Deutscher Bundestag **Drucksache 19/24247**

19. Wahlperiode 12.11.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Jürgen Martens, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/23851 –

Anfälligkeit kritischer Infrastrukturen vor Hackerangriffen in Deutschland

Vorbemerkung der Fragesteller

Kriminalpolizisten haben seit Beginn der Corona-Pandemie vor vermehrten Hackerattacken auf IT-Systeme von Krankenhäusern und Energieversorgern gewarnt. Im Fall einer stärkeren Auslastung vieler Kliniken wären die Folgen von Hackerangriffen besonders gravierend. So könnten Operationen nicht stattfinden oder Patienten müssten abgewiesen werden. Schlimmstenfalls hätten Hackerangriffe tödliche Folgen für Patienten.

Am 10. September 2020 war die Düsseldorfer Uniklinik von einem Hackerangriff betroffen. Kriminelle hatten sich Zugang zum IT-System der Klinik verschafft, verschlüsselten daraufhin 30 Datenserver und hinterließen ein Erpresserschreiben, in dem sie Lösegeld von der Klinik forderten. Als die Täter bemerkten, dass anstatt der Düsseldorfer Heinrich-Heine-Universität die Uniklinik von der Hackerattacke betroffen war, konnten trotz der Herausgabe des Schlüssels für die Datenentsperrung die dramatischen Folgen nicht mehr aufgehalten werden. Operationen mussten abgesagt werden und eine lebensbedrohlich erkrankte Patientin musste in ein anderes Krankenhaus eingeliefert werden, wo sie kurz danach verstarb. Die Polizei ermittelt, ob zwischen dem Tod der Patientin und den Folgen des Hackerangriffs ein Zusammenhang besteht (https://www.faz.net/aktuell/feuilleton/toedliche-folgen-hackerangriff-auf-universitaetsklinik-duesseldorf-16969390.html).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt deshalb vor weiteren Attacken auf Kliniken und vor der hohen Anfälligkeit öffentlicher Einrichtungen vor Hackerangriffen in der Bundesrepublik Deutschland.

1. Welche Erkenntnisse hat die Bundesregierung zur Anfälligkeit von IT-Systemen gegenüber Hackerangriffen folgender kritischer Infrastrukturen in der Bundesrepublik Deutschland (bitte pro Sektor nach Anlagenkategorien aufschlüsseln):

   a) Energie,

Die Bundesregierung ist sich über die Anfälligkeit von IT-Systeme und Gefahren durch Cyberangriffe auch im Energiebereich bewusst. Allerdings ist festzu-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 11. November 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

halten, dass allgemeine Aussagen zur IT-Anfälligkeit wegen der Heterogenität im Energiesektor nur schwer zu treffen sind. Daher hat die Bundesregierung mit der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) bestimmte Dienstleistungen und Bereiche sowie Anlagenkategorien einschließlich Schwellenwerte benannt, die für die Versorgung besonders relevant und daher besonders gegen Cyberangriffe zu schützen sind. Überdies liegt es vor allem und auch gerade im Interesse der Industrie, selbst und dauerhaft Schutzmaßnahmen gegen diese Gefahren zu entwickeln. Diese Vorsorge findet bereits in den Unternehmen statt.

b) Gesundheit (insbesondere Krankenhäuser),

c) Staat und Verwaltung,

d) Ernährung,

e) Transport und Verkehr,

f) Finanz- und Versicherungswesen,

g) Informationstechnik- und Telekommunikation und

h) Wasser?

Zur Beantwortung der Frage wird auf die beigefügte Anlage (Excel-Tabelle) verwiesen.

i) Welche anderen öffentlichen Einrichtungen (z. B. Polizei, Feuerwehr) sind besonders Ziel von Hackerattacken?

Der Bundesregierung liegen hierzu keine Informationen vor.

2. Wie viele erfolgreiche Hackerangriffe gab es in den Jahren 2015, 2016, 2017, 2018, 2019 und 2020 auf folgende Einrichtungen in der Bundesrepublik Deutschland (bitte pro Sektor nach Anlagenkategorien aufschlüsseln):

Nur für die Betreiber Kritischer Infrastrukturen besteht bei festgestellten Störungen eine Verpflichtung zur Meldung an das Bundesamt für Sicherheit in der Informationstechnologie (BSI) gemäß § 8b Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG).

