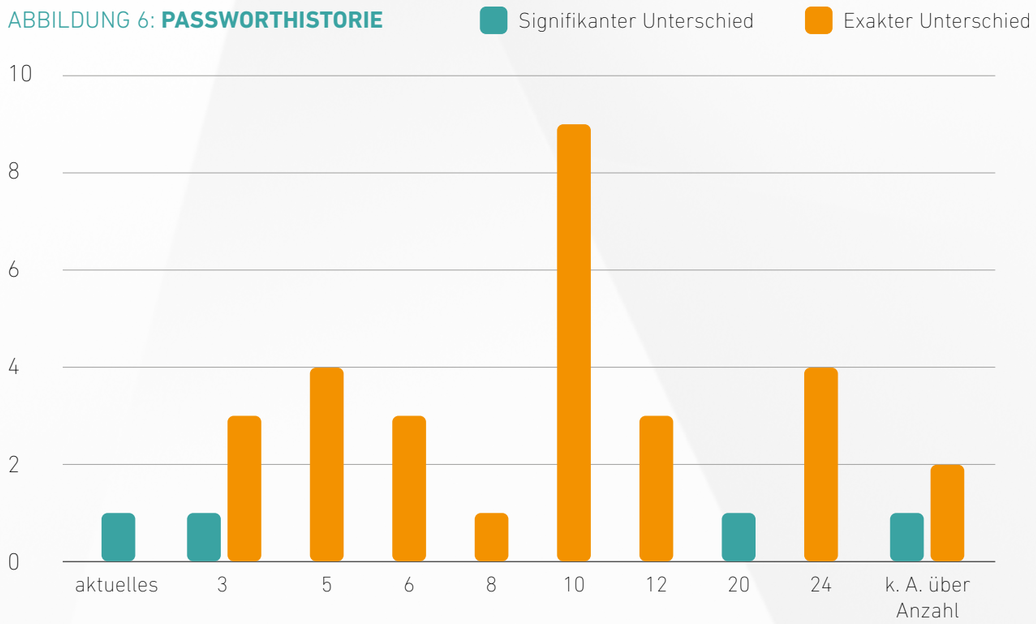
wiederverwenden dürfen. Die Historie reicht von den letzten drei bis zu 24 Passwörtern. In den meisten Fällen wird das komplette Passwort verglichen, in drei Fällen werden deutliche Unterschiede gefordert. Letzteres ist besonders kritisch, da die Passwörter deswegen höchstwahrscheinlich im Klartext gespeichert werden müssen.[15] Andernfalls lässt sich nur überprüfen, ob das neue Passwort genau einem alten Passwort entspricht.

> *„Den **deutlichsten Handlungsbedarf** sehen wir in Deutschland hinsichtlich des Passwortalters."*

Es ist somit möglich, ein simples System für den Wechsel zu nutzen. Beispiele hierfür sind: jedem neuen Passwort eine Zahl hinzufügen (1, 2, 3 etc.), weitere gleiche Zeichen anzuhängen (!, !!, !!! etc.) oder um ein Element wie den Namen des aktuellen Monats zu ergänzen (August, September, November etc.). Wenn ein Angreifer im Besitz eines Passworts ist, kann er das nächste Passwort also leicht erraten. Da es unzählige dieser Strategien gibt, entwickelt sich das Gestalten der Regeln zu einem Katz-und-Maus-Spiel zwischen den Administratoren und den Benutzern. Dies führt im schlimmsten Fall dazu, dass äußerst umfassende Verbote eingeführt werden, die in Kombination die Benutzbarkeit negativ beeinflussen.

Eine weitere Strategie der Nutzer, mit erzwungenen Änderungen und einer Passworthistorie umzugehen, besteht darin, das Passwort am Tag der Änderung mehrmals zu wechseln, sodass das Originalpasswort

ABBILDUNG 6: **PASSWORTHISTORIE**



[15] Es gibt Hashfunktionen, die gewisse Ähnlichkeitsvergleiche ermöglichen. Es wäre somit theoretisch möglich, dass diese zum Einsatz kommen. Uns ist nicht bekannt, dass dies in der Praxis vorkommt, und die Lösung hätte ebenfalls Sicherheitsnachteile.

ABBILDUNG 7: **GEFORDERTE ZEICHENGRUPPEN**

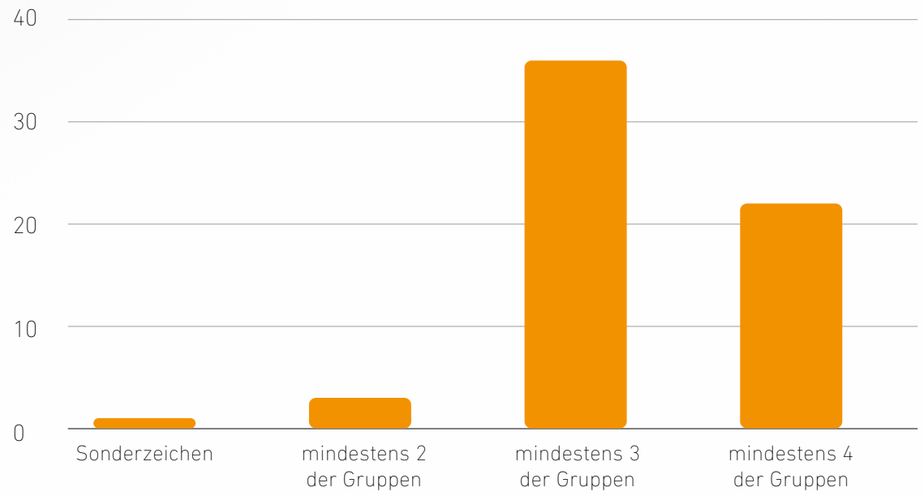


ABBILDUNG 8: **MINIMALE PASSWORTLÄNGE**

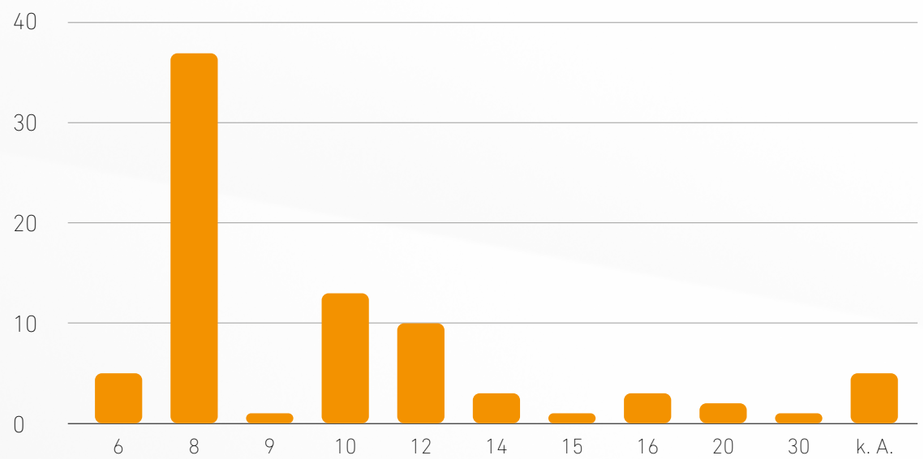
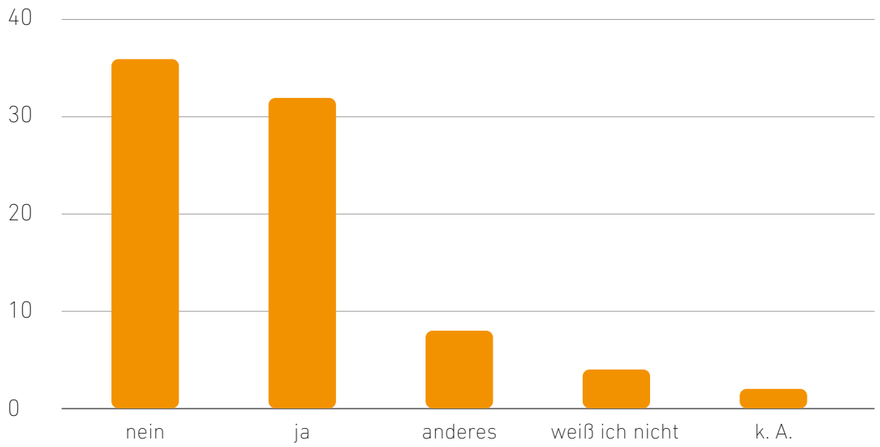


ABBILDUNG 9: **WERDEN HÄUFIGE PASSWÖRTER VERBOTEN?**



wieder genutzt werden kann. Diese Strategie wird häufig mit einem Mindestalter der Passwörter verhindert, was dazu führt, dass Nutzer 24 Stunden bis 14 Tage warten müssen, bevor sie ihr Passwort erneut verändern dürfen. Dies hat allerdings im schlimmsten Falle zur Folge, dass Nutzer ihr Passwort nicht wechseln dürfen, auch wenn sie vermuten, dass es beispielsweise dritten Personen bekannt geworden ist. Administratoren sollten zwar dazu in der Lage sein, eine Änderung des Passworts zu autorisieren, aber es dauert länger und es kann sein, dass sich der Nutzer nicht sofort bei ihnen meldet.

Die alte Empfehlung, Passwörter in regelmäßigen Abständen zu ändern und die Sammlung von flankierenden Regeln führen zu großen Benutzbarkeitsproblemen. Unternehmen und Auditoren sollten die neue Empfehlung des BSI hierzu umgehend umsetzen und nicht aus Gewohnheit oder intuitivem (aber wissenschaftlich widerlegtem) Sicherheitsverständnis auf regelmäßiger Passwortänderung bestehen.

4.3. ZEICHENGRUPPEN (KOMPLEXITÄT)

Etwas weniger eindeutig ist es im Fall der Zeichengruppen. In Abbildung 7 sind die geforderten Zeichengruppen der Teilnehmer zu sehen. Die vier Kategorien sind Großbuchstaben (A–Z), Kleinbuchstaben (a–z), Ziffern (0–9) sowie Sonderzeichen. 22 Teilnehmer gaben an, dass aus allen vier Zeichengruppen mindestens ein Zeichen genutzt werden muss. In 36 Fällen müssen drei der vier Zeichengruppen vorkommen. In manchen Fällen war vorgegeben, welche Zeichengruppen abgedeckt werden müssen, in anderen blieb dies dem Nutzer überlassen. Sieben Teilnehmer sagten nur, dass verschiedene Zeichengruppen genutzt werden müssen, spezifizierten aber nicht, welche oder wie viele. Elf Teilnehmer erwähnten keine Pflicht bezüglich von Zeichengruppen und waren somit NIST-konform. Allerdings folgen die meisten unserer Teilnehmer der alten Norm und den Empfehlungen des BSI und erzwingen drei oder mehr der verschiedenen Zeichengruppen. Die Benutzbarkeitsevaluierung zeigt, dass der Zwang zu drei oder vier Zeichengruppen als sehr störende Regel empfunden wird.

Den Richtlinien der NIST folgend, sollen Nutzern keine Regeln dieser Art auferlegt werden, da solche Restriktionen laut Studien nicht zu besseren Passwörtern führen.[16] Die Benutzbarkeitsevaluation zeigt jedoch, dass die Forderung, zwei verschiedene Zeichengruppen zu nutzen, nur die wenigsten Benutzer stört. Es wäre also zu untersuchen, ob diese Regel die Sicherheit von Passwörtern erhöht, ohne den Benutzer zu belasten.

[16] P.G. Inglesant, M. A. Sasse, The true cost of unusable password policies: password use in the wild, 2010.

TABELLE 3: HÄUFIGSTE KOMBINATIONEN INNERHALB DER PASSWORTRICHTLINIEN
bezogen auf die geforderte Anzahl der Zeichengruppen, das maximale Passwortalter und die Mindestlänge

Zeichengruppe	Maximales Passwortalter	Mindestlänge	Anzahl der Policies
4	90 Tage	8	5
3	90 Tage	8	4
4	-	8	3
3	-	8	3
4	180 Tage	8	2
3	365 Tage	12	2

TABELLE 4: WIE VIELE ANGESTELLTE ARBEITEN IM UNTERNEHMEN AN IT-SICHERHEITSRELEVANTEN THEMEN?

Oben = Größe des Unternehmens Unten = haben IT-Security-Experten	< 250 Mitarbeiter	≥ 250 Mitarbeiter
0 IT-Security-Mitarbeiter	11	4
≥ 1 IT-Security-Mitarbeiter	22	38

4.4. LÄNGE

In Abbildung 8 sind die Mindestlängen zu sehen. Die Mehrheit der Unternehmen setzt auf die Nutzung von mindestens acht bis zwölf Zeichen. Ein befragtes Unternehmen, das eine Passwortmindestlänge von 30 Zeichen fordert, stellt seinen Arbeitnehmern einen Passwortmanager zur Verfügung. NIST empfiehlt, eine Passwortmindestlänge von acht Zeichen vorzugeben. Das ist bei den Befragten auch die am häufigsten gewählte Minimallänge. Manche Unternehmen verlangen jedoch deutlich höhere Mindestlängen. Ohne die Risikoabschätzung zu kennen, ist eine solche Maßnahme schwer zu beurteilen. Es ist jedoch empfehlenswert, zu prüfen, ob technische Sicherheitsmaßnahmen wie Ratenbegrenzung gegen Onlineattacken und starke Hashfunktionen gegen Offlineattacken genutzt werden können, um ein ähnliches Sicherheitsmaß mit weniger Zeichen zu ermöglichen.

4.5. HÄUFIGE / GELEAKTE PASSWÖRTER

OWASP und NIST empfehlen, die Nutzung häufiger und geleakter Passwörter zu unterbinden. Obwohl das BSI in den alten Richtlinien dazu keine Aussage macht, geben bereits 32 Teilnehmer an, dies zu tun. Diese Regel ist insbesondere wichtig, um Offlineattacken zu erschweren. Denn auch Zehntausende Passwörter aus Leaks inklusive Variationen auszuprobieren, ist ein Leichtes für Angreifer und gängige Praxis.

