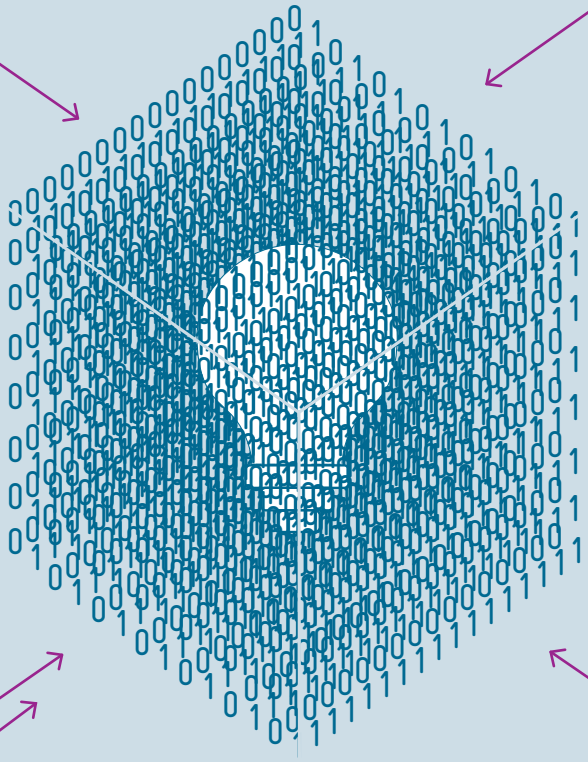
B 2 Cybersicherheit

Download Daten

Die fortschreitende Digitalisierung und digitale Vernetzung bieten neue Angriffspunkte auf Unternehmen. Innovationsaktivitäten von Unternehmen sind von dieser Gefahr direkt betroffen.

Schadprogramnme führen unerwünschte oder schadhafte Funktionen auf einem Computersystem aus.

Mit **Ransomware** verschlüsselt ein Angreifer die Daten eines IT-Systems, um die Nutzerinnen und Nutzer dazu zu bewegen, ein Lösegeld zu zahlen.

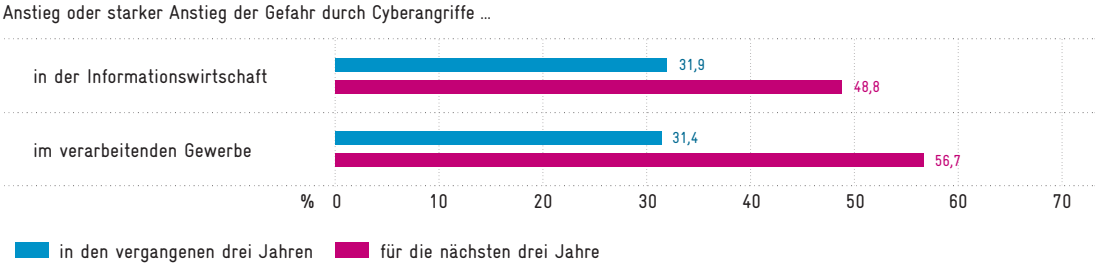


Advanced Persistent Threats weisen ein hohes Bedrohungspotenzial auf, weil die Angreifer gezielt und ausdauernd Schwachstellen ausfindig machen, um sie dann auszunutzen.

Durch **Social Engineering** werden Personen manipuliert, um sie dazu zu bringen, vertrauliche Informationen preiszugeben, Dateien oder Links mit hinterlegten Schadprogrammen zu öffnen oder Geld an unberechtigte Empfänger zu überweisen.

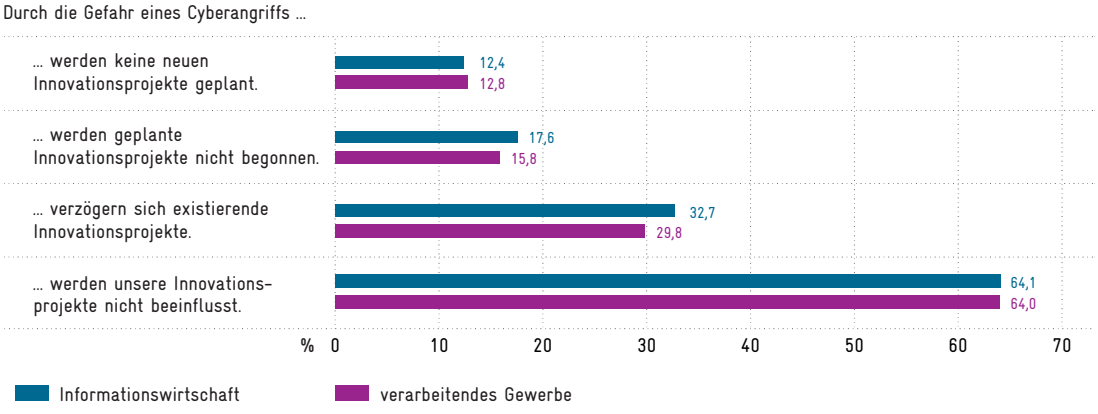
Bei **DDoS-Angriffen** fallen Netzwerkdienste aus, nachdem sie durch eine Vielzahl von Anfragen überlastet und somit blockiert wurden.

Einschätzung von Unternehmen zur Entwicklung der Gefahr durch Cyberangriffe[1)]



Branchenspezifische Hochrechnung der Ergebnisse auf die Frage: „Wie schätzen Sie die Veränderung der Gefährdung durch Cyberangriffe für Ihr Unternehmen ein?". Lesebeispiel: 56,7 Prozent der Unternehmen des verarbeitenden Gewerbes erwarten einen Anstieg oder starken Anstieg der Gefährdung durch Cyberangriffe für die nächsten drei Jahre.

Auswirkungen von Cyberbedrohungen auf Innovationsaktivitäten[2)]



Branchenspezifische Hochrechnung der Ergebnisse auf die Frage: „Welche Auswirkungen hat die Gefahr eines Cyberangriffs auf die Innovationstätigkeit Ihres Unternehmens?". Mehrfachnennungen möglich. Lesebeispiel: 12,8 Prozent der Unternehmen des verarbeitenden Gewerbes planen wegen der Gefahr eines Cyberangriffs keine neuen Innovationsprojekte.

Quellenverzeichnis Infografiken siehe Kapitel D 7.

B 2 Cybersicherheit

Die fortschreitende Digitalisierung und digitale Vernetzung bieten neue Angriffspunkte auf innovative Unternehmen. Die Mehrheit der innovativen deutschen Unternehmen in der Informationswirtschaft und im verarbeitenden Gewerbe sieht deshalb einen hohen Schutzbedarf ihrer Informationstechnik (IT) für Innovationstätigkeiten.[148] Außerdem geht über die Hälfte dieser innovativen Unternehmen davon aus, dass die Gefahr durch Cyberangriffe für ihr Unternehmen in den kommenden Jahren weiter wächst.[149] Die Innovationsaktivitäten der Unternehmen sind von dieser Gefahr direkt betroffen (vgl. B 2-2).[150] Somit ergeben sich aus Cyberangriffen mittelbar negative Auswirkungen auf das wirtschaftliche Wachstum Deutschlands. Das gilt insbesondere auch für den Wachstumsbeitrag digitaler Zukunftstechnologien wie der künstlichen Intelligenz oder des Internets der Dinge, denn der Erfolg dieser Technologien hängt u. a. von ihrer Sicherheit ab.