Unter dem Begriff Hackerangriffe wurden folgende Sachverhalte erfasst:

– Ausnutzung von Schwachstellen
– Hacking und Manipulationen
– Schadprogramme (Malware)
– Gezielte, mehrstufige kombinierte Angriffe (APT-Angriffe)
– Verhinderung von Diensten

a) Energie,

Energie (nach IT-Sicherheitsgesetz [IT-SIG])

2016: 3

2017: 7

2018: 4

2019: 10

2020: 26

b) Gesundheit (insbesondere Krankenhäuser),

Gesundheit (nach IT-SIG)

2016: 2

2017: 1

2018: 11

2019: 16

2020: 43

c) Staat und Verwaltung,

Staat und Verwaltung (nach SOFORT-Meldung)

2019: 63

2020: 70

d) Ernährung,

Ernährung (nach IT-SIG)

2016: 0

2017: 2

2018: 0

2019: 2

2020: 2

e) Transport und Verkehr,

Transport und Verkehr (nach IT-SIG)

2016: 2

2017: 1

2018: 28

2019: 10

2020: 8

f) Finanz- und Versicherungswesen,

Finanzen und Versicherungswesen (nach IT-SIG)

2016: 0

2017: 0

2018: 8

2019: 6

2020: 11

g) Informationstechnik- und Telekommunikation und

Informationstechnik- und Telekommunikation

2016: 1

nach IT-SIG: 0

nach TKG: 1

2017: 1

nach IT-SIG: 1

nach TKG: 0

2018: 9

nach IT-SIG: 0

nach TKG: 9

2019: 12

nach IT-SIG: 4

nach TKG: 8

2020: 4

nach IT-SIG: 1

nach TKG: 3

h) Wasser?

Wasser (nach IT-SIG)

2016: 3

2017: 2

2018: 2

2019: 2

2020: 7

i) Wie viele Hackerangriffe sind davon jeweils zur Anzeige gebracht worden?

Der Bundesregierung liegen dazu keine Erkenntnisse vor.

3. Wie viele Ermittlungsverfahren und Hauptverfahren wurden in den Jahren 2015, 2016, 2017, 2018, 2019 sowie 2020 eingeleitet?

   a) Wie viele Ermittlungsverfahren wurden in den Jahren 2015, 2016, 2017, 2018, 2019 und 2020 eingestellt?

   b) Wie viele Personen wurden 2015, 2016, 2017, 2018, 2019 und 2020 rechtskräftig verurteilt (bitte nach Straftatbestand aufschlüsseln)?

Der Bundesregierung liegen hierzu keine für statistisch vergleichende Betrachtungen im Anfragezeitraum geeigneten Informationen vor; es werden keine Statistiken zu in Deutschland eingeleiteten Ermittlungs- und Hauptverfahren, eingestellten Ermittlungsverfahren und rechtskräftig verurteilten Personen geführt. Belastbares Zahlenmaterial kann anhand der der Bundesregierung zur Verfügung stehenden Datenbasis nicht zugeliefert werden.

   c) Wie viele Meldungen wurden dem BSI gemäß der Meldepflicht nach § 8b Absatz 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) in den Jahren 2015, 2016, 2017, 2018, 2019 und 2020 gemeldet?

Hier wird auf die Beantwortung zu Frage 2a-h verwiesen.

4. Hat die Bundesregierung Erkenntnisse über die vermutete Dunkelziffer von Hackerangriffen auf die oben genannten kritischen Infrastrukturen?

Die Bundesregierung hat keine Erkenntnisse über die vermutete Dunkelziffer von Hackerangriffen auf die oben genannten kritischen Infrastrukturen.

Verschiedenste Studien und Unternehmensbefragungen unterstreichen die wiederholt im Bundeslagebild Cybercrime (vgl. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html) getroffene Einschätzung, wonach im Bereich der Cybercrime allgemein aber auch im Bereich der Angriffe auf Kritische Infrastrukturen im Speziellen von einem hohen Dunkelfeld ausgegangen werden muss.

Beispielhaft kann hier der 2020 publizierte Forschungsbericht Nr. 152 „Cyberangriffe gegen Unternehmen in Deutschland – Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019“ des Kriminologischen Forschungsinstituts (KFI) Niedersachsen e.V. angeführt werden (vgl. https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf). Demzufolge werden nur 11,9 Prozent der schwerwiegenden Cyberangriffe angezeigt. Auch diese Studie stellt nicht explizit auf KRITIS-Unternehmen ab.

5. Hat die Bundesregierung Erkenntnisse darüber, auf wie hoch sich der finanzielle Schaden aufgrund von Ransomware und erfolgreichen Hackerattacken in den letzten fünf Jahren von folgenden Einrichtungen beziffert:

   a) Krankenhäuser,

   b) Energieversorger,

   c) Polizei und

   d) Feuerwehr?