DISKUSSION

Unsere Datenerhebung zeigt eine große Vielfalt an Passwortrichtlinien. Die häufigste Richtlinie, bezogen auf das Zusammenspiel von Zeichenklasse, Mindestlänge des Passworts und Passwortalter, schreibt vor, dass mindestens acht Zeichen und alle vier Zeichenklassen genutzt werden müssen. Weiterhin muss das

Passwort alle 90 Tage gewechselt werden. Die zweithäufigste Richtlinie ist identisch bis auf den Aspekt, dass nur drei Zeichenklassen verwendet werden müssen. Diese Richtlinien wurden von fünf bzw. vier Teilnehmern angegeben. Wenn man 60 bis 180 Tage als Maximalalter, acht bis zwölf Zeichen Mindestlänge und drei bis vier Zeichenklassen zusammenfasst, kommt man auf 28 Teilnehmer. Trotzdem sieht man, wie in Tabelle 3 illustriert, ein sehr heterogenes Bild.

Während Heterogenität an sich nicht problematisch ist, scheint es uns unwahrscheinlich, dass die Unterschiede zwischen den Richtlinien auf wissenschaftlich fundierten Erkenntnissen beruhen, sondern eher darauf, dass Entscheider sich verschiedener Quellen bedienen und die Trade-offs selbst abwägen müssen. Dies erscheint wenig effizient, denn es erfordert von Unternehmen eine beachtliche Wissenstiefe bezüglich Angriffsarten gegen Passwörter, die von vielen kleinen Unternehmen nicht erwartet werden kann.

> *„Richtlinien müssen **benutzerfreundlich** gestaltet werden."*

Eine kürzlich veröffentlichte Umfrage des TÜVs[17] hat ergeben, dass sich viele Unternehmen Orientierungshilfen wünschen. Unsere Daten zeigen, dass insbesondere kleinere Unternehmen mit weniger als 250 Mitarbeitern seltener Angestellte haben, die sich explizit mit dem Thema IT-Sicherheit beschäftigen. Für diese stellt es sich als besonders schwierig dar, zu entscheiden, was im Kontext der BSI-Richtlinien für sie angemessen ist. Dies gilt sowohl für die alten als auch für die neuen Richtlinien.

Aufgrund dessen empfehlen wir, dass zusätzlich zu den neuen BSI-Richtlinien Instanziierungen angeboten werden, in denen konkrete Zahlen genannt werden. Es erscheint uns sinnvoll, sich dabei an den NIST-Richtlinien zu orientieren. Unternehmen, die IT-Sicherheitsexperten haben, können natürlich von den Empfehlungen abweichen. Allerdings würden die konkreten Zahlen jenen Unternehmen helfen, die solche Expertise nicht haben.

AUSBLICK

Passwortrichtlinien sollten dazu dienen, Menschen davor zu schützen, unsichere Passwörter zu wählen. Deswegen ist es besonders wichtig, dass die Richtlinien benutzerfreundlich sind, da sie sonst als Hindernis umgangen werden und im schlimmsten Fall das Gegenteil bewirken. Jedoch werden selbst die besten Passwortrichtlinien das Problem von unsicheren Passwörtern nur eindämmen, aber nicht beseitigen können. Aus unserer Sicht scheint es in vielen Fällen sinnvoll, Passwortmanager zu nutzen. Die Aufforderung des BSI, zu prüfen, ob Passwortmanager eingesetzt werden können, begrüßen wir sehr. Manche Unternehmen aus unserer Studie haben ihre Mitarbeiter bereits mit Passwortmanagern ausgestattet.

Trotzdem sollten Passwörter nur als temporäre Mittel auf dem Weg zu einer besseren Lösung gesehen werden. Zwei-Faktor-Authentisierung, zum Beispiel auch über Gerätezertifikate, ist in einigen Szenarien eine technische Lösung, die das Potenzial hat, den Menschen zu entlasten. Allerdings haben Zwei-Faktor-Authentisierungsmethoden auch Benutzbarkeitsprobleme, die für einen breiteren Einsatz noch gelöst werden müssen. Grundsätzlich sollten wir den Menschen nicht mehr als das schwächste Glied in der Cyber-Sicherheit betrachten. Bei Sicherheitsvorfällen dem Nutzer die Schuld zuzuweisen ist keine

[17] Verband der TÜV e.V., Cybersecurity Studie 6.1. Zuletzt geprüft: 28.01.2020. [Online]. Verfügbar: https://www.vdtuev.de/dok_view?oid=769635

zielführende Strategie. Falls menschliche Fehler zu Sicherheitsproblemen führen, sollten wir die ihnen zugrunde liegenden Technologien kritisch prüfen. Denn wenn Menschen sich nicht an Sicherheitsregeln halten, liegt dies meist daran, dass es oft zeitraubend oder schwierig bis unmöglich ist, sie umzusetzen. Sicherheitsexperten versuchen seit Jahren, diesem Verhalten mit Bewusstmachung (Security Awareness) gegenzusteuern – vergeblich. Wir benötigen bessere technische Lösungen, die im Gebrauch einfach sind. Ziel muss es sein, die Technologie dem Menschen anzupassen, um ihn zu entlasten und zu schützen.

ABSTRACT

Trotz vieler Probleme sind Passwörter weiterhin der am weitesten verbreitete Authentisierungsmechanismus. Viele Benutzer wählen jedoch unsichere Passwörter. Diese sind ein beliebtes Einfallstor für Angreifer. Mit dem Ziel, die Passwortsicherheit zu erhöhen, werden oft Passwortrichtlinien eingesetzt. Diese sollen den Benutzer zwingen, komplexere und somit schwerer zu erratende Passwörter zu wählen.

Dabei ist es wichtig, Richtlinien benutzerfreundlich zu gestalten. Sonst werden sie als Hindernis betrachtet, umgangen und bewirken im schlimmsten Fall das Gegenteil. Selbst die besten Passwortrichtlinien können das Problem von unsicheren Passwörtern jedoch nur eindämmen, aber nicht beseitigen. Sie sollten deswegen nur temporäre Hilfestellung auf dem Weg zu einer besseren Lösung sein, zum Beispiel Passwortmanager oder Zwei-Faktor-Authentisierung.

KÜNSTLICHE INTELLIGENZ IN DER CYBER-SICHERHEIT

Warum Deutschland bei der Entwicklung resilienter und sicherer KI eine Vorreiterrolle einnehmen muss

Verfahren und Systeme der Künstlichen Intelligenz (KI) sowie des maschinellen Lernens sind nicht neu. Durch die Fortschritte der IT-Technologien können sie ihre Wirkung nun jedoch richtig entfalten. Der Treibstoff des KI-Motors sind Daten, zum Beispiel Texte, Bilder, IP-Pakete in Netzen, Datenbankeinträge oder Messwerte von Sensoren. Durch vernetzte IT-basierte Systeme des Internet of Things (IoT) stehen solche Daten in großer Menge zur Verfügung. Die Menge der Daten und die Komplexität der Analyse übersteigen jedoch bei Weitem die kognitiven Fähigkeiten menschlicher Analysten. Nur mit maschinellen Lernverfahren und KI-basierten Systemen können zuverlässige Prognosen und Handlungsempfehlungen abgeleitet werden, die Menschen dabei unterstützen, schnelle und richtige Entscheidungen zu treffen.

Die Datenmassen werden mit leistungsstarken KI-Modellen verarbeitet, die große Rechen- und Speicherkapazitäten erfordern. Die nötigen Ressourcen liefern Hard- und Softwareplattformen, wie Cloud-Plattformen großer Anbieter, und vernetzte IT-Systeme. Damit sind die Voraussetzungen gegeben, um KI-Systeme in der Breite zu nutzen. Zudem können nun große Mengen strukturierter und unstrukturierter Daten aus ganz unterschiedlichen Quellen, in unterschiedlichen Formaten automatisiert verarbeitet werden. So können Zusammenhänge und Auswirkungen analysiert werden, die bislang außerhalb der Betrachtungsmöglichkeiten lagen.

Teilautonomes Fahren, zukünftige Mobilitätsplattformen, eine effiziente, bedarfsgerechte Gesundheitsversorgung, eine zukunftssichere, bezahlbare Energieversorgung, intelligente Fabrikkonzepte und nachhaltige Warenlogistikprozesse werden nur mit KI möglich sein. KI-Systeme werden also einen gravierenden Einfluss darauf haben, wie wir in Zukunft leben, arbeiten und produzieren. Sie werden unsere Kommunikation prägen und die Gestaltung gesellschaftlicher und politischer Prozesse wie demokratische Wahlen entscheidend verändern.

Es ist also eine zentrale Aufgabe für die Zukunft, KI-Systeme nachweislich sicher, zertifizierbar und verlässlich zu gestalten und sie vor Missbrauch zu schützen. KI-Systeme werden zu kritischen Infrastrukturkomponenten. Das umfasst nicht nur die Algorithmen, sondern das gesamte KI-Ökosystem: von den Sensoren für die Datenerhebung über die Kommunikationsverbindungen für den Datenaustausch bis zu den Plattformen für die Datenanalyse und -verarbeitung.

1. CYBER-SICHERHEIT DURCH KÜNSTLICHE INTELLIGENZ

Durch die zunehmende Vernetzung im IoT wächst die Anzahl von möglichen Angriffspunkten rasant. Die Systeme von Privatpersonen, Firmen und Staaten werden immer verwundbarer. Heutige Systeme ändern sich mit hoher Dynamik. Sie sind softwaregetrieben, werden kontinuierlich erweitert, mit Updates versehen oder verbinden sich automatisiert mit unterschiedlichen Geräten. Statische, perimeterbasierte Schutzmaßnahmen greifen daher zu kurz. Cyber-Sicherheit muss kontinuierlich über die gesamte Lebenszeit eines Systems geprüft und überwacht werden. Menschliche Analysten können die stetig wachsende Zahl von auszuwertenden Ereignissen und Daten nicht mehr bewältigen. Daher wird es für sie immer schwieriger, zuverlässige Aussagen über den Sicherheitszustand eines Systems zu treffen. Konzepte des maschinellen Lernens können dabei helfen.

Schon heute werden KI-Konzepte und -Methoden erfolgreich verwendet, um die Sicherheit von Systemen und deren Nutzern zu schützen. Beispielsweise werden KI-basierte Algorithmen auf Netzwerken (Intrusion Detection Systems) eingesetzt, um sämtliche Datenpakete eines Netzwerks automatisiert zu analysieren. Falls Pakete oder Sequenzen von Paketen vom erwarteten Verhalten abweichen, deutet das auf einen Angriff auf das System hin. In diesem Fall kann ein Sicherheitsexperte zurate gezogen werden, um gegebenenfalls Gegenmaßnahmen einzuleiten. Weitere nennenswerte Einsatzfelder von KI in der Cyber-Sicherheit sind Zugangskontrollsysteme, Authentifizierung, Softwaretesting und die Kryptoanalyse. Die Cyber-Sicherheit kann also in zahlreichen Anwendungsfällen von den Vorzügen der KI profitieren. Mit KI-basierten Threat-Intelligence-Systemen lassen sich mögliche Angriffe frühzeitiger, schneller und auch mit höherer Treffergenauigkeit bestimmen, sodass die Lagebewertung qualitativ erheblich verbessert werden kann sowie Risiken verkleinert und potenzielle Schäden verringert werden können. Zudem nutzen auch Angreifer zunehmend KI-Methoden und Algorithmen, um intelligente Attacken durchzuführen. Daher müssen auch zur Verteidigung automatisierte KI-Lösungen eingesetzt werden.

> „Deutschland ist prädestiniert, bei der Entwicklung vertrauenswürdiger KI **eine Vorreiterrolle** einzunehmen."

2. CYBER-SICHERHEIT VON KI-SYSTEMEN

Gerade im Bereich der Cyber-Sicherheit ist die Vertrauenswürdigkeit der verwendeten KI-Methoden von zentraler Bedeutung. Falls das KI-System falsche Entscheidungen trifft, können große Schäden entstehen. Man unterscheidet zwei Klassen von Fehlentscheidungen.

Die erste Klasse beschreibt Ungenauigkeiten der KI selbst. Diese entstehen während des Trainings der KI, in dem bekannte Paare, bestehend aus Datenpunkt und Label, die Entscheidungsgrenzen formen und das spätere Verhalten der KI bestimmen. Die daraus resultierenden Fehlentscheidungen werden also nicht durch einen Angriff gezielt hervorgerufen. Mögliche Ursachen sind stattdessen eine nicht ausreichende Größe des Trainingsdatensatzes, Ungenauigkeiten im Trainingsdatensatz oder fehlerhafte Parametereinstellungen durch den Nutzer.

Fehler der zweiten Klasse resultieren aus gezielten Angriffen. Diese können anhand des Zeitpunkts der Angriffe unterschieden werden. So kann der verwendete Datensatz vor oder während des Trainings manipuliert werden. Diese Art von Angriffen ist immer dann möglich, wenn die verwendeten Daten frei zugänglich sind und der Trainingsprozess der KI durch einen Angreifer identifiziert und beeinflusst werden kann.

Alternativ kann ein Angriff ein bereits trainiertes und erprobtes maschinelles Lernmodell adressieren. Ein Angreifer kann den Input, welcher von der KI analysiert werden soll, gezielt manipulieren. Dazu können gezielte Angriffsalgorithmen verwendet werden. Eigenschaften der KI werden effizient und gezielt ausgenutzt, als dass die Änderungen der manipulierten Daten zu klein sind, sodass ein

menschlicher Experte Unterschiede zu den originalen Daten erkennen könnte. Solche Angriffe sind derzeit meist nicht detektierbar. Das erschwert die Entwicklung von Gegenmaßnahmen erheblich.

Wenig erforscht ist, welche minimalen Änderungen der Eingabedaten zu welchen gravierenden Fehlentscheidungen der KI führen können. Für Einzelfälle wurde zwar vielfach gezeigt, wie ein solches Fehlverhalten herbeigeführt werden kann, allerdings ist unklar, ob sich diese Angriffe auf unterschiedliche KI-Modelle übertragen lassen und welche Folgen das hat. Zudem fehlen Systematiken und Konzepte, um KI-Systeme gegen diese Art von Angriffen abzusichern.

Darüber hinaus ist ein weiterer Punkt von großer Bedeutung, der die Vertrauenswürdigkeit von KI gefährden kann: die Transparenz und Erklärbarkeit der Entscheidungen der KI. Betrachtet man den aktuellen Stand der Forschung und mögliche Gefahren durch die Nutzung von KI, ist es nicht empfehlenswert, Entscheidungen eines Gesamtsystems gänzlich durch KI durchführen zu lassen. Ein menschlicher Experte sollte in regelmäßigen Abständen in den Entscheidungsprozess eingebunden werden, um die Verwundbarkeit durch KI zu minimieren.

