acatech

HORIZONTE

Cyber Security

Warum Cyber Security?

Gefährdungsfelder in wichtigen Lebensbereichen

Cyber Security in Deutschland und im internationalen Vergleich

Handlungsfelder und Gestaltungsspielräume

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

+++ Mit der vorliegenden Publikationsreihe untersucht acatech bedeutende Technikfelder, die sich klar am Horizont abzeichnen, deren Auswirkungen aber noch geklärt werden müssen. In dieser Reihe bereitet die Akademie solche Technikfelder fundiert und anschaulich auf. In diesen Prozess fließen der aktuelle Stand der internationalen Forschung, Entwicklung und Anwendung sowie die Wertschöpfungspotenziale der Technologien ein. Darüber hinaus nehmen die acatech HORIZONTE ethische, politische und gesellschaftliche Fragen sowie denkbare Entwicklungen und Gestaltungsoptionen in den Blick. Mit den acatech HORIZONTEN möchte die Akademie die Diskussion über neue Technologien anregen, politische Gestaltungsräume aufzeigen und Handlungsoptionen formulieren. Auf diese Weise möchte acatech einen Beitrag für eine vorausschauende Innovationspolitik leisten. +++

acatech

HORIZONTE

Cyber Security

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

Vorwort

Die Überlegung, sich dem Thema Cyber Security zu widmen, ist aus einem breit angelegten Diskussionsprozess entstanden, in den von Beginn an die Meinungen hochkarätiger Expertinnen und Experten eingeflossen sind: Zunächst identifizierten acatech Mitglieder, Senatsunternehmen sowie weitere Stakeholder aus Wissenschaft, Wirtschaft und Gesellschaft im acatech internen Foresight-Prozess eine Reihe wichtiger, disruptiver Zukunftsthemen. Im zweiten Schritt priorisierte der Begleitkreis, ein externes Gremium von Fachleuten verschiedener Disziplinen und Branchen, die Ergebnisse dieser ersten Umfrage und ergänzte sie durch eigene Vorschläge. Zuletzt bereitete die Portfoliokonferenz die priorisierten Ergebnisse für die Themenfindung beim acatech Präsidium vor. Dieses einigte sich nach intensiven Beratungen, Cyber Security als Thema der acatech HORIZONTE zu benennen.

Denn eine Grundvoraussetzung für den Wirtschaftsstandort Deutschland ist das Vertrauen sowohl der Unternehmen als auch der Privatnutzenden in das digitale Netz. Dabei spielen Cyber Security, Datensicherheit und Privacy eine wesentliche Rolle.

Aktuell ist jedes zweite deutsche Unternehmen jedoch von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen; weltweit kursierten letztes Jahr geschätzt sieben Milliarden geklaute digitale Identitäten von Privatpersonen, die von Kriminellen missbraucht werden können. Diese Fakten erfordern objektive Analysen, klare Stellungnahmen und sinnvolle Lösungsansätze.

Mit dem Ziel, eine fundierte und seriöse Diskussionsbasis zu schaffen, bringt acatech ausgewählte Expertinnen und Experten aus Wissenschaft und Wirtschaft zusammen, deren Einschätzungen und Handlungsoptionen zum Thema Cyber Security in die vorliegende Ausgabe der HORIZONTE einfließen.

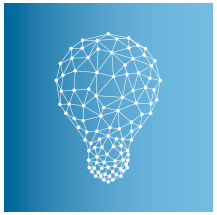
Im Mittelpunkt dieser HORIZONTE-Ausgabe steht, Gesellschaft und Politik zu Cyber Security faktenbasiert, jedoch ohne „Fachchinesisch" aufzuklären. In diesem Sinne wünschen wir Ihnen eine verständliche, anregende und spannende Lektüre!

Prof. Dr.-Ing. Dieter Spath
Präsident acatech

Prof. Dr.-Ing. Jürgen Gausemeier
Vizepräsident acatech

Prof. Dr. Martina Schraudner
Vorstandsmitglied acatech

Inhalt



Auf einen Blick

Neun Kernbotschaften

1. Weltweit nehmen Cyberangriffe an Vielfalt und Gefährdung rapide zu. In der digital vernetzten Welt werden IT-Systeme so komplex, dass die Risiken nur noch schwer abschätzbar sind: Eine einzige Schwachstelle reicht Cyberkriminellen, um in ein Gesamtsystem einzudringen und Schaden anzurichten. Die Angreifenden lernen ständig dazu. Deshalb ist es in der Cyber Security zwar notwendig, jedoch nicht ausreichend, aus den Fehlern der Vergangenheit zu lernen.

2. Die größten Gefährdungsfelder für Deutschlands innere Sicherheit, Wirtschaft und Demokratie sind die Bereiche Gesundheit, Stromversorgung, Industrie 4.0, Smart Home und IoT-Geräte, vernetzte Fahrzeuge und Medien. Diese bedürfen eines besonderen Schutzes vor Manipulationen und Cyberattacken.

3. Deutschland ist in der Forschung zu Cyber Security gut aufgestellt. In den Bereichen Kryptographie, Quantencomputing und Security Engineering (Security by Design), um nur einige zu nennen, zählen deutsche Forschende zur Spitzenklasse.

4. Jedoch fehlt in Deutschland die Umsetzung von Forschungsergebnissen in wirtschaftlich erfolgreiche Sicherheitsprodukte und -dienstleistungen: Aufgrund einer starken Abhängigkeit von Zulieferern aus den USA und Asien haben wir hierzulande wenig Kontrolle über die Sicherheit unserer grundlegenden IT-Infrastrukturen. Dies betrifft Cloud-Lösungen, Software- und Hardware-Produkte.

5. Die Stakeholder aus Politik, Wirtschaft und Wissenschaft arbeiten teils fragmentiert und parallel. Es bedarf einer strategiegeleiteten Orchestrierung sowie eines funktionierenden Regelkreises, bei dem die Akteure ihr Wissen transferieren und sich im Schadensfall und bei der Ursachenforschung gegenseitig unterstützen.

6. IT-Sicherheit wird oft nicht ernst genommen. Kunden und Kundinnen sind nicht bereit, mehr Geld für ein sicheres Produkt zu bezahlen, zumal die Konsequenzen eines unsicheren Produktes zunächst nicht spürbar sind. Hier muss der deutsche Staat Mindestsicherheitsstandards für IT-Produkte und -dienstleistungen einführen, die für alle Unternehmen und Branchen verpflichtend sind.

7. Ein Einfalltor für viele Hackerangriffe ist der Mensch. Vor allem kleine und mittelständische Unternehmen müssen ein kritischeres Bewusstsein für Cyberbedrohungen entwickeln und Mitarbeitende sowie IT-Fachkräfte regelmäßig fortbilden. Auch der deutsche Staat muss für digitale Aufklärung sorgen: An Schulen und Berufsschulen ist Sicherheitsbildung nötig; die Gesellschaft ist über Kampagnen zu sensibilisieren.

8. Die größte Schwachstelle ist jedoch nicht der Mensch, sondern Systeme, die den Menschen nicht ausreichend unterstützen. Es ist nun dringend an der Zeit, stärker in die Entwicklung und Herstellung sicherer Software- und Hardware-Systeme zu investieren, welche die Menschen technisch schützen, ohne ihnen unmögliche Aufgaben aufzubürden.

9. Die Verbreitung von Fake News über das Internet hat eine neue Dimension erreicht. Politisch motivierte Hacker, Terrororganisationen oder Geheimdienste überfluten die Öffentlichkeit mit falschen Informationen, sodass diese nicht mehr zwischen richtig und falsch unterscheiden kann. Mögliche Ziele sind, die Schwächen einer politischen Partei aufzuzeigen oder das gesamte demokratische System zu unterminieren.

1

Warum Cyber Security?

Weshalb sollte uns das Thema Cyber Security beschäftigen? Kann das Thema nicht den IT-Fachkräften im Unternehmen überlassen werden? Müssen sich auch Privatpersonen sowie Mitarbeitende einer Firma damit auseinandersetzen? Hört die Verantwortung der Politik damit auf, Cyber Policies in die Wege zu leiten? Lässt sich das Problem überhaupt bändigen? Lohnt sich also der Versuch, für mehr Cyber Security zu sorgen? ►


CYBER
SECURITY
www

1.1 Wie nahe am Abgrund stehen wir?

Unternehmen stufen Cyberkriminalität als das größte Problem der Zukunft ein. Studien zufolge wird Cyberkriminalität weltweit bis 2021 zu Schäden von jährlich sechs Billionen Dollar [1] führen. Das wäre im Vergleich zum Jahr 2015 eine Verdoppelung.

„Die Komplexität der Systeme wächst uns über den Kopf. Es ist illusorisch, Cyberangriffe wirklich zu verhindern."

Cyberangriffe verursachen monetäre Verluste. Sie erzeugen aber auch erhebliche gesellschaftliche, politische und persönliche Schäden. So wurden während der US-Wahlen 2016 gezielt Systeme der Demokraten angegriffen; sogenannte Social Bots, also Programme, die menschliche Verhaltensmuster simulieren, verbreiteten Falschmeldungen. Auch die EU-Kommission befürchtet Fake-News-Kampagnen und Cyberattacken während der Europawahl im Mai 2019. „Wir müssen verhindern, dass staatliche und nichtstaatliche Akteure unsere demokratischen Systeme untergraben und als Waffe gegen uns einsetzen", erklärt EU-Sicherheitskommissar Julian King [2] in einem Versuch, die Anbieter von Plattformen Sozialer Medien zum konsequenteren Kampf gegen Desinformationen zu drängen.

„Wir stehen direkt vor dem Abgrund. Die Lage ist ernst, aber nicht hoffnungslos."

Die Daten von Nutzenden zu erbeuten, ist ein weiteres Angriffsziel. Solche Attacken bleiben häufig lange unentdeckt: Erst Jahre später wurde bekannt, dass Hacker* 2013 Daten von ca. einer Milliarde Yahoo-Nutzern und 2014 Daten von 500 Millionen Nutzern erbeutet haben [3]. Zu den gehackten Daten zählten Namen, Telefonnummern, Geburtsdaten, verschlüsselte Passwörter und unverschlüsselte Sicherheitsfragen zur Passwortwiederherstellung. Auch ein Angriff auf Kundendaten des Business-Portals LinkedIn aus dem Jahr 2012 kam erst vier Jahre später an die Öffentlichkeit. Insgesamt wurden dabei rund 177 Millionen Datensätze gestohlen. Ebenfalls Opfer von Datendiebstahl wurden 145 Millionen Kunden des Online-Marktplatzes eBay [4].

„Risiken, die wir bislang hingenommen haben, können wir nicht länger ignorieren."

* Für eine bessere Lesbarkeit werden in dieser Publikation die Begriffe „Hacker" und „hacken" ausschließlich im Sinne eines unbefugten Eindringens in andere Netzwerke, Systeme und Programme, mit dem Ziel, Schaden anzurichten, verwendet. Hier ist nicht die akademische Hackerkultur gemeint, welche beispielsweise die Verbesserung technischer Infrastrukturen anstrebt, indem sie Sicherheitslücken aufzeigt. Darüber hinaus schließt der Begriff „Hacker" auch die weibliche Form mit ein.

1.2 Die Vision einer sicheren Cyberwelt

Der Verkauf persönlicher Daten ist auf dem Schwarzmarkt äußerst lukrativ: Auf illegalen Handelsportalen boten Hacker die bei Yahoo erbeuteten Daten für 200.000 Dollar an [5]. Cyberkriminelle können anhand der gestohlenen Namen, Geburtsdaten, Passwörter oder Versicherungsnummern die Identitäten der Opfer annehmen und diese für politische oder finanzielle Zwecke missbrauchen.

Die Schnelllebigkeit, die Komplexität und die hohe Vernetzung von IT-Systemen bewirken, dass Risiken nicht mehr kalkulierbar sind. Sicherheitsexperten gehen zudem davon aus, dass noch mehr Cyber-Security-Probleme existieren, als bislang bekannt sind, und auch Sicherheitslücken oft unentdeckt bleiben.

Die Ära der Vernetzung und Digitalisierung steht erst am Anfang. Dabei hängt die Integrität unserer IT-Systeme direkt mit dem Schutz und der Sicherheit der Bevölkerung zusammen und ist zu einem ebenso hohen Gut wie die Wasser- und Stromversorgung geworden. Vision muss es daher sein, eine „absolut sichere, beherrschbare Cyberinfrastruktur" zu schaffen. Diese Herausforderung ist gewaltig und nahezu unlösbar. Realistisch ist allerdings das Ziel, die Komplexität der Cyberwelt zu beherrschen, um die Risiken zu minimieren. Wo sich Deutschland auf dem Weg zu einer sicheren Cyberwelt befindet, zeigen die folgenden Kapitel.

„Beherrsche die Konsequenzen und die Komplexität, dann wird das Risiko kalkulierbar."

2

Gefährdungsfelder in wichtigen Lebensbereichen

Immer mehr Dinge des alltäglichen Lebens werden ans Internet angeschlossen. Im sogenannten Internet der Dinge (Englisch: Internet of Things, kurz: IoT) können Privathaushalte Kaffeemaschine und Türverriegelung verbinden. Im Zeitalter von Industrie 4.0 sind ganze Produktionsanlagen, Logistiksysteme, Zulieferbetriebe, Kunden und staatliche Infrastrukturen vernetzt. Im Prinzip gilt: Alles, was mit dem Internet verbunden ist, kann gehackt werden.

Je offener wir als Bürgerinnen, Unternehmer und Nationen mit Daten umgehen, umso anfälliger werden wir und umso lukrativer wird das Geschäft für Cyberkriminelle. Allein mit dem Verkauf der Kundendaten einer Firma, etwa an die Konkurrenz, lassen sich rund 70.000 Dollar verdienen [6].

Die folgenden Beispiele verdeutlichen das hohe Maß an Gefährdung in ausgewählten Lebensbereichen. ►

Gefährdungsfeld Kritische Infrastrukturen

Gesundheits-system

Ein Hacker schickt eine E-Mail mit schädlichem Anhang (Malware) an die Chefärztin eines Krankenhauses.

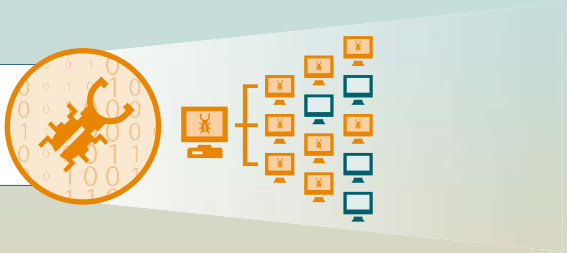
Beweggründe:

- Politisch oder ideologisch (Hacktivismus)
- Datenklau und -verkauf
- Sabotage
- Datenverschlüsselung mit Geldforderung zur Entschlüsselung

Eine wichtige E-Mail der Forschungskollegin aus den USA, gleich mal öffnen!

Die Chefärztin liest die E-Mail, vertraut ihr und öffnet ihren Anhang. Die Malware gelangt in das IT-System des Krankenhauses.

Durch die Vernetzung aller Rechner kann sich der Virus schnell verteilen. Der Hacker kann jetzt Daten verschlüsseln und Lösegeldforderungen stellen. Das Krankenhaus wird arbeitsunfähig.



Um Datenmissbrauch zu verhindern, muss das System heruntergefahren werden. Eine Wiederherstellung kann mehrere Wochen dauern. Das wirkt sich massiv auf den Arbeitsalltag im Krankenhaus aus.

Patientenakten sind nicht verfügbar und müssen händisch aktuell gehalten werden.

Viele Operationen müssen verschoben werden, nur Notoperationen werden genehmigt.

Krankenwagen können nicht anfahren. Notfälle werden auf umliegende Krankenhäuser verteilt, was für ländliche Regionen ein großes Problem sein kann.

Quelle: Eigene, modifizierte Darstellung auf Basis von Stern 2017 [10] und Süddeutsche Zeitung 2016 [11]

2.1 Kritische Infrastrukturen: Gesundheitssystem

Der Begriff Kritische Infrastrukturen (KRITIS) umfasst die Sektoren Staat und Verwaltung, Energie, Gesundheit, IT/Telekommunikation, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen sowie Ernährung [7]. Für Deutschland ist es existenziell, die Unternehmen und die Kundschaft dieser Sektoren durch vertrauenswürdige Technologien zu schützen. Dennoch meldeten Betriebe aus den KRITIS-Sektoren allein im Zeitraum von Juli 2017 bis Mai 2018 beim Bundesamt für Sicherheit der Informationstechnik (BSI) 145 Vorfälle von Cyberangriffen [8]. Dabei ist von einer weit höheren Dunkelziffer auszugehen. So stehen beispielsweise im Gesundheitssystem nur die größten Krankenhäuser Deutschlands (etwa zehn Prozent aller Krankenhäuser) in der Pflicht, Cyberangriffe beim BSI zu melden [9]. Kleinere Krankenhäuser und Arztpraxen, die zum Opfer von Cyberattacken werden, verschweigen diese Angriffe in der Regel. Zu groß ist die Befürchtung, dass Patientinnen und Patienten, aber auch die Ärzteschaft ihr Vertrauen verlieren. Die Abbildung illustriert einen Hackerangriff auf ein IT-System im Gesundheitsbereich, wie er in Deutschland vermehrt vorkommt.

„Das Internet ist ein Kartenhaus; Sicherheit wurde in seiner Architektur nicht berücksichtigt. Eingeplant wurde auch nicht, dass es viele Leute mit schlechten Absichten gibt."

2.2 Kritische Infrastrukturen: Stromversorgung

Spätestens seit den Cyberangriffen auf eine iranische Atomanlage und auf die ukrainische Stromversorgung ist klar: Politisch motivierte Cyberangriffe auf Kritische Infrastrukturen sind Realität geworden. Geheimdienste oder Terrororganisationen können dadurch Verunsicherung und Angst in der Bevölkerung schüren und die Autorität eines souveränen Staates diskreditieren. Das nachfolgende Schaubild veranschaulicht, wie ein Hacker durch das Eindringen in ein Stromnetzwerk ganze Städte lahmlegen kann. Die betroffenen Energieunternehmen benötigen Stunden bis Tage, um die Malware ausfindig zu machen und die Energieversorgung wiederherzustellen. So lange hat der Hacker Zugang zum Kontrollsystem des Stromnetzwerks und kann ganze Krankenhäuser, Flughäfen und die Wasserversorgung lahmlegen. Auch in Deutschland besteht die reale Gefahr eines solchen Angriffs. Der besondere Schutz der deutschen Stromnetze und Stromversorger sowie zusätzlich bereitgestellte Notstromreserven für den Fall einer Cyberattacke sind dringend nötig – doch derzeit nicht ausreichend vorhanden.

Gefährdungsfeld Kritische Infrastrukturen

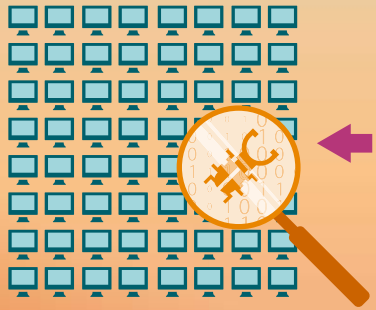
Stromversorgung

Ein Hacker verschickt E-Mails mit manipuliertem Inhalt an mehrere Mitarbeitende eines Stromkraftwerkes. Die E-Mail enthält einen Link auf eine Webseite mit Schadsoftware (Malware). Es genügt, wenn ein einziger Mitarbeiter die Malware aktiviert, indem er die Webseite besucht oder den schadhaften Anhang in der E-Mail öffnet, um dem Hacker Zugriff auf das gesamte Stromkraftwerk zu verschaffen.

Motivation: Terrororganisation oder Geheimdienste wollen Angst verbreiten und die Souveränität eines Staates diskreditieren.

Die Stromversorgung fällt in vielen Städten oder sogar landesweit aus.

- Tankstellen funktionieren nicht mehr.
- Der öffentliche Nah- und Fernverkehr kommt zum Erliegen. Die Menschen kommen nicht mehr zur Arbeit.
- Die Lebensmittelversorgung der Bevölkerung ist nach einigen Tagen nicht mehr gesichert.

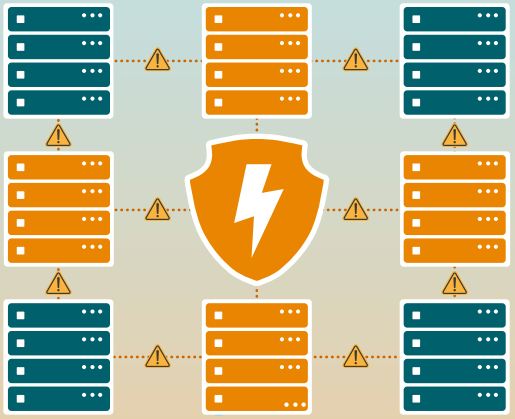


Mehrere Stunden oder sogar Tage sind nötig, um die Malware aufzufinden und die Stromnetzwerke wieder in Betrieb zu setzen.

Jedes IT-System ist angreifbar. Wie gut eine Einrichtung auf einen Cyberangriff vorbereitet ist, hängt davon ab, wie rasch dieser identifiziert und behoben werden kann.