In der Polizeilichen Kriminalstatistik (PKS) werden finanzielle Schäden im Bereich Cybercrime lediglich bei den Delikten Computerbetrug (ca. 87,7 Millionen Euro in 2019) und missbräuchlicher Nutzung von Telekommunikationsanlagen (ca. 0,3 Millionen Euro in 2019) erfasst. Die Bundesregierung führt keine

darüber hinausgehenden Statistiken zu finanziellen Schäden durch Ransomware-Angriffe auf die aufgeführten Einrichtungen.

Der Bundesverband Informationssicherheit, Telekommunikation und neue Medien e.V (bitkom) bezifferte in seinem Studienbericht 2020 „Spionage, Sabotage und Datenbiebstahl – Wirtschaftsschutz in der vernetzten Welt“ die Schäden, die im Jahr 2019 durch Cyberangriffe verursacht wurden, auf über 100 Milliarden Euro pro Jahr; dies stellt nahezu eine Verdopplung gegenüber dem Untersuchungszeitraum 2017/2018 (55 Milliarden Euro) dar.

6. Wie lange brauchen folgende Einrichtungen, um nach erfolgreichen Hackerangriffen aus dem Notbetrieb wieder in den ursprünglichen Normalbetrieb zu kommen (bitte Dauer in Stunden nennen):

   a) Krankenhäuser,

   b) Energieversorger,

   c) Polizei und

   d) Feuerwehr?

Hierzu liegen dem BSI keine belastbaren Statistiken vor.

Hintergrund hierfür ist, dass:

– die Daten nur selten von den Betreibern geliefert werden und der Datensatz daher recht klein ist,

– einzelne Ausreißer (z. B. APT-Vorfälle, die über Monate gehen), den Durchschnittswert stark beeinflussen,

– der tatsächliche Beginn einer Störung den Betreibern selbst oft nur grob bekannt ist.

Grundsätzlich hängt die Zeit, die es braucht, um von einem Notbetrieb in einen Normalbetrieb zu gehen, von vielen Faktoren ab. Hierzu zählen Tiefe der Kompromittierung, Komplexität der vorhandenen Netzwerkinfrastruktur, die vorhandene Datenmenge und verfügbaren Personalressourcen. In vielen Fällen ist es ein Ziel, aus dem Notbetrieb eben nicht wieder 1:1 in den ursprünglichen Normalbetrieb zu wechseln, sondern gleichzeitig auch wirksamere Schutzmaßnahmen oder neue Softwareversionen einzuführen. Dies kann die Zeit bis zur Wiederherstellung des Normalbetriebes zwar verlängern, erhöht aber die Widerstandsfähigkeit der Systeme gegen zukünftige Angriffe.

Grundsätzlich dauert eine Rückkehr nach erfolgreichen Hackerangriffen in den Normalbetrieb nicht Stunden, sondern vielmehr eine bis oftmals mehrere Wochen.

7. Wie viele Fälle von Ransomware sind der Bundesregierung in den Jahren 2015, 2016, 2017, 2018, 2019 und 2020 bekannt?

Belastbares Zahlenmaterial zu der Anzahl von Ransomware-Angriffen seit 2015 können seitens der Bundesregierung nicht zugeliefert werden.

Generell kann festgestellt werden, dass sich in den letzten Jahren der Trend von zielgerichteten, hochprofessionellen Ransomware-Angriffen fortsetzt, so u. a. auch im Oktober 2019 beim Angriff auf das Berliner Kammergericht Berlin. Wie im Bundeslagebild Cybercrime 2019 ausgeführt, hat die Intensität solcher Angriffe im Jahr 2019 weiter zugenommen.

Die Bundesregierung führt keine systematische Erfassung von Ransomware-Angriffen durch. Die Polizeiliche Kriminalstatistik bietet ebenfalls keine dezidierte Aufschlüsselungsmöglichkeit nach Ransomware-Fällen.

Im IT-Sicherheitsgesetz von 2015 wurde eine Meldepflicht für Betreiber Kritischer Infrastrukturen für Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt haben oder führen können, eingeführt. Es handelt sich hierbei nicht zwingend um Angriffe, sondern um gemeldete Vorfälle, da auch beispielsweise Störungen aufgrund von Soft- oder Hardwareausfällen oder Konfigurationsfehlern meldepflichtig sind. Demnach wurden in Kritischen Infrastrukturen zwischen Juni 2019 und Mai 2020 419 Störungen an das BSI gemeldet.