Die Cybersicherheit ist wiederum selbst Gegenstand von Innovationen und trägt mit ihren Produkten und Dienstleistungen unmittelbar zu wirtschaftlichem Wachstum und Wohlstand in Deutschland bei. Die Bruttowertschöpfung der deutschen IT-Sicherheitswirtschaft belief sich im Jahr 2017 auf 15,5 Milliarden Euro und machte damit 14,3 Prozent an der gesamten IT-Branche mit einer Bruttowertschöpfung von 108,6 Milliarden Euro aus – im Jahr 2010 waren es 12,9 Prozent. Von 2010 bis 2017 wuchs die Bruttowertschöpfung in der IT-Sicherheitswirtschaft nominal um durchschnittlich 5,6 Prozent pro Jahr. Dagegen fiel das durchschnittliche nominale Wachstum der gesamten IT-Branche und der Gesamtwirtschaft schwächer aus und belief sich im selben Zeitraum auf jeweils 4,3 Prozent und 3,4 Prozent pro Jahr.[151]

Darüber hinaus kommt Cybersicherheit eine wichtige Rolle bei der Aufrechterhaltung der Dienste kritischer Infrastrukturen (KRITIS) zu. Kritische Infrastrukturen finden sich in den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr.[152]

Einer Steigerung der Cybersicherheit – und damit einer Steigerung der Innovationsaktivitäten deutscher Unternehmen – stehen allerdings eine Reihe von Hemmnissen entgegen, die u. a. aus den Eigenschaften der Cybersicherheit resultieren. So besitzt die Cybersicherheit Eigenschaften eines öffentlichen Guts mit den damit verbundenen externen Effekten: Individuelle Akteure investieren zu wenig in Cybersicherheit, weil sie die positiven Effekte für andere Akteure nicht berücksichtigen. Außerdem haben Nutzerinnen und Nutzer von IT-Produkten wie Hard- oder Software nur begrenzt Einsicht in das Sicherheitsniveau, das von Anbietern bereitgestellt wird. Zudem fällt es Unternehmen oftmals schwer, das Risiko eines Cyberangriffs zu quantifizieren und daraus folgende Schäden abzuschätzen.

Aktuell sind sowohl Unternehmen als auch der Staat bestrebt, Cybersicherheitsfachleute einzustellen. Entsprechende Stellen bleiben jedoch für einen längeren Zeitraum unbesetzt. Gerade kleinere Unternehmen, die seltener über Cybersicherheitsfachleute in ihrer Belegschaft verfügen, haben daher Schwierigkeiten, auf externe Informationsangebote zu Cyberbedrohungen und deren Vermeidung einzugehen und Schutzmaßnahmen umzusetzen.

Cybersicherheit und Innovationen B 2–1

Varianten der Cyberbedrohung

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI, vgl. Box B 2-1) befasst sich Cybersicherheit mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik (IKT).[153] Der Begriff der Cybersicherheit geht dabei über den Begriff der IT-Sicherheit hinaus. „Das Aktionsfeld der klassischen IT-Sicherheit wird auf den gesamten

Cyberraum erweitert. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein."[154] Bei einem Cyberangriff handelt es sich um einen unberechtigten Zugriff auf IT-Systeme, der einen Datenabfluss oder eine Störung der Funktionsfähigkeit zum Ziel hat. Ein solcher Angriff auf IT-Systeme nutzt dabei selbst informationstechnische Mittel.[155]

Aufgrund der Fülle von unterschiedlichen Hardware- und Softwareprodukten existiert auch eine Vielzahl von Methoden für den unberechtigten Zugriff auf IT-Systeme. In seinem jüngsten Lagebericht analysiert das BSI die von ihm beobachteten Angriffsmethoden. Dazu zählen Identitätsdiebstahl, Schadprogramme (auch Malware genannt), Ransomware, Distributed Denial of Service (DDoS), Botnetze, Spam, Advanced Persistent Threat-Angriffe (APT-Angriffe) und Angriffe durch die Ausnutzung von moderner Prozessorarchitektur (vgl. Box B 2-2). Angriffe mit Schadprogrammen sind mit einem Anteil von 53 Prozent die häufigste Angriffsart, gefolgt von DDoS-Angriffen mit einem Anteil von 18 Prozent und APT-Angriffen mit einem Anteil von 12 Prozent.[156]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI)[157]

Box B 2-1

Das BSI zählt zum Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat (BMI). Es befasst sich mit allen Belangen rund um die IT-Sicherheit mit dem Ziel, einen sicheren Einsatz von Informations- und Kommunikationstechnik zu ermöglichen und voranzutreiben.

Neben dem Amtssitz des BSI in Bonn gibt es sogenannte Verbindungspersonen in sechs weiteren Städten. Dabei handelt es sich um zentrale Anlaufstellen für Länder und Kommunen, Bundes- und EU-Behörden in den jeweiligen Regionen, Unternehmen, Think Tanks und Entscheidungsträgerinnen und Entscheidungsträger aus der Gesellschaft. Darüber hinaus ist das Nationale Cyber-Abwehrzentrum (Cyber-AZ) beim BSI angesiedelt. Es soll die operative Zusammenarbeit verschiedener staatlicher Stellen optimieren und deren Maßnahmen koordinieren. Zu den Mitgliedern des Cyber-AZ gehören beispielsweise die Bundespolizei oder Geheimdienste.

Das „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes" (BSI-Gesetz) bestimmt die Aufgaben des BSI. Es soll in Verwaltung, Wirtschaft und Gesellschaft auf das Thema IT-Sicherheit aufmerksam machen und die genannten Institutionen darin unterstützen, eigenverantwortlich IT-Sicherheit umzusetzen. Dies erfolgt als Formulierung von Mindeststandards für die IT des Bundes und von Handlungsempfehlungen an Unternehmen sowie an Bürgerinnen und Bürger. Darüber hinaus ist das BSI dafür verantwortlich, Computer und Netze der Bundesverwaltung zu schützen. Diesbezüglich berichtet das BSI einmal jährlich dem Innenausschuss des Deutschen Bundestages.

Zu den Aufgaben des BSI gehören weiterhin (i) die Prüfung, Zertifizierung und Akkreditierung von IT-Produkten und -Dienstleistungen, (ii) die Warnung vor Schadprogrammen oder Sicherheitslücken in IT-Produkten und -Dienstleistungen, (iii) die IT-Sicherheitsberatung für die Bundesverwaltung und andere Zielgruppen, (iv) die Information und Sensibilisierung der Bürgerinnen und Bürger für das Thema IT- und Internet-Sicherheit, (v) die Entwicklung einheitlicher und verbindlicher IT-Sicherheitsstandards und (vi) die Entwicklung von Kryptosystemen für die IT des Bundes.