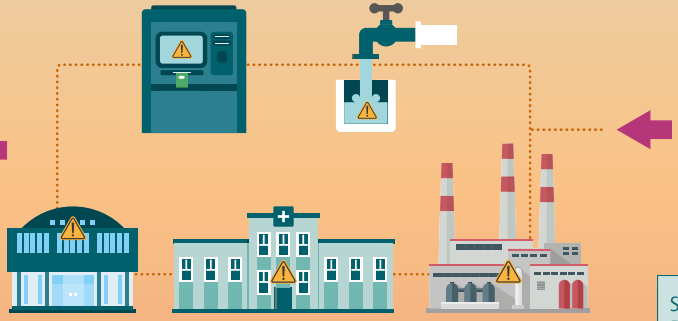
Chaos und Unruhen in der Bevölkerung sind wahrscheinlich.

Quelle: Eigene, modifizierte Darstellung auf Basis von SANS Security Awareness 2016 [12]



Alle IT-Server ohne Notstromversorgung fallen sofort aus. IT-Server mit unterbrechungsfreier Stromversorgung und Notstrom, etwa bei Krankenhäusern, funktionieren, bis der Dieselvorrat verbraucht ist.

Eine Datenübertragung sowie die Kommunikation per Kabel, Funknetz oder Satellit sind nicht möglich.



- Haushalte, Konzerne, Fabriken, Krankenhäuser, Flughäfen sind stunden- oder tagelang außer Betrieb.
- Geldautomaten sind ohne Funktion.
- Die Wasserversorgung als Folge der Stromunterbrechung ist lahmgelegt.

Sämtliche Steuerungs- und Kontrollsysteme für Produktion und Dienstleistungen fallen aus. Eine vollständige Datensicherung erfolgt bei Cloud-Providern, außerhalb des Bereiches der Stromunterbrechung. Das gilt nur für die Daten, die bereits vor dem Cyberangriff transferiert worden sind.

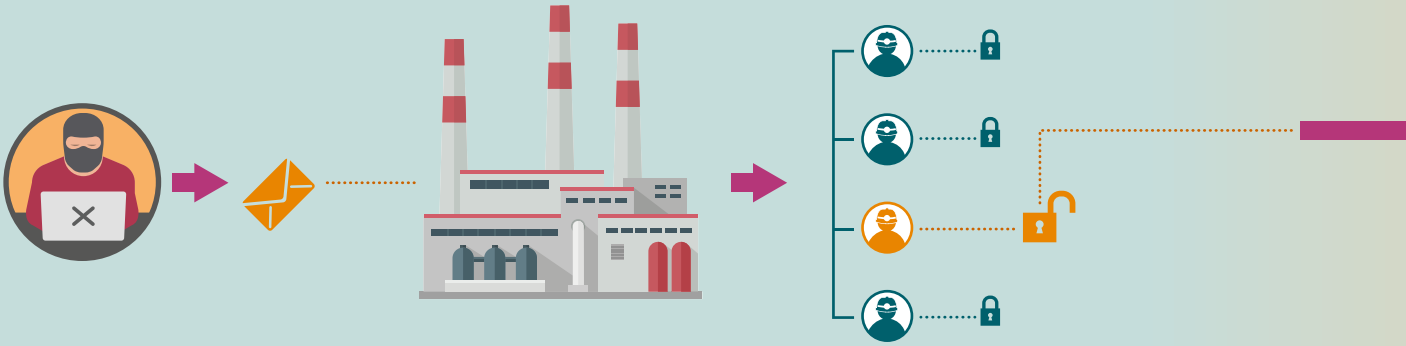
Je nach Unternehmensgröße werden die Daten üblicherweise stündlich oder täglich gesichert. Eine Wiederherstellung ist erst nach Rückkehr der Stromversorgung möglich. Alle nicht gesicherten Daten gehen verloren.

2.3 Produktion: Industrie 4.0

In der Industrie 4.0 kommunizieren und kooperieren intelligente Maschinen, Betriebsmittel, Produkte, Werkstücke sowie Lager- und Transportsysteme; es entstehen hochflexible unternehmensübergreifende Wertschöpfungsnetzwerke. Dabei verschmelzen ganze IT-Infrastrukturen in Produktion, Logistik, Vertrieb, Einkauf und Verwaltung, oft auch mit den IT-Infrastrukturen weiterer Unternehmensniederlassungen und Partnerunternehmen. Dies eröffnet Cyberkriminellen die Möglichkeit, über eine einzige Schwachstelle in ein Produktionssystem einzudringen und die Produktion zu stoppen, fehlerhafte Erzeugnisse herzustellen oder Anlagen zu zerstören. Die Abbildung zeigt einen erfolgreichen Angriff auf ein deutsches Stahlwerk aus dem Jahr 2014. Anders als bei der Bundesverwaltung bestand damals für Privatunternehmen keine Meldepflicht im Falle eines Cyberangriffs. Inzwischen gibt es eine Meldepflicht, diese betrifft jedoch nur Betriebe aus den KRITIS-Sektoren (▶ siehe auch Kapitel 4.4). Deshalb ist bislang ungewiss, wie zahlreich und erfolgreich derartige Übergriffe in Deutschland sind.

Gefährdungsfeld Produktion

Industrie 4.0



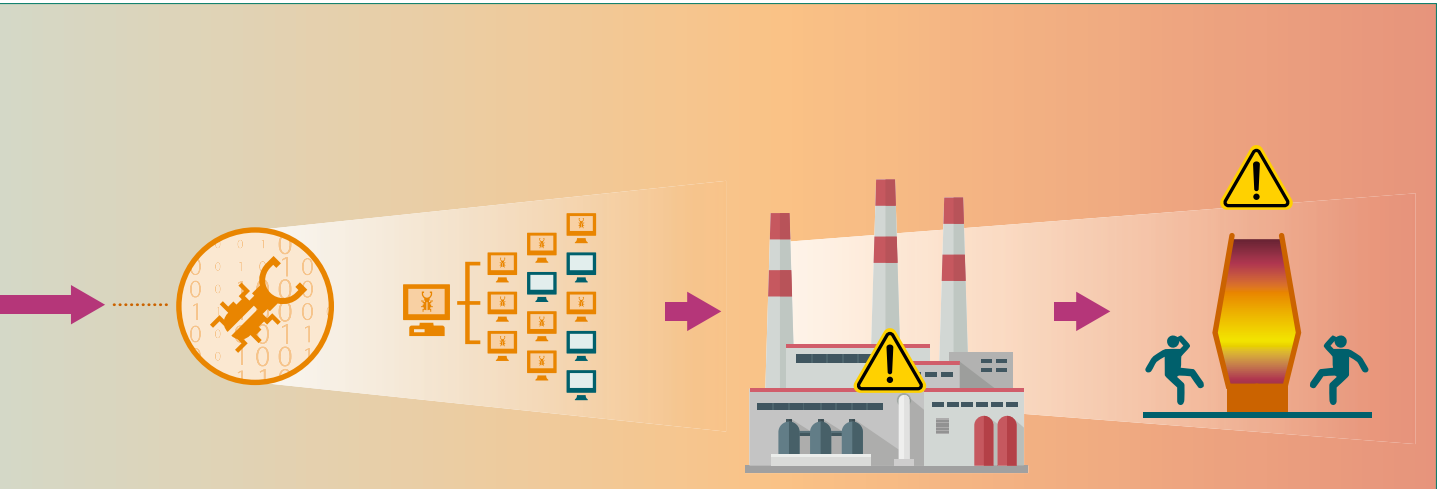
Ein Hacker gibt sich als Techniker aus, der ein angebliches IT-Problem lösen muss, und erhält von einem ahnungslosen Mitarbeiter die Zugangsdaten zum System.

Es gibt verschiedene Methoden, über einzelne Personen in ein System einzudringen. So kann der Hacker etwa über falsche Angaben das Vertrauen eines Unternehmensangehörigen gewinnen, um an vertrauliche Informationen zu gelangen oder sein Opfer zur Freigabe von Finanzmitteln zu bewegen. Eine weitere Methode ist das Versenden von E-Mails mit schadhafter Software. Die Inhalte der E-Mails sind so gestaltet, dass der Mitarbeiter sie für vertrauenswürdig hält und auf den Link klickt oder den Anhang öffnet. Dies verschafft dem Hacker Einsicht in die Zugriffsdaten und Passwörter, worüber er in das System eindringt.

Quelle: Eigene, modifizierte Darstellung auf Basis von KPMG 2015 [13]

Jeden Tag werden 300.000 neue Schadsoftware-Variationen entdeckt. Nicht jede davon wird erfolgreich eingesetzt. Aber eine veraltete Sicherheitstechnik oder ungeschultes Personal erleichtern deren Einsatz. Meistens werden Präventionsmaßnahmen, wie die Einführung eines E-Mail-Verschlüsselungsprogramms, aus Sorglosigkeit nicht umgesetzt. All dies spielt den Hackern in die Hände.

In Deutschland muss ein Unternehmen nicht an die Öffentlichkeit gehen, wenn es zu einem derartigen Hack kommt. Ebenso wenig besteht für Unternehmen eine Meldepflicht an das BSI, wenn es nicht unter die Kategorie Kritische Infrastrukturen fällt. Somit ist mit einer hohen Dunkelziffer an unentdeckten erfolgreichen Cyberangriffen zu rechnen.

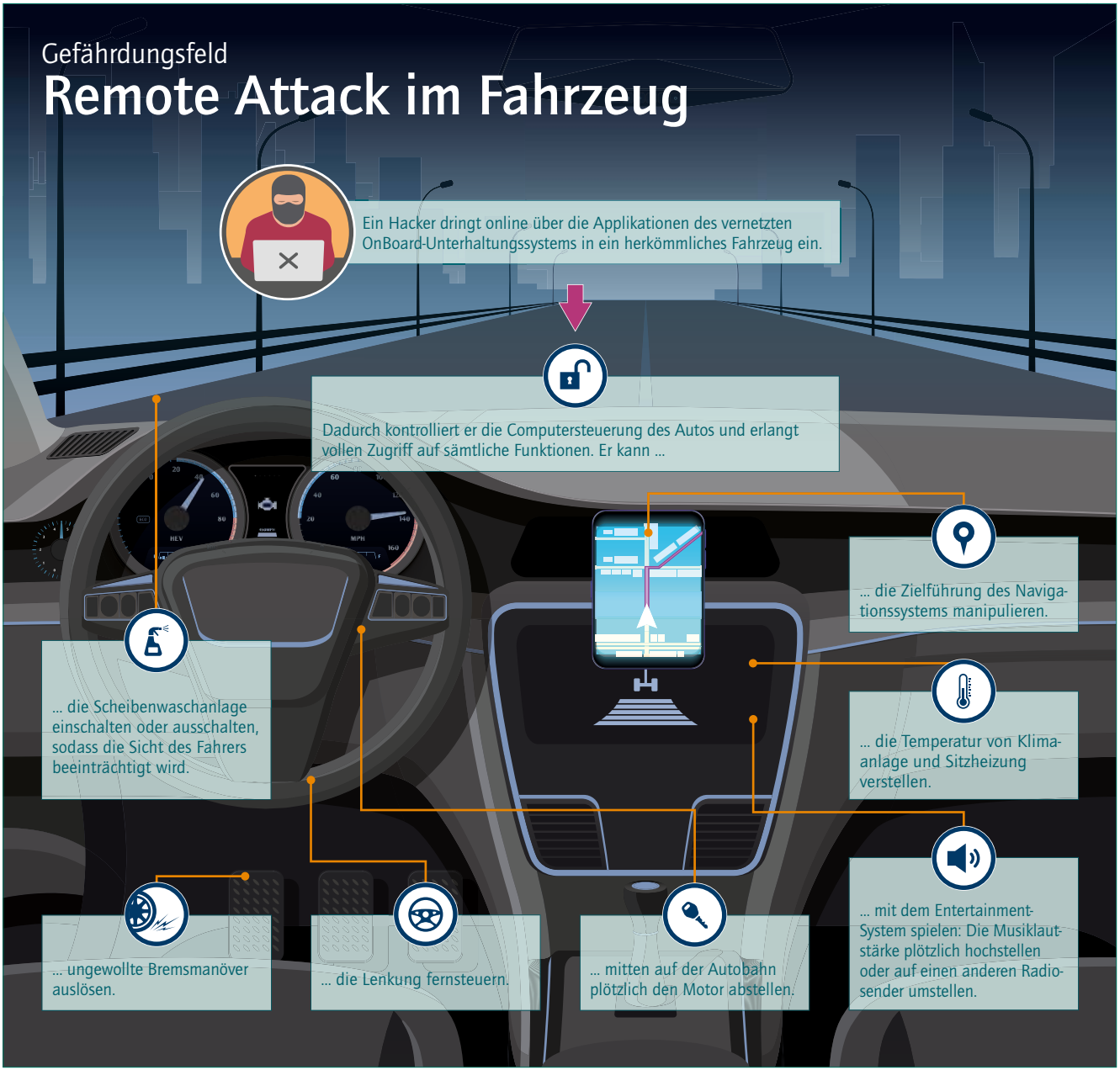


Der Hacker kann sich nun mit den gültigen Zugangsdaten einfach in das System einloggen.

Da in vielen Firmen sämtliche Abteilungen durch die IT zusammenhängen, reichen die Zugangsdaten eines einzigen Unternehmensangehörigen aus der Verwaltung aus, um Schäden an empfindlichen Produktionsprozessen zu verursachen. Je vernetzter diese Produktionsprozesse sind (Industrie 4.0), desto schneller können sich die Schäden verbreiten.

Der Hacker hat nun Zugriff auf das ganze Produktionssystem. Er kann Steuerelemente oder sogar ganze Abschnitte der Produktionsanlage zum Erliegen bringen.

Dadurch lässt sich zum Beispiel der Stahlhochofen nicht mehr steuern. Es kann zu einem erheblichen Sachschaden sowie zu einem großen Produktionsausfall kommen. Auch für die anwesenden Personen kann der verursachte Schaden verheerende Folgen haben.



Quelle: Eigene, modifizierte Darstellung auf Basis von Handelsblatt 2017 [19] und Spiegel Online 2014 [20]

2.4 Remote Attack im Fahrzeug

In den kommenden Jahren soll hochautomatisiertes und autonomes Fahren zu mehr Sicherheit im Verkehr führen. Gleichwohl können Hacking-Angriffe auf vernetzte oder autonome Fahrzeuge verheerende Folgen für Leib und Leben haben. Je stärker ein Auto mit dem Internet vernetzt ist, desto größer wird die Angriffsfläche. Einer Studie von Ernst and Young zufolge werden weltweit rund 100 Millionen Fahrzeuge bis zum Jahr 2025 mit dem Internet verbunden sein [18]. Versicherungsfachleute befürchten, dass sich die Cyberübergriffe auf Fahrzeuge aufgrund unzureichender Schutzmechanismen, vor allem bei Autos mit älteren OnBoard-Unterhaltungssystemen, in den kommenden Jahren vermehren werden [19]. Die Abbildung zeigt, wie ein Hacker über einen Remote Attack (▶ siehe Glossar) online in ein Fahrzeug eindringt und vollen Zugriff auf sämtliche Funktionen erlangt. Wie in einem Alptraum sitzt der Autofahrer während des gesamten Hacking-Angriffs machtlos in seinem Fahrzeug: Er hat keine Möglichkeit, das Auto über Knöpfe, Lenkrad oder Pedale zu bedienen; kämpft er doch gegen einen nicht greifbaren Eindringling, der weit entfernt ist.

2.5 Smart Home

Bis 2020 werden geschätzt 20 Milliarden Geräte mit dem Internet verbunden sein (Internet of Things, IoT) und bis 2030 werden über die Hälfte aller Haushalte intelligente vernetzte Geräte einsetzen – „smart" sein [14]. Aufgrund des Preisdrucks im Endkundenmarkt sparen viele Unternehmen an der Sicherheit ihrer Produkte und Dienstleistungen oder lassen diese komplett weg. Endnutzende erkennen den Mehrwert eines sicher ausgestatteten Produktes nicht sofort, da die (fehlende) Sicherheit erst bei einem Hacking-Angriff deutlich wird (siehe Kasten „Markt for Lemons"). Dabei ist das Gerät selbst oft nicht das Hauptziel, sondern die Gesamtinfrastruktur, wie etwa ein Smart Home. Die folgende Abbildung illustriert, wie ein Krimineller eine Überwachungskamera hackt und dadurch in alle anderen vernetzten Produkte im Smart Home virtuell und physisch eindringen kann.

Market for Lemons

Da die Endkundschaft meist nicht die Sicherheit der gekauften Produkte einschätzen kann, sinkt ihre Zahlungsbereitschaft für IT-Sicherheit. Stattdessen achtet sie auf wahrnehmbare Features wie das User Interface. Das wiederum veranlasst Betriebe, sich auf andere Produktmerkmale zu konzentrieren und noch weniger in die IT-Sicherheit zu investieren. In dieser fortwährenden Spirale verdrängen die unsicheren Produkte die sicheren solange, bis es keinen Markt mehr für letztere gibt. Dies bezeichnet die Wirtschaftstheorie als „Market for Lemons".

Gefährdungsfeld

Smart Home

Zunächst verschafft sich der Hacker Zugriff auf den Smart-Fernseher und infiziert diesen mit Schadsoftware. Über eine Nachricht auf dem Bildschirm verlangt er nun Lösegeld in Bitcoins.

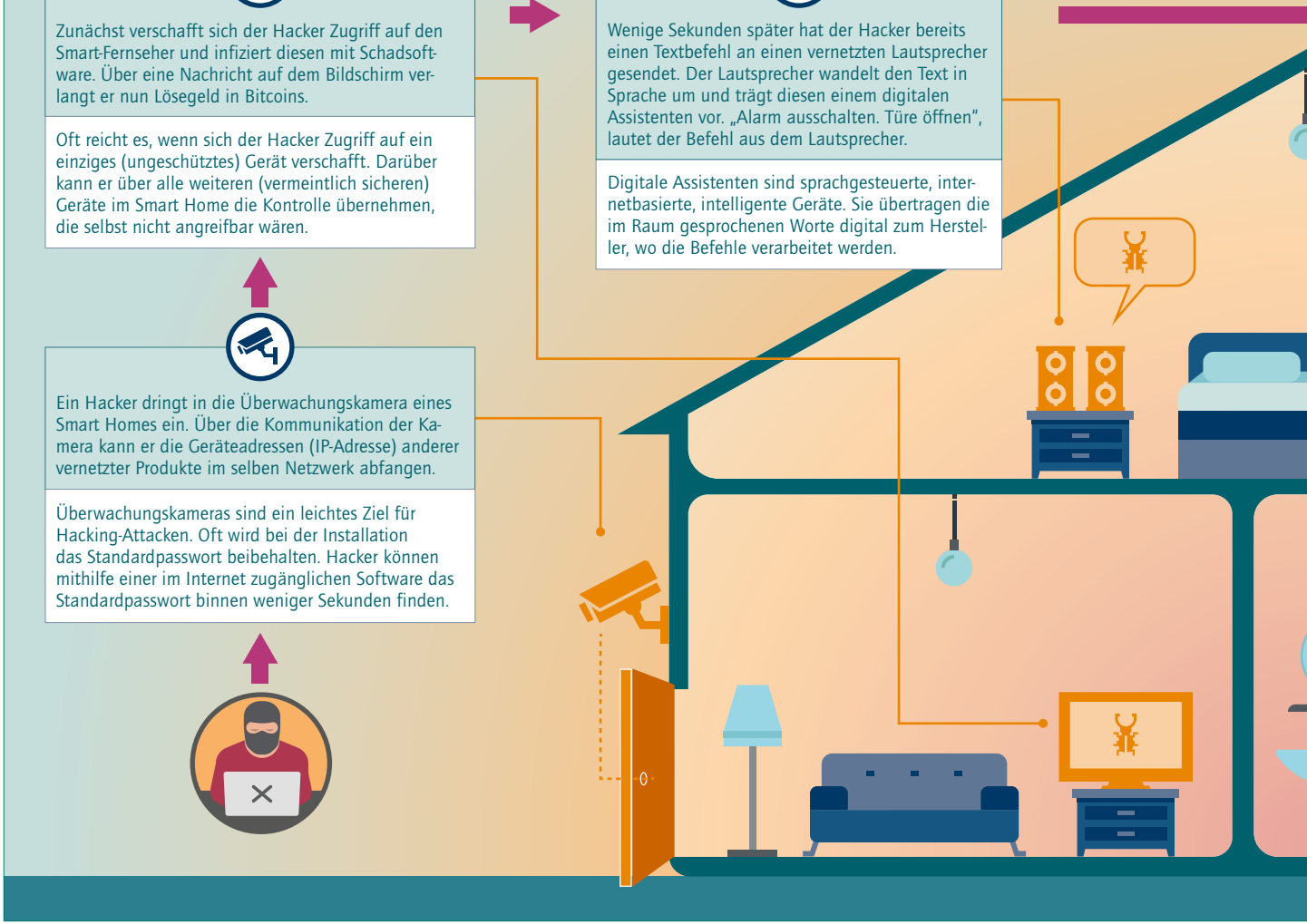
Oft reicht es, wenn sich der Hacker Zugriff auf ein einziges (ungeschütztes) Gerät verschafft. Darüber kann er über alle weiteren (vermeintlich sicheren) Geräte im Smart Home die Kontrolle übernehmen, die selbst nicht angreifbar wären.