Aktuelle diesbezügliche Zahlen werden jährlich in den BSI-Lageberichten zur IT-Sicherheit in Deutschland veröffentlicht, die unter folgender Adresse abgerufen werden können: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html

Juni 2019 bis Mai 2020: 419 Meldungen (S. 54, Jahreslagebericht 2020)

Juni 2018 bis Mai 2019: 252 Meldungen (S. 47, Jahreslagebericht 2019)

Juni 2017 bis Mai 2018: 145 Meldungen (S. 10, Jahreslagebericht 2018)

Einführung der Meldepflicht bis Juni 2017: 34 Meldungen (S. 10, Jahreslagebericht 2017).

a) Sind der Bundesregierung Fälle von Ransomware oder erfolgreichen Hackerattacken auf Gerichte bekannt (falls ja, bitte nach Bundesländern aufschlüsseln)?

Der Bundesregierung ist der Hackerangriff mittels Trojaner „Emotet“ vom 25. September 2019 im Bundesland Berlin bekannt.

8. Hat die Bundesregierung Erkenntnisse über den Tatort von erfolgreichen Hackerangriffen in den letzten fünf Jahren (bitte nach Land auflisten)?

   Gibt es Indizien bzw. Anhaltspunkte, ob Einzelpersonen oder kriminelle Organisationen bzw. Netzwerke dahinterstecken?

Generell ist dem Phänomenbereich Cybercrime immanent, dass der Ort der Tathandlung in den allermeisten Fällen nicht konkretisierbar ist. Die konkrete Lokalisierung der Cybertäter gestaltet sich aufgrund des Handlungsraums Internet schwierig.

Die zur Verfügung stehende Polizeiliche Kriminalstatistik stellt folgerichtig bei der Erfassung der Cyberdelikte auf den Erfolg der Handlung (Erfolgseintritt) ab. Konkrete Erkenntnisse zum eigentlichen „Tatort“ können hieraus nicht abgeleitet werden.

Nach Erkenntnislage der Bundesregierung herrscht im Phänomenbereich „Cybercrime-as-a-Service“ (CCaaS; Cyberstraftat als Dienstleistung) eine hohe Arbeitsteilung zwischen den Tatbeteiligten und eine Spezialisierung Einzelner auf ausgewählte relevante Tatteilbeiträge vor. Cyberkriminelle fokussieren sich vermehrt auf eine auftragsorientierte Begehung bzw. dienstleistungsorientierte Ermöglichung von Straftaten. So wurde festgestellt, dass aktive Straftäter einzelne Tatbeiträge an Außenstehende und auf bestimmte Cybercrime-Dienstleistungen spezialisierte Tätergruppen auslagern bzw. von diesen ankaufen. Die da-

mit einhergehende Zergliederung ermöglicht es auch weniger Cyberaffinen Straftätern, technisch komplexere Straftaten zu realisieren.

9. Welche Schutzmaßnahmen sind nach Auffassung der Bundesregierung notwendig, um vernetzte Autos vor Hackerangriffen z. B. auf das Verschließsystem besser zu schützen?

Grundsätzlich sind Maßnahmen zu ergreifen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen und dabei auf den konkreten Fall zugeschnitten sind, z. B. durch bestimmte Standardisierung oder technische Anforderungen. Weitere Maßnahmen sollten auch die Sensibilisierung und Wissensvermittlung der Öffentlichkeit umfassen.

Im Bereich der Typgenehmigung wurde unter aktiver Mitarbeit des Bundesministeriums für Verkehr und digitale Infrastruktur bei der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE) im Juni 2020 die UN-Richtlinie UN-R 155 verabschiedet. Die Richtlinie stellt im Rahmen der Typzulassung Anforderungen an die IT-Sicherheit in Kraftfahrzeugen auf drei verschiedenen Ebenen:

1. Hersteller müssen ein IT-Sicherheits-Management System und die gewissenhafte Berücksichtigung von IT-Sicherheitskonzepten in der Entwicklung, der Produktion und dem Betrieb von Fahrzeugen nachweisen. Dieser Nachweis wird zu einer Grundvoraussetzung für die Typgenehmigung von Fahrzeugtypen.
2. Die Umsetzung von IT-Sicherheitsmaßnahmen in der elektronischen Architektur von Fahrzeugtypen wird Teil der Typgenehmigung.
3. Die Marktüberwachung von typgenehmigten Fahrzeugen wird um die Überwachung von IT-Sicherheit erweitert.

a) Wie viele Fälle von erfolgreichen Hackerangriffen im Automobilsektor sind der Bundesregierung bekannt?