Mit dem Umsetzungsgesetz zur EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie)[158] wurden im Jahr 2017 auch neue Befugnisse für das BSI geschaffen. Einerseits wurden die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber KRITIS-Betreibern erweitert und gegenüber Anbietern digitaler Dienste neu geschaffen. Andererseits wurde die Zusammenarbeit zwischen den Bundesländern und dem BSI gestärkt: Damit kann das BSI die Bundesländer noch umfassender unterstützen und ihnen mit technischer Expertise zur Seite stehen.[159]

Box B 2-2

Aktuelle Angriffsmethoden gemäß BSI-Lagebericht[160]

Die folgende Beschreibung illustriert relevante Angriffsmethoden. Diese sind nicht überschneidungsfrei und können, z. B. in einem mehrstufigen Angriff, kombiniert werden.

Bei **Identitätsdiebstahl** handelt es sich um ein Phänomen mit hoher Bedeutung für Online-Geschäfte. Um Online-Dienste wie soziale Netzwerke, Streaming-Portale, Online-Shops oder Buchungsseiten zu nutzen, wird oft ein Zugang benötigt. Die Identifizierung beim Anbieter erfolgt über individuelle Zugangsdaten. Wenn diese Zugangsdaten entwendet werden, können Unbefugte umfangreichen Einblick in die Privatsphäre gewinnen und diese Informationen missbräuchlich verwenden. So konnten im Jahr 2013 durch einen Angriff die Namen, E-Mail-Adressen und Passwörter von drei Milliarden Yahoo-Kundinnen und -Kunden entwendet werden.[161] Die Hotelkette Marriott war über einen Zeitraum von fünf Jahren einem unberechtigten Zugriff auf Kundendaten ausgesetzt, durch den Namen, Passnummern und Kreditkartendaten von etwa 500 Millionen Kundinnen und Kunden entwendet wurden.[162] Daten aus Identitätsdiebstählen können genutzt werden, um Erkenntnisse für andere Angriffsarten wie z. B. Social Engineering zu gewinnen oder Kreditkartenbetrug zu begehen. Häufig werden entwendete Datensätze auf Online-Marktplätzen verkauft. Ob die eigenen Zugangsdaten entwendet und veröffentlicht wurden, kann online geprüft werden.[163]

Schadprogramme umfassen alle Arten von Computerprogrammen, die unerwünschte oder schädliche Funktionen auf einem Computersystem ausführen können.[164] Wie das BSI berichtet, erfasste das IT-Sicherheitsunternehmen AV-TEST im letzten BSI-Berichtszeitraum zwischen dem 1. Juni 2018 und dem 31. Mai 2019 ca. 114 Millionen Schadprogramm-Varianten, was etwa 312.000 Schadprogrammen täglich entspricht.[165] Laut Cybersicherheitsumfrage des BSI handelte es sich bei 53 Prozent der berichteten Angriffe um Schadprogramme.[166] Darüber hinaus gehören Angriffe mit Schadprogrammen zu den zehn größten Bedrohungen für Systeme zur Fertigungs- und Prozessautomatisierung (Industrial Control Systems).[167]

Mit **Ransomware** verschlüsselt ein Angreifer die Daten eines IT-Systems, um die Nutzerinnen und Nutzer dazu zu bewegen, ein Lösegeld zu zahlen. Allerdings führte das Zahlen von Lösegeld in der Vergangenheit nicht immer dazu, dass die Täter die Daten auch wieder entschlüsselten. Schadenshöhen auf einem aggregierten Level liegen nicht vor. Trotzdem veranschaulichen einzelne Schadensfälle das Schadenspotenzial von Ransomware-Angriffen. So meldete ein norwegisches Aluminiumunternehmen im März 2019 einen Ransomware-Angriff und stellte bereits nach einer Woche Verluste von ca. 40 Millionen Euro fest. Das Unternehmen zahlte, wie auch das BSI empfiehlt, kein Lösegeld, sondern stellte Daten aus Back-ups wieder her.

Eine Störung der IT-Systeme kann darüber hinaus über sogenannte **DDoS-Angriffe** (Distributed Denial of Service) erfolgen. Bei diesen Angriffen fallen Netz-

Cyberrisiken als Bedrohung für Innovationsaktivitäten

Cyberangriffe können verschiedenen Zwecken dienen, die Unternehmen allgemein und auch in Bezug auf ihre Innovationsaktivitäten treffen. Dabei werden Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit unterschieden.[170]

Bei Angriffen auf die Vertraulichkeit versuchen Täter, vertrauliche Informationen auszuspionieren, indem sie z. B. ein Funknetz abhören oder gelöschte Informationen wiederherstellen. Angriffe auf die Integrität können Manipulationen z. B. an Informationen, Software oder Schnittstellen sein. Bei Angriffen auf die Verfügbarkeit zielen Täter darauf ab, Informationen oder IT-Dienste zu sabotieren, beispielsweise durch DDoS-Angriffe.

Cyberangriffe verringern die potenziellen Erlöse und erhöhen die potenziellen Kosten von Innovationsaktivitäten. Dadurch reduzieren sich die Erträge dieser Aktivitäten und die Anreize für FuE. Der Cyberschutz von Innovationsaktivitäten ist mit Kosten verbunden, erhöht aber die Anreize für FuE in dem Maße, in dem die zusätzlichen Erträge der abgesicherten Innova-

werkdienste aus, nachdem sie durch eine Vielzahl von Anfragen überlastet und somit blockiert wurden. Zu solchen Diensten zählen z.B. E-Mail-Dienste oder die Internetseiten von Unternehmen. Mit einem Anteil von 18 Prozent an allen berichteten Angriffen sind DDoS-Angriffe laut Cybersicherheits-Umfrage die zweithäufigste Angriffsart.[168] Für eine Schätzung der Schäden verweist das BSI auf das Unternehmen Netscout, das für deutsche Unternehmen im Jahr 2018 einen DDoS-Gesamtschaden von etwa vier Milliarden Euro ermittelt hat. Für DDoS-Angriffe werden immer häufiger Cloud-Server angemietet. Im Winter 2018 wurden 59 Prozent der DDoS-Angriffe über Cloud-Server durchgeführt, während es zwei Jahre vorher noch 2 Prozent waren.

Botnetze bestehen aus einer Vielzahl vernetzter Geräte wie Computer, Smartphones oder IoT-Geräte (Internet of Things), über die ein Angreifer Kontrolle erlangt hat. Dadurch kann der Angreifer die Geräte für seine Ziele zweckentfremden. Bei Zielen finanzieller Natur können Geräte z.B. für das Schürfen von Kryptowährungen missbraucht werden.[169] Botnetze können aber auch der Sabotage dienen, indem sie für DDoS-Angriffe genutzt werden.

Unter **Spam** werden unerwünscht zugesandte E-Mails verstanden, die Werbung enthalten können, auf einen Betrug abzielen, Schadprogramme enthalten oder die Empfängerin bzw. den Empfänger dazu verleiten sollen, Zugangsdaten preiszugeben. Das BSI hat im Vergleich zum vorigen Berichtszeitraum einen Rückgang von Spam in Höhe von 40 Prozent registriert. Spam mit Schadprogrammen ging gar um 96 Prozent zurück. Allerdings ist die Effektivität von Spam erheblich gestiegen, sodass nicht davon ausgegangen werden kann, dass das Schadenspotenzial abgenommen hat. So existieren Schadprogramme, die den E-Mail-Verkehr eines infizierten Systems analysieren und neue Spam-Nachrichten an Kontakte des infizierten Systems senden, indem sie sich auf den bisherigen E-Mail-Verkehr beziehen. Solche E-Mails können auch sensibilisierte Personen täuschen.