Ein Hacker dringt in die Überwachungskamera eines Smart Homes ein. Über die Kommunikation der Kamera kann er die Geräteadressen (IP-Adresse) anderer vernetzter Produkte im selben Netzwerk abfangen.

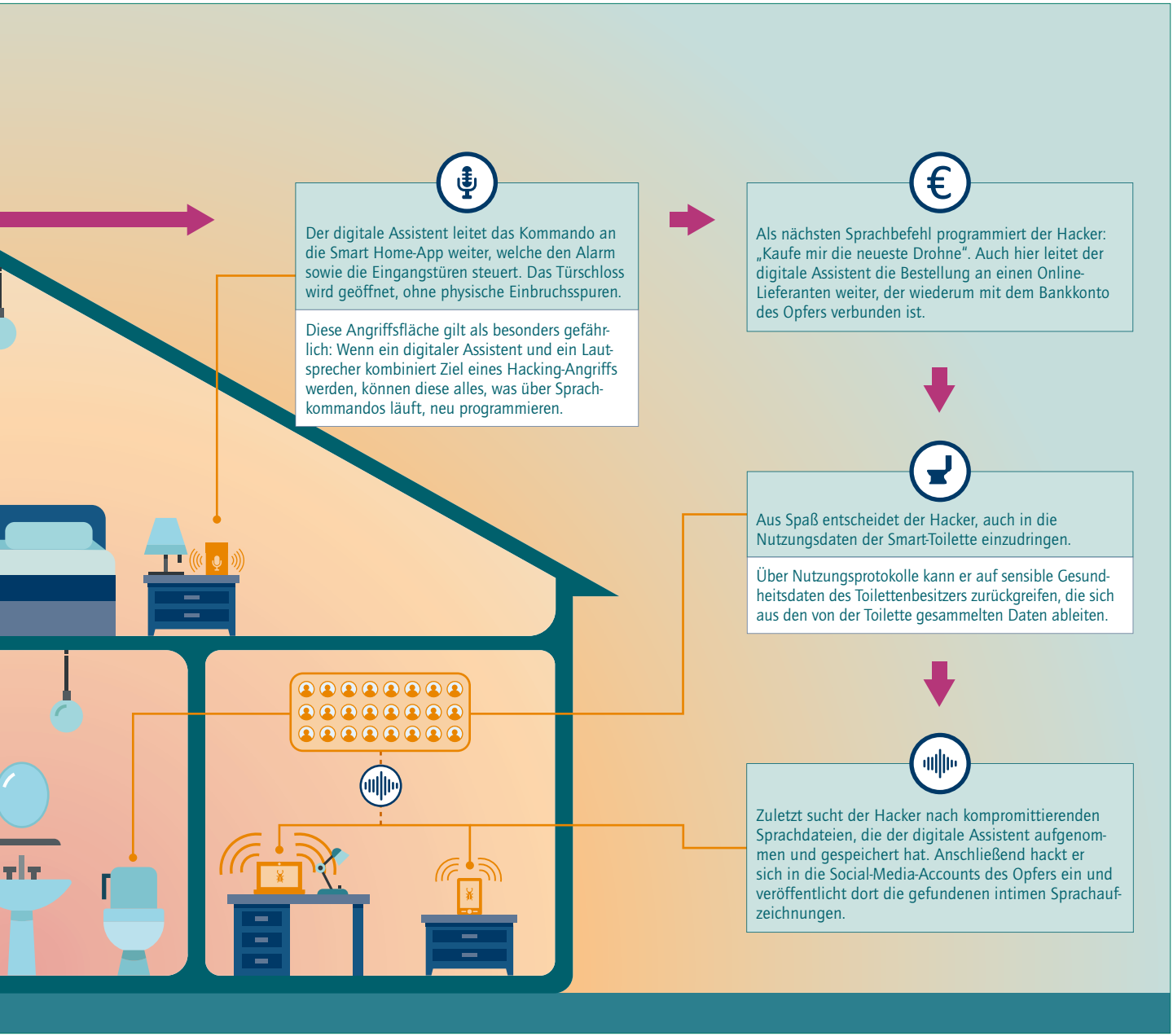
Überwachungskameras sind ein leichtes Ziel für Hacking-Attacken. Oft wird bei der Installation das Standardpasswort beibehalten. Hacker können mithilfe einer im Internet zugänglichen Software das Standardpasswort binnen weniger Sekunden finden.

Wenige Sekunden später hat der Hacker bereits einen Textbefehl an einen vernetzten Lautsprecher gesendet. Der Lautsprecher wandelt den Text in Sprache um und trägt diesen einem digitalen Assistenten vor. „Alarm ausschalten. Türe öffnen", lautet der Befehl aus dem Lautsprecher.

Digitale Assistenten sind sprachgesteuerte, internetbasierte, intelligente Geräte. Sie übertragen die im Raum gesprochenen Worte digital zum Hersteller, wo die Befehle verarbeitet werden.



Quelle: Eigene, modifizierte Darstellung auf Basis von Welt 2018 [15], heise online 2018 [16] und Spiegel Online 2013 [17]



Der digitale Assistent leitet das Kommando an die Smart Home-App weiter, welche den Alarm sowie die Eingangstüren steuert. Das Türschloss wird geöffnet, ohne physische Einbruchsspuren.

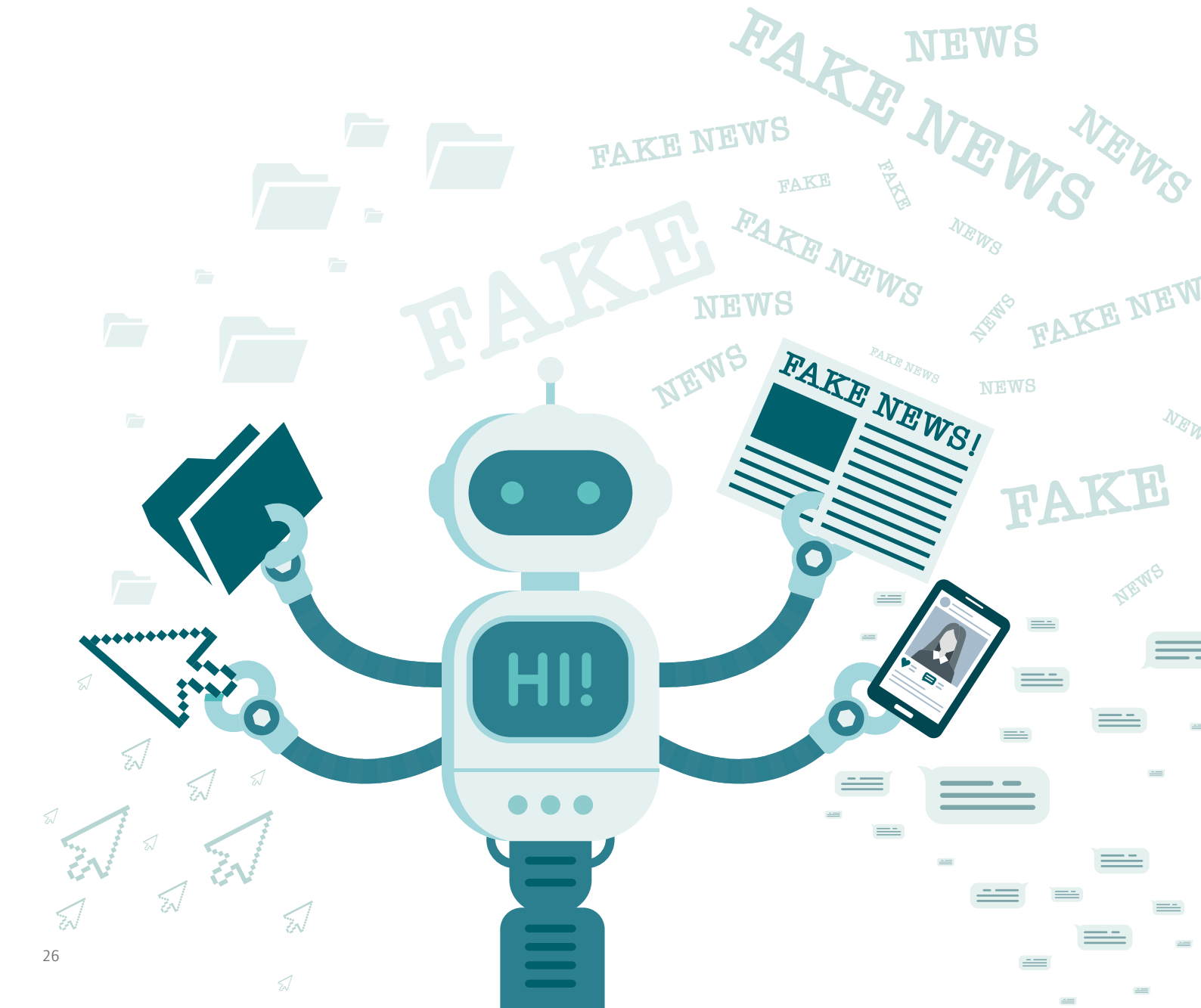
Diese Angriffsfläche gilt als besonders gefährlich: Wenn ein digitaler Assistent und ein Lautsprecher kombiniert Ziel eines Hacking-Angriffs werden, können diese alles, was über Sprachkommandos läuft, neu programmieren.

Als nächsten Sprachbefehl programmiert der Hacker: „Kaufe mir die neueste Drohne". Auch hier leitet der digitale Assistent die Bestellung an einen Online-Lieferanten weiter, der wiederum mit dem Bankkonto des Opfers verbunden ist.

Aus Spaß entscheidet der Hacker, auch in die Nutzungsdaten der Smart-Toilette einzudringen.

Über Nutzungsprotokolle kann er auf sensible Gesundheitsdaten des Toilettenbesitzers zurückgreifen, die sich aus den von der Toilette gesammelten Daten ableiten.

Zuletzt sucht der Hacker nach kompromittierenden Sprachdateien, die der digitale Assistent aufgenommen und gespeichert hat. Anschließend hackt er sich in die Social-Media-Accounts des Opfers ein und veröffentlicht dort die gefundenen intimen Sprachaufzeichnungen.


FAKE NEWS
NEWS
FAKE NEWS
NEWS
FAKE
FAKE
NEWS
FAKE NEWS
FAKE
NEWS
NEWS
NEWS
FAKE NEWS
NEWS
FAKE NEWS!
FAKE
NEWS
HI!

2.6 Politik und Gesellschaft: Doxing und Fake News

Im Dezember 2018 veröffentlichte ein 20-jähriger Hacker gestohlene Daten von knapp tausend deutschen Personen aus Politik, Journalismus und Öffentlichkeit. Hunderte von Abgeordneten fanden ihre privaten Informationen, darunter private Nachrichten, Urlaubsfotos, Kreditkartendaten, Briefe und E-Mails, plötzlich in den Sozialen Medien. Dies ist nur ein Beispiel für das sogenannte Doxing, dem Veröffentlichen gestohlener Daten im Internet. Weltweit wurden allein im Jahr 2018 im Internet rund sieben Milliarden gestohlene Identitäten aus unterschiedlichen Quellen gefunden.

Neben Personen des öffentlichen Lebens werden auch vermehrt deutsche Bürgerinnen und Bürger zum Angriffsziel einer politisch motivierten Hacking-Szene. Diese will über Falschmeldungen, sogenannte Fake News, die öffentliche Debatte lenken: 2018 erhielten die acht erfolgreichsten Fake News mehr Aufmerksamkeit in den Sozialen Medien als fast alle Artikel der größten Nachrichtenseiten in Deutschland. Eine der erfolgreichsten manipulierten Nachrichten des Jahres war „Staat zahlt Harem 7500 Euro im Monat: Syrer lebt jetzt mit 2 Ehefrauen und 8 Kindern in Deutschland." Die Nachricht postete anonymousnews.ru, eine Webseite, die gezielt Falschmeldungen und Hassinhalte verbreitet [21].

Das nachfolgende Schaubild illustriert zwei Szenarien: Das erste Szenario zeigt, wie Datenklau den Ruf von Politikern und Politikerinnen schädigen kann. Sensible, private Informationen, oft vermischt mit Falschmitteilungen, geraten an die Öffentlichkeit. In einem zweiten Szenario veröffentlicht eine kriminelle Person massenhaft Falschinformationen. Hierfür nutzt sie sogenannte Social Bots, Computerprogramme, die menschliches Verhalten imitieren. In beiden Szenarien können Bürgerinnen und Bürger nicht mehr oder nur schwer zwischen echten und falschen Meldungen unterscheiden. Ziel dieser Attacken ist es, Wahlen zu manipulieren oder Meinungen prominenter Fachleute oder von Menschen aus der Politik zu verzerren, um so letztlich die Legitimität des demokratischen Systems zu unterminieren. Zudem verbreiten sich Fake News im Internet auch ohne Hacking-Angriff rasend schnell.

„90 Prozent des Internets ist angreifbar."

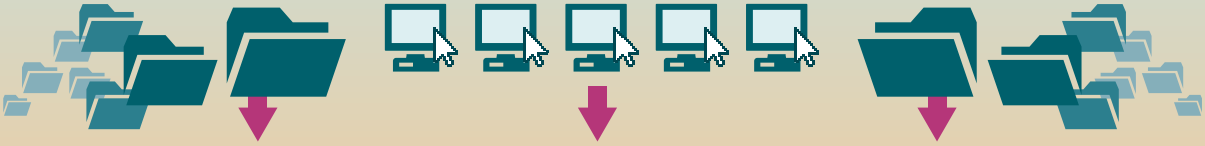
Gefährdungsfeld

Politik und Gesellschaft

Szenario 1

Doxing

In Szenario 1 kauft ein Hacker auf dem Schwarzmarkt geklaute Daten. Somit hackt er sich in die E-Mail- und Social-Media-Accounts von Politikern und Prominenten ein.



Er kann nun anschließend private Daten und Nachrichten von E-Mail- und Social-Media-Accounts herunterladen und durchsucht sie nach kompromittierendem Material.

Da Passwörter oft schwach sind und für mehrere Accounts verwendet werden, hat der Hacker Zugriff auf weitere Accounts desselben Users, schlimmstenfalls auf Cloud-Dienste, in denen wichtige Dokumente gespeichert sind.

Zudem nimmt der Hacker die Online-Identität seines Opfers an und postet in dessen Namen Fake News. Dadurch erhofft er sich, Falschmeldungen über eine vertrauenswürdige Quelle als echt darzustellen und zu verbreiten.

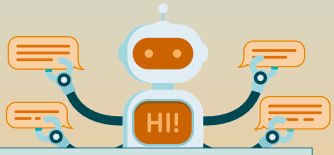
Hat der Hacker genügend Material gesammelt, macht er die brisanten Dokumente publik (Doxing). Ziel ist es, seine Opfer durch Offenbarung ihrer Geheimnisse und Schwächen bloßzustellen und einzuschüchtern. Nicht zuletzt soll sogar eine politische Partei oder das gesamte politische System geschwächt werden.

Quelle: Eigene, modifizierte Darstellung auf Basis von Computerwoche 2019 [22] und Bundeszentrale für politische Bildung 2017 [23]

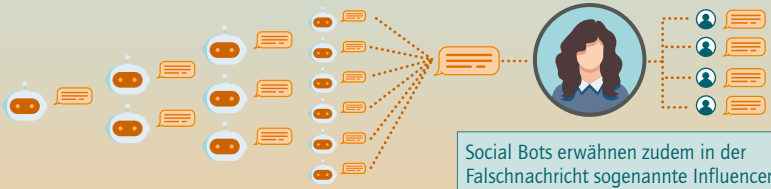
Szenario 2

Verbreitung von Fake News

In Szenario 2 generiert der Hacker ein Computerprogramm, das menschliches Verhalten imitiert (Social Bot).

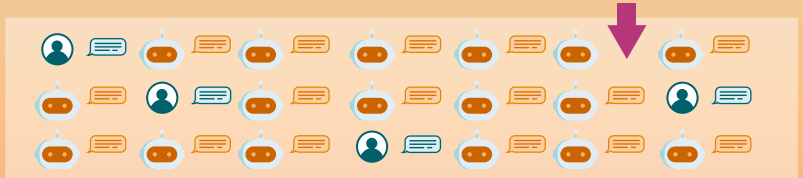


Der Social Bot postet mit seinem gefälschten Profil eine Falschnachricht in unterschiedlichen sozialen Medien.



Weitere Social Bots teilen den falschen Beitrag, wodurch dieser populärer und von vielen Menschen gesehen wird. Diese halten den Beitrag oft für echt.

Social Bots erwähnen zudem in der Falschnachricht sogenannte Influencer, sodass diese eine Benachrichtigung erhalten und auf den Beitrag aufmerksam werden. Halten sie die Falschnachricht ebenso für echt, teilen sie diese mit ihren zahlreichen Followern.



Gleichzeitig starten Social Bots Fake-Diskussionen. Diese enthalten etwa extreme Meinungen oder Beleidigungen und erwecken den Anschein, dass viele Menschen diese Meinung für richtig halten. Die Diskussionen echter Personen gehen in der Masse der Fake News unter.

Gerade wenn Journalisten und Politiker Falschnachrichten in prominenten Medien publizieren, finden diese in der breiten Gesellschaft Gehör und werden so zur tatsächlichen Gefahr.

Der Hacker überflutet die Gesellschaft mit so vielen Informationen, dass nicht mehr zwischen falschen und echten Nachrichten und Meinungen unterschieden werden kann.

Die öffentliche Meinung wird gezielt in eine bestimmte Richtung gesteuert. Wahlergebnisse können beeinflusst werden. Das demokratische System soll unterminiert werden.

2.7 Gefährdungsfelder und Handlungsmöglichkeiten

Was können Einzelne für mehr Sicherheit im Cyberraum tun? Viele der geschilderten Angriffe ließen sich durch menschliches Verhalten abwehren. Einige Experten vertreten sogar die Meinung, dass 95 Prozent aller Cyberangriffe durch sofort aufgespielte Software-Updates vermeidbar sind. Die folgenden Ratschläge zeigen, wie sich jede und jeder zu Hause, mit Kindern, am Arbeitsplatz und in den Sozialen Medien besser schützen kann. Dabei gilt: Der beste Schutz ist ein verantwortungsbewusster Umgang mit dem Internet.

MIT KINDERN/JUGENDLICHEN

- Bedenken Sie, dass Kinder und Jugendliche einfacher als Erwachsene zu beeinflussen sind. Sprechen Sie mit Ihren Kindern über die Verantwortung, die mit der Nutzung sozialer Netzwerke einhergeht. Erläutern Sie Ihren Kindern Datenschutz, Privatsphäre, Informationen im Internet sowie Schutz vor Mobbing.
- Schalten Sie Applikationen ein, die den Zugriff auf bestimmte Funktionen des Telefons regulieren. So bieten Sie Ihren Kindern einen kontrollierten Zugang.

AM ARBEITSPLATZ

- Nehmen Sie an unternehmensinternen IT-Schulungen teil und setzen Sie erworbene Kenntnisse beruflich und privat um.
- Hegen Sie ein gewisses Misstrauen: Klicken Sie nicht alles an, was in Ihrer Mailbox landet.
- Sperren Sie Ihren Bildschirm beim Verlassen des Arbeitsplatzes.
- Notieren Sie sich Ihre Passwörter nicht auf Zettel in der Nähe des Computers.
- Schließen Sie keine unbekannten USB-Sticks an Ihren Computer an. Diese könnten mit schadhafter Software infiziert sein.
- Abteilungen, die keinen Zugriff auf die Daten anderer Abteilungen benötigen, sollen auch nicht unnötig miteinander verbunden sein. Dies kann im Fall einer Cyberattacke die rasche Verbreitung des Angriffs vermeiden.
- Achten Sie auch in der Arbeit auf sichere Passwörter.

IN DEN SOZIALEN MEDIEN

- Begegnen Sie reißerischen, emotional geladenen Artikeln mit Misstrauen: Hacker können über Fake News Menschen manipulieren, verunsichern und die öffentliche Meinung steuern.
- Lesen Sie einen Text genau und prüfen Sie, ob die Information aus einer vertrauenswürdigen Quelle stammt, bevor Sie einen Beitrag teilen.
- Praktizieren Sie laterales Lesen: Öffnen Sie einen weiteren Tab in Ihrem Webbrowser und suchen Sie auf mehreren Webseiten und Nachrichtenportalen nach Berichten zum selben Thema.
- Wenn Sie eine Suchmaschine im Internet verwenden, vertrauen Sie nicht darauf, dass die Top-Treffer auch verlässliche Webseiten sind. Suchmaschinen ordnen Ergebnisse nicht nach Wahrheitsgehalt oder nach Seriosität. Verschaffen Sie sich daher einen Überblick über die vorgeschlagenen Seiten und wählen Sie dann seriöse Portale und nutzen Sie mehrere Quellen für die Informationsrecherche.
- Überprüfen Sie dubiose Meldungen auf sogenannten Faktencheck-Webseiten [21]. Hier bringt die gemeinnützige Presse Fake News ans Licht mit dem Ziel, mehr Transparenz zu schaffen.