Der Bundesregierung liegen hierzu keine Informationen vor. Eine statistische Erfassung dieser Cyberdelikte erfolgt derzeit nicht.

b) Befasst sich die Bundesregierung mit der wachsenden Gefahr von DDoS-Attacken (DDoS = Distributed Denial of Service) auf vernetzte Autos insbesondere bei der Einführung von 5G-Netzen?

Die Bundesregierung befasst sich grundsätzlich und fortwährend mit verschiedenen Themen, die die IT-Sicherheit von Kraftfahrzeugen betreffen. Im Übrigen wird auf die Antwort zu Frage 9 bezüglich der Aktivitäten auf Ebene der UNECE verwiesen.

c) Wie viele vernetzte Autos werden in den nächsten fünf Jahren voraussichtlich in Deutschland und in der EU unterwegs sein?

Angaben zu einer zukünftigen Marktdurchdringung können auch mit Blick auf die unklare Entwicklung der Zulassungszahlen durch die Bundesregierung nicht gemacht werden.

Kleine Anfrage des Abgeordneten Dr. Jürgen Martens u. a. und der Fraktion der AfD
Anfälligkeit kritischer Infrastrukturen vor Hackerangriffen in Deutschland
BT-Drucksache 19/23851

Frage 1
Welche Erkenntnis hat die Bundesregierung zur Anfälligkeit von IT-Systemen gegenüber Hackerangriffen folgender kritischer Infrastrukturen in der Bundesrepublik Deutschland? (bitte pro Sektor nach Anlagenkategorien aufschlüsseln)
b. Gesundheit (insbesondere Krankenhäuser)
c. Staat und Verwaltung
d. Ernährung
e. Transport und Verkehr
f. Finanz- und Versicherungswesen
g. Informationstechnik - und Telekommunikation
h. Wasser