3. RESILIENTE KI

Die Entwicklung vertrauenswürdiger, resilienter KI ist eine der zentralen Zukunftsaufgaben, um die Chancen von KI effektiv nutzen zu können. Resilienz umfasst hier die Eigenschaft, dass die verwendete KI auch bei erwarteten Veränderungen der Umwelt oder bei Angriffen zuverlässig arbeitet.

Resiliente KI-Systeme müssen das gesamte KI-Ökosystem umfassen. Nur mit vertrauenswürdigen Daten, die in großer Menge verfügbar sind, können umfangreiche Trainingsdurchläufe durchgeführt werden, die besonders für komplexe Modelle nötig sind. Zum anderen ist die Vertrauenswürdigkeit der verwendeten Algorithmen und Konzepte entscheidend. Die verwendeten Methoden und Modelle müssen transparent und deren Entscheidungen erklärbar sein. Durch die oft fehlende Transparenz bei der Entscheidungsfindung können beispielsweise bei Grenzfällen unerwartete oder falsche Entscheidungen getroffen werden. Außerdem können fachkundige Angreifer die KI manipulieren, indem sie, wie bereits beschrieben, ihre Umwelt gezielt verändern.

Deutschland ist prädestiniert, bei der Entwicklung vertrauenswürdiger KI eine Vorreiterrolle einzunehmen. Denn der Standort verfügt über ausgezeichnete Kompetenzen in den Bereichen der Zertifizierung, der KI und der IT-Sicherheit. Zudem gehört der faire und vertrauenswürdige Umgang mit sensitiven Daten zu den Grundwerten unseres Demokratieverständnisses.

4. ZERTIFIZIERUNG VON KÜNSTLICHER INTELLIGENZ

Um Künstliche Intelligenz für weitere sicherheitskritische Bereiche nutzbar zu machen, bedarf es dringend Methoden und Prozessen zur Zertifizierung. Dies umfasst sowohl Methoden des Datenmanagements als auch die Zertifizierbarkeit der verwendeten KI selbst.

Im Folgenden wird lediglich auf Herausforderungen eingegangen, die bei der Steigerung der Resilienz von KI zum Tragen kommen. Dieser Bereich der KI-Zertifizierung bedarf neuer Lösungen, für welche die klassischen Ansätze der Cyber-Sicherheit zum Teil nicht ausreichen. Im Gegensatz dazu kann der Teilaspekt der Verwaltung, Verwendung, Sicherung und Bereitstellung der Daten mit klassischen Ansätzen gelöst werden.

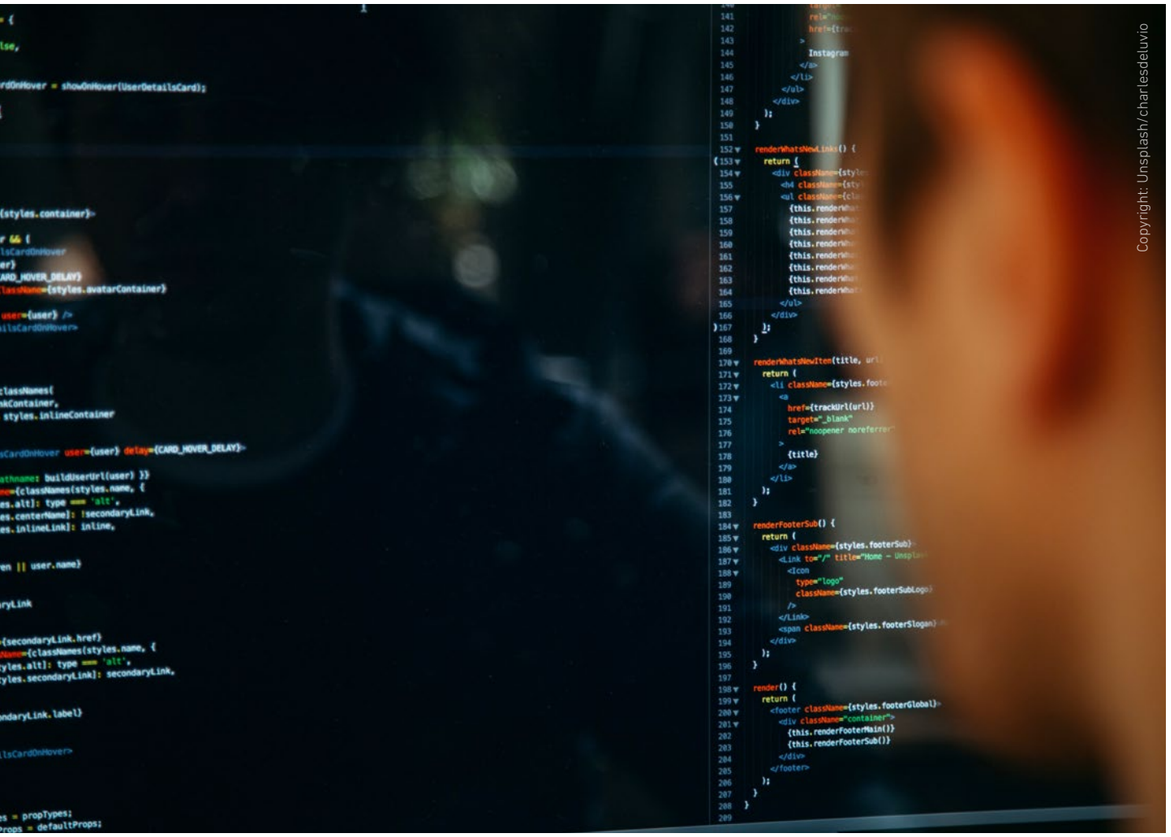
Es muss weiter untersucht werden, wie die Entscheidungsgenauigkeit von KI verbessert werden kann. Dies trifft sowohl auf den Normalfall als auch auf den Fall eines Angriffs zu. In beiden Fällen soll die KI so agieren, wie es vor und während des Trainings durch den Anwender angestrebt wurde. Momentan kann KI in beiden beschriebenen Fällen zufriedenstellende Resultate erzielen, was in bestimmten Szenarien, bei Grenzfällen oder während eines Angriffs aber zu Inkonsistenzen führen kann.

Benötigt werden zudem Methoden, um Angriffe auf die verwendete KI zu erkennen. Der aktuelle Stand der Forschung auf diesem Gebiet umfasst einige vielversprechende Lösungen, die größtenteils praktischer Natur sind und das System nicht formal vor Angriffen schützen können. Dementsprechend muss weiterhin Forschung betrieben und besonders formalen Lösungen große Aufmerksamkeit gewidmet werden. Im Gegensatz zu praktischen Ansätzen agieren formale Detektionsmethoden unter allen möglichen Bedingungen der KI und ihrer Umwelt vorhersehbar und treffen begründbare Aussagen. Dies würde eine Zertifizierung der Detektionsmethoden möglich machen.

Außerdem muss die Transparenz der Entscheidungen von KI gesteigert werden. Dies erleichtert es zum einen, Ergebnisse im Nachhinein zu analysieren und die Trainingsprozesse zu verbessern. Zum anderen steigert dies die Chancen, Angriffe frühzeitig zu erkennen. Zudem würden Grenzfälle, die in Fehlentscheidungen münden, besser verstanden. Schon in das Training könnten Präventionsmaßnahmen eingebaut werden.

Als finaler und umfangreichster Punkt soll eine Zertifizierung von KI-Methoden, -Modellen und Algorithmen möglich gemacht werden. Diese Zertifikate sollen den Grad der Resilienz zum Ausdruck bringen und als Handlungsempfehlung für Anwender dienen. Über Probleme bei der Zertifizierung von KI und über die Voraussetzungen werden im Folgenden detaillierte Aussagen gemacht. Die daraus folgenden Handlungsempfehlungen können als Leitfaden für zukünftige Aktionen von Wirtschaft, Industrie und Forschung dienen.

Grundlage für eine Zertifizierung ist es, Empfehlungen von Expertenkommissionen in konkrete Anforderungen


Copyright: Unsplash/charlesdeluvio

zu übersetzen, die sich von technischen Prüforganisation oder Wirtschaftsprüfern kontrollieren lassen. Die Prüforganisationen werden von einer zentralen Stelle akkreditiert. Für KI-Systeme fehlen bislang sowohl Prüfkataloge, Prüfverfahren für KI-Algorithmen (unter anderem Verfahren des maschinellen Lernens) als auch technische Richtlinien für die Entwicklung resilienter KI-Produkte.

Benötigt werden:

1. Prüfkataloge, die einerseits auf unternehmerische Prozesse und Governance-Anforderungen abzielen sowie andererseits die technische Qualität und Sicherheit der Anwendungen adressieren. Hierzu müssen je nach Kritikalität der Anwendung unterschiedliche Zertifizierungsstufen entwickelt werden.
2. Ergänzend dazu sind spezifische Kataloge und technische Prüfverfahren für unterschiedliche Branchen (zum Beispiel Medizin, Mobilität, Logistik, Produktion) dringend erforderlich, um den unterschiedlichen Anforderungen, auch regulatorischer Art, der Branchen geeignet Rechnung zu tragen.

Um Unternehmen in die Lage zu versetzen, KI-Systeme sicher zu betreiben, müssen spezifische, neue Verfahren entwickelt werden, die KI-Anwendungen robust machen und gegen Manipulationen absichern.

5. POSITIONIERUNG DER KI IN DEUTSCHLAND

Um die aktuelle Position Deutschlands im Bereich KI international einordnen zu können, müssen zwei Aspekte betrachtet werden: In welchem Umfang wird KI in Deutschland bereits erfolgreich verwendet? Wie groß ist der Beitrag Deutschlands an der internationalen KI-Forschung?

Heute setzen zwar erst rund zehn Prozent der Unternehmen in Deutschland KI-Methoden ein. Jedoch ist zu erwarten, dass dieser Anteil mit der leichteren Verfügbarkeit von KI-Modellen und -Frameworks rasant steigen wird. Laut einer Studie der Bitkom[1] greifen bereits heute 12 Prozent der Unternehmen in Deutschland auf KI zurück, um Prozesse in Fabriken zu optimieren. Dies spiegelt das Verständnis der deutschen Industrie in Bezug auf KI sehr gut wider. Einerseits erkennt sie die Chancen und Vorzüge der Technologie. Andererseits ist das Vertrauen in die von KI getroffenen Entscheidungen noch nicht gänzlich ausgereift, um auch sicherheitskritische Domänen durch KI steuern zu lassen.

Momentan befindet sich die internationale Forschung an KI im Bereich der Cyber-Sicherheit noch in ihren Anfängen. Im Vergleich zu anderen Standorten, vor allem den USA mit ihren Big Playern wie Google oder Amazon und den universitären Forschungsgruppen, lassen sich deutliche Defizite beim Forschungserfolg erkennen. Ein Indikator dafür sind internationale Forschungskonferenzen für KI und die dazugehörigen Unterkategorien. Hier sind Forschungseinrichtungen und Konzerne aus den USA deutlich erfolgreicher und tragen mit einer größeren Zahl von Publikationen stärker zur internationalen Forschung an KI bei. 2017 wurden bei zwei der zentralen Forschungskonferenzen für KI, NIPS[2] und ICML[3], keine wissenschaftlichen Beiträge aus Deutschland vorgestellt. Google war bei beiden Konferenzen der Vertreter mit den meisten wissenschaftlichen Veröffentlichungen. Dies unterstreicht die Stärke US-amerikanischer Konzerne im Bereich KI und sollte als Weckruf verstanden werden, den Anschluss nicht zu verlieren. Über die nächsten Jahre ist es entscheidend, die Präsenz deutscher KI-Forschung bei den oben erwähnten Konferenzen zu steigern.

Zwei mögliche und stark korrelierende Ursachen für dieses Defizit können zum einen mangelnde Investitionen in die Erforschung von resilienter KI sein und zum anderen ein nicht ausgereiftes Bewusstsein und Erkennen der Chancen durch KI. Besonders intensive Aufklärungsarbeit muss hier zur Sensibilisierung im Hinblick auf Verwundbarkeit geleistet werden. Den Nutzern von KI ist meist nicht sofort ersichtlich, welche Gefahren die Verwendung und vor allem Abhängigkeit von nicht resilienten KI-Verfahren bergen.

6. HANDLUNGSEMPFEHLUNGEN

KI ist für den IT-Standort Deutschland ein entscheidender Faktor in Bezug auf die momentane und vor allem zukünftige Wettbewerbsfähigkeit auf europäischer und internationaler Ebene. Durch die immer größer werdenden Herausforderungen in Verbindung mit beispielsweise dem Internet of Things und Big Data müssen geeignete, performante und resiliente Methoden genutzt und weiterentwickelt werden. Falls dies nicht möglich ist und der Anschluss an die Spitzenforschung auf diesem Gebiet verloren geht, wird Deutschland auch seine Marktposition als Hightech-produktionsstandort verlieren.

Bereits heute besteht eine sehr hohe Abhängigkeit der deutschen Industrie, aber auch der öffentlichen Verwaltung von den sogenannten Hyperscalern, also Cloud-Plattformen, die Datenmengen in großem Maßstab verarbeiten. Dass diese Hyperscaler im nächsten Schritt auch KI-Frameworks zur Veredelung der Daten anbieten werden, ist nur eine Frage der Zeit. Damit steigt die Abhängigkeit, nicht nur in Bezug auf die Verarbeitung hochsensibler Daten, die in diese Clouds übertragen werden, sondern auch in Bezug auf den Algorithmus, der intransparente Analysen durchführt. Handlungsempfehlungen, die aus nicht transparenten Analysen resultieren, führen zu Unsicherheit und fehlender Nachvollziehbarkeit. Fehlerhafte Prognosen

> *„In welchem Umfang wird KI in Deutschland bereits **erfolgreich** verwendet?“*

[1] Bitkom, „Künstliche Intelligenz zieht in Fabrikhallen ein“, 01.04.2019. Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://www.bitkom.org/Presse/Presseinformation/Industrie-40-Kuenstliche-Intelligenz-zieht-Fabrikhallen-ein
[2] Medium, „NIPS accepted papers stats“, 05.12.2017. Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://medium.com/machine-learning-in-practice/nips-accepted-papers-stats-26f124843aa0
[3] Medium, „ICML accepted papers institution stats“, 24.05.2017. Zuletzt geprüft: 17.01.2020. [Online]. Verfügbar: https://medium.com/@karpathy/icml-accepted-papers-institution-stats-bad8d2943f5d

können von menschlichen Nutzern kaum als solche identifiziert werden, wenn unklar ist, auf welcher Basis die Prognose entstanden ist. Die ursprünglichen Besitzer der Daten haben keine Kontrolle mehr darüber, was mit ihren Daten in den Cloud-Plattformen passiert. Daten unterschiedlicher Quellen werden zusammengebracht, die Ergebnisdaten der Analysen werden möglicherweise auch anderweitig genutzt und kommerzialisiert, ohne dass die Dateneigentümer davon Kenntnis erlangen oder dies unterbinden können. Die digitale Souveränität wäre massiv gefährdet.