Eine besondere Bedrohung stellen **APT-Angriffe** (Advanced Persistent Threat, auf Deutsch „fortgeschrittene, andauernde Bedrohung") dar. Sie zeichnen sich durch ein hohes Bedrohungspotenzial aus, weil die Angreifer gezielt und ausdauernd Schwachstellen ausfindig machen, um sie dann auszunutzen. Die Bedrohungslage wird dadurch verschärft, dass sich potenzielle Täter immer leichter Zugang zu leistungsfähigen Werkzeugen für APT-Angriffe verschaffen können.

Neben dem Ausnutzen von Schwachstellen in Software können auch Schwächen in der Hardware für Angriffe genutzt werden. Ein Beispiel hierfür sind **Angriffe unter Ausnutzung moderner Prozessorarchitektur** wie die Spectre-Varianten, Meltdown oder Foreshadow. Diese Schwachstellen können vermutlich nicht vollständig behoben werden. Allerdings waren dem BSI bisher keine Anzeichen dafür bekannt, dass diese Angriffsmethode aktiv ausgenutzt wurde.

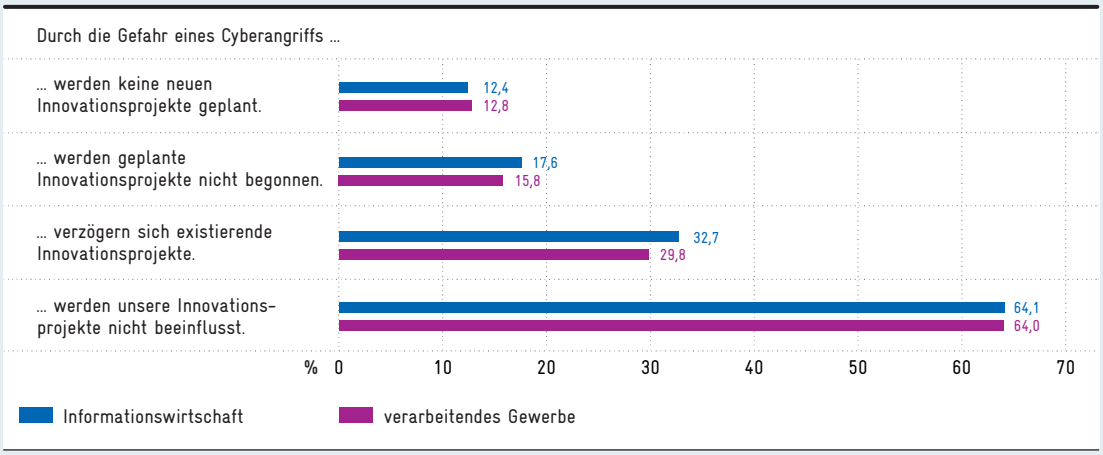
tionsaktivitäten die zusätzlichen Kosten der Cybersicherheit decken.

Eine im Auftrag der EFI durchgeführte repräsentative Umfrage[171] zeigt, wie sich die Bedrohung durch Cyberangriffe auf die Innovationsaktivitäten der Unternehmen auswirken kann. Jeweils 64 Prozent der Unternehmen der Informationswirtschaft[172] und des verarbeitenden Gewerbes[173] sehen keine Beeinflussung ihrer Innovationsprojekte durch die Gefahr eines Cyberangriffs (vgl. Abbildung B 2-3). Bei 32,7 Prozent der Unternehmen in der Informationswirtschaft und 29,8 Prozent der Unternehmen im verarbeitenden Gewerbe verzögern sich existierende Innovationsprojekte durch die Gefahr eines Cyberangriffs. Diese Anteile sind bei Unternehmen, die von einem Anstieg oder starken Anstieg der Gefährdung durch Cyberangriffe in den nächsten drei Jahren ausgehen, deutlich höher als bei Unternehmen, die einen solchen Anstieg nicht erwarten.[174] Bei 17,6 Prozent der Unternehmen in der Informationswirtschaft und 15,8 Prozent der Unternehmen im verarbeitenden Gewerbe werden geplante Innovationsprojekte durch die Gefahr eines Cyberangriffs nicht begonnen. Bei 12,4 Prozent der Unternehmen in der Informationswirtschaft und 12,8 Prozent der Unternehmen im verarbeitenden Gewerbe

Abb B 2-3

Download
Daten

Auswirkungen von Cyberbedrohungen auf Innovationsaktivitäten

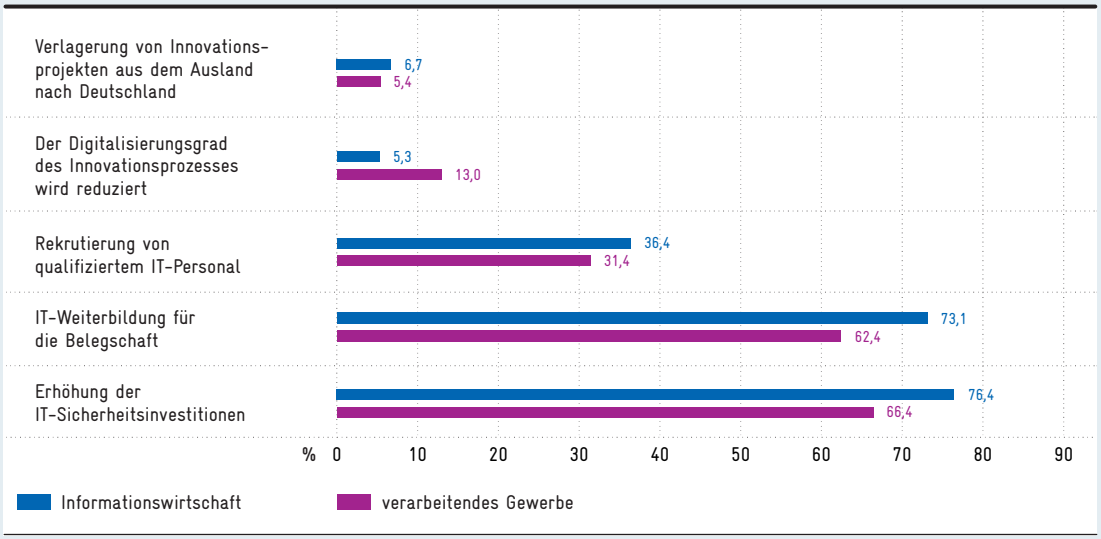


Branchenspezifische Hochrechnung der Ergebnisse auf die Frage: „Welche Auswirkungen hat die Gefahr eines Cyberangriffs auf die Innovationstätigkeit Ihres Unternehmens?". Mehrfachnennungen möglich. Lesebeispiel: 12,8 Prozent der Unternehmen des verarbeitenden Gewerbes planen wegen der Gefahr eines Cyberangriffs keine neuen Innovationsprojekte.
Quelle: ZEW Konjunkturumfrage Informationswirtschaft 3. Quartal 2019. Berechnungen in ZEW (2020).