Frage 1	Sektor	Anlagen-kategorie	Erkenntnisse zur Anfälligkeit von IT-Systemen vor Hackangriffen
b.	Gesundheit	1.1 Krankenhaus	Anfälligkeit von IT-Systemen aufgrund des Einsatzes von Medizingerätetechnik mit teilw. veralteten Betriebssystemen in einer zertifizierten Laufzeitumgebung sowie Anfälligkeiten in bezug auf die physische Sicherheit im Krankenhaus (offener Betrieb, offenes Haus). Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie die direkte Netzanbindung von Fachabteilungen/MVZs sowie im Bereich der Universitätskliniken von Forschung und Lehre, welche letztendlich einen nicht gänzlich geschlossenen Perimeter zur Folge haben.
		2.1.1 Produktionsstätte für unmittelbar lebenserhaltende Medizinprodukte, die Verbrauchsgüter sind	Diese Anlagenkategorie ist geprägt von industriellen Kontrollsystemen (ICS). Diese verfügen oftmals aufgrund langer Investitionszyklen über nicht mehr aktuelle Software- und Betriebssystemsversionen, welche nicht aktualisiert werden können.
		2.2.1 Abgabestelle	Keine registrierte Anlage in Deutschland
		3.1.1 Produktionsstätte für verschreibungspflichtige Arzneimittel zur Anwendung im oder am menschlichen Körper	Diese Anlagenkategorie ist geprägt von industriellen Kontrollsystemen (ICS). Diese verfügen oftmals aufgrund langer Investitionszyklen über nicht mehr aktuelle Software- und Betriebssystemsversionen, welche nicht aktualisiert werden können.
		3.1.2 Anlage oder System zur Steuerung von Entnahme und Weiterverarbeitung von Blut- oder Plasmaspenden zur Anwendung im oder am menschlichen Körper	Anfälligkeit von IT-Systemen vor Hackerangriffen aufgrund des Einsatzes von Medizingerätetechnik mit teilw. veralteten Betriebssystemen in einer zertifizierten Laufzeitumgebung
		3.2.1 Betriebs- und Lagerraum	Diese Anlagenkategorie ist geprägt von industriellen Kontrollsystemen (ICS). Diese verfügen oftmals aufgrund langer Investitionszyklen über nicht mehr aktuelle Software- und Betriebssystemsversionen, welche nicht aktualisiert werden können.
		3.2.2 Anlage oder System zum Vertrieb von verschreibungspflichtigen Arzneimitteln	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		3.3.1 Apotheke	Keine registrierte Anlage in Deutschland
		4.1.1 Transportsystem	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte.
		4.1.2 Kommunikationssystem zur Auftrags- und Befundübermittlung	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		4.2.1 Labor	Anfälligkeit von IT-Systemen vor Hackerangriffen aufgrund des Einsatzes von Medizingerätetechnik mit teilw. veralteten Betriebssystemen in einer zertifizierten Laufzeitumgebung.
c.	Staat und Verwaltung	Bundesverwaltung	Ergänzend zur allgemeinen IT-Bedrohungslage besteht die Bedrohung durch staatliche Stellen. In den Regierungsnetzen werden zentral Schutzmaßnahmen eingesetzt, um die Bedrohungslage zu mitigieren.
		Landesverwaltung	Ergänzend zur allgemeinen IT-Bedrohungslage besteht die grundsätzliche Bedrohung durch staatliche Stellen.
d.	Ernährung	Anlage zur Herstellung von Lebensmitteln	Diese Anlagenkategorie ist geprägt von industriellen Kontrollsystemen (ICS). Diese verfügen oftmals aufgrund langer Investitionszyklen über nicht mehr aktuelle Software- und Betriebssystemsversionen, welche nicht aktualisiert werden können.
		Anlage zur Behandlung von Lebensmitteln	Diese Anlagenkategorie ist geprägt von industriellen Kontrollsystemen (ICS). Diese verfügen oftmals aufgrund langer Investitionszyklen über nicht mehr aktuelle Software- und Betriebssystemsversionen, welche nicht aktualisiert werden können.
		Anlage oder System zur Distribution von Lebensmitteln	Diese Anlagenkategorie ist geprägt von industriellen Kontrollsystemen (ICS). Diese verfügen oftmals aufgrund langer Investitionszyklen über nicht mehr aktuelle Software- und Betriebssystemsversionen, welche nicht aktualisiert werden können.
		Anlage oder System zur zentralen standortübergreifenden Steuerung	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Anlage zur Behandlung von Lebensmitteln	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Anlage oder System zur Distribution von Lebensmitteln	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Anlage oder System zur Bestellung von Lebensmitteln	Hier gilt die allgemeine IT-Bedrohungslage, bei exponierten Systeme dieser Anlagenkategorie besteht eine Verwundbarkeit gegenüber DDoS Angriffen.
		Anlage zum Inverkehrbringen von Lebensmitteln	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Anlage oder System zur zentralen standortübergreifenden Steuerung	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
e.	Transport und Verkehr	Anlage oder System zur Passagierabfertigung an Flugplätzen	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Anlage oder System zur Frachtabfertigung an Flugplätzen	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Infrastrukturbetrieb eines Flugplatzes	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Flugsicherung und Luftverkehrskontrolle	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Personenbahnhof der Eisenbahn	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Güterbahnhof	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte.
		Zugbildungsbahnhof	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte.
		Schienennetz und Stellwerke der Eisenbahn	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte.
		Verkehrssteuerungs- und Leitsystem der Eisenbahn	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		Leitzentrale der Eisenbahn	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Anlage oder System zum Betrieb von Bundeswasserstraßen	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		Verkehrssteuerungs- und Leitsystem der See- und Binnenschifffahrt	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		Leitzentrale von Betreibern und Verkehrsunternehmen der Seeschifffahrt	Hier gilt die allgemeine IT-Bedrohungslage insbesondere anfällig für zB. DDoS-Angriffe, da es sich um teilweise exponierte Systeme handelt.
		Anlage oder System zur Disposition von Binnenschiffen (nur Güterverkehr)	Keine registrierte Anlage in Deutschland
		Verkehrssteuerungs- und Leitsystem	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		Schienennetz und Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV)	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		Verkehrssteuerungs- und Leitsystem des ÖPNV	Keine registrierte Anlage in Deutschland
		Leitzentrale des ÖSPV (Betreiber, Verkehrsunternehmen)	Die Systeme bestehen in der Regel aus Komponenten eines Herstellers oder nur weniger Hersteller. Durch die zentrale Funktion der Systeme ergeben sich sehr lange Laufzeiten und eine Abhängigkeit zu diesen Herstellern und zu den IT-Sicherheitsfunktionalitäten der Produkte. Ebenfalls Anfälligkeiten durch die Netzanbindung externer Dienstleister sowie von Kunden, Partnern und eigenen Niederlassungen.
		Anlage oder System zum Betrieb eines Logistikzentrums in den Segmenten Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik	Hier gilt die allgemeine IT-Bedrohungslage insbesondere anfällig für zB. DDoS-Angriffe, da es sich um teilweise exponierte Systeme handelt.
		Anlage oder IT-System zur Logistiksteuerung oder -verwaltung in den Segmenten Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik	Hier gilt die allgemeine IT-Bedrohungslage insbesondere anfällig für zB. DDoS-Angriffe, da es sich um teilweise exponierte Systeme handelt.
		Anlage zur Wettervorhersage, zur Gezeitenvorhersage oder zur Wasserstandsmeldung	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
		Satellitennavigationssystem	Hier gilt die allgemeine IT-Bedrohungslage, keine spezifischen Verwundbarkeiten.
f.	Finanz- und Versicherungswesen	Autorisierungssystem	Systeme zur Autorisierung und zur Anbindung an Autorisierungssysteme, sowie des Einbringens in den Zahlungsverkehr und zur Anbindung an Interbanken-Zahlungsverkehrssysteme sind nach Erkenntnissen des BSI typischerweise sehr gut mit Vorkehrungen im Bereich der IT-Sicherheit nach dem Stand der Technik geschützt. In den meisen Fällen liegen zudem Zertifizierungen nach ISO 27001 bzw. PCI-DSS vor bzw. es werden spezielle, abgesicherte Protokolle zur Übertragung genutzt.
		System zur Anbindung an ein Autorisierungssystem aus Sicht des Geldautomatenbetreibers	
		System zur Aufbereitung durch den Geldautomatenbetreiber	
		System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)	
		Clearing-System	Clearing-Systeme, Settlement-Systeme und Kontoführungssysteme weisen hohe Reifegrade in Bezug auf IT-Sicherheit auf.
		Settlement-System	
		Kontoführungssystem	
		Cash Center	Die unter die BSI-Kritis-V fallenden Cash-Center und IT-Systeme für das Cash-Management sind angehalten IT-Sicherheit nach dem Stand der Technik umzusetzen. Diese Umsetzung wird vom BSI im Rahmen der Nachweisprüfung überprüft. IT-Sicherheit wird in diesen Bereichen sehr verlässlich umgesetzt.
		IT-System für das Cash-Management	
		System zur Anbindung an ein Autorisierungssystem aus Sicht des Terminalbetreibers	siehe Systeme zur Anbindung an Autorisierungssysteme
		System zur Aufbereitung durch den POS-Terminalbetreiber	
		System zur Annahme der POS-Transaktionsdaten beim Zahlungsdienstleister des Zahlungsempfängers	siehe Clearing-, Settlement-, Kontoführungssysteme
		System zur Annahme einer Überweisung oder Lastschrift	Anlagen zur Annahme von Überweisungen und Lastschriften, die bspw. Online-banking Systeme umfassen, sind wegen der offensichtlichen direkten Sichtbarkeit mehrfach im Fokus von DDoS-Angriffen
		System einer Clearingstelle oder zentralen Gegenpartei zur Verrechnung von Wertpapier- und Derivatgeschäften	siehe Clearing-, Settlement-, Kontoführungssysteme
		System zur Anbindung für die Verrechnung und Verbuchung von Wertpapier- und Derivatgeschäften	siehe System zur Annahme einer Überweidung oder Lastschrift
		Wertpapier-Settlement-System	siehe Clearing-, Settlement-, Kontoführungssysteme
		Depotführungssystem	
		System eines Zentralverwahrers	
		System zur Aufbereitung der Zahlungsanweisung	keine registrierte Anlage in Deutschland
		Vertragsverwaltungssystem (Lebensversicherung)	Die Betreiber der unter die BSI-Kritis-V fallenden Systeme im Bereich der Versicherungsdienstleistungen sind angehalten, IT-Sicherheit nach dem Stand der Technik, z.B. nach branchenspezifischen Sicherheitsstandards (B3S) umzusetzen. Diese Umsetzung wird vom BSI im Rahmen der Nachweisprüfung überprüft. Damit ließ sich feststellen, dass die IT-Sicherheit einen höheren Stellenwert gewonnen hat und berücksichtigt wird.
		Vertragsverwaltungssystem (private Krankenversicherung)	
		Vertragsverwaltungssystem (Komposit)	
		Leistungssystem (Lebensversicherung)	
		Leistungssystem (Sozialversicherungsträger der gesetzlichen Renten-, Unfall- und Arbeitslosenversicherung)	
		Leistungssystem (private Krankenversicherung)	