Somit kommt der Forschung zu vertrauenswürdiger, resilienter KI eine tragende Rolle zu. Es ist für Deutschland unabdingbar, den Anschluss an die internationale Entwicklung im Bereich KI zu halten. Nur so bleibt Deutschland ein erfolgreicher IT-Standort und kann unabhängig agieren. Deutschland muss zumindest eine Beurteilungskompetenz aufbauen, aber auch technologische Alternativen entwickeln, um Lock-in-Effekten entgegenzuwirken. Dadurch soll nicht nur die Wettbewerbsfähigkeit bewahrt, sondern idealerweise auch ein Wettbewerbsvorteil erarbeitet werden.

Eine weitere zentrale Handlungsempfehlung betrifft die Entwicklung von Verfahren zur KI-Zertifizierung. Nur durch diese Maßnahme werden die Risiken reduziert, welche durch eine teilweise Abhängigkeit von KI entstanden sind, und die Verwendung von KI sowohl in der Breite als auch in sicherheitskritischen Infrastrukturen wird möglich. Außerdem würde eine notwendige Zertifizierung vor dem Gebrauch von KI die Nutzer sensibilisieren. Nutzer, die bislang ohne vorhergehende Risikoanalysen auf KI gesetzt haben, werden nun vor die Aufgabe gestellt, ihre Systeme zertifizieren zu lassen und sowohl Zeit als auch Geld in eine risikobewusste Verwendung von KI zu investieren. Durch diese Sensibilisierung kann die Verwundbarkeit durch KI bereits frühzeitig verhindert werden.

Die Implementierung einer KI-Zertifizierung ist äußerst anspruchsvoll und zeitlich herausfordernd. Dies ist sowohl in der Breite der Thematik als auch in der Geschwindigkeit der technologischen Entwicklungen begründet. Deshalb sind Einzelmaßnahmen zum Aufbau einer KI-Zertifizierung nicht zielführend: Die erhoffte Vorreiterrolle für Deutschland und Europa kann so nicht erzielt werden. Es bedarf eines koordinierten Ansatzes für die Entwicklung einer KI-Zertifizierung, insbesondere für einzelne Spezialkataloge, der die wesentlichen Akteure in Deutschland mit ihren jeweiligen Schwerpunkten und Kompetenzen integriert.

Außerdem müssen in den ersten Schritten und frühen Entwürfen für Prozesse zur Zertifizierung nicht alle zuvor erwähnten Ziele erreicht werden. So kann, begründet durch die hohe Komplexität und den damit verbundenen Forschungsbedarf, zu Beginn auf die Schaffung von Transparenz der KI-Entscheidungen verzichtet werden. Eine erhoffte Zertifizierbarkeit würde schon erreicht, falls die Entscheidungen der KI garantiert in einem zuvor definierten Rahmen liegen würden. Diese Maßnahme würde es bereits in naher Zukunft möglich machen, KI und verwandte Algorithmen nur dann zuzulassen, wenn sie resiliente Methoden nutzen. Sobald dieser erste Schritt vollzogen ist, wird die Aufmerksamkeit der Forschung und Industrie auf der Schaffung von resilienter KI liegen. Dies würde weitere Erfolge in diesem Forschungsgebiet begünstigen und die Vorreiterrolle Deutschlands auch auf diesem neuen und größtenteils von anderen Nationen angeführten Gebiet wieder stärken. Letztendlich kann nur durch ein schnelles Handeln und Einleiten von geeigneten Maßnahmen und Investitionen im Bereich KI die Wettbewerbsfähigkeit Deutschlands auch in den nächsten Jahrzehnten gewährleistet werden.

ABSTRACT
Durch Fortschritte der IT-Technologien können Künstliche Intelligenz und maschinelles Lernen zunehmend ihre Wirkung entfalten. Der Treibstoff des KI-Motors sind Daten, die durch vernetzte IT-basierte Systeme des Internet of Things (IoT) in großer Menge zur Verfügung stehen. KI-Systeme werden sich entscheidend darauf auswirken, wie wir in Zukunft leben, arbeiten und produzieren. Sie werden unsere Kommunikation prägen und die Gestaltung gesellschaftlicher und politischer Prozesse grundlegend verändern. Die Vertrauenswürdigkeit derartiger Systeme ist für Unternehmen aller Branchen, aber auch für staatliche Institutionen von höchster Wichtigkeit. Unternehmerische Entscheidungen werden zunehmend auf Ergebnissen von KI-Systemen basieren. Es entsteht eine gefährliche Abhängigkeit, da die Ergebnisse von maschinellen Lernverfahren meist

Copyright: freepik/slidesgo

„Noch setzen erst rund 10 Prozent der Unternehmen KI-Systeme ein."

nicht nachvollziehbar sind und auch die Qualität der Daten, die zum Anlernen genutzt werden, für die Nutzer nicht prüfbar ist. Aufgrund ihres Einsatzes in einer Vielzahl sicherheitskritischer Bereiche werden verlässliche, transparente und zertifizierte KI-Systeme benötigt. Hersteller müssen IT-Systeme und -Lösungen nicht nur einmalig bei der Produkt- und Systemeinführung auf Schwachstellen testen, sondern diese Tests kontinuierlich wiederholen. Tests sollten dabei technologisch breit aufgestellt sein. Bei Quellcodetests sollten statische und dynamische Methoden zum Einsatz kommen. Bei Systemtests müssen alle Komponenten berücksichtigt werden. Die Ergebnisse der Tests müssen transparent und überprüfbar sein. Hersteller müssen ihre Geräte, Dienste und Anwendungen über die komplette Lebenszeit mit Sicherheitsupdates versorgen.

KRYPTOAGILITÄT UND POST-QUANTEN-KRYPTOGRAFIE

Wie wir uns gegen Gefahren von morgen wappnen können

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht in regelmäßigen Abständen die technische Richtlinie TR-02102, die Empfehlungen für den Einsatz kryptografischer Verfahren gibt. Neben der allgemeinen Richtlinie finden sich speziellere für konkrete Einsatzszenarien wie die Nutzung von Kryptografie in Kommunikationsprotokollen (zum Beispiel IPsec oder TLS). Allen gemein ist eine klare Empfehlung der Algorithmen für einen festgelegten Zeitraum, in der Regel für fünf Jahre. Die aktuelle Version spricht beispielsweise Empfehlungen bis maximal Ende 2025 aus. Der Grund dafür ist die rasante technologische Entwicklung in allen Bereichen der Informationstechnik, insbesondere aber (un)erwartete Entwicklungen in der Kryptoanalyse. So ist selbst bei etablierten, international standardisierten kryptografischen Verfahren nicht klar, wie sich deren Sicherheit längerfristig verhalten wird. Dies bezieht sich gleichermaßen auf symmetrische Verfahren wie den Advanced Encryption Standard AES oder die Secure-Hash-Function-Familie SHA-2 sowie auf Public-Key-Verfahren wie das RSA-Kryptosystem oder elliptische Kurven. Zwar ist anzunehmen, dass die meisten Algorithmen auch weit nach Ende 2025 noch ein bestimmtes Sicherheitsniveau erreichen werden. Ein Bruch einzelner Verfahren ist jedoch nicht ausgeschlossen und eine seriöse Abschätzung über einen Zeitraum von fünf Jahren hinaus praktisch unmöglich.

Einen besonderen Einschnitt in die Sicherheit kryptografischer Verfahren stellt die Entwicklung eines skalierbaren Quantencomputers dar. Ein derartiger Computer wirkt sich weitreichend auf das Sicherheitsniveau der angesprochenen Algorithmen aus und macht eine Verdoppelung der Schlüssellänge aller symmetrischen Verschlüsselungsverfahren sowie der Ausgabelänge von Hashfunktionen nötig. Viel weitreichender sind allerdings die Auswirkungen auf Public-Key-Verfahren: Der (Quanten-)Algorithmus von Shor ermöglicht es nämlich, alle heute gebräuchlichen Public-Key-Verfahren zu brechen.

Unabhängig von der Entwicklung eines skalierbaren Quantencomputers wird die technologische Entwicklung es erfordern, mit immer längeren Schlüsseln zu arbeiten. Der nächste Sprung findet schon Ende 2022 statt, wenn heute gebräuchliche Schlüssellängen für das RSA-Kryptosystem nach der BSI-Richtlinie um 50 Prozent vergrößert werden müssen, um den aktuellen Entwicklungen in der Kryptoanalyse zu begegnen. Dabei hat eine derartige Vergrößerung der Schlüssellängen weitreichende Folgen. Der Berechnungsaufwand steigt, was insbesondere kleine eingebettete Geräte oder Smartcards vor Probleme stellt. Zudem müssen teilweise die Kommunikationsprotokolle angepasst werden, welche die kryptografischen Verfahren einsetzen. Bei einer derartigen Änderung müssen diese Protokolle erneut standardisiert werden, was wiederum einen sehr langwierigen Prozess nach sich zieht.

1. GEFAHREN DURCH IMPLEMENTIERUNGSANGRIFFE

Eine wesentliche Ursache für die Schwäche von Kryptosystemen ist deren Anfälligkeit für sogenannte Implementierungsangriffe. Im Gegensatz zur klassischen Kryptoanalyse, die sich auf die Ein- und Ausgaben einer Berechnung konzentriert, beschäftigen sich Implementierungsangriffe explizit mit Eigenschaften, die auf der Implementierungsebene zutage treten. Solche Eigenschaften sind beispielsweise die Ausführungszeit des Algorithmus bzw. von Teilen des Algorithmus, der präzise datenabhängige Stromverbrauch während der Berechnung oder die Möglichkeit, während der Berechnung Fehler in Zwischenwerte einzubringen. Wichtige Ausprägungen von Implementierungsangriffen sind die mittlerweile weithin bekannten passiven Seitenkanalangriffe sowie die aktiven Fehlerangriffe. Solche Angriffe setzen meistens einen Zugriff eines Angreifers auf das Gerät voraus, um beispielsweise Messungen des Stromverbrauchs durchzuführen oder Fehler einzubringen – in vielen eingebetteten Systemen sehr realistisch.

Mächtige Implementierungsangriffe können jedoch auch ohne einen physischen Zugriff erfolgen. Ein wichtiges Beispiel sind die sogenannten Cache-Seitenkanalangriffe als Vertreter einer breiter formulierten Klasse von Mikroarchitekturangriffen. Bei diesen geht ein Angriff von einem Softwareprozess auf der gleichen CPU aus, die in einem anderen Prozess eine kryptografische Berechnung durchführt – ein sehr realistisches und gefährliches Szenario im Cloud Computing.

Seitenkanalangriffe auf Basis von Messungen des Stromverbrauchs oder Magnetfelds und Fehlerangriffe in verschiedenen Ausprägungen werden bereits

seit etwa 20 Jahren intensiv untersucht. Die letztgenannte Klasse von Seitenkanalangriffen hat sich jedoch erst in den letzten Jahren dramatisch entwickelt. Die wegweisenden Angriffe Meltdown und Spectre gegen sämtliche x86 CPUs wurden beispielsweise erst Anfang 2018 veröffentlicht.

Es gibt unzählige Varianten von Implementierungsangriffen und viele bekannte Gegenmaßnahmen, die gewisse Angriffe verhindern oder erschweren können. Für wichtige kryptografische Algorithmen wie den AES-Algorithmus ist die Härtung gegen Seitenkanalangriffe aber ein ungelöstes Problem. Bestimmte Gegenmaßnahmen können die Angriffe zwar erschweren und schaffen in Kombination ein sehr hohes Sicherheitsniveau. Dennoch bleiben zeitnahe Angriffe möglich, beispielsweise durch Verbesserungen der Angriffstechnik oder intensivierten Aufwand. Zudem werden auch ständig neue Angriffsvarianten entdeckt. Alles in allem ist der Bereich der Implementierungsangriffe gegen standardisierte und mathematisch hochsichere Algorithmen hoch volatil, sodass konkrete Implementierungen jeweils zeitnah unsicher werden könnten. Leider erfordert eine darauffolgende Härtung der Implementierung in den meisten Fällen eine Modifikation derselben.