Abb B 2-4

Download
Daten

Maßnahmen der Unternehmen zur Minimierung von Cyberrisiken

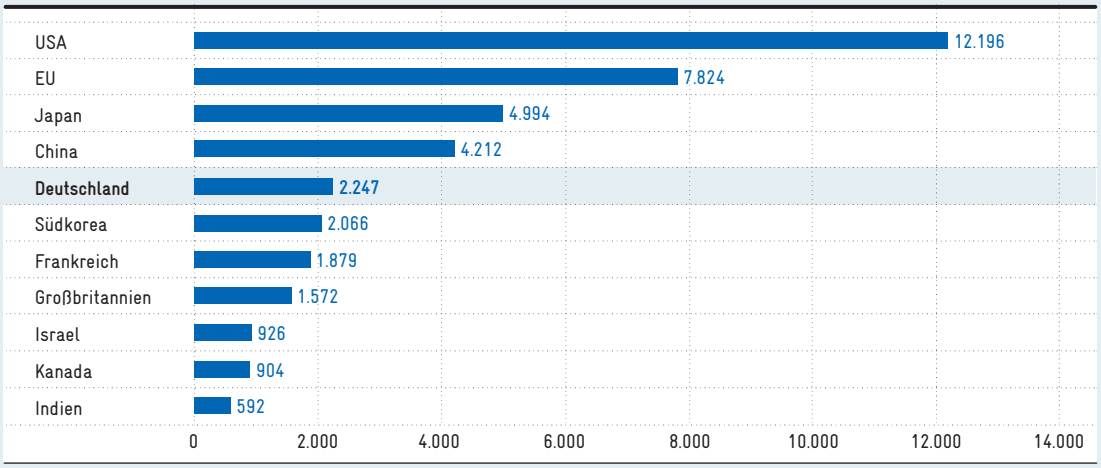


Branchenspezifische Hochrechnung der Ergebnisse auf die Frage: „Werden in Ihrem Unternehmen die folgenden Maßnahmen zur Minimierung von Cyberrisiken vorgenommen?". Mehrfachnennungen möglich. Lesebeispiel: 13,0 Prozent der Unternehmen des verarbeitenden Gewerbes reduzieren den Digitalisierungsgrad des Innovationsprozesses, um Cyberrisiken zu minimieren.
Quelle: ZEW Konjunkturumfrage Informationswirtschaft 3. Quartal 2019. Berechnungen in ZEW (2020).

Abb B 2-5

Download Daten

Anzahl transnationaler Patente im Bereich Cybersicherheit (Top 10 Länder und EU) 2000–2017



Quelle: Eigene Darstellung basierend auf Berechnungen des Max-Planck-Instituts für Innovation und Wettbewerb.

werden durch die Gefahr eines Cyberangriffs keine neuen Innovationsprojekte geplant.

Die Befragung zeigt zudem, dass auch bei Unternehmen ohne laufende Innovationsprojekte die Gefahr eines Cyberangriffs bei der Entscheidung, keine neuen Innovationsprojekte zu planen, eine Rolle spielt. So verzichten aus diesem Grund 14,5 Prozent der Unternehmen der Informationswirtschaft und 16,2 Prozent der Unternehmen im verarbeitenden Gewerbe ohne laufende Innovationsprojekte darauf, neue Innovationsprojekte zu planen.

Um Cyberrisiken zu minimieren, setzen die Unternehmen der Informationswirtschaft und des verarbeitenden Gewerbes vor allem auf Investitionen in die IT-Sicherheit, auf IT-Weiterbildung der Belegschaft und auf die Rekrutierung von qualifiziertem IT-Personal (vgl. Abbildung B 2-4). Vereinzelt wird auch der Digitalisierungsgrad von Innovationsprozessen zurückgefahren oder es werden Innovationsprojekte aus dem Ausland nach Deutschland verlagert. Um Cyberrisiken zu minimieren, verringern 19,2 Prozent der Unternehmen des verarbeitenden Gewerbes mit 5 bis 19 Beschäftigten den Digitalisierungsgrad ihres Innovationsprozesses. Dies trifft nur auf 4,7 Prozent der Unternehmen des verarbeitenden Gewerbes mit 20 bis 99 Beschäftigten zu und auf 3,6 Prozent der Unternehmen des verarbeitenden Gewerbes mit mindestens 100 Beschäftigten. Eine Reduktion des Digitalisierungsgrads als Antwort auf Cyberbedrohungen erscheint insbesondere dann kritisch, wenn dadurch Produktivitätspotenziale verloren zu gehen drohen.

Patentaktivitäten in der Cybersicherheit

In Anbetracht der zunehmenden und sich stetig verändernden Cyberrisiken[175] besteht ein hoher Bedarf, diesen Risiken mit innovativen Cybersicherheitslösungen zu begegnen. Innovationen in der Cybersicherheit ermöglichen sowohl die Erhöhung des Schutzniveaus als auch eine Ausweitung von Wertschöpfungspotenzialen.[176] Einen Hinweis auf Innovationsaktivitäten können Patentanmeldungen geben.[177] Für die folgende Analyse bezieht sich die Expertenkommission auf internationale Patentierungsaktivitäten, die sich durch transnationale Patentanmeldungen abbilden lassen. Die Zuordnungen der Patente zu Ländern erfolgt dabei über die Nationalität der Erstanmelderin bzw. des Erstanmelders. Abbildung B 2-5 zeigt die Verteilung transnationaler Patentfamilien aus dem Bereich der Cybersicherheit der Jahre 2000 bis 2017 für die zehn Länder mit den meisten Patenten sowie für die EU.[178] Deutsche Erfinderinnen und Erfinder liegen mit 6,2 Prozent der Patente mit deutlichem Abstand hinter Erfinderinnen und Erfindern aus den USA (33,5 Prozent), Japan (13,7 Prozent) und China (11,6 Prozent). Die Erfinderinnen und Erfinder aus Ländern der EU kommen zusammen auf 21,5 Prozent. Die USA und China haben im Laufe des betrachteten Zeitraums immer mehr an Bedeutung gewonnen und weisen insbesondere am aktuellen Rand einen überdurchschnittlichen Anstieg der Patentanmeldungen auf.[179]

Vergleicht man die Patentaktivitäten eines Landes im Bereich Cybersicherheit mit den Patentaktivitäten eines Landes insgesamt, fällt auf, dass Deutschland im Gegensatz zu den USA und Israel nicht auf den Bereich der Cybersicherheit spezialisiert ist.[180] Die Spezialisierung der USA und Israels spiegelt sich auch in Auswertungen des amerikanischen Branchendienstes Cybersecurity Ventures wider. Dort sind unter den 150 innovativsten Cybersicherheits-Unternehmen der Welt 112 Unternehmen aus den USA, 18 Unternehmen aus Israel und nur eines aus Deutschland.[181]

B 2-2 Herausforderungen auf der Unternehmensebene

Eine Reihe von Hemmnissen kann dazu beitragen, dass Unternehmen eine für sie wünschenswerte Absicherung gegen Cyberrisiken nicht erreichen. Hierzu zählt insbesondere das Problem, Cybersicherheitsfachleute zu rekrutieren, die Unternehmen besser schützen, Angriffe erkennen und abwehren. Zusätzlich bestehen Informationsdefizite zur jeweils aktuellen Bedrohungslage, zum Ausmaß von Schäden und zur Qualität von IT-Sicherheitsprodukten.