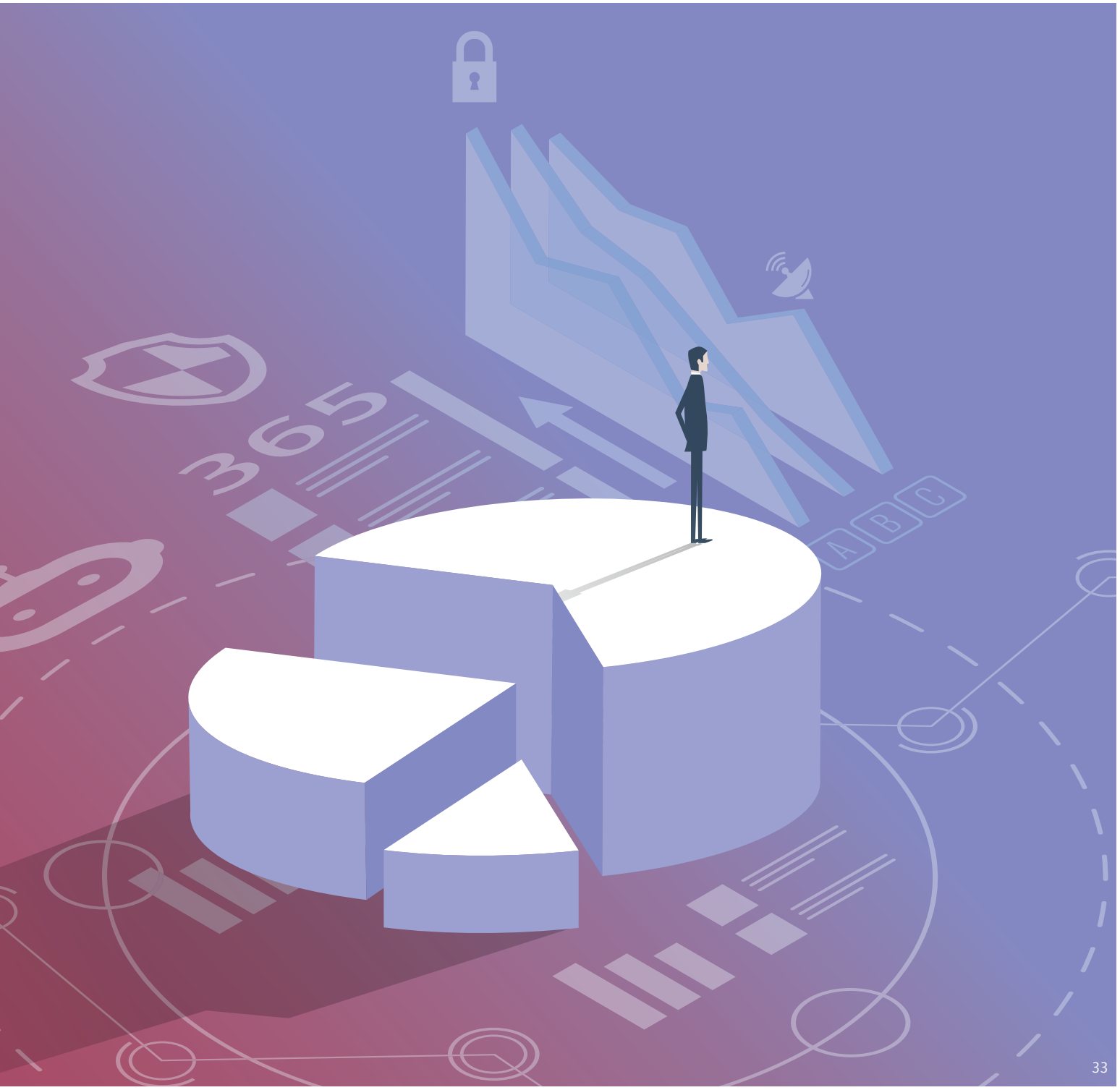
ZU HAUSE

- Spielen Sie verfügbare Software-Updates sofort auf Ihren Rechner, auf Ihr Tablet oder Smartphone. Verschieben Sie dies nicht auf später! Stellt ein Unternehmen ein Update zur Verfügung, können kriminelle Personen dieses Update unmittelbar analysieren, die Sicherheitslücke ausfindig machen und in nur wenigen Stunden über die offene Lücke Ihr Gerät angreifen, solange Sie Ihre Updates nicht aufgespielt haben.
- Halten Sie Anti-Viren- und Firewall-Software auf dem Rechner unbedingt auf dem aktuellen Stand. Auch hier gilt es, Sicherheitslücken sofort zu schließen.
- Verwenden Sie Passwörter oder Passphrasen nicht für verschiedene Systeme gleichzeitig. Anderenfalls hat ein Hacker Zugriff auf Ihre weiteren Konten, sobald er eines Ihrer Passwörter geknackt hat. Passwörter oder Passphrasen sollten möglichst lange und komplex sein; Passwortmanager („Wallets“) helfen hierbei. Verwenden Sie, wenn möglich, eine Zwei-Faktor-Authentifizierung.
- Ändern Sie beim Erwerb eines neuen Smart Home-Geräts sofort das Standard-Passwort.
- Laden Sie keine Apps oder Computerprogramme von Webseiten herunter, die nicht vertrauenswürdig sind.
- Bei kostenlosen Apps oder Services sind oft Ihre Daten der Preis.

3

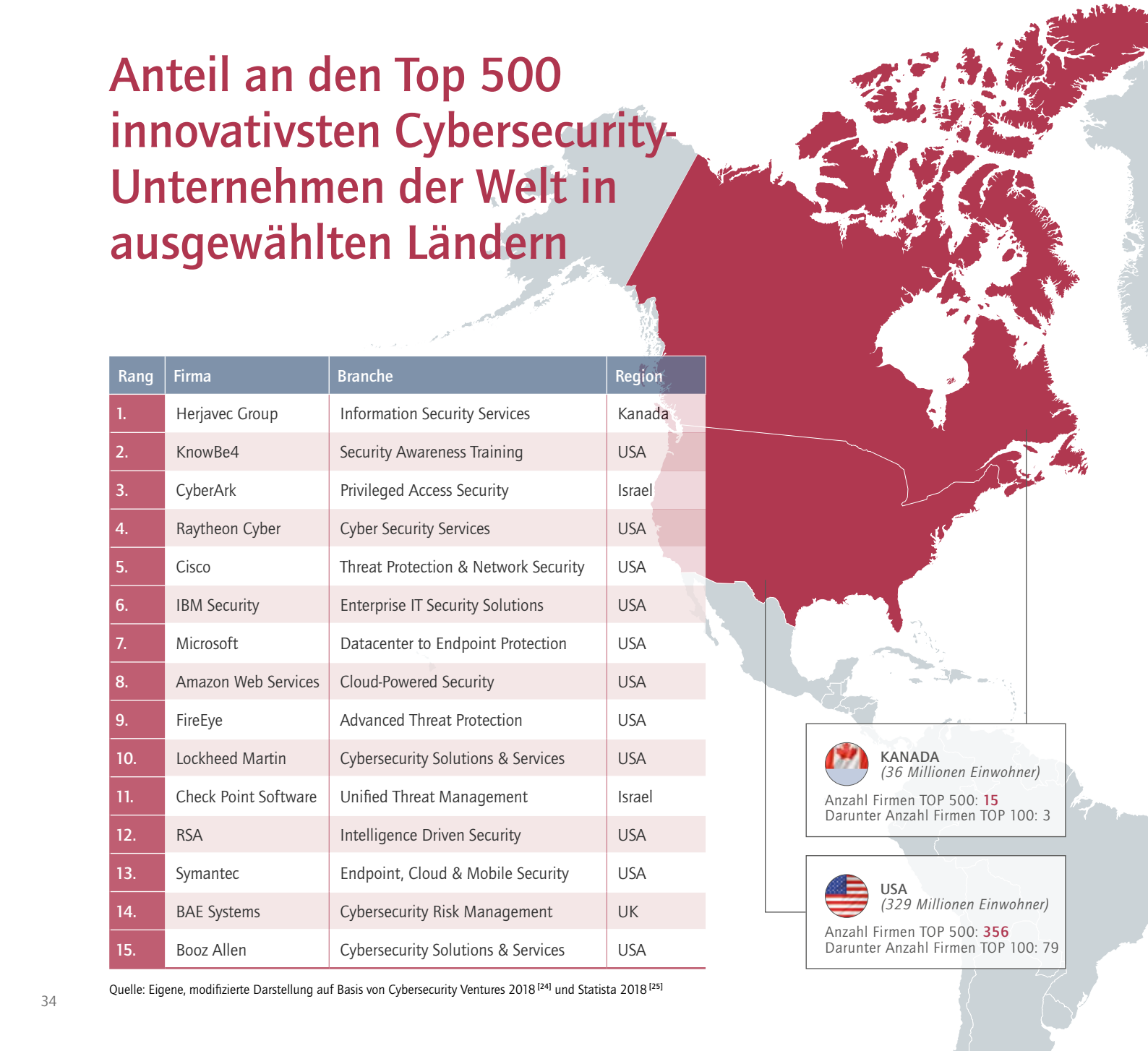
Cyber Security in Deutschland und im internationalen Vergleich

Deutschland genießt seit Jahrzehnten in der Forschung und in der Entwicklung von High-Tech-Produkten „Made in Germany“ weltweit hohes Ansehen. Technologischer Fortschritt ist jedoch ohne Digitalisierung und Vernetzung nicht mehr möglich. Digitalisierung und Vernetzung ohne Cyber Security ist wiederum fahrlässig. Doch wird Deutschland im digitalen Zeitalter in puncto Cyber Security mithalten können? ►

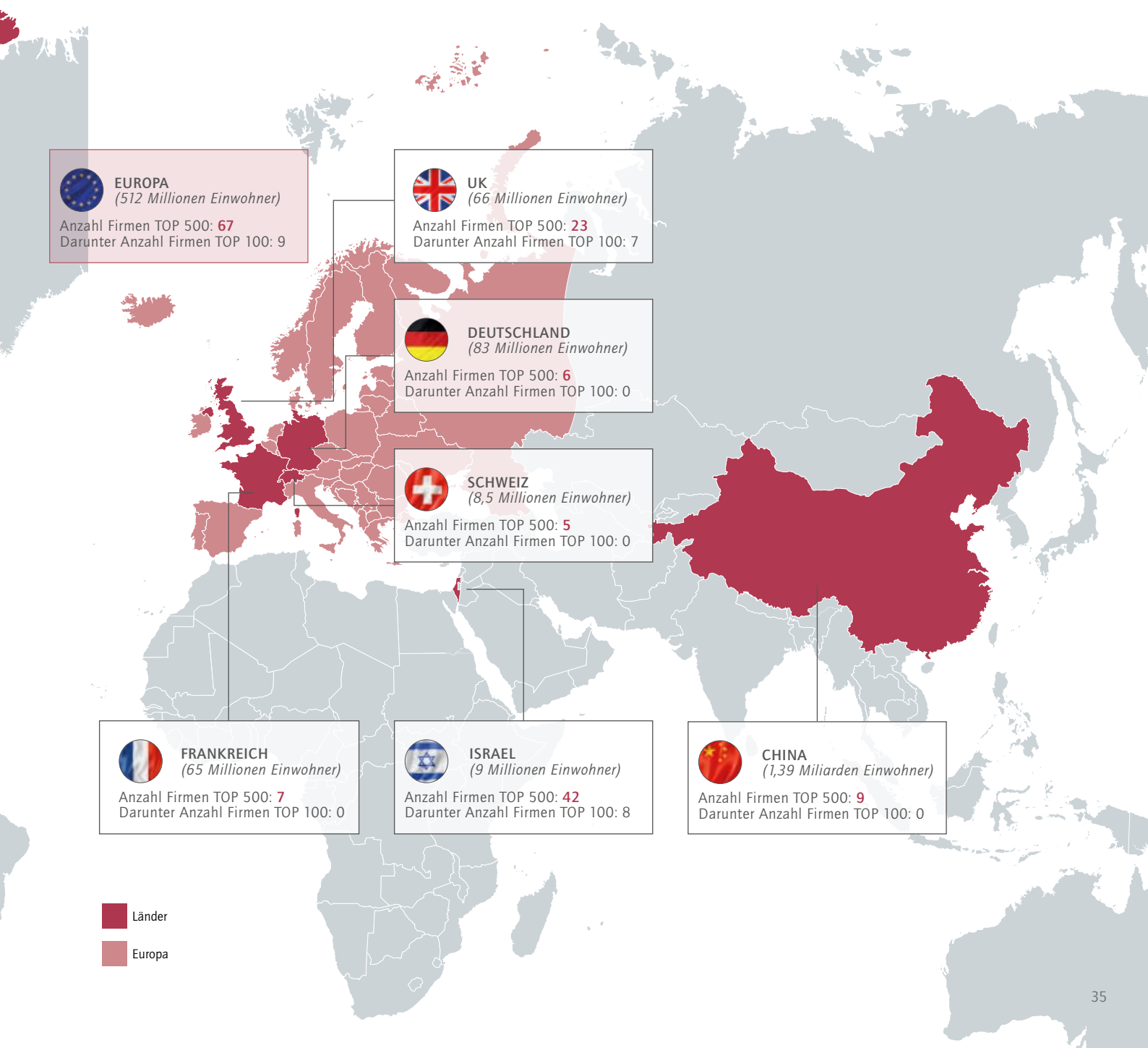

365
A B C

Anteil an den Top 500 innovativsten Cybersecurity-Unternehmen der Welt in ausgewählten Ländern

Rang	Firma	Branche	Region
1.	Herjavec Group	Information Security Services	Kanada
2.	KnowBe4	Security Awareness Training	USA
3.	CyberArk	Privileged Access Security	Israel
4.	Raytheon Cyber	Cyber Security Services	USA
5.	Cisco	Threat Protection & Network Security	USA
6.	IBM Security	Enterprise IT Security Solutions	USA
7.	Microsoft	Datacenter to Endpoint Protection	USA
8.	Amazon Web Services	Cloud-Powered Security	USA
9.	FireEye	Advanced Threat Protection	USA
10.	Lockheed Martin	Cybersecurity Solutions & Services	USA
11.	Check Point Software	Unified Threat Management	Israel
12.	RSA	Intelligence Driven Security	USA
13.	Symantec	Endpoint, Cloud & Mobile Security	USA
14.	BAE Systems	Cybersecurity Risk Management	UK
15.	Booz Allen	Cybersecurity Solutions & Services	USA



Quelle: Eigene, modifizierte Darstellung auf Basis von Cybersecurity Ventures 2018 [24] und Statista 2018 [25]


EUROPA
(512 Millionen Einwohner)
Anzahl Firmen TOP 500: 67
Darunter Anzahl Firmen TOP 100: 9
UK
(66 Millionen Einwohner)
Anzahl Firmen TOP 500: 23
Darunter Anzahl Firmen TOP 100: 7
DEUTSCHLAND
(83 Millionen Einwohner)
Anzahl Firmen TOP 500: 6
Darunter Anzahl Firmen TOP 100: 0
SCHWEIZ
(8,5 Millionen Einwohner)
Anzahl Firmen TOP 500: 5
Darunter Anzahl Firmen TOP 100: 0
FRANKREICH
(65 Millionen Einwohner)
Anzahl Firmen TOP 500: 7
Darunter Anzahl Firmen TOP 100: 0
ISRAEL
(9 Millionen Einwohner)
Anzahl Firmen TOP 500: 42
Darunter Anzahl Firmen TOP 100: 8
CHINA
(1,39 Miliarden Einwohner)
Anzahl Firmen TOP 500: 9
Darunter Anzahl Firmen TOP 100: 0
Länder
Europa

3.1 Wie gut ist die deutsche Cyber-Security-Branche aufgestellt?

Das Anbieterverzeichnis des Bundesverbands für IT-Sicherheit führt insgesamt 169 deutsche Anbieter von Sicherheitslösungen auf [26]. Von diesen Unternehmen zählten jedoch 2018 nur fünf zu den Top 500 innovativsten Cyber-Security-Firmen weltweit; keines davon ist unter den Top 100 [24]. Ein sechstes deutsches Unternehmen ist zwar auf der Liste der Top 500 geführt, jedoch nicht beim Anbieterverzeichnis des Bundesverbandes für IT-Sicherheit gelistet.

> *„Nur, weil wir bisher keine Lücken gefunden haben, bedeutet dies nicht, dass es keine gibt."*

Im deutschsprachigen Raum stieg die Anzahl der Start-ups im Cyber-Security-Segment von 2014 bis 2018 um schätzungsweise über 250 Prozent [27]. Nach einer anderen Quelle waren es im Jahr 2018 dennoch nur 51 Start-ups* in Deutschland aus diesem Gebiet [28]. Auch in einer neuen Studie des Deutschen Startup Monitors sind von den insgesamt 1.550 befragten Gründern und Gründerinnen lediglich 0,6 Prozent [29] aus der Sicherheitsbranche. Umgerechnet sind das neun Cyber-Start-ups. Gänzlich verlässliche Quellen zur tatsächlichen Anzahl deutscher Cyber-Start-ups gibt es bislang nicht. Im Vergleich dazu zählte Israel, bei nur einem Zehntel der Bevölkerung Deutschlands, im Jahr 2017 über 300 Start-ups im Cyberbereich [30].

In Deutschland fördert das Bundesministerium für Bildung und Forschung (BMBF), etwa im Rahmen der Initiative StartUpSecure [31], die Gründerszene im Bereich IT-Sicherheit. Dennoch erhalten Technologie-Start-ups in Israel oder in den USA erheblich höhere Unterstützung von privaten Acceleratoren und staatlichen Förderprogrammen [27]. Deshalb sehen sich viele deutsche Start-ups gezwungen, ins Ausland zu gehen. Vor allem China investiert viel Wagniskapital in deutsche und europäische Zukunftstechnologien. Zwar befürchten die Geschäftsleitungen junger Unternehmen selbst den weiteren Ausverkauf, können und wollen aber nicht auf die besseren Wachstumschancen in China verzichten. Deutschland läuft Gefahr, Millionenbeträge in die Grundlagenforschung zu investieren und zuzusehen, wie die Wertschöpfung im Ausland stattfindet [32].

Die Abwanderung von Know-how und der starke Aufholbedarf der deutschen Gründerszene im Cyberbereich führen zu einer weiteren Problematik: Deutschland ist derzeit stark von internationalen IT-Unternehmen und Cloud-Anbietern abhängig. Insbesondere bei Hardware-Komponenten unbekannter oder nicht vertrauenswürdiger Unternehmen besteht die Gefahr möglicher Backdoors, also Hintertüren, über die Herstellerfirmen heimlich auf den Computer oder das IoT-Gerät zugreifen können. Solche Zugriffe bemerken Nutzende nicht.

* Berücksichtigt wurden Start-ups, die in oder nach 2011 gegründet wurden.

3.2 Deutschland in der Cyberforschung

In Deutschland gibt es zahlreiche exzellente Einrichtungen, die ausschließlich oder in großen Teilen zu Cyber Security forschen. Zusätzlich listet das Bundesministerium für Bildung und Forschung (BMBF) auf seiner „Security Research Map“ [33] nahezu 600 Institutionen, die in der zivilen Sicherheitsforschung tätig sind – Tendenz steigend. Darunter befinden sich Hochschulen, Forschungsinstitute, Unternehmen, Verbände und Behörden.

Aktuell fördert die Bundesregierung zwei große Rahmenprogramme: „Selbstbestimmt und sicher in der digitalen Welt 2015 bis 2020“ zur Entwicklung sicherer, innovativer IT-Lösungen für Bürger, Wirtschaft und Staat, sowie „Forschung für die zivile Sicherheit 2018 bis 2023“, in dem neue Ansätze zum Schutz der Gesellschaft und Wirtschaft vor Terror oder Kriminalität entwickelt werden sollen.

Zudem bündelt das BMBF seit 2011 nationale Forschungskompetenzen in drei IT-Kompetenzzentren, die sich etwa mit Kernfragen der Cyber Security in Wirtschaft, Gesellschaft und Verwaltung oder Lösungsansätzen für die Kernprobleme des Datenschutzes beschäftigen.[34].

Cyber Security kann aufgrund der Komplexität und Reichweite nicht nur als alleinstehendes Forschungsfeld betrachtet werden. Aus diesem Grund bezieht die Sicherheitsforschung in Deutschland generell auch Forscher und Forscherinnen anderer Disziplinen mit ein, die Schnittstellen zur Cyber Security aufweisen, wie etwa die Medizinbranche. So fließen idealerweise unterschiedliche Perspektiven und Methoden zusammen, um gemeinsam sicherheitsrelevante Problemstellungen, beispielsweise im Gesundheitsbereich, zu erarbeiten.

Die Bundesregierung fördert also die Entstehung vortrefflicher Forschungscluster [35]. Jedoch findet dieses wertvolle Know-how aus der Forschung viel zu selten den Weg in praxisorientierte und vermarktbare Sicherheitslösungen (▶ siehe Kapitel 4.1).