		Schadensystem (Komposit)	
		Auszahlungssystem (Lebensversicherung)	
		Auszahlungssystem (Sozialversicherungsträger der gesetzlichen Renten-, Unfall- und Arbeitslosenversicherung)	
		Auszahlungssystem (private Krankenversicherung)	
		Auszahlungssystem (Komposit)	
		Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung	
g.	IT+TK	Zugangsnetz	Anfällig insbesondere für DDoS-Angriffe, da es sich um exponierte Systeme handelt.
		Übertragungsnetz	
		IXP	
		DNS-Resolver	
		autoritative DNS-Server	
		Rechenzentrum (Housing)	Geringere Anfälligkeit, da die Systeme nicht idR exponiert sind.
		Serverfarm (Hosting)	Anfällig insbesondere für DDoS-Angriffe, da es sich um exponierte Systeme handelt.
		Content Delivery Netwerk	Geringere Anfälligkeit, da das Gesamtsystem robust konzipiert ist.
		Anlage zur Erbringung von Vertrauensdiensten	Geringere Anfälligkeit, da die Systeme idR nicht exponiert sind. Einzig die Systeme zur Auftragserteilung und Download der Zertifikate sowie die Sperrliste könnten anfällig für DDoS Angriffe sein.
h.	Wasser	Kanalisation	siehe Leitzentrale, da in gegenseitiger Abhängigkeit stehend
		Kläranlage	siehe Leitzentrale, da in gegenseitiger Abhängigkeit stehend
		Leitzentrale (Abwasser)	Die unter die BSI-Kritis-V fallenden Abwasserbeseitigungsanlagen sind angehalten IT-Sicherheit nach dem Stand der Technik, z.B. nach dem branchenspezifischen Sicherheitsstandard (B3S) umzusetzen. Diese Umsetzung wird vom BSI im Rahmen der Nachweisprüfung überprüft. Damit ließ sich feststellen, dass über die Jahre hier die IT-Sicherheit stark zugenommen hat und die Anfälligkeit der IT-Systeme gegenüber Angriffen deutlich zurück gegangen ist.
		Gewinnungsanlage (Wasserwerk)	siehe Leitzentrale, da in gegenseitiger Abhängigkeit stehend
		Aufbereitungsanlage (Wasserwerk)	siehe Leitzentrale, da in gegenseitiger Abhängigkeit stehend
		Wasserverteilungssystem	siehe Leitzentrale, da in gegenseitiger Abhängigkeit stehend
		Leitzentrale (Trinkwasser)	Die unter die BSI-Kritis-V fallenden Einrichtungen zur Trinkwasserversorgung sind angehalten IT-Sicherheit nach dem Stand der Technik, z.B. nach dem branchenspezifischen Sicherheitsstandard (B3S) umzusetzen. Diese Umsetzung wird vom BSI im Rahmen der Nachweisprüfung überprüft. Damit ließ sich feststellen, dass über die Jahre hier die IT-Sicherheit stark zugenommen hat und die Anfälligkeit der IT-Systeme gegenüber Angriffen deutlich zurück gegangen ist.