Bedarf an Fachkräften und Kompetenzen

Für zahlreiche Unternehmen stellt der Mangel an qualifizierten IT-Sicherheitsfachkräften eine Bedrohung für die IT-Sicherheit ihres Unternehmens dar.[182]

Die EU-Kommission hat für die EU-Mitgliedsstaaten untersucht, wie lange es dauert, Stellen, die digitale Fähigkeiten erfordern, zu besetzen.[183] Diese Analyse zeigt, dass ein relativ hoher Anteil von offenen Stellen im Bereich Cybersicherheit auch nach 90 Tagen noch unbesetzt ist. In den Bereichen Machine Learning oder Internet der Dinge ist nach 90 Tagen ein deutlich größerer Anteil dieser Stellen besetzt als im Bereich Cybersicherheit.[184]

Dem hohen Bedarf an Cybersicherheitsfachleuten stehen in Deutschland nur wenige Studiengänge für Cybersicherheit gegenüber.[185] Studierendenstatistiken für das relativ junge Studienfach Cybersicherheit liegen nicht vor. Bislang wurden Studieninhalte zum Thema Cybersicherheit zumeist in Informatik-Studiengängen vermittelt. Die Anzahl Studierender des Studienfachs Informatik ist vom Studienjahr 2010/2011 bis zum Studienjahr 2017/2018 von 69.559 auf 115.005, also um fast zwei Drittel, gestiegen.

Weil der Cyberraum viele Bereiche des Lebens berührt, ist es wichtig, Cybersicherheit nicht nur als rein technische Disziplin zu verstehen. Schnittstellen bestehen u. a. mit den Sozial-, Wirtschafts- und Rechtswissenschaften und sollten dementsprechend in Studienangeboten berücksichtigt werden.

Um Cybersicherheit flächendeckend erhöhen zu können, bedarf es nicht nur akademisch ausgebildeter Fachkräfte; Cybersicherheit sollte auch verstärkt in die berufliche Aus- und Weiterbildung integriert werden. Damit kann dem Umstand Rechnung getragen werden, dass das Cybersicherheitsniveau nicht nur durch technische Innovationen determiniert wird, sondern auch durch den Umgang mit Hardware und Software. Es existiert derzeit kein spezifischer Ausbildungsgang für IT-Sicherheitsfachleute. Aktuell werden auch die Ausbildungsgänge zu den IT-Berufen Fachinformatiker/in, Informatikkaufmann/-frau, IT-System-Elektroniker/in und IT-System-Kaufmann/-frau modernisiert.[186] Seit August 2018 werden verstärkt Ausbildungsinhalte zur IT-Sicherheit vermittelt.

Im Jahr 2017 wurden in diesen vier IT-Berufen insgesamt 16.869 neue Ausbildungsverträge geschlossen. Außerdem wurde mit der neu geschaffenen Berufsbildposition „Digitalisierung der Arbeit, Datenschutz und Informationssicherheit“ eine integrative Vermittlung von Inhalten zur Informationssicherheit in die Ausbildung für industrielle Metall- und Elektroberufe sowie für Mechatronik aufgenommen.

Um Cybersicherheitskompetenzen auszubauen und an sich ändernde Anforderungen anzupassen, ist es im Eigeninteresse der Unternehmen, ihren Cybersicherheitsfachleuten Weiterbildungen zu ermöglichen und bestehende Personalressourcen zu nutzen. Dabei können neben klassischen Weiterbildungsangeboten auch innovative Ansätze einen Beitrag leisten. So existieren Angebote, die mit Methoden wie Gamification das Abwehren von Angriffen trainieren (vgl. Box B 2-6).

Neben Fachkräften für Cybersicherheit haben auch alle anderen Beschäftigten Einfluss auf das Cybersicherheitsniveau eines Unternehmens. So werden oftmals E-Mails, die für die meisten Beschäftigten in Unternehmen wichtiger Bestandteil des Arbeitsalltags sind, als Einfallstor für Cyberangriffe genutzt.[187] In einer Unternehmensbefragung von KPMG[188] wurden Unachtsamkeit von 90 Prozent der Unternehmen und unzureichend geschultes Personal von 83 Prozent der Unternehmen zu den Faktoren gezählt, die E-Crime[189]

Box B 2-6

Beispiel: Weiterbildung durch Gamification

Fähigkeiten für die Abwehr von Cyberangriffen müssen regelmäßig trainiert und auf den neuesten Stand gebracht werden. Anbieter von sogenannten Cyber Ranges bieten solche Trainings an. Allerdings befinden sich Cyber Ranges häufig in den Räumlichkeiten der Anbieter, sodass die Cybersicherheitsfachleute wegen des Trainings einige Zeit im Unternehmen ausfallen und sich damit die Kosten des Trainings erhöhen.

Das israelische Unternehmen Cympire hat eine softwarebasierte Umgebung zum Training der Abwehr von Cyberangriffen entwickelt, die die IT-Infrastruktur der Kundinnen und Kunden nachbilden kann. Dadurch können Trainings standortunabhängig stattfinden und der dafür notwendige Zeitbedarf reduziert werden. Zusätzlich enthält das Angebot von Cympire innovative Elemente wie Gamification, die geeignet sind, die Motivation der Fachleute für Trainings zu erhöhen.

begünstigen. Deshalb sind Sensibilisierung und Weiterbildung der gesamten Belegschaft in Bezug auf Cybersicherheit wichtig. In vielen Unternehmen gibt es bereits entsprechende Maßnahmen. Allerdings zeigen Befragungen, dass kleinere Unternehmen hier weniger aktiv sind.[190]

Abbau von Informationsdefiziten

Informationsdefizite erschweren Unternehmen den Umgang mit Cyberbedrohungen.[191] Zum einen können Unternehmen das Risiko von Cyberangriffen und daraus folgenden Schäden nicht verlässlich abschätzen. Zum anderen können sie als Nachfrager aufgrund der hohen und zunehmenden Komplexität von IT-Systemen sowie der sich rasch ändernden Sicherheitsanforderungen die Qualität von Cybersicherheitsprodukten und -dienstleistungen häufig nur schwer beurteilen.

Informationsdefizite zu den Risiken von Cyberangriffen und den daraus folgenden Schäden können durch verschiedene Maßnahmen verringert werden. Betreiber kritischer Infrastrukturen, Anbieter von Online-Diensten und Telemedienanbieter sind gesetzlich verpflichtet, Cyberangriffe an das BSI zu melden. Das BSI stellt seinerseits über das Computer Emergency Response Team des Bundes (CERT-Bund) Warn- und Informationsdienste bereit.[192] Daneben existieren Initiativen, in denen Unternehmen untereinander oder mit staatlichen Stellen Informationen zu Cyberangriffen austauschen.[193] Gerade kleine und mittlere Unternehmen (KMU) verfügen aber oft nicht über die nötigen Ressourcen, um sich in solche Initiativen einzubringen.