Neben den staatlich geförderten Einrichtungen wartet Deutschland auch mit ausgezeichneten Initiativen in der industriellen Sicherheitsforschung auf: Hier kooperieren einige privatfinanzierte IT-Forschungsinstitute eng mit ausgewählten Industrieunternehmen. Diese vertrauen ihren Kooperationspartnern aus der Privatforschung ihre Daten an, um anwendungsorientierte Cyberforschung zu betreiben. Als Gegenleistung zur Freigabe hochsensibler Firmendaten bieten die Forschungsinstitute den Unternehmen sofortige Meldungen von Sicherheitsvorfällen in Realzeit. Cyberattacken lassen sich somit rechtzeitig erkennen und optimalerweise auch bekämpfen. Allerdings profitieren meist Großkonzerne von diesen anwendungsorientierten Forschungskooperationen. Mittelständischen und vor allem kleinen Unternehmen fehlt es hierzu an finanziellen Mitteln, IT-Expertise und teilweise auch an Cyber-Security-Bewusstsein (▶ siehe Kapitel 4.3).

3.3 Der Cyberbehörden-Dschungel

Im Bereich Cyber Security gibt es in Deutschland viele Beteiligte. Auf Initiative unterschiedlicher Bundesministerien sind in den vergangenen Jahren zahlreiche neue Allianzen, Agenturen und Bündnisse entstanden, die sich mit dem Thema Cyber Security befassen. Insgesamt gibt es auf Bundes- und Länderebene etwa 40 Cyberbehörden [36]. Die folgende Tabelle listet einige Einrichtungen und Initiativen auf Bundesebene auf, die sich mit Cyber Security beschäftigen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet sich zwar als „zentraler IT-Sicherheitsdienstleister des Bundes", dessen Kompetenzen und Fähigkeiten die Politik noch weiter ausbauen will [8]. Von den Industrieunternehmen, die von 2016 bis 2018 Datendiebstahl, Industriespionage oder Sabotage an eine staatliche Stelle meldeten, wendeten sich aber laut einer Bitkom-Studie nur 14 Prozent an das BSI [37]. Dies weist auf eine noch sehr geringe Wahrnehmung des BSI als zentrale, nationale Cyberbehörde hin.

„Es gibt in Deutschland zahlreiche Cyberbehörden, aber keine zentrale Cyberdoktrin."

Institution	Angesiedelt bei	Gründung	Ziel
Abteilung für Cybersicherheit	BKA	Angekündigt [38]	
Abteilung für Cybersicherheit	BfV	Angekündigt [38]	
Agentur für Innovation in der Cybersicherheit (ADIC)	BMVg, BMI	Angekündigt	Finanzierung und Förderung von ambitionierten Forschungs- und Entwicklungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cyber Security. Ergänzt Cyber Innovation Hub und ZITiS.
Agentur zur Förderung von Sprunginnovationen	BMBF, BMWi	Angekündigt	Förderung der Umsetzung hochinnovativer Ideen aus Wissenschaft, Forschung und Wirtschaft in erfolgreiche Produkte, Dienstleistungen und Arbeitsplätze.
Allianz für Cybersicherheit	BSI	2012	Wirtschaftsunternehmen besser auf die Herausforderungen der Digitalisierung einstellen.
Bundesamt für Sicherheit in der Informationstechnik (BSI)	BMI	1991	Zentraler IT-Sicherheitsdienstleister des Bundes. Unabhängige, neutrale Behörde mit über 800 Mitarbeitenden, die sich für eine sichere Informations- und Kommunikationstechnik einsetzen.
Bündnis für Cybersicherheit	BMI, BDI	2018	Kooperation zwischen Staat und Wirtschaft, um die digitale Souveränität Deutschlands zu stärken.
Computer Emergency Response Team für Bundesbehörden (CERT-Bund)	BSI		Zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen. Enge Zusammenarbeit mit dem IT-Lagezentrum sowie IT-Krisenreaktionszentrum.
Cyber Innovation Hub der Bundeswehr (CIH)	BMVg	2018	Förderung digitaler Innovationen innerhalb der Bundeswehr.
Cyber-Abwehrzentrum (Cyber-AZ)	BSI	2011	Optimierung der Koordinierung von Schutz- und Abwehrmaßnahmen. Besteht aus Verbindungspersonen von: Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesministerium für Verteidigung (BMVg), Bundesnachrichtendienst (BND), Bundeskriminalamt (BKA), Zollkriminalamt (ZKA), Bundespolizei (BPOL), Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).
German Competence Centre against Cyber Crime (G4C)	Kooperation BKA, BSI	2014 (?)	Entwicklung von Maßnahmen zum Schutz vor Cyberkriminalität. Eigenständiger Verein mit Mitgliedern, Kooperation mit BKA im Informationsaustausch.

Institution	Angesiedelt bei	Gründung	Ziel
IT- Krisenreaktionszentrum	BSI	2005	Sicherstellung einer schnellen Reaktion auf schwerwiegende Vorfälle, um rechtzeitig Gegenmaßnahmen zu ermöglichen und Schäden größeren Ausmaßes zu vermeiden.
IT- Lagezentrum	BSI	2005	Zentrale Meldestelle für IT-Sicherheitsvorfälle in der Bundes- und Landesverwaltung sowie den Kritischen Infrastrukturen.
IT-Planungsrat	BMI	2010	Koordinierung der Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik.
Kommando Cyber- und Informationsraum (KdoCIR)	Bundeswehr	2017	Verantwortung des Cyber- und Informationsraums.
Nationaler Cyber-Sicherheitsrat	Bundesregierung	2011	Schutz kritischer Infrastrukturen und der Cyber-Außenpolitik Deutschlands.
UP KRITIS	BSI, BBK	2007	Öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS).
Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	BMI	2017	Cyberbezogene Lösungen und Know-how waren bislang auf fast 40 Behörden in Bund und Ländern verteilt. Jetzt bündelt die ZITiS diese Expertise und berät als zentrale Stelle die Sicherheitsbehörden umfassend in technischen Fragen und zu Strategien.

Quelle: Eigene Darstellung. Ausgewählte Cyberbehörden in Deutschland und ihre aktuellen Aufgabenbereiche

3.4 Internationale Schlaglichter

Es gibt seitens der führenden Industrienationen zahlreiche Bestrebungen im Bereich Cyber Security. Eine führende Rolle nimmt dabei Israel ein, das weltweit als *die* Cybernation gilt. Ministerpräsident Benjamin Netanjahu kündigte im Jahr 2015 das Vorhaben an, Israel zu einer der weltweit fünf besten Cybernationen zu machen. Das Ziel wurde zwei Jahre später erreicht: Nahezu ein Fünftel der globalen Privatinvestitionen in Cyber Security flossen 2017 nach Israel. Die Pro-Kopf-Wagniskapitalinvestitionen sind so hoch wie in keinem anderen Land der Welt. [39]

Nicht nur wirtschaftlich-technologische Gründe bewegen Israel, Cyberabwehr zur nationalen Priorität zu machen. Historische, militärische und geographische Überlegungen untermauern eine dezidiert offensive Cyberpolitik. Schon in der Schule werden israelische Teenager in Cyber-Sicherheitsstudien unterrichtet. Während der Wehrpflicht in sogenannten „Cyber Intelligence Units" erhalten junge Männer und Frauen eine erstklassige Ausbildung und praxisnahe Erfahrung. Diese Einheiten gelten als wichtiges Karrieresprungbrett [40].

„Das institutionelle Setting ist in Deutschland, im Vergleich zu Israel, eher dezentral organisiert."

Bereits 2014 erkor Netanjahu die Wüstenstadt Beerscheba zu Israels Cyber Hub. Die Siedlung, auch Israels „Silicon Valley" genannt, wurde 2013 auf Initiative des Israel National Cyber Bureau, der Ben-Gurion-Universität und der Gemeinde Beerscheba gegründet. Wissenschaft, Staat und Privatwirtschaft kooperieren hier auf engstem Raum. Unternehmen, die sich in Beerscheba niederlassen, werden mit Steuervergünstigungen belohnt und können mit hochqualifizierten Fachkräften rechnen. Zahlreiche multinationale Technologiekonzerne und israelische IT-Firmen unterhalten in Beerscheba Dependancen oder Innovationslabore; mehr als 120 Cyber-Start-ups sind bereits ansässig [41]. In den kommenden Jahren sollen auch über 10.000 „Cybersoldaten" der israelischen Armee nach Beerscheba umgesiedelt werden. Viele dieser Soldatinnen und Soldaten schlagen nach Abschluss der mehrjährigen Wehrpflicht eine zivile Karriere in der Privatwirtschaft oder in der Forschung ein. So haben ehemalige Mitglieder der israelischen Cyber Intelligence Units bereits mehrere Start-ups im Sicherheitsbereich gegründet, die zu weltweit renommierten Firmen aufgestiegen sind. Drei dieser Firmen, CyberArk, Check Point und Palo Alto Networks [42], stehen laut Cybersecurity Ventures auf Platz drei, elf und sechzehn der 500 innovativsten Cyberunternehmen der Welt (▶ siehe Kapitel 3.1).

3.5 Der Staat im Spagat zwischen Schutz und Ethik

Autoritär regierende Staaten verstehen Zensur, Überwachung und die klare Festlegung nationaler Cybergrenzen als Grundlage ihrer digitalen Souveränität im Cyberraum. Durch eine dezidierte, zentral gesteuerte Cyber-Security-Strategie und ohne öffentliche Diskussionen zu ethischen Fragen verschaffen sie sich einen unbestreitbaren technologischen Vorsprung gegenüber Ländern wie Deutschland.

Hierzulande umfasst die digitale Souveränität* Freiheit im Internet und Cyberschutz. Mit steigender Bedrohungslage, beispielsweise durch Terror, wird der Balanceakt zwischen dem Schutz der Bürgerinnen und Bürger in der physischen Welt und dem Schutz ihrer Privatsphäre in der Cyberwelt zunehmend zur Herausforderung.

* Digitale Souveränität bezeichnet allgemein den souveränen Umgang mit digitalen Medien. Dies umfasst die Medienkompetenz des Einzelnen, staatliche Regulierung sowie sichere Datenübermittlung und IT-Systeme.

Cyber Security im Zusammenspiel von Staat,

Anforderungen der Bürgerinnen und Bürger

Freiheit im Internet. Jederzeit sicher online einkaufen, auf kostenlosen Plattformen chatten, E-Mails schreiben sowie Fotos, Videos, Sprachnachrichten und Dokumente austauschen und hochladen.

Meinungsfreiheit und Schutz der demokratischen Grundordnung. Jederzeit in sozialen Netzwerken meine Meinung äußern zu können, ohne dass dies negative Folgen für mich hat.

Schutz der Daten und Privatsphäre vor Hackerangriffen und dem Staat. **Datensouveränität** (nur ich darf meine Daten einsehen) statt **Big Brother** (Deutschland darf nicht zum Überwachungsstaat werden).

Was der Staat

Der Markt für Sicherheitslösungen und Online-Dienste wird von ausländischen Unternehmen dominiert, die die hohen deutschen Sicherheitsanforderungen meist nicht erfüllen. Deutsche Nutzende laden sensible Daten auf Plattformen internationaler Unternehmen hoch, die oft keine sichere oder gar keine Verschlüsselung anbieten. Die Anbieter können dadurch selbst jederzeit auf die Daten zugreifen. **Auf den Umgang ausländischer Unternehmen mit deutschen Kundendaten übt der deutsche Staat (derzeit) keinen Einfluss aus.**

#$!%

Die Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten, ist in Artikel 5 des deutschen Grundgesetzes verankert. Dies gilt nicht für Fotos von „hilflosen Personen", Kindern und Jugendlichen. Ebenso strafbar sind Volksverhetzung und Beleidigung. **In diesen Fällen überwiegt der Schutz die Meinungsfreiheit.**

In bestimmten Fällen haben Strafverfolgungsbehörden ein berechtigtes Interesse, Daten von Bürgern einzusehen. Dies führt zu einem **Spannungsfeld zwischen Bürgerrechten und der Strafverfolgung** im öffentlichen Interesse, bei der Bürgerfreiheiten temporär eingeschränkt werden. Mit fortschreitender Technologie steigen die Möglichkeiten, Bürger zu überwachen; gleichzeitig stellen geheime Kommunikationswege die Strafverfolgung vor neue Herausforderungen. Hier müssen Grenzen immer aufs Neue diskutiert und festgelegt werden.

Quelle: Eigene Darstellung. Informationen aus Fraunhofer SIT 2017 [35], BMI 2016 [43] und Spiegel Online 2016 [44]

Unternehmen, Bürgerinnen und Bürgern

leisten kann

Die Bundesregierung bekundet in ihrer Cybersicherheitsstrategie die Absicht, **Maßnahmen zur Stärkung deutscher Start-ups** im Bereich Cybersicherheit zu verbessern.

Durch die im Jahr 2018 europaweit in Kraft getretene Datenschutzgrundverordnung (DSGVO) gibt es einen erhöhten Datenschutz für alle Einzelpersonen und sensible Firmendaten. Der daraus entstehende **Verlust an Überwachungsmöglichkeiten von Verdächtigen könnte unter Umständen paradoxerweise dazu führen, dass auch Kriminelle und Terroristen von mehr Cybersicherheit profitieren.**

Anforderungen von Unternehmen

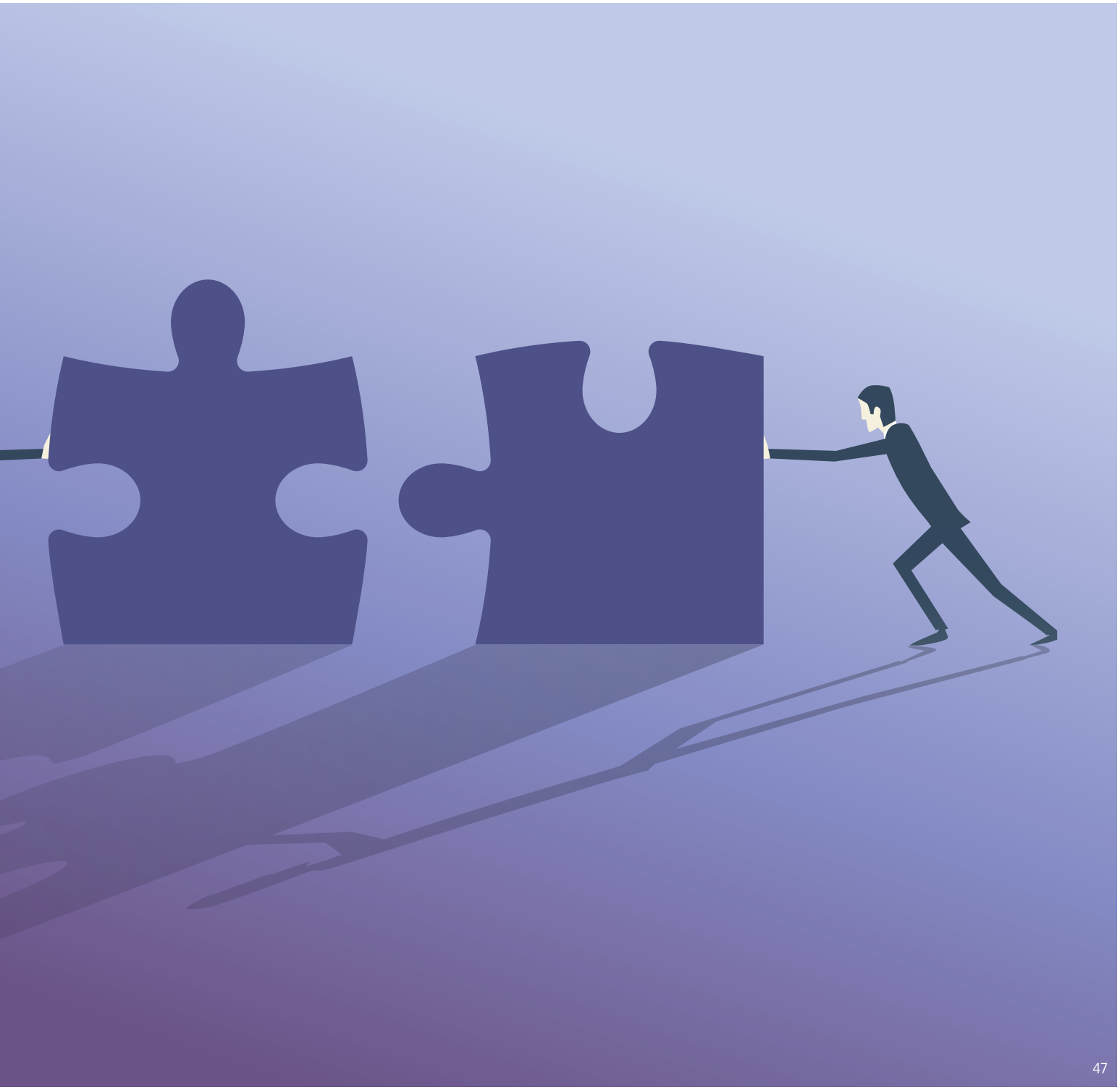
Mehr Wagniskapital für Start-ups im Cyberbereich. Nationale Sicherheitslösungen müssen auf den Weltmarkt kommen, wenn die deutsche Wirtschaft auf der Digitalisierungsstrecke nicht zurückbleiben will. Deutschland hat das Potenzial, eine führende Rolle in der Cyber Security einzunehmen.

Mehr Hilfestellungen zum Umgang mit der DSGVO. Von der DSGVO profitieren derzeit die Großkonzerne, welche mit juristischen Formulierungen die Bedenken der Kunden aus dem Weg räumen. Bei kleinen und mittelständischen Unternehmen führt die DSGVO zu einem Digitalisierungsrückgang.

4

Handlungsfelder und Gestaltungsspielräume

In einem immer komplexer werdenden System ist nicht vorherzusehen, welche Herausforderungen im Bereich Cyber Security entstehen werden. Fest steht: Deutschland agiert primär dezentral; ein stringenter, integrierender Cyber-Security-Strategieprozess fehlt. Wie lassen sich die unterschiedlichen Konzepte, die Handelnden und die Strukturen zusammenbringen, um sich dem Ziel absoluter Cyber Security in Deutschland anzunähern? Im Folgenden werden einige Gestaltungsspielräume aufgezeigt. ►



4.1 Die deutsche Cyberforschung: Mehr Nutzen für die Praxis

In Deutschland mangelt es nicht an guten Forscherinnen und Forschern. In Sachen Kryptographie, Security Engineering (Security by Design) und Quantencomputing-Forschung, um nur einige zu nennen, ist Deutschland sogar unter den Spitzenreitern. Gemessen an der Zahl inländischer Patentanmeldungen zählt die Bundesrepublik im internationalen Vergleich zu den Ländern mit hoher Innovationstätigkeit [45].

Finanzielle und wettbewerbsbasierte Anreize

Auch im Cyber-Security-Bereich fordern die Expertinnen und Experten, anwendungsorientierter zu forschen. Sie warnen vor einem Cyber-Hype und blindem Aktivismus, bei dem staatliches Geld in kurzlebige Projekte fließt. Bedarfsorientiert sind Forschungsthemen auszuwählen, die realen Praxisnutzen schaffen und die IT-Sicherheit verbessern. Brennende, ungelöste Fragen in puncto Cyber Security sind prominenter und attraktiver in der deutschen Forschungslandschaft zu platzieren. Die US-amerikanische Defense Advanced Research Projects Agency (DARPA) verfolgt mit der „Cyber Grand Challenge" [46] einen solchen Ansatz. Die DARPA fördert in diesem Wettbewerb unter Sicherheitskoryphäen die Lösung angewandter Forschungsaufgaben im Bereich Cyber Security und lobte zuletzt für den ersten Preis zwei Millionen Dollar aus. Derartige Anreize könnten auch deutsche Forschende motivieren, praxisorientierter zu arbeiten.

Open Data: BSI als Datentreuhänder

Für die Prävention von Cyberattacken ist es wichtig, der Forschung Schadensfälle im Sinne von „Open Data" zu bieten. Doch während die Zahl der Cyberangriffe steigt, erhält die Forschung diesbezügliche Daten im Regelfall nicht. Eine Ausnahme sind vereinzelte Kooperationen zwischen Großunternehmen und privatfinanzierten Forschungsinstituten (▶ siehe Kapitel 3.2). Diese Erkenntnisse sind für die Ursachenforschung erforderlich. Dementsprechend fordern Wissenschaftlerinnen und Wissenschaftler immer lauter, Daten zu tatsächlichen Cyberangriffen bereitzustellen. Dabei kann nach Meinung der Fachleute das BSI als neutraler „Treuhänder der Daten" fungieren. Zudem sollen die Quellcodes heimischer und internationaler IT-Produkte in einem geschützten, gesicherten Bereich beim BSI hinterlegt sein.* Die freie Einsicht der Forschenden in diese Quellcodes könnte helfen, die Gefahr ungewollter Produktfunktionen, wie Backdoors, zu erkennen und zu verringern. Dies ist nur sinnvoll, sofern sichergestellt werden kann, dass eine Software ausschließlich auf den einsehbaren Quellcodes basiert und diese nicht etwa im Nachhinein verändert wurden.

„Es mangelt in Deutschland nicht an gut gemeinten Ideen, es mangelt an der Stoßkraft."

* Quellcode ist der für den Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes.