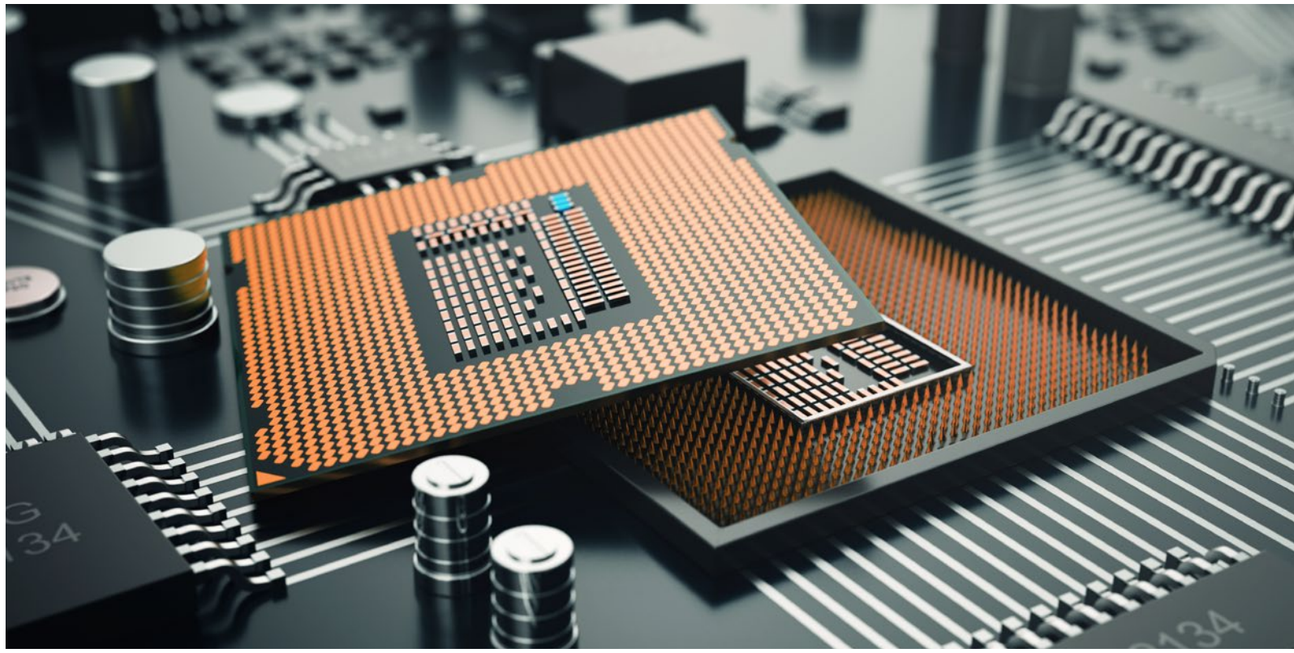
2. NOTWENDIGKEIT VON KRYPTOAGILITÄT

Für alle geschilderten sicherheitskritischen Fälle müssen Systeme so entwickelt und vorbereitet werden, dass einfach auf neue kryptografische Algorithmen, Schlüssellängen oder bessere Implementierungen migriert werden kann. Wünschenswert sind neue Protokolle und Systemarchitekturen, die Kryptoagilität, also den Austausch von kryptografischen Verfahren, ohne Beeinträchtigung des eigentlichen Protokolls in viel höherem Maße ermöglichen als heute. Bleibt es bei einer gleichermaßen rasanten technologischen Entwicklung, müssen wir darauf vorbereitet sein, dass einzelne Verfahren schnell und zuverlässig ausgetauscht werden können, ohne die Interoperabilität zu gefährden – denn der Quantencomputer ist nur eine von vielen künftigen Möglichkeiten, kryptografische Verfahren anzugreifen.

Die Forderung nach Kryptoagilität ist keineswegs neu. Bereits in der Vergangenheit sind bestimmte Verschlüsselungsverfahren und Hashfunktionen als unsicher eingestuft worden. So lief beispielsweise die Zertifizierung des Verschlüsselungsverfahrens DES 1998 aus, die Hashfunktion MD5 gilt seit spätestens 2008 als unsicher und SHA-1 wird seit 2017 von vielen Systemen nicht mehr akzeptiert. In der Folge mussten diese Verfahren in den Systemen ersetzt werden. Noch heute sehen wir jedoch Systeme, die Daten mittels 3DES verschlüsseln, RSA mit zu geringen Schlüssellängen nutzen und Implementierungen verwenden, die nicht mehr sicher gegen aktuelle Seitenkanal- und Fehlerangriffe sind. Die Gründe hierfür sind vielfältig. Zum Teil ist die Hardware nicht für aktuelle kryptographische Verfahren ausgelegt oder sie kann die notwendigen Schlüssellängen nicht verarbeiten. Häufig ist es auch sehr aufwendig, die eingesetzte Software zu aktualisieren, weil sich selbst kleine Änderungen auf viele Teile des Systems auswirken können. Allgemein gilt, dass in diesen Fällen die Architektur nicht für Änderungen ausgelegt wurde.

Handlungsempfehlung

Implementierungsangriffe entwickeln sich ständig weiter und haben im Gegensatz zur klassischen mathematischen Kryptoanalyse eine reale Wirksamkeit, sodass kryptografische Schlüssel aus Geräten extrahiert werden. Agilität in Bezug auf die Implementierung von kryptografischen Algorithmen ist also essenziell für langfristige Sicherheit. Systeme, die langfristig als sicher gelten sollen, benötigen daher nicht nur Agilität hinsichtlich des Austauschs von Algorithmen, sondern auch hinsichtlich des Austauschs oder zumindest der Modifikation von deren Implementierung. Eine solche Agilität erfordert die Möglichkeit zur Modifikation der entsprechenden Software und im Idealfall der Hardware, was vor allem bei Systemen mit konfigurierbaren Hardwarebausteinen, sogenannten FPGAs, möglich ist. Grundsätzlich entspricht diese Forderung der mittlerweile breit akzeptierten Meinung, dass Systeme mit Aktualisierungen versorgt werden müssen, um eine längerfristige Sicherheit zu wahren. Systeme müssten daher in einer Art konzipiert und entwickelt werden, dass eine Agilität der kryptografischen Implementierung auf allen Ebenen gewährleistet ist. Nur das kann helfen, um Implementierungsangriffen entgegenzutreten, die aktuell noch unbekannt sind.



Eine Möglichkeit dafür ist zum Beispiel, alle notwendigen Sicherheitsfunktionen über eine Kryptobibliothek oder Hardware so einzubinden, dass die Software völlig unabhängig von den konkret eingesetzten kryptografischen Verfahren und Schlüssellängen funktioniert. Weiter muss der Hersteller dafür sorgen, dass alle Bestandteile seines Systems sicher aktualisierbar sind, und er muss Prozesse etablieren, über die er feststellen kann, ob und wodurch seine Lösung angreifbar ist oder werden könnte.

Die Politik könnte zum Beispiel durch zwei Maßnahmen die oben genannten Probleme lösen: Erstens sollte bei einer Sicherheitszertifizierung nicht nur der aktuelle Sicherheitszustand des Systems untersucht werden, sondern auch, ob und wie das Thema Kryptoagilität vom Hersteller umgesetzt wird.

Dies hat allerdings nur Auswirkungen auf zertifizierte Systeme. Die allermeisten Lösungen streben jedoch gar keine Sicherheitszertifizierung an. Um auch hier ein Mindestmaß an Sicherheit gewährleisten zu können, sollte zweitens das Thema Softwarehaftung wieder verstärkt diskutiert und sollten Lösungen hierfür gefunden werden. Ein Hersteller verhält sich grob fahrlässig, wenn er Sicherheitslücken, die sich zukünftig ergeben können, nicht beheben kann, weil er hierfür keine Prozesse vorgesehen hat.

3. POST-QUANTEN-KRYPTOGRAFIE

Wie bereits ausgeführt, werden Quantencomputer erhebliche Auswirkungen auf die Sicherheit heute eingesetzter Kryptoverfahren haben. Bei symmetrischen Verschlüsselungsverfahren, wie zum Beispiel AES, reduziert sich die Schlüsselsuche durch einen von Grover 1996 entwickelten Suchalgorithmus. Die Sicherheit kann aber durch die Verdoppelung der Schlüssellänge wieder auf das ursprüngliche Niveau gehoben werden. Ähnliche Auswirkungen ergeben sich bei Hashfunktionen (SHA256 usw.). Auch hier kann durch die Vergrößerung des Bildbereichs das notwendige Sicherheitsniveau wieder erreicht werden. Darüber hinaus werden hierfür Quantencomputer benötigt, die eine sehr große Anzahl von Qbits benötigen.

Viel stärker wirken sich Quantencomputer aber auf aktuell genutzte asymmetrische Verfahren aus. Lediglich heutzutage kaum praxisrelevante Public-Key-

Verfahren scheinen nach aktuellem Kenntnisstand Quantencomputern zu widerstehen. Der Einsatz dieser Verfahren ist jedoch nicht ohne Weiteres möglich, da sie entweder enorme Schlüsselgrößen oder sehr komplexe Implementierungen erfordern. Ein von Shor[1] 1994 entwickelter Algorithmus bricht auf einem Quantencomputer entsprechender Größe sehr effizient kryptografische Verfahren, deren Sicherheit auf dem Faktorisierungsproblem basiert, wie dies zum Beispiel bei dem sehr weit verbreiteten RSA-Verfahren und der RSA-Signatur der Fall ist. Aber auch das derzeit noch sehr schwer zu lösende Problem der Berechnung diskreter Logarithmen, das beispielsweise dem Signaturstandard DSA, dem Verschlüsselungsverfahren ElGamal oder dem in der Praxis sehr verbreiteten Schlüsseleinigungsverfahren Diffie-Hellman zugrunde liegt. Eine Anpassung der Schlüssellänge wie bei symmetrischen Verfahren ist hier nicht möglich. Die Größe der Schlüssel müsste soweit erhöht werden, dass etwa die Schlüsselgenerierung nicht mehr effizient durchführbar ist. Im Gegensatz zu den Folgen für symmetrische Verfahren genügen hier schon Quantencomputer mit deutlich weniger Qbits.

*„Der **Quantencomputer** ist nur eine von vielen künftigen Möglichkeiten, kryptografische Verfahren anzugreifen."*

Damit werden durch Quantencomputer nahezu alle der heute eingesetzten Public-Key-Verfahren (Signatur-, Schlüsselaustausch- und asymmetrische Verschlüsselungsverfahren) unsicher. Dies betrifft die meisten aktuell verwendeten kryptografisch abgesicherten Internetverbindungen (zum Beispiel über https oder Virtual Private Network [VPN]). Die NSA warnt bereits vor den Auswirkungen von Quantencomputern und hat eine Migration hin zu quantencomputerresistenten Verfahren eingeleitet.[2] Auch das BSI hat sich des Themas angenommen.[3] Darüber hinaus hat das NIST im Jahr 2017 einen Standardisierungsprozess für quantencomputerresistente Verfahren gestartet[4], und die ISO ist mit einer Study Period in dieser Sache ebenfalls aktiv geworden.[5]

Stand der Forschung

Benötigt werden quantencomputerresistente Signaturverfahren. Signaturverfahren sind essenziell, beispielsweise für einen sicheren Updateprozess und für die Authentisierung von Kommunikationspartnern. Eine Vielzahl von smarten Geräten baut spontan eine Kommunikationsverbindung im IoT auf. Hierbei werden Schlüsselverteilungsverfahren wie Diffie-Hellman genutzt, um eine sichere Kommunikation zu ermöglichen. Quantencomputerresistente Schlüsseleinigungs-/Schlüsselaustauschprotokolle sind somit eine essenzielle Voraussetzung für eine sichere Kommunikation in IoT und anderen vernetzten Szenarien.

Derzeit werden in der Wissenschaft folgende Klassen von quantencomputerresistenten Algorithmen vorgeschlagen:

1. **hashbasierte Signaturverfahren**[6]
2. **gitterbasierte Verfahren**[7]
3. **codebasierte Verfahren**[8]
4. **isogeniebasierte Verfahren**[9]
5. **Verfahren, basierend auf multivariaten Polynomsystemen**[10]

Hash- und codebasierte Verfahren existieren bereits seit dem Ende der 70er-Jahre und gelten allgemein als sicher. Dabei können hashbasierte Signaturverfahren nur für Signaturen und nicht für eine Schlüsseleinigung verwendet werden. Codebasierte Verfahren können auch zur Schlüsseleinigung verwendet werden, haben aber den Nachteil sehr großer Schlüssellängen. Alle anderen Vorschläge wurden hinsichtlich ihrer Sicherheit gegenüber kryptoanalytischen Methoden mittels klassischer Computer noch nicht hinreichend untersucht. Genau hier setzt die Aktivität der oben erwähnten NIST-Initiative an. Vorschläge in Bezug auf quantencomputerresistente Verfahren für Signaturen und Schlüsseleinigungs-/Schlüsselaustauschprotokolle werden eingereicht, veröffentlicht und von WissenschaftlerInnen bewertet. Der Wettbewerb befindet sich aktuell in Stufe 2. Mit einem Abschluss ist 2020 zu rechnen.

Handlungsempfehlungen

Es ist unabdingbar, dass in Deutschland die Forschung im Bereich Post-Quantum-Kryptografie weiter verstärkt wird, damit Kompetenzen in diesem Feld auf- und ausgebaut werden, da dies für die zukünftige Cyber-Sicherheit unserer Systeme essenziell ist. Jedoch darf sich dies nicht auf die Erforschung neuer Verfahren beschränken, sondern muss Hand in Hand gehen mit der Entwicklung von agilen Kryptokonzepten. Die sichere Implementierung von Post-Quanten-Verfahren sowie die Entwicklung geeigneter Test- und Validierungstools müssen von Anfang an integraler Bestandteil zukünftiger Forschungsaktivitäten sein. Bereits jetzt müssen Migrationsstrategien entwickelt und erprobt werden, die einen einfachen Übergang auf Post-Quanten-Kryptoverfahren ermöglichen.

ABSTRACT

Einen besonderen Einschnitt in die Sicherheit kryptografischer Verfahren stellt die Entwicklung eines skalierbaren Quantencomputers dar. Ein derartiger Computer wirkt sich weitreichend auf das Sicherheitsniveau der angesprochenen Algorithmen aus und macht eine Verdoppelung der Schlüssellänge aller symmetrischen Verschlüsselungsverfahren sowie der Ausgabelänge von Hashfunktionen nötig. Viel weitreichender sind allerdings die Auswirkungen auf Public-Key-Verfahren: Der (Quanten-)Algorithmus von Shor ermöglicht es nämlich, alle heute gebräuchlichen Public-Key-Verfahren zu brechen.

Unabhängig von der Entwicklung eines skalierbaren Quantencomputers wird die technologische Entwicklung es erfordern, mit immer längeren Schlüsseln zu arbeiten. Der nächste Sprung findet schon Ende 2022 statt, wenn heute gebräuchliche Schlüssellängen für das RSA-Kryptosystem nach der BSI-Richtlinie um 50 Prozent vergrößert werden müssen, um den aktuellen Entwicklungen in der Kryptoanalyse zu begegnen.