Weitere Maßnahmen, um Informationsasymmetrien auf dem Markt für Cybersicherheitsprodukte und -dienstleistungen zu verringern, sind Zertifizierungen und Gütesiegel sowie Mindeststandards. Eine weitere Möglichkeit, mit Informationsasymmetrien umzugehen, sind Haftungsregeln, die im Schadensfall die Hersteller für Sicherheitslücken verantwortlich machen. Dies schafft Anreize, schon bei der Produktentwicklung stärker auf Sicherheit zu achten (Security-by-design), um Entschädigungszahlungen oder teure Versicherungspolicen zu vermeiden.[194]

In Deutschland existiert mit dem BSI eine nationale Zertifizierungsstelle für IT-Sicherheit. Dort können Unternehmen für bestimmte Produkte oder Leistungen eine Sicherheits- oder Personenzertifizierung oder eine Zertifizierung als IT-Sicherheitsdienstleister beantragen.[195] Sowohl für Zertifizierungen als auch für Mindestanforderungen an IT-Sicherheit hat die Umsetzung auf europäischer Ebene erst vor Kurzem begonnen und stellt eine sehr komplexe Herausforderung dar. Der im Juni 2019 in Kraft getretene EU Cyber Security Act[196] bildet die Grundlage für Zertifizierungen. Das New Legislative Framework[197] als Rechtsrahmen für die Markt- und Produktüberwachung dient als Basis für Mindestanforderungen an Cybersicherheit in Produkten.

Versicherungen gegen Cyberrisiken

Neben Investitionen in Cybersicherheit können Unternehmen Cyberversicherungen nutzen, um ihre Kosten durch Cyberangriffe zu begrenzen. Cyberversicherungen sind oft eine Kombination aus Haftpflicht-, Betriebsausfall- und Datenversicherung für Dritt- und Eigenschäden.[198] Zu den Leistungen einer Cyberversicherung können gehören[199]: Entschädigung bei Betriebsunterbrechungen, Erstattung der Kosten für die Datenwiederherstellung, Übernahme von Drittschäden, Bezahlung der IT-Forensik, Angebot einer Rechtsberatung für Datenschutzverletzungen,

Bezahlung von Krisenkommunikation und von Call-center-Kosten.

Die ersten Cybersicherheitspolicen in Deutschland wurden 2011 angeboten.[200] Demnach handelt es sich um einen vergleichsweise jungen Versicherungsmarkt. Laut einer Bitkom-Befragung haben 14 Prozent der Industrieunternehmen eine Cyberversicherung abgeschlossen.[201] Dabei fällt dieser Anteil bei kleinen, mittleren und großen Unternehmen unterschiedlich aus. 10 Prozent der Unternehmen mit 10 bis 99 Beschäftigten haben eine Cyberversicherung. Bei Unternehmen mit 100 bis 499 Beschäftigten sind dies 23 Prozent und bei Unternehmen mit mehr als 500 Beschäftigten 32 Prozent.

Gründe gegen den Abschluss einer Cyberversicherung sind z. B. die Einschätzung, nur einem geringen Risiko von Cyberangriffen ausgesetzt zu sein, ein ungünstiges Kosten-Nutzenverhältnis sowie ein zu hoher Aufwand für die Risikobeurteilung.[202]

B 2-3 Cybersicherheit und die Rolle des Staates

Dem Staat kommen bei der Wahrung der Cybersicherheit verschiedene Rollen zu. Er trägt durch die Förderung von FuE in der Cybersicherheit dazu bei, die notwendige Expertise für den Schutz vor Cyberangriffen zu schaffen. Gleichzeitig unterstützt er damit die Rolle der Cybersicherheit als Innovationstreiber, durch den neue Produkte und Dienste entstehen können. Der Staat stellt zudem verlässliche Informationen zur Bedrohungslage und zu Schutzmaßnahmen bereit. Aufbauend auf diesen Informationen können Unternehmen ihre Aktivitäten zur Cybersicherheit besser steuern und ihre Innovationstätigkeit schützen. Darüber hinaus liegt es in der Verantwortung des Staates, durch rechtliche und regulatorische Maßnahmen sowie durch Strafverfolgung für Sicherheit im Cyberraum zu sorgen.[203]

F&I-Förderung für Cybersicherheit

Das Bundesministerium für Bildung und Forschung (BMBF) fördert Forschung in der IT-Sicherheit über das Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt 2015–2020“ mit rund 180 Millionen Euro.[204] Schwerpunkte des Forschungsrahmenprogramms sind Hightech-Technologien für die IT-Sicherheit, sichere und vertrauenswürdige IKT-Systeme, Anwendungsfelder der IT-Sicherheit sowie Privatheit und der Schutz von Daten. Als Teil des Forschungsrahmenprogramms werden seit 2011 die drei Kompetenzzentren CISPA[205] (Saarbrücken), KASTEL[206] (Karlsruhe) und CRISP[207] (Darmstadt) durch das BMBF gefördert. Aus dem Kompetenzzentrum CRISP ist im Dezember 2019 das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE hervorgegangen, das die Arbeit von mehr als 500 Forschenden der Fraunhofer-Institute SIT und IGD, der Technischen Universität Darmstadt und der Hochschule Darmstadt bündelt.[208]

Das BMBF fördert zudem von 2017 bis 2020 den Gründungsinkubator StartUpSecure mit zwei Millionen Euro jährlich. Partner sind CISPA, CRISP, KASTEL und das Horst Görtz Institut für IT-Sicherheit an der Ruhr-Universität Bochum.[209] Nach Angaben des BMBF wurden mit StartUpSecure bisher zehn Startups initiiert.

Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) forscht und entwickelt in den Bereichen digitale Forensik, Telekommunikationsüberwachung, Krypto- und Big-Data-Analyse. Das Budget der ZITiS betrug im Jahr 2019 ca. 36 Millionen Euro. Mit der Schaffung der Agentur für Innovation in der Cybersicherheit (Cyberagentur) investiert die Bundesregierung darüber hinaus bis 2023 bis zu 402,5 Millionen Euro in neue Technologien der Cybersicherheit.[210] Die Cyberagentur soll als GmbH gegründet werden und in diesem Jahr den Geschäftsbetrieb aufnehmen.[211] Mit der Cyberagentur sollen F&I-Projekte im Bereich der Cybersicherheit initiiert und gefördert sowie Beschaffungsverfahren[212] beschleunigt werden.[213] Allerdings wird die Cyberagentur eine engere Anbindung an die Politik erfahren als die zivile SprinD (vgl. Kapitel A 1). Zu dieser stärkeren Anbindung an die Politik gehört eine Transparenzpflicht gegenüber dem Deutschen Bundestag, dessen Haushaltsausschuss beispielsweise auch über neue Geschäftszweige oder Ausgründungen entscheidet. Daneben wird die Cyberagentur in der Auswahl ihrer Projekte wesentlich durch die Bedarfe der beiden aufsichtführenden Ministerien, Bundesministerium der Verteidigung (BMVg) und Bundesministerium des Innern, für Bau und Heimat (BMI), geleitet.