Bei der konkreten Ausgestaltung gibt es jedoch, vor allem im Hinblick auf Datenschutz, noch viele ungelöste Fragen, wie das folgende (fiktive) Beispiel illustriert:

Der mittelständischen Chips Productions GmbH aus Fischbach wurden sensible Daten gestohlen. Der Betrieb meldet der zentralen Cyberbehörde, dem BSI, den Schadensfall in der Hoffnung, den Cyberspionagefall so rasch wie möglich aufzuklären. Das BSI soll als Datentreuhänder den Fall mit den gesammelten Informationen für die Forschung freigeben, die den Übergriff in industrienahen Anwendungslaboren unter die Lupe nimmt. In welcher Form können hierbei die Daten aus Sicht der Chips Productions GmbH sinnvoll und sicher anonymisiert werden, ohne ihrem Firmenruf zu schaden und Geschäftsgeheimnisse zu offenbaren? Sind die Daten für die Forschung auch ohne weitere Erklärung durch die (anonyme) Firma verständlich und verwertbar? In welcher Detailtiefe sollen die Daten verfügbar gemacht werden und wo liegen die Grenzen zwischen Transparenz und Datenschutz?

Diese Fragen sind leicht gestellt, aber schwer zu beantworten. Die Lösung erfordert ein Zusammenspiel von Forschung, Unternehmen und BSI. Forschende können beraten und Firmen dabei unterstützen, Cyberangriffe zu minimieren und deren Ursache zu erforschen, um im Schadensfall schnell zu reagieren. Unternehmerinnen und Unternehmer benötigen bei der Freigabe sensibler Daten positive Anreize und gesetzlichen Schutz. Es liegt nun an der Politik, Entscheidungen zu treffen und geeignete Rahmenbedingungen zu schaffen.

„Das BSI vermittelt schon heute Informationen und Erkenntnisse zu Cyberangriffen an seine Zielgruppen in Staat, Wirtschaft und Gesellschaft. So werden etwa technische Informationen aus Meldungen, die das BSI im Rahmen der Meldepflicht von KRITIS-Betreibern erhält, in anonymisierter und sanitarisierter Form an andere Unternehmen gegeben, damit sich diese gegen aktuelle Gefährdungen besser schützen können."

Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik

4.2 Cyber Security als Gesellschaftsprojekt: Sensibilisierung und IT-Bildung

Wer ist nun für Cyber Security zuständig? Der deutsche Staat, die IT-Expertin, der CEO des Unternehmens oder die einzelnen Mitarbeiter und Mitarbeiterinnen? Können wir als Bürgerinnen und Beschäftigte überhaupt etwas zu mehr Cyber Security beitragen?

IT-Ausbildungsberufe und IT-Führerschein für Mitarbeitende

Der Faktor Mensch gilt als größte Gefahrenquelle für die Unternehmenssicherheit. Unzureichend ausgebildete Mitarbeitende sind über alle Branchen und Unternehmensgrößen hinweg das größte Sicherheitsrisiko [47]. Dabei wären beispielsweise sogenannte automatisierte Attacken, bei denen Kriminelle massenhaft bekannte Sicherheitslücken ausnutzen, mit geringem Aufwand abzuwenden. Oft mangelt es an Bewusstsein sowie an einem Grundwissen zur Handhabung von Sicherheitslösungen.

Deutschland hat zwar bereits zahlreiche universitäre Studiengänge zum Thema Cyber- und IT-Sicherheit eingeführt. Eine sinnvolle, wichtige Ergänzung wären Ausbildungsberufe in diesem Bereich, die es derzeit in Deutschland nicht gibt. Hierbei könnten Interessierte in Unternehmen Erfahrung sammeln und ihr Wissen sofort lösungsorientiert anwenden. Ein von der IHK zertifizierter Ausbildungsberuf zum „Cyber Security Professional" ist im Rahmen einer privat-öffentlichen Partnerschaft bereits eingeführt. Angesichts der rasanten Entwicklung der IT-Systeme und möglichen Cyberschwachstellen ist es unabdingbar für Unternehmen, sämtliche Mitarbeitenden und insbesondere IT-Fachkräfte kontinuierlich fortzubilden. Ein IT-Führerschein könnte IT-Fachleute jährlich aufs Neue zertifizieren. Laut einer Umfrage des BSI [8], wird allerdings auch das Personal im Allgemeinen in Bezug auf IT-Sicherheit bei nahezu 50 Prozent der deutschen Unternehmen nicht in regelmäßigen Abständen geschult.

Forscher, die sich mit dem Faktor Mensch in der Cyber Security intensiv befassen, warnen davor, die primäre Verantwortung beim Menschen zu sehen: Selbst wenn sich Endnutzer und -nutzerin an alle Sicherheitsregeln halten, um einen Hacking-Angriff zu vermeiden, benötigen sie die Hilfe der Technik. Mit anderen Worten: Sie können ein Passwort noch so sicher auswählen, wenn E-Mail-Provider die Passwörter nicht geeignet verschlüsselt, können Kriminelle diese Systeme hacken und dadurch alle (nicht gut verschlüsselten) Passwörter einsehen. Auf diese Weise wurden in den vergangenen Jahren bereits Milliarden von Nutzungsdaten erbeutet. Es ist nun dringend an der Zeit, stärker in die Entwicklung und Herstellung sicherer Software- und Hardware-Systeme zu investieren, welche die Menschen technisch schützen, ohne ihnen unmögliche Aufgaben aufzubürden. Solange es diese sichere Technik schlichtweg nicht gibt, müssen die Einzelnen versuchen, sich so gut es geht selbst vor Angriffen zu schützen.

„Genauso wie wir die Grundregeln der Hygiene verstanden haben, müssen die Einzelnen die Verhaltensweisen der digitalen Welt erlernen."

Die Bevölkerung sensibilisieren

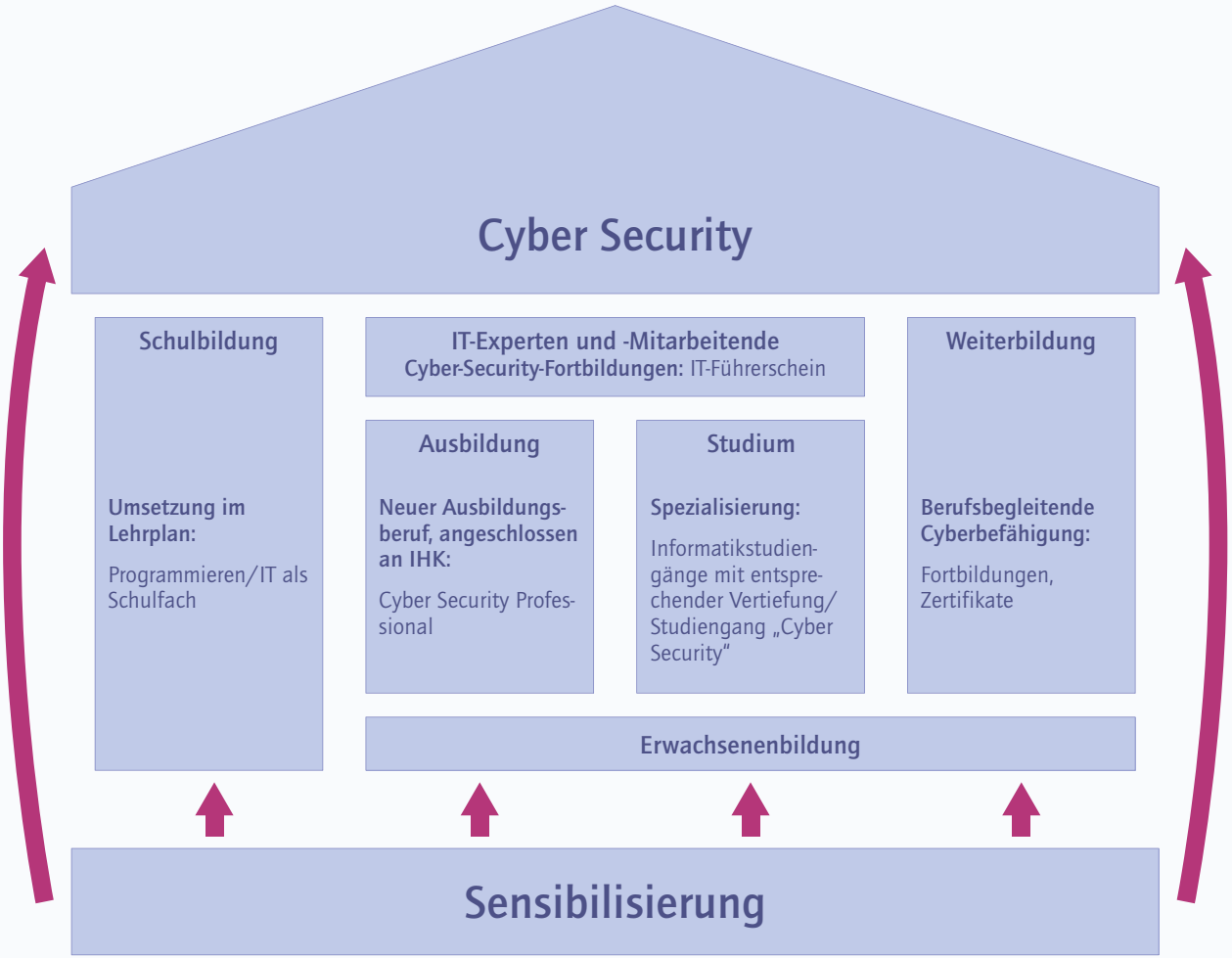
Der Bevölkerung mangelt es nach wie vor an Bewusstsein für Cyber Security: Software-Updates werden oft weggeklickt und nicht zeitnah aufgespielt; Anti-Viren-Programme sind nicht oder nur veraltet installiert. Wie schon im Jahr 2017 waren 2018 in Deutschland „123456" das beliebteste und „12345" das zweitbeliebteste Passwort [48]. Selbst beim Datenschutz, der in Deutschland bei Diskussionen zu Cyber Security an prominenter Stelle steht, gehen viele Nutzerinnen und Nutzer nachlässig mit ihren eigenen Daten um. Services werden genutzt, weil sie kostenlos zur Verfügung stehen. Die weit verbreitete Kostenloskultur im Cyberraum hat Konsequenzen: Der (oft nur im Kleingedruckten) implizierte Preis für die kostenlose Nutzung von E-Mail-Accounts, Chat-Programmen und Sozialen Medien ist oft die Datenverwertung für eigene Zwecke seitens der Anbietenden oder sogar der Verkauf dieser Daten an Drittfirmen. Trotz dieser Tatsache ist die Zahlungsbereitschaft unter den Nutzenden erschreckend gering. Gerade um der allgemeinen Sorglosigkeit in der Cyberwelt entgegenzuwirken, sind Sensibilisierungskampagnen beim Umgang mit Privatdaten, Updates und Passwörtern über alle Alters- und Bevölkerungsschichten hinweg notwendig. Auch hier müsste der Staat für bessere Aufklärung und Ausbildung sorgen.

Kinder und Jugendliche sensibilisieren

Etwa 68 Prozent der Kinder und Jugendlichen können sich ein Leben ohne Internet nicht vorstellen [49]. Dabei fühlen sich immer mehr von ihnen unsicher im Netz. Österreich hat im Schuljahr 2018/2019 flächendeckend mit der Umsetzung der „Digitalen Grundbildung" [50] begonnen. Dabei erwerben Schülerinnen und Schüler Kompetenzen unter anderem in den Bereichen gesellschaftliche Aspekte der Digitalisierung, Informations-, Daten- und Medienkompetenz, Soziale Medien, Sicherheit, technische Problemlösungen und Computational Thinking. Auch für Deutschland wäre es dringend empfehlenswert, digitale Kompetenzen in deutschen Schullehrplänen flächendeckend und verbindlich zu verankern.

„Die größte Schwachstelle ist nicht der Mensch, sondern Systeme, die den Menschen nicht ausreichend unterstützen."

Fortlaufende IT-Bildung und Sensibilisierung



4.3 Wie werden Deutschlands Unternehmen wieder sicherer?

Zwischen 2012 und 2014 hatte jedes zweite deutsche Unternehmen Wirtschaftsspionage oder einen Verdachtsfall zu beklagen [51]. Der in Deutschland geschätzte wirtschaftliche Schaden durch Industriespionage ist laut einer Studie der Münchner Sicherheitsfirma Corporate Trust von 2,8 Milliarden Euro (2007) auf 4,2 Milliarden Euro (2012) [52] bis hin zu 11,8 Milliarden Euro (2014) [51] dramatisch gestiegen. Der Digitalverband Bitkom beziffert in einer Studie den Gesamtschaden, der deutschen Unternehmen aufgrund von Cyberangriffen von 2016 bis 2018 entstanden ist, auf 43,4 Milliarden Euro. Die Zahl der Industrieunternehmen, die in diesem Zeitraum Opfer entsprechender Attacken wurden, hat sich mittlerweile von ursprünglich 50 Prozent (2014) auf knapp 70 Prozent (2018) erhöht [37].

Mit den verfügbaren Methoden und Technologien ließen sich 80 Prozent [53] der heute erfolgreichen Cyberattacken vermeiden. Wo liegt also das Problem und was schlagen Sachverständige vor?

Vor allem kleine und mittlere Unternehmen (KMU) kämpfen mit zwei konkurrierenden Ängsten: Einerseits zögern sie, viel Geld für Sicherheitslösungen auszugeben, deren Effektivität nicht oder nur schwer a priori abzuschätzen ist. Gleichzeitig fürchten sie, nicht ausreichend geschützt zu sein. Vielen von ihnen fehlt es – im Vergleich zu den großen Unternehmen – an Finanzmitteln für einen umfassenden Cyberschutz. Zudem unterliegen viele auch dem Irrglauben, als „Hidden Champions" gar nicht erst ins Visier der Wirtschaftsspionage zu geraten [47]. Doch genau so wird der deutsche Mittelstand als Innovations- und Technologiemotor des Landes [54] zur hochattraktiven Zielscheibe für Cyberangriffe und den Diebstahl geistigen Eigentums.

IT-Grundschutz-Zertifikate und Produkthaftung

Auch IT-Laien und kleinere Firmen müssen über die Möglichkeit verfügen, die Qualität von IT-Produkten und Sicherheitslösungen zu bewerten. Cyber Security ist ein wesentlicher Baustein für jedes Unternehmen. Zwar bietet das BSI seit 2006 sogenannte „IT-Grundschutz-Zertifikate" [55] für IT-Dienstleister an. Ein Sicherheits-Auditing und der Erwerb dieser Zertifikate sind jedoch freiwillig. Eine Ausnahme bilden sensible Bereiche, etwa im Gesundheits- und Energiesektor. Überdies deckt die Zertifizierung bislang nur ein kleines Produktspektrum [43] ab. Einige Fachleute gehen daher einen Schritt weiter und fordern eine deutschlandweit zentralgesteuerte, verpflichtende Zertifizierung durch herstellerunabhängige BSI-Audits für alle in Deutschland angebotenen IT-Produkte und -dienstleistungen.

Eine besondere Herausforderung ist die Schnelllebigkeit von IT-Produkten, die innerhalb von Monaten durch neue Produkte, Versionen und Updates ersetzt werden. Dies wirft die brisante Frage auf, wie überhaupt praktikable Sicherheitsstandards für

„Eine Prüfung auf Cyber Security findet in den geringsten Fällen statt. Das Bundesamt für Sicherheit in der Informationstechnik bietet Überprüfungen an. Diese sind aber nicht verpflichtend."

Produktzertifizierungen festgelegt werden können, die über einen längeren Zeitraum gültig bleiben. Allein bei der schieren Menge neuer Produkte würde das BSI womöglich an die Grenzen seiner Kapazitäten stoßen. In diesem Fall würden staatliche Regulierungen den Unternehmen Innovationskraft und Agilität rauben und dabei paradoxerweise mehr Schaden als Nutzen anrichten.

Andere Expertinnen und Experten fordern die Einführung von Produkthaftungsregeln im Kontext der Cyber Security, die es derzeit in Deutschland nicht gibt. Dies würde für Unternehmen Anreize setzen, die Sicherheit ihrer Produkte und Dienstleistungen von Anfang an mitzudenken (Security by Design). Ein Problem dabei ist, dass die meisten IT-Produkte nicht aus Deutschland kommen. Wie und ob internationale Firmen in die Pflicht genommen werden können, für die Sicherheit all ihrer Produkte zu haften, müsste noch geklärt werden.

„Deutschland muss als Wirtschafts- und Innovationsstandort Vorreiter einer Digitalisierung sein, die notwendige Absicherungen von vornherein einbezieht: Informationssicherheit ist das neue Made in Germany in der Digitalisierung. Dies in Staat, Wirtschaft und Gesellschaft zu gestalten, ist Aufgabe der nationalen Cybersicherheitsbehörde Deutschlands, des Bundesamts für Sicherheit in der Informationstechnik."

Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik

„Zertifizierung ist gut. Wichtiger ist die Produkthaftung."

„It takes two to Tango" – Hard- und Software im Zusammenspiel

Hard- und Software müssen zusammenwirken, um die Sicherheit eines Endgerätes zu gewährleisten. Deutschland ist bei der Herstellung von nischenspezifischen Hardwarekomponenten gut aufgestellt. So stammen 35 Prozent der weltweit verkauften Sicherheitschips, die auf SIM-Karten, Personalausweisen oder Kreditkarten zu finden sind, aus deutscher Produktion. Massiver Nachholbedarf besteht allerdings bei entsprechenden Software-Lösungen; hier werden nahezu alle Anwendungen aus dem Ausland bezogen. Selbst wenn ein Gerät mit einem vertrauenswürdigen Sicherheitschip ausgestattet ist, könnten sich in den weiteren Hard- und Software-Komponenten dieses Gerätes Backdoors oder andere Sicherheitslücken befinden, über die ein Hacker in das Gerät eindringen kann.

Cyber Maturity Index als Selbstcheck für Unternehmen

In einem zweiten Schritt könnten Unternehmen entlang eines Cyber Maturity Index prüfen, auf welchem Sicherheitsstandard sie sich befinden. Hierbei könnten BSI-Auditoren Unternehmen in unterschiedliche Sicherheitsstufen einordnen. Unternehmerinnen und Unternehmer hätten so Anhaltspunkte, ihre eigene Cyber Security zu bewerten und gleichzeitig das Vertrauen ihrer Kundschaft zu erhöhen.

Cyber Security Made in Germany

In Deutschland gibt es nur wenige Unternehmen, die im Bereich Cyber Security international erfolgreich sind. Unter den weltweit Top-500-Cyber-Security-Firmen sind nach einer Studie von Cybersecurity Ventures [24] allein 42 israelische Unternehmen, davon acht unter den Top 100. Deutschland weist lediglich sechs Cyberunternehmen in den Top 500 auf, von denen es kein einziges auf einen Platz unter den Top 100 schafft (▶ siehe auch Kapitel 3.1).

Die Hardware liefern derzeit einige wenige Firmen aus den USA und China. Qualität und Sicherheit dieser IT-Produkte beeinflussen die gesamte deutsche Wirtschaftskraft. Es ist daher notwendig, dass sich Deutschland bei der Entwicklung neuer Technologien und nationalen Sicherheitslösungen engagiert. Die Experten und Expertinnen bemängeln hier einen fehlenden Gründungsgeist: Vertreterinnen und Vertreter der deutschen Industrie ließen oft eine skeptische bis ablehnende Haltung gegenüber Neuem erkennen.

„Eine [allgemeine] Verpflichtung zu einer Zertifizierung würde die individuelle Entwicklung von Vorgaben erfordern, die auf die Bedürfnisse der jeweiligen Anwendungsbereiche zugeschnitten sind. Zudem bedarf sie der Entscheidung und Mitwirkung derjenigen, die für diesen Bereich jeweils die Verantwortung für die dort entstehenden IT-Sicherheitsrisiken tragen. Eine allgemeine Verpflichtung zur Zertifizierung für IT-Produkte wäre aus heutiger Sicht daher unverhältnismäßig."

Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik

In diesem Bewusstsein kündigte die Bundesregierung in ihrer Cyber-Security-Strategie 2016 Bestrebungen an, die Gründungskultur und Wettbewerbsfähigkeit deutscher IT- und Cyber-Security-Firmen zu verbessern [43]. Analog zur erfolgreichen Entwicklung von High-Tech-Produkten und der damit einhergehenden hohen Anerkennung deutscher Qualität „Made in Germany", hätte auch „Cyber Security Made in Germany" [57] das Potenzial, heimische Sicherheitslösungen zu entwickeln und diese erfolgreich auf dem Weltmarkt zu platzieren.

Im Dezember 2018 wurde der Cybersecurity-Act beschlossen. EU-flächendeckende, einheitliche Cyber-Security-Zertifizierungen sollen Onlinedienste und digitale Geräte für Europas Verbraucherinnen und Verbraucher sicherer machen. Über drei Sicherheitsstufen (niedrig, mittel oder hoch) sollen nun Verbraucher das Risiko für Cyberattacken von IT-Produkten und Dienstleistungen besser einschätzen können. Bis zum Jahr 2023 will die EU-Kommission entscheiden, ob die zunächst freiwillige Zertifizierung Pflicht wird [56].

„Auf dem Papier ist die deutsche Cyber-Security-Strategie gar nicht schlecht, jedoch fehlt das Handeln: Der Staat muss hier in Schlüsseltechnologien investieren und auch als Anwender eine Vorbildrolle einnehmen."