Es ist daher unabdingbar, dass in Deutschland die Forschung im Bereich Post-Quanten-Kryptografie weiter verstärkt wird, damit Kompetenzen in diesem Feld auf- und ausgebaut werden, da dies für die zukünftige Cyber-Sicherheit unserer Systeme essenziell ist. Kryptografische Verfahren, Schlüssellängen und Zufallszahlengeneratoren, die heute sicher sind, können morgen schon unsicher sein. Entwicklungen im Bereich Quantencomputing werden dazu führen, dass asymmetrische Verschlüsselungsverfahren wie RSA unsicher werden. Deshalb empfehlen wir, für IT-Lösungen, die eine lange Lebenszeit haben können, ein kryptoagiles Design als Bestandteil eines Mindeststandards aufzunehmen. Das bedeutet, dass sie die Möglichkeit bieten sollten, kryptografische Verfahren und Zufallszahlengeneratoren auszutauschen sowie Schlüssellängen zu erhöhen, ohne ihre eigentliche Funktion zu beeinträchtigen oder Hardware auszuwechseln. Die Fähigkeiten zur Evaluation und Analyse von Post-Quanten-Kryptoverfahren müssen weiter ausgebaut werden. Dies ist eine zentrale Voraussetzung für hochsichere Systeme. Bereits jetzt müssen Migrationsstrategien entwickelt und erprobt werden, die einen einfachen Übergang auf Post-Quanten-Kryptoverfahren ermöglichen.

[1] P. W. Shor, „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," in: J. Siam. Comput., 1997,Seiten 1484–1509.
[2] National Security Agency (NSA), „Commercial National Security Algorithm Suite," Information Assurance by the NSA, 2015.
[3] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Entwicklungsstand Quantencomputer," Studie des BSI, 2018.
[4] National Institute of Standards and Technology (NIST), „Post-Quantum Cryptography Standardization," 2016.
[5] ISO/IEC, „Meeting report of Study Period on Quantum resistant cryptography," ISO/IEC JTC 1/SC27/WG 2 (Cryptography and security mechanisms).
[6] R. C. Merkle, „Secrecy, authentication, and public key systems," Ph.D. thesis, Electrical Engineering, 1979.
[7] M. Ajtai, „Generating Hard Instances of Lattice Problems (Extended Abstract)," in Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, New York, ACM, 1996, Seiten 99–108.
[8] R. J. McEliece, „A Public-Key Cryptosystem Based On Algebraic Coding Theory," Deep Space Network Progress Report, Bd. 44, 1978, Seiten 114–116, 1978.
[9] D. Jao und L. De Feo, „Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic," in Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Seiten 19–34.
[10] T. Matsumoto und H. Imai, „Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption," in Advances in Cryptology --- EUROCRYPT ,88, , 1988, Seiten 419–453.

ALLES ODER NICHTS?

Über die Mittel zum Schutz der Demokratie in einer digitalen Welt

Das Internet und die sozialen Medien bieten eine Zentralisierung von Informationen und Vernetzung von Menschen. Soziale Medien sind nicht nur beschränkt auf den privaten Bereich, sondern wurden in den vergangenen Jahren auch als Plattform für politische Aktionen wie den Arabischen Frühling[1,2] genutzt. Das Internet und die sozialen Medien können die Demokratie unterstützen und stärken, sie aber durch die Verbreitung von manipulierten Informationen und Manipulationen der Wähler auch gefährden.[3,4,5] Beide Arten von Manipulationen können die Wählermeinungen und als Folge ihre politischen Entscheidungen beeinflussen. Freie politische Entscheidungen gelten jedoch als Grundlage für die Demokratie.[6] Manipulationen in der politischen Szene wurden schon in verschiedenen Fällen wie den US-amerikanischen und französischen Wahlkämpfen sowie dem Brexit-Referendum nachgewiesen.[7,8]

Medienmanipulationen, d.h. Manipulationen von Informationen und Bildern, hat es schon immer gegeben, aber der Aufstieg und Einfluss der sozialen Medien haben deren Bedeutung in den letzten Jahren verstärkt.[9] Der Anteil der Menschen, die soziale Medien als Hauptinformationsquelle nutzen, stieg in Deutschland zwischen 2014 und 2016 von 23 auf 31 Prozent.[10] Statt klassische und verifizierte Quellen zu nutzen, wird Plattformen vertraut, die auf nutzergenerierten Inhalten basieren. Die Offenheit dieser Plattformen ermöglicht die Veröffentlichung von Inhalten, die bei politischer Zensur nicht möglich wäre. Zugleich öffnet sie die Tür zu möglichen Manipulationen dieser Inhalte, da die Veröffentlichung der Inhalte nicht (oder nur wenig) geprüft wird.

1. ERFUNDENE UND VERFÄLSCHTE INFORMATIONEN

Medienmanipulationen können verschiedene Formen annehmen, die sich in ihrem Grad und ihrer Art unterscheiden. Basierend auf der Klassifikation von S. Zannettou, M. Sirivianos, J. Blackburn und N. Kourtellis[11] können Informationen völlig neu erfunden, mit reellen Fakten gemischt oder zu späteren Zeitpunkten wieder benutzt werden. Wenn diese Informationen zugunsten einer politischen Partei ausgenutzt werden, handelt es sich um einen Fall von Propaganda, der das Ergebnis einer Wahl beeinflussen kann. Verschwörungstheorien, Gerüchte und Hoaxes gehören ebenfalls zu den Manipulationsstrategien.[12] Besonders in sozialen Medien und Onlineforen bilden sich sogenannte Echokammern, in denen sich Nutzer mit ähnlichen Interessen und Überzeugungen austauschen.[13] Dort werden tendenziöse Berichte und Inhalte geteilt, die aufgrund der herrschenden Einzelmeinung nicht hinterfragt und diskutiert werden, und dort wird die Meinung der Teilnehmer verstärkt.[14] Soziale Medien wie zum Beispiel Facebook tragen daher zur politischen Polarisierung ihrer Mitglieder bei.[15,16] Auch Medien, die ursprünglich als Satire veröffentlicht wurden, bilden einen Nährboden für falsche Informationen, wenn diese nicht als satirische Informationen markiert, weitergeleitet oder interpretiert werden.[17]

Hinter diesen Medienmanipulationen verstecken sich verschiedene Profile, die diese initiieren und verbreiten können.[18] Zur offensichtlichen ersten Quelle von Manipulationen gehören Politiker oder politische Parteien[19], die direkt im Wahlkampf auftreten, aber auch ausländische Regierungen, die sich dadurch Einfluss im jeweiligen Land erhoffen. Auch Aktivisten und politische Organisationen, die Lobbyismus betreiben, können Manipulationen einsetzen, um den politischen Diskurs zu beeinflussen. Dafür können verschiedene Mittel benutzt werden, um die Verbreitung der manipulierten Informationen zu steigern. Dazu zählt zum Beispiel der Einsatz von bezahlten Nutzern, die manipulierte Informationen zu spezifischen Gruppen gezielt teilen, oder von sogenannten Trollen, die durch ihre provokante Art emotional aufgeladene Diskussionen hervorrufen sollen.[20] Auch Social Bots gehören zu dieser Landschaft. Bei Social Bots handelt es sich um Konten in sozialen Medien, die durch ein Computerprogramm kontrolliert werden, automatisch Inhalt erstellen und die Fähigkeit zur Interaktion besitzen.[21,22] Durch ihre spezifische Art, Inhalte zu erstellen und zu teilen, können Bots teilweise von regulären Konten unterschieden werden. Je stärker das Verhalten eines Bots dem eines normalen Kontos ähnelt, desto schwieriger ist dessen Erkennung. Geschätzt gibt es auf Facebook 60 Millionen Bots, auf Twitter werden zwischen neun und 15 Prozent der Konten von Bots kontrolliert.[23]

2. MANIPULATION DURCH GEZIELTE PLATZIERUNGEN

Zusätzlich zur Manipulation der Medien selbst können auch besondere Inhalte gezielt platziert werden. Durch die Onlineplatzierung gezielter und personalisierter Inhalte kann die Effizienz politischer Kampagnen optimiert werden.[24] Dass Bürger einer politischen Beeinflussung ausgesetzt sind, kann dadurch unbemerkt bleiben, sie können unbewusst manipuliert werden. Im Vergleich zu Medienmanipulationen können die kommunizierten Fakten korrekt sein, aber besonders deren Auswahl sowie die Bedingungen der Veröffentlichung werden personalisiert, um eine Meinungsänderung zu erzielen. Auch eine Kombination von Medienmanipulation und Wählermanipulation ist möglich. In diesem Fall werden manipulierte Inhalte gezielt bestimmten Nutzergruppen gezeigt.

> *„Geschätzt gibt es auf Facebook **60 Millionen** Bots."*

Die Mechanismen hinter möglichen Wählermanipulationen sind die gleichen wie bei personalisierter Werbung. Zunächst werden Daten über die Onlinenutzer gesammelt. Nutzer werden zwar durch Cookie-Hinweise über die mögliche Sammlung von Daten informiert, aber diese Hinweise sind auf den Webseiten unterschiedlich.[25] Zusätzlich kann das wiederholte Erscheinen von Cookie-Hinweisen zu einem Gewöhnungseffekt der Nutzer führen, die der Datensammlung meist zustimmen, ohne näher darüber nachzudenken.[26] Zudem kann eine Ablehnung der Cookies eine schlechte oder gar nicht funktionierende Website zur Folge haben. Bei einer Zustimmung werden mittels der Cookies zahlreiche Informationen über die Besucher gesammelt. Diese Informationen werden jedem einzelnen Besucher zugeordnet und beinhalten beispielsweise Hinweise über seinen Standort, Browser oder wiederholte Besuche. Theoretisch können

[1] G. Wolfsfeld, E. Segev, T. Sheafer, „Social media and the arab spring: Politics comes first", in The International Journal of Press/Politics, 18(2), 2013.
[2] N. Eltantawy, J. B. Wiest, „The Arab spring. Social media in the Egyptian revolution: reconsidering resource mobilization theory", in International Journal of Communication, 5, 2011.
[3] P. T. Metaxas, E. Mustafaraj, „Social media and the elections" in Science, 338(6106), 2012.
[4] C. Shao, G. L. Ciampaglia, O. Varol, et al., „The spread of low-credibility content by social bots", in Nature Communications, 9(1), 2018.
[5] K. Clayton, S. Blair, J. A. Busam, S. Forstner, J. Glance, G. Green, A. Kawata, A. Kovvuri, J. Martin, E. Morgan, M. Sandhu, „Real solutions for fake news? Measuring the effectiveness of general warnings and fact-check tags in reducing belief in false stories on social media" in Political Behavior, 2019.
[6] W. Merkel, „Die Herausforderungen der Demokratie„ In Demokratie und Krise, 2014.
[7] F. Liberini, M. Redoano, A. Russo, A. Cuevas, R. Cuevas, "Politics in the facebook era. Evidence from the 2016 us presidential elections". CAGE Online Working Paper Series, (389), 2018.
[8] S. Zannettou, M. Sirivianos, J. Blackburn, N. Kourtellis, „The web of false information: Rumors, fake news, hoaxes, click- bait, and various other shenanigans", in Journal of Data and Information Quality, 11(3):10:1–10:37, 2019.
[9] C. Shao, G. L. Ciampaglia, O. Varolet al. „The spread of low-credibility content by social bots" in Nature Communications, 9(1), 2018.
[10] S. Hölig, U. Hasebrink, „Reuters Institute Digital News Survey 2016 – Ergebnisse für Deutschland", Online: https://www.hans-bredow-institut.de/webfm_send/1135 (Zugriff Februar 2020), 2016.
[11] S. Zannettou, M. Sirivianos, J. Blackburn, N. Kourtellis, „The web of false information: Rumors, fake news, hoaxes, click- bait, and various other shenanigans", in Journal of Data and Information Quality, 11(3):10:1–10:37, 2019.
[12] ebd.
[13] E. Colleoni, A. Rozza, A. Arvidsson, „Echo chamber or public sphere? Predicting political orientation and measuring political homophily in Twitter using big data", in Journal of Communication, 64(2), 2014.
[14] K. Garimella, G. De Francisci Morales, A. Gionis, M. Mathioudakis, „Political discourse on social media: Echo chambers, gatekeepers, and the price of bipartisanship", in Proceedings of the International Conference on World Wide Web, 2018.
[15] F. Liberini, M. Redoano, A. Russo, A. Cuevas, R. Cuevas, "Politics in the facebook era. Evidence from the 2016 us presidential elections". CAGE Online Working Paper Series, (389), 2018.
[16] K. Garimella, G. De Francisci Morales, A. Gionis, M. Mathioudakis, „Political discourse on social media: Echo chambers, gatekeepers, and the price of bipartisanship", in in Proceedings of the International Conference on World Wide Web, 2018.
[17] S. Zannettou, M. Sirivianos, J. Blackburn, N. Kourtellis, „The web of false information: Rumors, fake news, hoaxes, click- bait, and various other shenanigans", in Journal of Data and Information Quality, 11(3):10:1–10:37, 2019.
[18] ebd.
[19] ebd.
[20] ebd.
[21] E. Ferrara, O. Varol, C. Davis, F. Menczer, A. Flammini, „The rise of social bots" in Commununications of the ACM, 59(7), 2016.
[22] K. Shu, A. Sliva, S. Wang, J. Tang, H. Liu, „Fake news detection on social media: A data mining perspective" in SIGKDD Exploration Newsletter, 19(1), 2017.
[23] D. M. J. Lazer, M. A. Baum, Y. Benkler, A. J. Berinsky, K. M. Greenhill, F. Menczer, M. J. Metzger, B. Nyhan, G. Pennycook, D. Rothschild, M. Schudson, S. A. Sloman, C. R. Sunstein, E. A. Thorson, D. J. Watts, J. L. Zittrain, „The science of fake news", in Science, 359(6380), 2018.
[24] F. Zuiderveen Borgesius, J. Möller, S. Kruikemeier, R. O Fathaigh, K. Irion, T. Dobber, C. H. de Vreese, „Online political microtargeting: Promises and threats for democracy" in Utrecht Law Review, 14(1), 2018.
[25] C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, „ (Un) informed Consent: Studying GDPR Consent Notices in the Field", in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019.
[26] ebd.

nur Webseiten auf diese Informationen zugreifen, wenn sie selbst die Cookies gesetzt haben. Die Nutzung von Cookies von Drittanbietern ermöglicht es aber, Informationen, die von verschiedenen Webseiten gesammelt werden, zu kombinieren. Dann werden Inhalte von anderen Anbietern auf die Seite geladen, sodass auch diese die gewünschten Informationen erhalten. Werden Inhalte der gleichen Drittanbieter auf verschiedenen Seiten geladen, die von dem gleichen Nutzer besucht werden, bekommt der Anbieter einen tiefen Einblick in das Verhalten der Nutzer.[27] Zum Beispiel kann er analysieren, wie, wann und in welcher Reihenfolge der Nutzer bestimmte Webseiten besucht hat. Eine Studie der Princeton University zeigt darüber hinaus, dass Drittanbieter immer mehr „Session-Replay"-Skripte nutzen.[28] Mithilfe dieser Skripte werden alle Interaktionen der Nutzer mit der Webseite automatisch aufgezeichnet. Dabei handelt es sich zum Beispiel um Mausbewegungen oder Texteinträge, die der Besucher eingegeben hat, auch wenn er diese nicht geschickt hat. Darüber hinaus fördert die Nutzung von Single-Sign-on-Log-ins, mit denen Nutzer sich zum Beispiel mit ihren Facebook- oder Google-Konten auf verschiedenen Webseiten anmelden können, die Sammlung von Daten und deren Zuordnung.[29] Vor allem soziale Netze wie Facebook bekommen dadurch tiefe Einblicke in das Verhalten der Nutzer, ihre Interessen und ihre sozialen Beziehungen.[30] Da Informationen auch über die sozialen Kontakte gesammelt werden, kann das Porträt der Nutzer durch die Datensammler detailliert skizziert werden. Es wird eine stetig wachsende Menge an Daten über die Nutzer erhoben, meist ohne dass diesen die Breite und Tiefe dieser Sammlung bewusst ist. Durch die mangelnde Benutzerfreundlichkeit von Cookie-Hinweisen[31] bieten diese keine geeignete Lösung zur Information und Zustimmung der Nutzer über die Datensammlung.

Die gesammelten Informationen können zudem genutzt werden, um Internetnutzer zu profilieren und zu kategorisieren. In eine Kategorie gehören dann Nutzer mit dem gleichen Profil. Unter Profil können verschiedene Dimensionen verstanden werden. Facebook bietet zum Beispiel in den USA die Möglichkeit, Nutzer nach 614 verschiedenen Attributen zu sortieren[32], um diese besser mit Werbung zu adressieren. Diese Attribute werden in drei Hauptkategorien, nämlich Demografie, Verhalten und Interesse, unterteilt. In der Kategorie „Politik" werden die Nutzer nach politischer Ausrichtung (sehr konservativ, konservativ, gemäßigt, liberal, sehr liberal) unterschieden bzw. nach der Wahrscheinlichkeit ihrer möglichen politischen Ausrichtung. Zudem kombiniert Facebook eigene Daten mit externen Datenquellen. Diese externen Datenquellen nutzen nicht nur online gesammelte Informationen, sondern erweitern diese auch mit Offlinedatensätzen, die über die Nutzer verfügbar sind.

Durch die Informationsgewinnung und die darauf basierende Nutzerprofilierung können Internetplattformen, das heißt Webseiten oder soziale Onlinenetzwerke, diese Kenntnisse ausnutzen, um zum Beispiel personalisierte Inhalte zu präsentieren. Dadurch werden die dargestellten Inhalte dem Verhalten oder Interesse der Nutzer angepasst. Diese Personalisierung öffnet auch die Tür zu möglichen Manipulationen.[33] Durch den Einsatz von gezielten Triggern kann das zukünftige Verhalten der Nutzer beeinflusst werden.[34] Das Phänomen ist schon bei personalisierter Werbung zu beobachten, wo Nutzern die gleichen ausgewählten Produkte auf verschiedenen Webseiten gezeigt werden. Dasselbe gilt für politische Zwecke. Der US-amerikanische Wahlkampf von 2016 dient als Beispiel für diese Methode. Durch eine Analyse der Werbungspreise von Facebook hat eine Studie gezeigt, dass Werbung für die Kandidaten abhängig von deren Gewinnchancen geschaltet wurde.[35] Die Preise waren am höchsten, wenn die Chancen der Kandidaten noch unklar waren, und sanken, wenn das Ergebnis deutlicher wurde. Die Studie zeigt aber auch, dass diese Werbung das Verhalten und die Meinung der Wähler beeinflusst hat. Durch die Werbung wurden nicht nur Wähler zur Wahl ermutigt – auch die Wahlentscheidungen von Wählern mit gemäßigten politischen Ansichten wurden beeinflusst.

Der Fall der US-amerikanischen Wahlen zeigt deutlich, dass es nicht nur technisch möglich, sondern auch wirkungsvoll ist, Wähler durch die Freischaltung von personalisierter Werbung zu manipulieren. Diese Manipulationsversuche und -erfolge sind eine Gefahr für existierende Demokratien, da das Prinzip von freien Wahlen nicht mehr vollständig garantiert wird.

3. HERAUSFORDERUNGEN

Die Erkennung von manipulierten Informationen ist nicht trivial. Teilweise werden diese Inhalte eigens erstellt, um die Leserschaft zu manipulieren.[36] Zudem werden sie mitunter über die Konten bezahlter Nutzer verbreitet, die sich kaum von regulären Konten unterscheiden lassen. Eine mögliche Maßnahme zur Erkennung ist eine kritische individuelle Betrachtung durch die Nutzer. Es hat sich aber gezeigt, dass Menschen Informationen generell nicht hinterfragen, wenn diese ihre ursprüngliche Meinung unterstützen und sie nicht dazu motiviert werden.[37] Je öfter diese Inhalte veröffentlicht werden, desto eher stufen Leser sie als wahr ein – ein Phänomen, das durch den Einsatz von Bots unterstützt wird. Es zeigt sich, dass Nutzer falsche Inhalte nur schwer von richtigen unterscheiden können.[38] Auch wenn sie informiert werden, dass die Inhalte nicht korrekt sind, können diese dennoch ihre Haltung beeinflussen.[39] Der Grad der Haltungsänderung hängt von den kognitiven Fähigkeiten des Nutzers ab.[40] Besonders kann die Art und Weise, wie Nutzer über die Unkorrektheit der Inhalte informiert werden, ihre Haltung und ihre Einschätzung der Korrektheit der zugrunde liegenden

[27] J. R. Mayer, J. C. Mitchell, „Third-party web tracking: Policy and technology", in Proceedings of the IEEE Symposium on Security and Privacy, 2012.
[28] G. Acar, S. Englehardt, A. Narayanan, „No boundaries: Exfiltration of personal data by session-replay scripts" Online: https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/ (Zugriff Februar 2020), 2017.
[29] S. Landau, T. Moore, „Economic tussles in federated identity management", in First Monday 17, 10, 2012.
[30] H. Krasnova, Hanna, N. Eling, O. Abramova, P. Buxmann, „Dangers of ‚Facebook Login' for mobile apps: Is there a price tag for social information?" in Proceedings of the International Conference on Information Systems, 2014.
[31] C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, „ (Un) informed consent: Studying GDPR consent notices in the field", in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2019.
[32] A. Andreou, G. Venkatadri, O. Goga, K. P. Gummadi, P. Loiseau, A. Mislove, „Investigating ad transparency mechanisms in social media: A case study of Facebook's explanations", in Proceedings of the Network and Distributed System Security Symposium, 2018.
[33] M. Bourreau, A. De Streel, I. Graef, „Big Data and Competition Policy: Market power, personalised pricing and advertising", in Personalised Pricing and Advertising, 2017.
[34] A. Hughes, „Weapons of mass consumption: Social and digital media in political campaigns", in Market Driven Political Advertising, 2018.
[35] F. Liberini, M. Redoano, A. Russo, A. Cuevas, R. Cuevas, „Politics in the Facebook era. Evidence from the 2016 us presidential elections", CAGE Online Working Paper Series, (389), 2018.
[36] K. Shu, A. Sliva, S. Wang, J. Tang, H. Liu, „Fake news detection on social media: A data mining perspective" in SIGKDD Exploration Newsletter, 19(1), 2017.
[37] D. M. J. Lazer, M. A. Baum, Y. Benkler, A. J. Berinsky, K. M. Greenhill, F. Menczer, M. J. Metzger, B. Nyhan, G. Pennycook, D. Rothschild, M. Schudson, S. A. Sloman, C. R. Sunstein, E. A. Thorson, D. J. Watts, J. L. Zittrain, „The science of fake news", in Science, 359(6380), 2018.
[38] V. L. Rubin, „On deception and deception detection: Content analysis of computer-mediated stated beliefs" in Proceedings of the 73rd ASIS&T Annual Meeting on Navigating Streams in an Information Ecosystem, 47, 2010.
[39] J. De Keersmaecker, A. Roets, „ 'Fake news': Incorrect, but hard to correct. The role of cognitive ability on the impact of false information on social impressions", in Intelligence, 65, 2017.
[40] ebd.

Information beeinflussen.[41] Dabei spielt etwa die Formulierung der Warnung eine wichtige Rolle.[42] Für die Nutzer ist es sehr schwierig, die Glaubwürdigkeit von Quellen und Inhalten selbst zu prüfen. Nutzer mit Workshops oder ähnlichen Maßnahmen dafür zu qualifizieren, glaubwürdige von unglaubwürdigen Quellen zu trennen, ist jedoch keine realistische Lösung.[43] Es können jederzeit neue unglaubwürdige Quellen auftreten oder bestehende sich ändern, sodass diese Lösung einen zu hohen Aufwand für die Nutzer bedeuten würde.

Die europäische Datenschutz-Grundverordnung (DSGVO), die 2018 in Kraft getreten ist, trägt zu mehr Schutz der Bürger bei. Deren Rechte bezüglich Datensammlung, Transparenz und Kontrolle wurden verstärkt. Auch wenn die Grundverordnung aus gesetzlicher Sicht einen maßgeblichen Fortschritt darstellt, bleibt es für die Bürger jedoch schwierig, ihre Rechte in der Praxis wahrzunehmen.[44] Denn die dafür notwendigen Schritte sind sehr aufwendig. Wie schon am Beispiel der Cookies gezeigt, wurden Lösungen meist nicht aus Nutzersicht entwickelt. Als Ergebnis sind der resultierende Aufwand und die damit verbundenen Hürden für die Nutzer immer noch zu hoch. Damit verbleibt der Vorteil bei den Plattformen und Anbietern, die weiter Daten über die Nutzer sammeln – zwar unter Einwilligung, jedoch unter einer erzwungenen Einwilligung. Wie zuvor gezeigt, bilden die dadurch gesammelten Daten die Grundlage für die Freischaltung personalisierter Inhalte und damit für mögliche Wählermanipulationen, die im Fall von politischen Wahlkämpfen die Demokratie gefährden. Auch ein Verzicht auf Internetaktivitäten, um Manipulationen zu umgehen, ist keine realistische, zielführende und geeignete Lösung, da sie zu einer gesellschaftlichen Isolierung der betreffenden Menschen führen könnte.

> *„Nutzer können technische Wege nutzen, um ihre **Privatsphäre** zu schützen.“*

4. TECHNOLOGISCHE ANSÄTZE ZUR ERKENNUNG VON MANIPULATIONEN

Statt die Verantwortung für die Erkennung von Medienmanipulationen auf die Leser zu übertragen, bieten technologische Ansätze eine valide Alternative zur Erkennung und Beseitigung manipulierter Informationen.

Der erste der derzeit verfolgten Ansätze ist die Nutzung von Verfahren des maschinellen Lernens, die, basierend auf der Identifizierung von relevanten Charakteristiken, eine automatische Erkennung von manipulierten Inhalten unterstützen können. Die Machbarkeit dieses Ansatzes wurde mit verschiedenen Zielen getestet.[45] Zum Beispiel wurde die Erkennung von frühen Verbreitungswellen manipulierter politischer Inhalte[46] und politischer Kampagnen in Twitter untersucht.[47] Weiterhin wurde untersucht, ob die politische Tendenz von Nutzerkonten und deren Inhalten automatisch klassifiziert werden kann[48] oder ob manipulierte Bilder, etwa des Orkans „Sandy“, erkannt werden können.[49] Dafür werden Lösungen wie die frei verfügbare Plattform „Hoaxy“[50,51] vorgeschlagen, welche die Verbreitung von manipulierten Inhalten sowie deren spätere Korrekturen analysieren und sich gegenseitig beeinflussen. Auch wenn diese Ansätze gute Ergebnisse erzielen und weitere Erkenntnisse zu politischen Manipulationen liefern, bleiben die Erkennungsraten unter 100 Prozent und bieten daher Hinweise und keine Garantien.

Die Gewährleistung der Authentizität sowie der Integrität der Informationen sind klassische Schutzziele der IT-Sicherheit. Digitale Unterschriften bieten Lösungen zu dieser Problematik, da die Identität der Ursprungsquelle nachgewiesen wird und eine Änderung der Informationen oder Bilder erkannt werden kann. Digitale Unterschriften können aber von den Medien getrennt werden. Deswegen bieten digitale Wasserzeichen eine bessere Alternative zum Schutz vor Manipulationen. In diesem Fall wird der Quelle ein Wasserzeichen, basierend auf der Charakteristik des Mediums, hinzugefügt, für den normalen Nutzer bleibt es meist unsichtbar oder unhörbar. Sollte die Quelle manipuliert werden, würden sich die Charakteristiken, die im Wasserzeichen festgehalten wurden, vom Ursprung unterscheiden. Dadurch könnte eine Manipulation erkannt werden. Die eingesetzten Wasserzeichen sollten aber nicht nur widerstandsfähig gegen mögliche gutartige Änderungen der Medien, beispielsweise Skalierungen, sondern auch gegen mögliche Angriffe sein.

Derzeit werden auf maschinellem Lernen basierende Lösungen auch eingesetzt, um Bots zu identifizieren sowie deren Aktivitäten und verbreitete Themen zu analysieren. Die gewonnenen Informationen können mittels einer Webanwendung wie „Bot Electioneering Volume (BEV)“[52] oder „Botometer“[53] an die Öffentlichkeit kommuniziert werden. Basierend auf einer Analyse der Daten und Metadaten eines Twitter-Kontos wie etwa Kontakte, Inhalte oder Aktivitäten, vergibt zum Beispiel Botometer eine Punktzahl, welche die Wahrscheinlichkeit anzeigt, dass es sich bei einem Konto um einen Bot handelt.[54] Jedoch sind weitere Fortschritte notwendig, um die Nutzbarkeit solcher Lösungen zu erhöhen und die Interpretation der gelieferten Informationen durch die Öffentlichkeit zu erleichtern.[55]

Auch eines der derzeit hochaktuellen Themen der IT-Sicherheit, die Blockchain-Technologie, kann eingesetzt werden, um die Ursprungsquelle zu verifizieren[56] oder die Verbreitung von manipulierten Inhalten in sozialen Onlinenetzwerken zu erkennen und zu unterbinden.[57,58] Zum Beispiel werden die Blockchain-basierten Verträge benutzt, um die Vertrauenswürdigkeit der Nutzer und der ausgetauschten Informationen zu bewerten.[59] Dafür bekommt jeder Nutzer ein virtuelles Guthaben, das die Glaubwürdigkeit des Nutzers und der veröffentlichten Informationen widerspiegeln soll. Informationen mit niedrigen Werten werden dadurch weniger verbreitet.