Autorisierungssystem

System zur Anbindung an ein Autorisierungssystem aus Sicht des Geldautomatenbetreibers

System zur Aufbereitung durch den Geldautomatenbetreiber

System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)

Clearing-System

Settlement-System

Kontoführungssystem

Cash Center

IT-System für das Cash Management

System zur Anbindung an ein Autorisierungssystem aus Sicht des Terminalbetreibers

System zur Aufbereitung durch den POS-Terminalbetreiber

System zur Annahme der POS-Transaktionsdaten beim Zahlungsdienstleister des Zahlungsempfängers

System zur Annahme einer Überweisung oder Lastschrift

System einer Clearingstelle oder zentralen Gegenpartei zur Verrechnung von Wertpapier- und Derivatgeschäften

System zur Anbindung für die Verrechnung und Verbuchung von Wertpapier- und Derivatgeschäften

Wertpapier-Settlement-System

Depotführungssystem

System eines Zentralverwahrers

System zur Aufbereitung der Zahlungsanweisung

Vertragsverwaltungssystem (Lebensversicherung)

Vertragsverwaltungssystem (private Krankenversicherung)

Vertragsverwaltungssystem (Komposit)

Leistungssystem (Lebensversicherung)

Leistungssystem (Sozialversicherungsträger der gesetzlichen Renten-, Unfall- und Arbeitslosenversicherung)

Leistungssystem (private Krankenversicherung)

Schadensystem (Komposit)

Auszahlungssystem (Lebensversicherung)

Auszahlungssystem (Sozialversicherungsträger der gesetzlichen Renten-, Unfall- und Arbeitslosenversicherung)

Auszahlungssystem (private Krankenversicherung)

Auszahlungssystem (Komposit)

Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333