4.4 Gesetzgebung und Regulierung: Die Rolle des Staates in der Cyber Security

Freiheit und Sicherheit zu gewährleisten, ist eine Kernaufgabe des Staates. Dies gilt auch im Cyberraum, so lautet die deutsche Cyber-Security-Strategie [43]. Der Erlass sinnvoller, umsetzbarer Cybergesetze zum Schutz von Wirtschaft, Bürgerinnen, Bürgern und Kritischen Infrastrukturen bleibt dabei eine Herausforderung.

IT-Sicherheitsgesetz 2.0 ist auf dem Weg

Mit der im Mai 2018 in Kraft getretenen EU-Datenschutzgrundverordnung (DSGVO) stehen sämtliche Unternehmen in der Pflicht, eine Verletzung des Schutzes personenbezogener Daten innerhalb von 24 Stunden bei der zuständigen Aufsichtsbehörde zu melden. Diese Meldepflicht gilt für jeden Cybervorfall über alle Branchen hinweg. Sie tritt jedoch nur in Kraft, sofern ein Risiko für die Rechte und Freiheiten von Personen vorliegt [58]. Besteht in dieser Hinsicht kein Risikoverdacht, stehen Unternehmen in Europa und Deutschland generell zunächst nicht in der Pflicht, Cybervorfälle zu melden.

Eine Ausnahme sind Kritische Infrastrukturen, die besonders zu schützen sind und deshalb jeden Vorfall melden müssen. Dies legte der deutsche Staat im „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz) fest [59]. KRITIS-Unternehmen umfassen die Sektoren Staat und Verwaltung, Energie, Gesundheit, IT/Telekommunikation, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen sowie Ernährung [7]. Nach dem IT-Sicherheitsgesetz müssen sie

- eine mit Informationssicherheit beauftragte Person benennen, die dem BSI als Kontakt zur Verfügung steht.
- ein Informationssicherheitsmanagement betreiben, um Cyberangriffe zu identifizieren.
- eine Meldestelle einrichten, die das BSI über Cyberangriffe informiert.

Dabei ist zu beachten: Das Gesetz ist in seiner jetzigen Form als Mindeststandard zu verstehen. Die gestellten Minimalanforderungen sind ausschließlich für KRITIS-Unternehmen bindend. Unternehmen, die nicht unter diese Kategorien fallen, unterliegen keinerlei Pflicht, sich an diese Mindeststandards zu halten. Im Jahr 2016 erfüllte nicht einmal die Hälfte der KRITIS-relevanten Unternehmen die Anforderungen des Gesetzes [47].

Im Zuge des IT-Sicherheitsgesetzes 2.0 wird derzeit zwar diskutiert, den Bereich Kritischer Infrastrukturen zu erweitern. Von einem für die Gesamtwirtschaft verbindlichen IT-Gesetz ist jedoch nicht die Rede. Zu diskutieren ist auch die Frage, inwieweit sich im Rahmen des IT-Sicherheitsgesetzes 2.0 die Befugnisse des BSI nochmals erweitern lassen [60].

Die eindringliche Forderung der Experten lautet: Das BSI sollte als einzige zentrale Kontrollinstanz sicherstellen, dass alle Unternehmen die gesetzlichen Bestimmungen unbedingt einhalten. Allerdings dürfen deutschen Unternehmen daraus keine Wettbewerbsnachteile entstehen, wenn diese – etwa im Vergleich zur asiatischen Konkurrenz – bei Nichteinhalten der Sicherheitsstandards mit Sanktionszahlungen bestraft werden. Hier ist auf einen gesunden Mittelweg zwischen Sicherheit und Wettbewerbsfähigkeit der deutschen Wirtschaft zu achten.

4.5 Ohne Regelkreis keine digitale Souveränität

In Deutschland gibt es in der Cyber Security viele unterschiedliche Akteure, die nur bedingt orchestriert und strategiegeleitet miteinander kooperieren: Ungeprüfte, im Ausland hergestellte, nicht zertifizierte IT-Produkte kommen auf den deutschen Markt. Kostbare Datenmengen über Schadensfälle bleiben für die Ursachenforschung geheim. Anreize für Forschende, ihre Ergebnisse in vermarktbare Produkte zu transferieren, fehlen. Die Verwaltung ist dezentral; immer wieder entstehen neue Behörden, Initiativen und Allianzen. Bund und Länder sind nicht verpflichtet, sich verbindlich über Cyberangriffe auszutauschen. Manchem Politiker und mancher Politikerin fehlt diesbezüglich das Bewusstsein. Viele KMUs sind zu wenig sensibilisiert; die Bevölkerung schätzt die Kostenloskultur. Solange die einzelnen Cyber-Security-Akteure parallel zueinander arbeiten, bleibt das Leitbild der digitalen Souveränität naiv.

Die Lösung liegt im strategischen Aufbau eines Regelkreises, bei dem die Beteiligten kooperieren und einen geschlossenen Kreis bilden, der gegenüber äußeren Einflüssen stabil bleibt. Ein erster Schritt wäre ein funktionierender Wissenstransfer von Schadensfällen und neuen Erkenntnissen zwischen Behörden, Forschung und Privatwirtschaft im Sinne von „Open Data“. Dabei ist zu vermeiden, dass vereinzelte (neu hinzukommende) Bündnisse zu einer noch stärkeren Dezentralisierung führen (▶ siehe Kapitel 3.3). Einstimmig fordern daher die Fachgrößen eine klare Rolle des BSI als die zentrale, unabhängige, politisch neutrale Behörde für Cyber Security (▶ siehe Kapitel 4.4). Als solche muss sie die lokalen Zuständigkeiten bündeln und die Herausforderung bewältigen, Firmen, Forschungseinrichtungen und Hochschulen mit ins Boot zu holen.

Es mag als Mammutaufgabe erscheinen, den Regelkreis von sensiblen Informations- und Datenflüssen zwischen vielen unterschiedlichen Einrichtungen zu schließen. Jedoch kann es auch nicht Deutschlands Anspruch sein, zum Weltmeister von Cyberbündnissen und -strategien auf dem Papier zu werden. Vielmehr muss es das Ziel deutscher Politik sein, eine Spitzenposition von Schlüsseltechnologien zu erreichen und auszubauen und diese Technologien samt ihrer Unternehmen, Kritischen Infrastrukturen und Personen zu schützen.

„Deutschland ist generell auf einem guten Weg: Wir haben viel Expertise zum Thema IT-Sicherheit im Land. Jedoch fehlen Verpflichtungen und Cyber-Security-Richtlinien für die Industrie.“

Glossar

Viele Cyberangriffe basieren auf bekannten, äußerst effektiven Hacking-Strategien. Die folgende Übersicht stellt einige der populärsten Angriffstypen vor:

1. Malware

Malware ist ein Sammelbegriff für schädliche Computerprogramme wie Viren, Trojaner, Würmer und Ransomware. Meist dringt Malware über das Herunterladen eines E-Mail-Anhangs in einen Computer oder ein System ein. Eine weitere Möglichkeit ist das Herunterladen von Daten oder Programmen aus einer nicht bekannten oder nicht vertrauenswürdigen Quelle. Auch beim Browsen im Web können schädliche Programme eindringen – vor allem durch aktive Inhalte einer Webseite, die mit einem Plug-in wie Flash oder Java abgespielt werden.

Ist ein Computer von einer Malware infiziert worden, kann diese unbemerkt im Hintergrund Dateien löschen, sensitive Daten sammeln und verschicken, Sicherheitssoftwares wie Firewalls und Antivirenprogramme deaktivieren und weitere schädliche Programme installieren. Dadurch kann der Computer so geschädigt werden, dass er nicht mehr funktionsfähig ist.

Bei der sogenannten Ransomware werden Daten auf dem befallenen Rechnersystem unzugänglich gemacht, meist durch Verschlüsselung. Das Opfer wird dann erpresst: Nach Zahlung eines Lösegeldes wird ihm ein Schlüssel zur Wiedernutzbarmachung seiner Daten in Aussicht gestellt. Die Zahlung des Lösegeldes führt allerdings nicht zwangsläufig zur Rettung der Daten, weshalb davon grundsätzlich abzuraten ist.

Bevor Anwenderinnen und Anwender ein Programm oder einen E-Mail-Anhang herunterladen, sollten sie sich jedes Mal vergewissern, ob die Quelle wirklich vertrauenswürdig ist. Der Browser sollte immer auf dem aktuellsten Stand gehalten werden. Aktive Inhalte sind abzuschalten, sodass sie nicht automatisch abgespielt werden. Regelmäßige Backups stellen sicher, dass keine wichtigen Daten verloren gehen.

2. Phishing und Spear-Phishing

Bei einer Phishing-Attacke gibt sich ein Angreifer als vertrauenswürdiger Kontakt aus, um an sensitive Informationen wie Kreditkartendaten oder Passwörter zu gelangen oder um eine Malware auf dem Computer des Opfers zu installieren. Meist geschieht dies durch eine E-Mail, in welcher der Empfänger aufgefordert wird, einen bestimmten Link anzuklicken oder einen Anhang zu öffnen. Diese E-Mail erscheint täuschend echt und enthält häufig offizielle Logos und Designs von Organisationen, um sich als diese auszugeben.

Wird der Anhang der Phishing-E-Mail geöffnet, installiert sich die Malware automatisch auf dem Computer. Wird der Link angeklickt, wird das Opfer meist auf eine betrügerische Webseite weitergeleitet. Diese gibt sich zum Beispiel als eine offizielle Login-Website eines Social-Media-Dienstes aus und fordert die Userinnen und User dazu auf, ihre Benutzerdaten einzugeben, wodurch die Hacker ihre E-Mail-Adressen und Passwörter erbeuten.

Während normale Phishing-Attacken darauf abzielen, möglichst viele Nutzende in die Falle tappen zu lassen und deshalb nicht personalisiert sind, lassen Hacker beim Spear-Phishing möglichst viele persönliche Informationen einfließen, damit die E-Mail dem Opfer so legitim wie möglich erscheint.

Vor dem Öffnen von Anhängen ist deshalb immer sicherzustellen, dass der Absender wirklich eine offizielle E-Mail-Adresse verwendet hat. Links in einer E-Mail sollten nie angeklickt werden, sondern die offizielle Webseite sollte separat im Browser aufgerufen werden.

3. SQL Injection

Mit der Programmiersprache SQL (Structured Query Language) lassen sich Informationen in Datenbanken verwalten. Viele Webseiten verwenden Datenbanken, um wichtige Informationen wie Kreditkartendaten von Kunden zu speichern. Bei einer SQL-Injection-Attacke wird eine Sicherheitslücke in der Datenbank genutzt, um Zugriff auf diese zu bekommen und dadurch Daten auszuspähen, zu verändern oder die Kontrolle über den Server zu erhalten.

Kommandos in der Programmiersprache SQL lassen sich über Elemente einer Webseite einschleusen, die Nutzereingaben vorsehen, wie zum Beispiel ein Such- oder Eingabefeld für Bezahlinformationen. Ist eine Webseite nicht dagegen geschützt, bestimmte Sonderzeichen in SQL, wie Anführungszeichen oder Semikolons, die normalerweise für die Eingabe von Programmiercodes notwendig sind, zu erkennen und auf sichere Art zu behandeln, können bestimmte eingegebene Kommandos auch dazu benutzt werden, Dateien in der Datenbank abzulegen und dadurch einen beliebigen Code auf dem System auszuführen.

4. Cross-Site-Scripting (XSS)

Während sich bei einer SQL-Injection-Attacke ein Hacker Zugriff auf private Daten verschafft, indem er die Datenbank einer Website angreift, ist bei einer Cross-Site-Scripting-Attacke (XSS) der Nutzer selbst das Angriffsziel: Der Hacker schleust einen schädlichen Code über eine Schwachstelle in eine vermeintlich vertrauenswürdige Webseite ein. Meist basiert dieser Code auf der Programmiersprache JavaScript. Damit lassen sich Webseiten dynamischer gestalten, zum Beispiel mit einem aufpoppenden Willkommensgruß, einer Aufforderung zum Newsletter-Abo oder Werbebannern. Der eingefügte schädliche Code wird im Browser der Nutzenden ausgeführt, wenn sie die Webseite besuchen, ohne dass diese etwas bemerken.

Hacker können nutzende Personen dadurch auf mehreren Wegen in die Falle locken. Beispiele sind ein Kommentar auf einem Blog oder ein Forenbeitrag, in dem der Hacker eine schädliche Webseite verlinkt hat. In einer anspruchsvolleren Variante kann sich ein Hacker Zugriff auf die Datenbank einer Webseite verschaffen und seinen schädlichen Code dort einschleusen. Klicken Anwenderin oder Anwender auf diese Webseite, kann der schädliche Code übertragen und vom Browser heruntergeladen werden. Dadurch kann der Hacker die Personen zum Beispiel unbemerkt auf eine nicht-offizielle Webseite weiterleiten, die der Original-Webseite täuschend ähnlich ist. Geben die Betroffenen nun Daten wie Passwörter oder Kreditkartennummer ein, kann der Hacker diese abfangen. Wer sich gegen Cross-Site-Scripting schützen möchte, sollte die JavaScript-Unterstützung im Browser ausschalten.

5. Man-in-the-Middle (MitM)

Bei der Man-in-the-Middle-Technik versuchen Angreifer, sich heimlich zwischen dem Opfer und einer aufgerufenen Webseite zu platzieren. Der Hacker kann dann unentdeckt die gesendeten Nachrichten abhören oder sich als eine der beiden Parteien ausgeben. Dies ist besonders gefährlich auf vertraulichen Seiten wie Online-Banking-Portalen.

Meist nutzen Hacker für eine Man-in-the-Middle-Attacke öffentliche WLAN-Router. Zum einen können sie Sicherheitslücken in einem bestehenden Router nutzen, um den Zugriff der Anwender und Anwenderinnen zu kontrollieren und deren Informationen abzufangen. Zum anderen richten Hacker auch schädliche Router ein, die sich als legitim ausgeben. So können Hacker ihr Laptop oder Handy als WLAN-Hotspot konfigurieren und ihm einen Namen geben, der in öffentlichen Bereichen wie Flughäfen oder Cafés häufig verwendet wird. Verbinden sich nun Personen mit dem schädlichen Hotspot und verwenden ihn, um Online-Shops aufzurufen, kann der Hacker die Login-Daten stehlen.

Wer sich selbst vor Man-in-the-Middle-Attacken schützen will, sollte nie eine Verbindung zu offenen WLAN-Routern aufbauen. Falls sich dies nicht vermeiden lässt, helfen Browser-Plug-ins, eine sicherere HTTPS-Verbindung aufzubauen. Allerdings gewährleisten sie keinen hundertprozentigen Schutz.

6. Remote Exploit/Remote Attack

Der Fachbegriff Remote bezeichnet in der IT einen entfernten Zugriff auf Server, Geräte oder Computer. Ein Exploit (deutsch: auszunutzen, ausbeuten) nutzt Schwachstellen, die bei der Entwicklung eines Programms entstanden sind, um in Computersysteme einzudringen oder diese zu beeinträchtigen. Remote Exploits sind eine aktive Form des Angriffs aus der Ferne auf Schwachstellen in der Netzwerksoftware mittels manipulierter Datenpakete oder spezieller Datenströme.

Solche Remote Exploits, auch Remote Attacks genannt, sorgen zunehmend für Aufruhr, vor allem im Zusammenhang mit selbstfahrenden Fahrzeugen. So war es der Sicherheitsforschung möglich, sich über Funktechnik (wie Mobilfunk oder Bluetooth) Kontrolle zu einem Fahrzeug zu verschaffen und es fremdzusteuern. Oft ist das Einfalltor für Hacker dabei eine Sicherheitslücke im Infotainmentsystem des Fahrzeugs.

7. Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)

Bei einer Denial-of-Service-Attacke (DoS) werden Systeme, Server oder Netzwerke mit einem unerwartet hohen Aufkommen an Anfragen überlastet, sodass der normale Dienst für den User nicht mehr oder nur stark eingeschränkt funktioniert. DoS-Attacken gehen meist von einem einzelnen infizierten Computer aus. Nutzen Hacker dagegen eine große Anzahl infizierter Computer, um ihren DoS-Angriff durchzuführen, spricht man von einem Distributed-Denial-of-Service-Angriff (DDoS). Eine Grundvoraussetzung hierfür ist die Installation von Malware auf fremden Rechnern, sogenannter Botnetz-Agenten, die sich ohne Wissen des Computerbesitzers aus der Ferne steuern lassen und gleichzeitig weitere Computer infizieren, um das Botnetz zu erweitern. Botnetze können aus Hunderttausenden infizierten Computern bestehen, die auf allen Kontinenten verteilt sind. Da die Angriffe von verschiedenen Rechnern stammen, ist es nicht möglich, die Attacken durch Sperren der IP-Adressen zu beenden.

Neben Computern verwenden Angreifer zunehmend auch IoT-Geräte als Botnetze, um DDos-Angriffe durchzuführen, wie etwa Smart-TVs, Garagentoröffner und Überwachungskameras bis hin zu Industriewerkzeugen, Maschinen oder Fahrzeugen. IoT-Geräte sind generell schlecht geschützt; der Markt wächst jedoch rasant. Dadurch ergibt sich eine immense Vergrößerung der Angriffsfläche, was wiederum DDoS-Angriffe begünstigt.

Interviewpartnerinnen und Interviewpartner

In Ergänzung zur Arbeit der Projektgruppe und zur Auswertung von Fachliteratur und anderen Studien haben die Mitarbeitenden der acatech Geschäftsstelle für diese Publikation telefonisch oder persönlich Experteninterviews mit 18 Vertreterinnen und Vertretern aus Wissenschaft, Wirtschaft, Politik und Gesellschaft geführt. Die Gespräche fanden zwischen August 2018 und Januar 2019 statt. Die genannten Funktionen der Interviewpartnerinnen und -partner beziehen sich auf den Gesprächszeitpunkt. Einige ausgewählte Kerngedanken der Befragten sind im Text als anonymisierte Zitate aufgeführt.

Das acatech Präsidium dankt allen Beteiligten sehr herzlich für ihre Teilnahme an den Interviews:

- Markus Beckedahl, Netzpolitik, Gründer und Chefredakteur
- Paul Duplys, Robert Bosch, Leiter Competence Segment Safety, Security & Privacy (Corporate Research)
- Prof. Dr. Claudia Eckert, Technische Universität München, Leiterin Lehrstuhl Sicherheit in der Informatik/Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC), Leiterin
- Alexander von Gernler, genua GmbH, Leiter Research/ Gesellschaft für Informatik e.V., Vizepräsident
- André Grochowy, Munich Re, Senior Cyber Underwriter, Corporate Underwriting
- Reik Hesselbarth, Rohde & Schwarz Cybersecurity, Geschäftsführer
- Detlef Houdeau, Infineon Technologies AG, Senior Direktor
- Jan-Peter Kleinhans, Stiftung Neue Verantwortung, Projektleiter IT-Sicherheit im Internet der Dinge
- Prof. Dr. Christoph Meinel, Hasso-Plattner-Institut, Institutsdirektor und CEO/Digital Engineering Fakultät – Universität Potsdam, Dekan
- Stephan Micklitz, Google Germany, Direktor Engineering
- Prof. Dr. Jörn Müller-Quade, Karlsruher Institut für Technologie, Leiter der Forschungsgruppe Kryptographie und Sicherheit
- Arne Schönbohm, Bundesamt für Sicherheit in der Informationstechnik (BSI), Präsident
- Dr. Haya Shulman, Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Abteilungsleiterin Cybersecurity Analytics and Defences
- Prof. Dr. Matthew Smith, Rheinische Friedrich-Wilhelms-Universität Bonn/ Fraunhofer FKIE/Code-Intelligence GmbH, Professor
- Christian Stüble, Rohde & Schwarz Cybersecurity, Chief Technical Officer
- Thomas Tschersich, T-Systems International GmbH, Deutsche Telekom AG, Senior Vice President Internal Security & Cyber Defense
- Prof. Dr. Michael Waidner, Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Leiter/Technische Universität Darmstadt
- Eva Weiß-Margis, T-Systems International GmbH, Telekom Security, Internal Security & Cyber Defense, Vice President Security Officer

Literaturverzeichnis

[1] Morgan, S. (2017): Cybercrime Damages $6 Trillion By 2021. In: Cybersecurity Ventures. Online verfügbar unter https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, zuletzt geprüft am 22.02.2019.

[2] Deutsche Welle (2018): EU-Kommission warnt vor Cyberattacken vor Europawahl. Online verfügbar unter https://www.dw.com/de/eu-kommission-warnt-vor-cyberattacken-vor-europawahl/a-44903543, zuletzt geprüft am 22.02.2019.

[3] Goel, V.; Perlroth, N. (2016): Yahoo Says 1 Billion User Accounts Were Hacked. In: The New York Times. Online verfügbar unter https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html, zuletzt geprüft am 22.02.2019.

[4] Briegleb, V. (2014): 145 Millionen Kunden von eBay-Hack betroffen. In: Heise Security. Online verfügbar unter https://www.heise.de/security/meldung/145-Millionen-Kunden-von-eBay-Hack-betroffen-2195974.html, zuletzt geprüft am 22.02.2019.

[5] Goel, V.; Perlroth, N. (2016): Hacked Yahoo Data Is for Sale on Dark Web. Online verfügbar unter https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html, zuletzt geprüft am 22.02.2019.