Aufklärung und Sensibilisierung

Mit der Initiative „IT-Sicherheit in der Wirtschaft“ unterstützt das Bundesministerium für Wirtschaft und Energie (BMWi) seit 2011 Maßnahmen zur nachhaltigen Verbesserung des Bewusstseins für IT-Sicherheit speziell bei KMU.[214] Zu den Angeboten dieser Initiative gehören u. a. IT-Sicherheitschecks[215] und ein IT-Sicherheitsnavigator[216], die Unternehmen dabei helfen sollen, ihren Datenschutz zu verbessern, oder einen Überblick über Hilfsangebote liefern. Kampagnen wie „KMU aware – Awareness im Mittelstand“[217] oder die Posterkampagne „IT-Sicherheit ist KEIN Spiel“[218] sollen dazu beitragen, Unternehmen für die Cybersicherheit zu sensibilisieren. Weitere Programme wie „KMU innovativ IKT“[219] des BMBF oder „go-digital“ und die „Mittelstand 4.0-Kompetenzzentren“ des BMWi sowie der „ERP-Digitalisierungs- und Innovationskredit“ der KfW enthalten ebenfalls Elemente zur Förderung der IT-Sicherheit.

Eine zentrale Aufgabe im Bereich der Cybersicherheit übernimmt das BSI (vgl. Box B 2-1), zu dessen vorrangigen Aufgaben die Informationsbereitstellung und Beratung zu allen wichtigen Themen der IT-Sicherheit und die Unterstützung beim Ergreifen geeigneter Maßnahmen gehören.[220] Das BSI richtet sich mit Informationen und Beratung an Bürgerinnen und Bürger[221], Unternehmen[222] und die Verwaltung von Bund und Ländern[223]. Es nutzt unterschiedliche Formate wie jährliche Lageberichte, Meldungen des CERT-Bund[224] oder Bürger-CERT und Kooperationsplattformen wie die Allianz für Cybersicherheit.[225]

Daneben stellt die Initiative „Deutschland sicher im Netz“, ein Verein unter Schirmherrschaft des BMI, eine Vielzahl von Angeboten für Verbraucherinnen und Verbraucher sowie kleine Unternehmen zum sicheren und souveränen Umgang mit der digitalen Welt bereit.[226]

Maßnahmen für sichere digitale Infrastrukturen

Es ist Aufgabe der Bundesregierung – und ihrer europäischen Partner – für die Sicherheit digitaler Infrastrukturen zu sorgen. Mit dem Ausbau des Mobilfunknetzes auf den neuen 5G-Standard hat das Thema Sicherheit von digitalen Infrastrukturen eine hohe Aufmerksamkeit in Politik und Öffentlichkeit erlangt. Eine Empfehlung der Europäischen Kommission zielt darauf ab, eine Toolbox zu entwickeln, die sowohl technische als auch nicht-technische Kriterien für die Bewertung von Cyberrisiken für 5G-Netze definiert und Maßnahmen für die Sicherung der 5G-Netze umfasst.[227] Nicht-technische Kriterien für Cyberrisiken können beispielsweise die Vertrauenswürdigkeit von Herstellern oder Bezugsquellen betreffen und deren regulatorisches Umfeld berücksichtigen. Die Förderung der Hersteller- bzw. Anbietervielfalt im europäischen Binnenmarkt kann zur Resilienz von Netzen beitragen.[228] Zudem haben multilaterale Projekte wie die Datencloud GAIA-X (vgl. Kapitel A 1) das Ziel, Impulse für die Schaffung sicherer digitaler Infrastrukturen auf nationaler und EU-Ebene zu geben.

Handlungsempfehlungen B 2–4

Die Bundesregierung hat frühzeitig die Bedeutung von Cybersicherheit erkannt und u. a. FuE-Programme sowie Informationsmaßnahmen zur Stärkung der Cybersicherheit auf den Weg gebracht. Zudem wurde das BSI zur zentralen Institution für die Gewährleistung von Cybersicherheit ausgebaut. Die Bedrohungslage von Unternehmen ist allerdings einem steten Wandel unterzogen, sodass bestehende Programme zur Förderung der Cybersicherheit auf den Prüfstand gestellt und, falls nötig, angepasst werden müssen. Aus innovationspolitischer Sicht ist es insbesondere kritisch, dass sich bei Unternehmen aufgrund der Gefahr von Cyberangriffen Innovationsprojekte verzögern oder Unternehmen Innovationsprojekte erst gar nicht beginnen. Vor diesem Hintergrund empfiehlt die Expertenkommission:

Bedarf an Fachkräften und Kompetenzen decken

– Die Vermittlung von Cybersicherheitskenntnissen in der beruflichen Aus- und Weiterbildung sowie an Hochschulen ist weiter voranzutreiben, um der zunehmenden Nachfrage nach Cybersicherheitsfachleuten zu begegnen. Dabei sollten nicht nur technische Aspekte abgedeckt, sondern auch juristische Fragestellungen (Cyber-Law) und ethische Aspekte (Cyber-Ethik) berücksichtigt werden.

Sicherheit digitaler Infrastrukturen gewährleisten

- Die Zulassung von Komponenten digitaler Infrastrukturen sollte auf Basis von Kriterien erfolgen, die im gesamten europäischen Binnenmarkt gelten. Diese Kriterien sollten technische und nicht-technische Aspekte berücksichtigen und für Anbieter aus EU- und Nicht-EU-Ländern gleichermaßen gelten. Entsprechende Initiativen der EU-Kommission, z. B. für den Aufbau der 5G-Netze, sollten unterstützt werden.
- Die Bundesregierung sollte multilaterale Initiativen wie die Datencloud GAIA-X forcieren, um so Impulse für die Schaffung sicherer digitaler Infrastrukturen auf nationaler und EU-Ebene zu geben.

Cyberagentur zügig starten

- Die Cyberagentur sollte den Geschäftsbetrieb zügig aufnehmen und durch bedarfsorientierte Beschaffung innovative Projekte fördern, die der Sicherung der Technologiesouveränität Deutschlands in der Cybersicherheit dienen. Dabei ist es wichtig, stetig und offen neue technologische Entwicklungen zu verfolgen, um flexibel auf sich verändernde Bedarfe reagieren zu können. Eine Evaluierung der Cyberagentur sollte überprüfen, welche Impulse sie für F&I-Aktivitäten in der Cybersicherheit setzt.

Informationslage zu Cyberbedrohungen verbessern

- Insbesondere für KMU ist es wichtig, niedrigschwellige Informations- und Beratungsangebote zur Verfügung zu stellen. Bestehende Programme zur Förderung von Cybersicherheit in KMU sollten auf ihre Wirksamkeit überprüft und an die sich ständig verändernde Bedrohungslage angepasst werden.
- Um die Informationslage zur Qualität von Cybersicherheitsprodukten und -dienstleistungen zu verbessern, sollten Initiativen zur Entwicklung von Mindeststandards und Zertifizierungen insbesondere auf europäischer Ebene unterstützt werden.
- Es ist zu prüfen, ob die bestehenden Meldepflichten bei Cyberangriffen ausgeweitet werden müssen, um die Informationslage über Cyberrisiken zu verbessern und effektiver mit Cyberbedrohungen umgehen zu können.