Schließlich sind die Erkennung und die Bekämpfung von bösartigen Bots auch ein Thema, das die Sicherheitsexperten beschäftigt. Auch wenn sich die Charakteristiken der Bots unterscheiden können, besteht das Hauptziel oft in der Unterbindung der automatischen Ausführung von Befehlen, die zur Verbreitung von manipulierten Inhalten oder Kommentaren beitragen. Dies kann beispielsweise mit der Einführung eines Captcha, das nur durch einen Menschen zu lösen ist, erreicht werden. Die Bots werden jedoch ständig weiterentwickelt, um eingeführte Gegenmaßnahmen zu umgehen, was wiederum die Entwicklung neuer Gegenmaßnahmen fördert.

[41] K. Clayton, S. Blair, J. A. Busam, S. Forstner, J. Glance, G. Green, A. Kawata, A. Kovvuri, J. Martin, E. Morgan, M. Sandhu, „Real solutions for fake news? Measuring the effectiveness of general warnings and fact-check tags in reducing belief in false stories on social media“ in Political Behavior, 2019.
[42] ebd.
[43] F. M. Zahedi, A. Abbasi, Y. Chen, „Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance“, in Journal of the Association for Information Systems, 16(6), 16, 6 (2015), Seite 448.
[44] T. Urban, D. Tatang, M. Degeling, T. Holz, N. Pohlmann, „A study on subject data access in online advertising after the GDPR“, in Data Privacy Management, Cryptocurrencies and Blockchain Technology, 2019.
[45] S. Zannettou, M. Sirivianos, J. Blackburn, N. Kourtellis, „The web of false information: Rumors, fake news, hoaxes, click- bait, and various other shenanigans“, in Journal of Data and Information Quality, 11(3):10:1–10:37, 2019.
[46] J. Ratkiewicz, M. Conover, M. R. Meiss, B. Gonalves, A. Flammini, F. Menczer, „Detecting and tracking political abuse in social media“, in Proceedings of the International AAAI Conference on Weblogs and Social Media, 2011.

[47] E. Ferrara, O. Varol, C. Davis, F. Menczer, A. Flammini, „The Rise of Social Bots“, in Communications of the ACM, 59(7), 2016.
[48] D. X. Zhou, P. Resnick, Q. Mei „Classifying the political leaning of news articles and users from user votes“, in Proceedings of the International AAAI Conference on Weblogs and Social Media, 2011.
[49] A. Gupta, H. Lamba, P. Kumaraguru, A. Joshi, „Faking sandy: Characterizing and identifying fake images on twitter during hurricane sandy“, in Proceedings of the 22nd International Conference on World Wide Web (WWW companion), 2013.
[50] C. Shao, G. L. Ciampaglia, A. Flammini,, F. Menczer, „Hoaxy: A platform for tracking online misinformation“, in Proceedings of the International Conference on World Wide Web (WWW companion), 2016.
[51] C. Shao, P. Hui, L. Wang, X. Jiang, A. Flammini, F. Menczer, G. L. Ciampaglia, „Anatomy of an online misinformation network“, in PloS one, 13(4), 2018.
[52] K. Yang, P. Hui, F. Menczer, „Bot Electioneering Volume: Visualizing social bot activity during elections“, in Proceedings of the 28th International Conference on World Wide Web (WWW companion), 2019.
[53] K. Yang, O. Varol, C. A. Davis, E. Ferrara, A. Flammini, F. Menczer, „Arming the public with Artificial Intelligence to counter social bots“, in Human Behavior and Emerging Technologies, 1(1), 2019.
[54] O. Varol, E. Ferrara, C. A. Davis, F. Menczer, A. Flammini, „Online human-bot interactions: Detection, estimation, and characterization“, in Proceedings of the 11th International AAAI Conference on Web and Social Media, 2017.
[55] K. Yang, O. Varol, C. A. Davis, E. Ferrara, A. Flammini, F. Menczer, „Arming the public with Artificial Intelligence to counter social bots“, in Human Behavior and Emerging Technologies, 1(1), 2019.
[56] S. Huckle, M. White, „Fake news: a technological approach to proving the origins of content, using blockchains“, in: Big data, 5(4), 2017.
[57] H. Wang, Y. Chen, Q. Li, „Towards trusted social networks with blockchain technology“, in Proceedings of the 1st Symposium on Foundations and Applications of Blockchain, 2018.
[58] M. Saad, A. Ahmad, A. Mohaisen, „Fighting fake news propagation with blockchains“. in Proceedings of the IEEE Conference on Communications and Network Security, 2019.
[59] H. Wang, Y. Chen, Q. Li, „Towards trusted social networks with blockchain technology“, in Proceedings of the 1st Symposium on Foundations and Applications of Blockchain, 2018.

Nutzer können technische Wege nutzen, um ihre Privatsphäre zu schützen. Dies fordert aber ihre aktive Beteiligung, zum Beispiel bei der Auswahl, Konfiguration oder Installation bestimmter Lösungen. Nutzer müssen also auch dabei einigen Aufwand betreiben, um sich zu schützen. Geläufige Lösungen, die direkt in der Hand der Nutzer liegen, finden sich in den Einstellungen ihrer Browser. Damit können sie Cookies, Tracker und Drittanbietercookies generell verbieten. Das kann aber zu Darstellungsproblemen der Webseiten führen. Deswegen bietet etwa Firefox eine manuelle und spezifische Freischaltung von vertrauten Webseiten. Dies verursacht zwar auch Aufwand für die Nutzer, aber das Tracking wird von den „vertrauten" Webseiten wieder freigegeben. Die Frage ist dabei, wie die Nutzer die Vertrauenswürdigkeit der Webseiten bewerten können. Zusätzlich haben die Nutzer die Möglichkeit, die Cookies mit der Schließung des Browsers löschen zu lassen. Diese Lösung bietet aber nur einen Schutz zwischen Sitzungen. Innerhalb einer Sitzung bleiben die Cookies aktiv. Insgesamt bleiben die Selbstschutzmaßnahmen, die in der Hand der Nutzer liegen, aber wenig wirksam.

Weitere Maßnahmen, die der Nutzer einsetzen kann, können ein falsches Schutzgefühl hervorrufen. Ein Beispiel dafür ist der „private" Modus, der von verschiedenen Browsern angeboten wird. Der dabei gebotene Schutz bezieht sich auf andere Nutzer des Geräts, die den Verlauf oder die Sucheingaben nicht entdecken sollten. Aufgrund des Namens erwarten Nutzer stattdessen möglicherweise einen vollständigen Schutz. Ebenso können Nutzer die Option „nicht verfolgen" auswählen. Diese Option bleibt aber eine Präferenz und sichert nicht die Durchsetzung der unterliegenden Maßnahmen. Die Installation eines Werbefilters, das heißt einer Browser-Erweiterung, die Werbung unterbindet, kann sinnvoll sein. Aber auch bestimmte Werbefilter können Daten über Nutzer sammeln. Weiterhin können bestimmte Router und Virtual Private Networks (VPN) mit Werbefiltern ausgestattet werden.

Um die Anonymität der Nutzer im Internet zu gewährleisten, gibt es weitere technische Lösungen, die in der Bevölkerung möglicherweise weniger bekannt sind als Browser-basierte Möglichkeiten. Das Ziel dieser Lösungen ist, Daten zu verstecken oder zu verschleiern, die zu einer Identifikation der Nutzer führen können. Beispiele dafür sind die IP-Adresse, die den Standort des Nutzers offenlegt und einen direkten Link zum User erstellt, oder Browser-Charakteristiken (Sprache, Zeitzone, Betriebssystem, Computermarke, Version usw.). Dafür können Nutzer Anonymisierungsdienste in Anspruch nehmen, der bekannteste darunter ist Tor. Diese Dienste agieren als Proxy, das heißt als Zwischenhändler für die Nutzer, und senden die Anfrage anstelle der Nutzer zu der Website. Dabei erscheinen diese Dienste als Quelle der Anfrage für die Website statt der Nutzer selbst, die hinter diesen Diensten versteckt bleiben. Diese Dienste leiten dann die Antwort der Website an die Nutzer weiter. Um diese Dienste zu realisieren, stehen verschiedene technische Architekturen zur Verfügung und die Interaktionen für die Nutzer können variieren. Ein Nachteil solcher Lösungen ist aber, dass die Anfragen zu den Webseiten sowie deren Antwort länger brauchen können und dadurch die Benutzererfahrung beeinträchtigen. Dienste wie Tor können kostenlos benutzt werden.

5. HANDLUNGSEMPFEHLUNGEN

Der Schutz der Ausübung der demokratischen Prinzipien in der digitalen Welt ist ein grundlegendes aber auch ein vielschichtiges Problem, dessen komplexe Lösung weitere Anstrengungen benötigt. Hierzu ist eine gründlichere Problemanalyse unabdingbar, um die aktuell existierenden isolierten Analysen sowie die vereinzelt vorhandenen technischen Gegenmaßnahmen auf eine breitere Basis zu stellen. Dies ist weiterhin Grundvoraussetzung für die Entwicklung neuer technischen Lösungen, um das Problem einzudämmen. Eine zentrale Rolle kommt hierbei der Berücksichtigung menschlichen Verhaltens und der Benutzbarkeit zu, insbesondere wenn eine enge Interaktion zwischen allen Stakeholdern erfolgt. Gleichzeitig fordern wir eine eine bessere Untersuchung der möglichen Auswirkungen von technischen Lösungsansätzen über deren rein technische Ebene hinaus und mit besonderem Fokus auf Rechtskonformität, Weiterentwicklung des rechtlichen Rahmens sowie gesellschaftliche Auswirkungen.

ABSTRACT

Internet und soziale Medien können beides: die Demokratie stützen und stärken. Oder aber gefährden, in dem sie manipulierte Infos verbreiten. Wir sollten die Bedeutung von Internet und sozialen Medien für die politische Willensbildung nicht unterschätzen. Immer mehr Menschen nutzen soziale Medien als Hauptinformationsquellen. Sie vertrauen dabei Plattformen, deren Inhalte nutzergeneriert sind und journalistischen Standards häufig nicht genügen. Denn die Plattformen prüfen in der Regel den Wahrheitsgehalt der Inhalte kaum oder gar nicht. Das ermöglicht dann nicht nur manipulierte Inhalte, sondern beeinflusst zum Beispiel vor Wahlen die politischen Entscheidungen der Wähler. In den Wahlkämpfen in den USA und in Frankreich, sowie beim Brexit-Referendum wurden nachweislich Infos und Bilder verfälscht. Solche Tendenzen bedrohen demokratische Systeme, zu deren Grundlagen die freie politische Entscheidung gehört.

THEMEN-VERANTWORTLICHE

Kryptoagilität | Post-Quanten-Kryptografie | Künstliche Intelligenz
Prof. Dr. Claudia Eckert

Smart Cities
Prof. Dr. Matthias Hollick

Technische Souveränität
Prof. Dr. Norbert Pohlmann

Demokratie und Gesellschaft
Prof. Dr. Delphine Reinhardt

Faktor Mensch | Authentifikation | Passwortrichtlinien
Prof. Dr. Angela Sasse / Prof. Dr. Matthew Smith

Der vorliegende Bericht beruht wesentlich auf der Unterstützung folgender wissenschaftlicher Mitarbeiter, die die Arbeiten des Wise Council of Cyber Security Experts mit enormem Engagement und großer Expertise begleitet haben: Konstantin Böttinger (Fraunhofer AISEC), Eva Gerlitz (Fraunhofer FKIE), Maximilian Häring (Fraunhofer FKIE), Johann Heyszl (Fraunhofer AISEC), Anne Hofmeister (TU Darmstadt), Marian Margraf (Fraunhofer AISEC) und Philipp Sperl (Fraunhofer AISEC).

IMPRESSUM

Herausgeber:

CYBER SECURITY CLUSTER BONN E. V.
BONNPROFITS GRÜNDUNGSZENTRUM

Godesberger Allee 139
53175 Bonn
Telefon: 0228 37769035
E-Mail: info@cyber-security-cluster.eu

Amtsgericht Bonn VR 11418

Art Direction:
Sabrina Golba, Ilka Kampmann

Layout:
Sabrina Golba, Sebastian Veenhof

Bildredaktion:
Sabrina Golba

Projektmanagement / CvD:
Yvonne Schmitz, Christian Schiller

Autoren dieser Ausgabe:
Prof. Dr. Claudia Eckert, Prof. Dr. Matthias Hollick, Prof. Dr. Norbert Pohlmann, Prof. Dr. Delphine Reinhardt, Prof. Dr. Angela Sasse, Prof. Dr. Matthew Smith, Dirk Backofen, Ingrid Kirsch

Agentur:

Palmer Hargreaves GmbH
Vogelsanger Straße 66
50823 Köln
Telefon: 0221 933 22 0
E-Mail: cologne@palmerhargreaves.com

Litho:
Palmer Hargreaves GmbH

Druck:
Johnen-Druck GmbH & Co. KG,
Bernkastel-Kues

Copyright:
© 2020 by Cyber Security Cluster Bonn e. V.

Nachdruck nur mit Quellenangabe und Belegexemplar. Der Inhalt gibt nicht in jedem Fall die Meinung des Herausgebers wieder.

CYBER
SECURITY
CLUSTER BONN

Cyber Security Cluster Bonn e.V.

BonnProfits Gründungszentrum
Godesberger Allee 139
53175 Bonn

Telefon: 0228 37769035
Email: info@cyber-security-cluster.eu

CYBER
SECURITY
CLUSTER BONN