[6] VICE News (2018): This Is How Easy It Is To Get Hacked. Online verfügbar unter https://www.youtube.com/watch?v=G2_5r-PbUDNA, zuletzt geprüft am 22.02.2019.

[7] UP KRITIS: Die Sektoren Kritischer Infrastrukturen in Deutschland. Online verfügbar unter https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/UPK.html, zuletzt geprüft am 22.02.2019.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2018): Die Lage der IT-Sicherheit in Deutschland 2018. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=-publicationFile&v=5, zuletzt geprüft am 22.02.2019.

[9] Steiner, H.; Günther, O. (2018): Kliniken im Visier von Hackern. Online verfügbar unter https://www.tagesschau.de/wirtschaft/kliniken-hacker-101.html, zuletzt geprüft am 22.02.2019.

[10] Liedtke, D. (2017): Diagnose Hackerangriff: Wie Cyberattacken deutsche Kliniken lahmlegen. In: Stern. Online verfügbar unter https://www.stern.de/gesundheit/krankenhaus/hackerangriff–wie-cyberattacken-deutsche-kliniken-lahmlegen-7762362.html, zuletzt geprüft am 22.02.2019.

[11] Süddeutsche Zeitung (2016): Computervirus legt Klinik in Neuss lahm. Online verfügbar unter https://www.sueddeutsche.de/digital/hackerangriff-computervirus-legt-klinik-in-neuss-lahm-1.2861656, zuletzt geprüft am 22.02.2019.

[12] SANS Security Awareness (2016): Anatomy of an ICS Network Attack – Security Awareness Video. Online verfügbar unter https://www.youtube.com/watch?v=_eNB1gq5gbA, zuletzt geprüft am 22.02.2019.

[13] KPMG (2015): Hacker nehmen Industrie 4.0 ins Visier. Online verfügbar unter https://home.kpmg/de/de/home/themen/2015/01/hacker-nehmen-industrie-4-0-ins-visier.html, zuletzt geprüft am 22.02.2019.

[14] Lüthe, C. (2018): Bis 2030 werden mehr als 50 % aller Haushalte smart sein. In: Bundeszentrale für politische Bildung. Online verfügbar unter http://www.bpb.de/lernen/digitale-bildung/medienpaedagogik/268079/bis-2030-werden-mehr-als-50-aller-haushalte-smart-sein, zuletzt geprüft am 22.02.2019.

[15] Gehm, F. (2018): So leicht dringen Hacker in Ihr Smart Home ein. In: Welt. Online verfügbar unter https://www.welt.de/wirtschaft/article181408256/So-leicht-dringen-Hacker-in-ihr-Smart-Home-ein.html, zuletzt geprüft am 22.02.2019.

[16] Bleich, H. (2018): Amazon gibt intime Alexa-Sprachdateien preis. In: heise online. Online verfügbar unter https://www.heise.de/newsticker/meldung/Amazon-gibt-intime-Sprachdateien-preis-4254716.html, zuletzt geprüft am 22.02.2019.

[17] Gotzner, P. (2013): Ihre Toilette wurde geknackt. In: Spiegel Online. Online verfügbar unter http://www.spiegel.de/netzwelt/gadgets/smart-home-sicherheitsluecke-bei-fernsteuerbaren-toiletten-aufgedeckt-a-914988.html, zuletzt geprüft am 22.02.2019.

[18] Decker, H. (2017): Ist ein Hackerangriff auf ein Auto möglich? In: Frankfurter Allgemeine Zeitung. Online verfügbar unter https://www.faz.net/aktuell/wirtschaft/netzwirtschaft/wikileaks-enthuellungen-ist-ein-hackerangriff-auf-ein-auto-moeglich-14916347.html, zuletzt geprüft am 22.02.2019.

[19] Handelsblatt (2017): Autos werden zum Ziel von Hackern. Online verfügbar unter https://www.handelsblatt.com/unternehmen/dienstleister/cyberangriffe-autos-werden-zum-ziel-von-hackern/20470674.html, zuletzt geprüft am 22.02.2019.

[20] Harder, S. (2014): Hacker-Angriff aufs Auto. Bremsenversagen via Bluetooth. In: Spiegel Online. Online verfügbar unter http://www.spiegel.de/auto/aktuell/hacker-koennen-autos-ueber-funkverbindungen-aus-der-ferne-angreifen-a-985464.html, zuletzt geprüft am 22.02.2019.

[21] Röttger, T. (2018): Faktencheck. In: Correctiv. Online verfügbar unter https://correctiv.org/faktencheck/2018/02/08/nein-der-staat-bezahlt-keine-7500-euro-fuer-einen-harem, zuletzt geprüft am 22.02.2019.

[22] Dose, J. (2019): Fakten und Bewertungen zum Hackerangriff auf Politiker. In: ComputerWoche. Online verfügbar unter https://www.computerwoche.de/a/fakten-und-bewertungen-zum-hackerangriff-auf-politiker,3546365, zuletzt geprüft am 22.02.2019.

[23] Bundeszentrale für politische Bildung (2017): Was sind Social Bots? Online verfügbar unter https://www.bpb.de/252585/was-sind-social-bots, zuletzt geprüft am 22.02.2019.

[24] Cybersecurity Ventures (2018): Cybersecurity 500 List, 2018 Edition. Online verfügbar unter https://cybersecurityventures.com/cybersecurity-500/, zuletzt geprüft am 22.02.2019.

[25] Statista (2018): Einwohnerzahl in EU und Euro-Zone 2018. Online verfügbar unter https://de.statista.com/statistik/daten/studie/14035/umfrage/europaeische-union-bevoelkerung-einwohner/, zuletzt geprüft am 22.02.2019.

[26] TeleTrusT, Bundesverband IT- Sicherheit e.V.: TeleTrusT-Anbieterverzeichnis IT-Sicherheit. Online verfügbar unter https://www.teletrust.de/anbieterverzeichnis/Liste/, zuletzt geprüft am 22.02.2019.

[27] Grumbach, M. (2018): Der geheime Boom bei deutschen IT-Sicherheits-Startups. In: Gründerszene. Online verfügbar unter https://www.gruenderszene.de/technologie/boom-it-security-startups, zuletzt geprüft am 22.02.2019.

[28] Builders in Tech: SecureTech Startups GSA. Online verfügbar unter https://buildersintech.com/de_DE/market-insights/it-security/it-security-startups-gsa/, zuletzt geprüft am 22.02.2019.

[29] Kollmann, T.; Hensellek, S.; Jung, P.; Kleine-Stegemann, L. (2018): Deutscher Start-Up Monitor 2018. In: Bundesverband Deutsche Startups e.V. Online verfügbar unter https://deutscherstartupmonitor.de/fileadmin/dsm/dsm-18/files/Deutscher%20Startup%20Monitor%202018.pdf, zuletzt geprüft am 22.02.2019.

[30] Start-Up Nation Central (2017): Start-up National Central Cybersecurity Brief. Israel: a Global Center for Cyber Security. Online verfügbar unter https://www.startupnationcentral.org/sector/cybersecurity/, zuletzt geprüft am 22.02.2019.

[31] Bundesministerium für Bildung und Forschung (BMBF): StartUp-Secure – Die Initiative für Start-ups in der IT-Sicherheit. Online verfügbar unter https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/startup-secure, zuletzt geprüft am 22.02.2019.

[32] Seibel, K. (2018): So soll Deutschland den Rückstand bei der Startup-Finanzierung aufholen. In: Gründerszene. Online verfügbar unter https://www.gruenderszene.de/business/startup-finanzierung-deutschland-aufholen, zuletzt geprüft am 22.02.2019.

[33] Bundesministerium für Bildung und Forschung (BMBF): Security Research Map. Online verfügbar unter https://www.securityresearchmap.de/#, zuletzt geprüft am 22.02.2019.

[34] Bundesministerium für Bildung und Forschung (BMBF): Kompetenz- und Forschungszentren für IT-Sicherheit. Online verfügbar unter https://kompetenz-it-sicherheit.de/?doing_wp_cron=1544477419.6636219024658203125000, zuletzt geprüft am 22.02.2019.

[35] Waidner, M.; Backes, M.; Müller-Quade, J. (2017): Positionspapier: Cybersicherheit in Deutschland. In: Fraunhofer-Institut für Sichere Informationstechnologie (SIT). Online verfügbar unter https://www.kompetenz-it-sicherheit.de/wp-content/uploads/2017/02/Positionspapier_der_drei_Kompetenzzentren_IT-Sicherheit_web.pdf, zuletzt geprüft am 22.02.2019.

[36] Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS): Aufgaben und Ziele der ZITiS. Online verfügbar unter https://www.zitis.bund.de/DE/ZITiS/Aufgaben/aufgaben_node.html, zuletzt geprüft am 22.02.2019.

[37] Berg, A.; Haldenwang, T. (2018): Wirtschaftsschutz in der Industrie. In: Bitkom. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/Bitkom-PK-Wirtschaftsschutz-Industrie-13-09-2018-2.pdf, zuletzt geprüft am 22.02.2019.

[38] Bundesministerium für Wirtschaft und Energie (BMWi) (2018): Digital-Gipfel 2018: Künstliche Intelligenz und Cybersecurity. Online verfügbar unter https://www.youtube.com/watch?v=JHCcUqyTe6I, zuletzt geprüft am 22.02.2019.

[39] Ferguson, B. (2018): How Israel Rules The World Of Cyber Security. In: VICE News. Online verfügbar unter https://www.youtube.com/watch?v=ca-C3voZwpM, zuletzt geprüft am 22.02.2019.

[40] Welt (2014): Israel bildet seine Cyber-Kämpfer schon in der Schule aus. Online verfügbar unter https://www.welt.de/newsticker/dpa_nt/infoline_nt/computer_nt/article129483151/Israel-bildet-seine-Cyber-Kaempfer-schon-in-der-Schule-aus.html, zuletzt geprüft am 22.02.2019.

[41] Gruber, A. (2018): Warum Cyber-Cracks in die Wüste ziehen. In: Spiegel Online. Online verfügbar unter http://www.spiegel.de/netzwelt/web/beer-sheva-als-cybersecurity-zentrum-nicht-cool-aber-erfolgreich-a-1195135.html, zuletzt geprüft am 22.02.2019.

[42] cyber spark: Israel Cyber Innovation Arena. Human Capital. Online verfügbar unter http://cyberspark.org.il/, zuletzt geprüft am 22.02.2019.

[43] Bundesministerium des Innern (BMI) (2016): Cyber-Sicherheitsstrategie für Deutschland. Online verfügbar unter https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf, zuletzt geprüft am 22.02.2019.

[44] Kitz, V. (2016): Das wird man doch wohl mal sagen dürfen – oder? In: Spiegel Online. Online verfügbar unter http://www.spiegel.de/panorama/meinungsfreiheit-was-darf-ich-sagen-und-was-nicht-a-1074146.html, zuletzt geprüft am 22.02.2019.

[45] Mittermaier, J. (2018): EPA Jahresbericht 2017: Deutschland legt bei europäischen Patentanmeldungen weiter zu – stärkstes Wachstum bei Computertechnik. In: Europäisches Patentamt (EPA). Online verfügbar unter https://www.presseportal.de/pm/24954/3884700, zuletzt geprüft am 22.02.2019.

[46] Fraze, D.: Cyber Grand Challenge (CGC). In: Defense Advanced Research Projects Agency (DARPA). Online verfügbar unter https://www.darpa.mil/program/cyber-grand-challenge, zuletzt geprüft am 22.02.2019.

[47] Engemann, P.; Fischer, D.; Gosdzik, B.; Koller, T.; Moore, N. (2017): Im Visier der Cyber-Gangster. In: PricewaterhouseCoopers (PwC). Online verfügbar unter https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf, zuletzt geprüft am 22.02.2019.

[48] Hasso-Plattner-Institut: Die Top Ten deutscher Passwörter. Online verfügbar unter https://hpi.de/pressemitteilungen/2018/die-top-ten-deutscher-passwoerter.html, zuletzt geprüft am 22.02.2019.

[49] Zeit Online (2018): Jugendliche sehen Internet skeptischer. Online verfügbar unter https://www.zeit.de/digital/internet/2018-11/divsi-studie-internet-datensicherheit-beleidigungskultur-cybermobbing-verrohung, zuletzt geprüft am 22.02.2019.

[50] Österreichisches Bundesministerium Bildung, Wissenschaft und Forschung (BMBWF): Digitale Grundbildung. Online verfügbar unter https://bildung.bmbwf.gv.at/schulen/schule40/dgb/index.html, zuletzt geprüft am 22.02.2019.

[51] Corporate Trust (2014): Studie Industriespionage 2014. Online verfügbar unter https://www.vdr-service.de/fileadmin/services-leistungen/fachmedien/fachliteratur_studien/corporate-trust_industriespionage_2014.pdf, zuletzt geprüft am 22.02.2019.

[52] Corporate Trust (2012): Studie: Industriespionage 2012. Online verfügbar unter https://www.corporate-trust.de/wp-content/uploads/2016/06/CT-Studie-2012_FINAL.pdf, zuletzt geprüft am 22.02.2019.

[53] Waidner, M. (2018): Security at Large. In: Ringvorlesung Fraunhofer SIT, Kassel. Online verfügbar unter https://www.uni-kassel.de/eecs/fileadmin/datas/fb16/iteg/Veranstaltungen/2018-01-17_Michael_Waidner_ITeG_Ringvorlesung.pdf, zuletzt geprüft am 22.02.2019.

[54] Bundesministerium für Wirtschaft und Energie (BMWi): Erfolgsmodell Mittelstand. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Dossier/politik-fuer-den-mittelstand.html, zuletzt geprüft am 22.02.2019.

[55] Bundesamt für Sicherheit in der Informationstechnik (BSI): ISO 27001 Zertifizierung auf Basis von IT-Grundschutz. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/itgrundschutzzertifikat_node.html, zuletzt geprüft am 22.02.2019.

[56] Fischer, E. (2018): EU macht IT sicherer. In: Handelsblatt. Online verfügbar unter https://www.handelsblatt.com/politik/international/cybersecurity-act-eu-macht-it-sicherer/23745642.html, zuletzt geprüft am 22.02.2019.

[57] Neugebauer, R.; Jarke, M.; Thoma, K. (2014): Strategie- und Positionspapier Cyber-Sicherheit 2020. In: Fraunhofer-Gesellschaft zur Förderung e. V. Online verfügbar unter https://www.iese.fraunhofer.de/content/dam/iese/de/dokumente/Fraunhofer-Strategie-und_Positionspapier_Cyber-Sicherheit2020.pdf, zuletzt geprüft am 22.02.2019.

[58] Schonscheck, O. (2018): Meldepflichten nach DSGVO richtig umsetzen. In: Datenschutz Praxis. Online verfügbar unter https://www.datenschutz-praxis.de/fachartikel/die-neue-informationspflicht-bei-datenschutzverstoessen/, zuletzt geprüft am 22.02.2019.

[59] Bundesamt für Sicherheit in der Informationstechnik (BSI): Das IT-Sicherheitsgesetz. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/it_sig_node.html, zuletzt geprüft am 22.02.2019.

[60] Müller, M. (2018): IT-Sicherheitsgesetz 2.0: BMI skizziert erste Weiterentwicklungen. In: UdL Digital. Online verfügbar unter https://www.udldigital.de/it-sicherheitsgesetz-2-0-bmi-skizziert-erste-weiterentwicklungen/, zuletzt geprüft am 22.02.2019.

Mitwirkende

Gesamtleitung acatech HORIZONTE:

Prof. Dr.-Ing. Jürgen Gausemeier, acatech Vizepräsident/Heinz Nixdorf Institut der Universität Paderborn, Seniorprofessor

Projektgruppe Cyber Security:

Paul Duplys, Robert Bosch, Leiter Competence Segment Safety, Security & Privacy (Corporate Research)

Prof. Dr. Claudia Eckert, Technische Universität München, Leiterin Lehrstuhl Sicherheit in der Informatik/Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC), Leiterin

Alexander von Gernler, genua GmbH, Leiter Research/ Gesellschaft für Informatik e.V., Vizepräsident

André Grochowy, Munich Re, Senior Cyber Underwriter, Corporate Underwriting

Prof. Dr. Christoph Meinel, Hasso-Plattner-Institut, Institutsdirektor und CEO/Digital Engineering Fakultät – Universität Potsdam, Dekan

Stephan Micklitz, Google Germany, Direktor Engineering

Prof. Dr. Jörn Müller-Quade (Leiter), Karlsruher Institut für Technologie, Leiter der Forschungsgruppe Kryptographie und Sicherheit

Christian Stüble, Rohde & Schwarz Cybersecurity, Chief Technical Officer

Prof. Dr. Michael Waidner, Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Leiter/Technische Universität Darmstadt

Eva Weiß-Margis, T-Systems International GmbH, Telekom Security, Internal Security & Cyber Defense, Vice President Security Officer

Leitung Innovationsforum:

Prof. Dr. Martina Schraudner, acatech Vorstandsmitglied/Fraunhofer Center for Responsible Research and Innovation (CeRRI), Leiterin

Konzeption, Text und Experteninterviews:

Christina Müller-Markus, acatech Geschäftsstelle, Innovationsforum (federführende Autorin)

Dr. Anna Frey, acatech Geschäftsstelle, Technologien

Alexandra Heimisch-Röcker, acatech Geschäftsstelle, Innovationsforum

Kerstin Podere, acatech Geschäftsstelle, Innovationsforum (Koordination/Redaktion)

Anna-Laura Liebenstund, acatech Geschäftsstelle, Innovationsforum

Mit Unterstützung durch:

Sebastian Grünwald, acatech Geschäftsstelle, Innovationsforum

Iris Michalik, acatech Geschäftsstelle, Innovationsforum

Elisabeth Paul, acatech Geschäftsstelle, Innovationsforum

Vivian Würf, acatech Geschäftsstelle, Innovationsforum

HERAUSGEBER:
acatech – Deutsche Akademie der Technikwissenschaften

ADRESSEN STANDORTE
Geschäftsstelle
Karolinenplatz 4
80333 München

T +49(0)89/520309-0
F +49(0)89/520309-900

Hauptstadtbüro
Pariser Platz 4a
10117 Berlin

T +49(0)30/2063096-0
F +49(0)30/2063096-11

Brüssel-Büro
Rue d'Egmont/Egmontstraat 13
B-1000 Brüssel

T +32(0)2/2 13 81-80
F +32(0)2/2 13 81-89

horizonte@acatech.de
www.acatech.de
https://www.acatech.de/horizonte

Vorstand i.S.v. § 26 BGB: Prof. Dr.-Ing. Dieter Spath, Karl-Heinz Streibich, Prof. Dr.-Ing. Jürgen Gausemeier, Prof. Dr. Reinhard F. Hüttl, Prof. Dr. Hermann Requardt, Prof. Dr.-Ing. Thomas Weber, Manfred Rauhmeier, Prof. Dr. Martina Schraudner

Empfohlene Zitierweise:
acatech (Hrsg.): *Cyber Security* (acatech HORIZONTE), München 2019

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, der Entnahme von Abbildungen, der Wiedergabe auf fotomechanischem oder ähnlichem Wege und der Speicherung in Datenverarbeitungsanlagen bleiben – auch bei nur auszugsweiser Verwendung – vorbehalten.

Copyright © acatech – Deutsche Akademie der Technikwissenschaften • 2019

Layout und Satz:
Atelier Hauer+Dörfler GmbH, Berlin

Druck:
Komplan Biechteler GmbH & Co. KG, München

München 2019
acatech HORIZONTE ISSN 2625-9605

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Über acatech

acatech vertritt die deutschen Technikwissenschaften im In- und Ausland in selbstbestimmter, unabhängiger und gemeinwohlorientierter Weise. Als Arbeitsakademie berät acatech Politik und Gesellschaft in technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Darüber hinaus hat es sich acatech zum Ziel gesetzt, den Wissenstransfer zwischen Wissenschaft und Wirtschaft zu unterstützen und den technikwissenschaftlichen Nachwuchs zu fördern. Zu den Mitgliedern der Akademie zählen herausragende Wissenschaftlerinnen und Wissenschaftler aus Hochschulen, Forschungseinrichtungen und Unternehmen. acatech finanziert sich durch eine institutionelle Förderung von Bund und Ländern sowie durch Spenden und projektbezogene Drittmittel. Um den Diskurs über technischen Fortschritt in Deutschland zu fördern und das Potenzial zukunftsweisender Technologien für Wirtschaft und Gesellschaft darzustellen, veranstaltet acatech Symposien, Foren, Podiumsdiskussionen und Workshops. Mit Studien, Empfehlungen und Stellungnahmen wendet sich acatech an die Öffentlichkeit. acatech besteht aus drei Organen: Die Mitglieder der Akademie sind in der Mitgliederversammlung organisiert; das Präsidium, das von den Mitgliedern und Senatoren der Akademie bestimmt wird, lenkt die Arbeit; ein Senat mit namhaften Persönlichkeiten vor allem aus der Industrie, aus der Wissenschaft und aus der Politik berät acatech in Fragen der strategischen Ausrichtung und sorgt für den Austausch mit der Wirtschaft und anderen Wissenschaftsorganisationen in Deutschland. Die Geschäftsstelle von acatech befindet sich in München; zudem ist acatech mit einem Hauptstadtbüro in Berlin und einem Büro in Brüssel vertreten.

acatech

DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN