Deutscher Bundestag **Drucksache 19/21675**

19. Wahlperiode 17.08.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Reinhard Houben, Michael Theurer, Dr. Marcel Klinge, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/21476 –

Cybersicherheit im deutschen Mittelstand

Vorbemerkung der Fragesteller

Deutsche Unternehmen, auch KMUs (kleine und mittlere Unternehmen), sehen sich zunehmend mit Cyberangriffen und Datendiebstahl konfrontiert. Laut einer Studie („Wirtschaftsschutz in der digitalen Welt“) des Digitalverbands Bitkom wurden 2019 drei von vier Unternehmen Opfer von Sabotage, Datendiebstahl oder Spionage. Durch die Angriffe (analog und digital) entsteht der deutschen Wirtschaft jährlich ein Schaden von 102,9 Mrd. Euro. Damit hat sich der Schaden seit 2016 nahezu verdoppelt (2016/2017: 55 Mrd. Euro p. a.). So haben digitale Angriffe in den vergangenen beiden Jahren bei 70 Prozent der Unternehmen einen Schaden verursacht, im Jahr 2017 waren es erst 43 Prozent.

So gaben 21 Prozent der Unternehmen an, dass sensible digitale Daten abgeflossen sind, bei 17 Prozent wurden Informationssysteme und Produktionssysteme oder Betriebsabläufe digital sabotiert, und bei 13 Prozent wurde die digitale Kommunikation ausgespäht. Dennoch spielen analoge Angriffe nach wie vor eine große Rolle. Bei 32 Prozent wurden IT-Geräte oder Telekommunikationsgeräte gestohlen, sensible Dokumente, Maschinen oder Bauteile wurden bei jedem sechsten entwendet. Ein wachsendes Problem ist demnach „Social Engineering“. Hierbei werden Mitarbeiter dazu gebracht, sensible Informationen preiszugeben, mit denen man beispielsweise Schadsoftware auf Firmenrechner installieren konnte. 22 Prozent der befragten Unternehmen waren davon analog betroffen, 15 Prozent digital.

Lediglich bei 13 Prozent der Unternehmen gab es Hinweise auf Delikte durch externe Strafverfolgungsbehörden oder Aufsichtsbehörden. Eine dramatische Mehrheit der Unternehmen (96 Prozent) fordern deswegen eine engere Zusammenarbeit mit Staat und Behörden. Außerdem fordern sie mehr Unterstützung durch die Behörden bei Fragen der IT-Sicherheit. 91 Prozent der Unternehmen sehen die Notwendigkeit von Verbesserung beim Informationsaustausch zwischen staatlichen Stellen. Die breite Mehrheit der Unternehmen (82 Prozent) sieht in Zukunft eine Verschärfung der Sicherheitslage und gehen von einer Zunahme der Cyberangriffen auf die Unternehmen aus (https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 17. August 2020 übermittelt.

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

Im Jahr 2015 wurde das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ verabschiedet. An einem Nachfolger, dem IT-Sicherheitsgesetz 2.0, wird seit zwei Jahren gearbeitet. Bereits 2018 verkündete der Bundesminister des Innern, für Bau und Heimat, Horst Seehofer, die Einführung des Gesetzes. Der Cybersicherheitsrat wurde mit der Cybersicherheitsstrategie 2011 errichtet und mit der Cybersicherheitsstrategie 2016 reformiert, bleibt aber bis heute, laut Medienberichten, eine „leere Hülle“. Das Nationale Cyber-Abwehrzentrum sollte ursprünglich alle operativen Akteure der Cybersicherheit in Deutschland (Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundeskriminalamt und Bundeswehr) zusammenbringen. „Bis heute wurde versäumt, die Plattform auf eine vernünftige rechtliche Grundlage zu stellen. Diese sollte unter anderem regeln, welche Informationen ausgetauscht werden können, dürfen und müssen. Seit Jahren werden Reformen angestrebt, die getrost als gescheitert angesehen werden können“, schreibt netzpolitik.org (https://netzpolitik.org/2020/eine-vertane-chance-fuer-die-it-sicherheit-in-deutschland/#spendenleiste). Auf diese Defizite machte die Fraktion der FDP bereits im Februar 2019 aufmerksam (vgl. Bundestagsdrucksache 19/7698).

Unter dem Titel „Mehr Sicherheit für die digitale Transformation“ veröffentlichte der „Weisenrat für Cybersicherheit“ am 6. Juni 2020 seinen ersten Jahresbericht. Im Bericht spricht der Weisenrat acht Handlungsempfehlungen für Politik und Wirtschaft aus, die als Entscheidungshilfe zur Gestaltung gesetzlicher Rahmenbedingungen verstanden werden können. Das Cyber Security Cluster Bonn hat den unabhängigen Weisenrat für Cybersicherheit 2019 ins Leben gerufen, um einen weiteren Beitrag zur Immunisierung der Gesellschaft gegen Cyberattacken zu leisten (https://cyber-security-cluster.eu/_Resources/Persistent/a/1/d/9/a1d95dca3a8642822f22eb1372cd2b66e271d4fe/Mehr%20Sicherheit%20f%C3%BCr%20die%20digitale%20Transformation%20-%20Jahresbericht%20des%20Weiserats%20f%C3%BCr%20Cyber-Sicherheit.pdf).

1. Welcher besonderen Gefahr sieht die Bundesregierung mittelständische Unternehmen durch Cyberangriffe ausgesetzt?

Die Landschaft der mittelständischen Unternehmen ist heterogen ausgeprägt. Insoweit variiert auch das jeweils etablierte IT-Sicherheitsniveau. Die bei den mittelständischen Unternehmen zur Verfügung stehenden Ressourcen im IT-Bereich dienen in erster Linie der Aufrechterhaltung der Office- und Produktionssysteme. Das Thema IT-Sicherheit hat im Tagesgeschäft eines mittelständischen Unternehmens oftmals eine nachgeordnete Bedeutung. Um hier das Bewusstsein für Cybersicherheit zu verbessern, müssten Mitarbeiter entsprechend regelmäßig geschult werden. Diese Anforderungen können aber aus Budgetgründen und Personalmangel in den meisten Fällen nicht erfüllt werden, so dass Cyberangriffe auf kleine und mittelständische Unternehmen öfter erfolgreich sind als bei größeren Unternehmen.

Großer Risikofaktor für Cyberangriffe ist die Digitalisierung. Die damit einhergehenden technischen Möglichkeiten bieten für die Täter eine größere Angriffsfläche, wodurch die Angriffe spezifizierter werden. Organisatorische Maßnahmen werden in kleinen Unternehmen seltener eingesetzt als in größeren Unternehmen. In kleinen Unternehmen sind schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit sowie zum Notfallmanagement deutlich seltener vorhanden als in den großen Unternehmen (Forschungsbericht Cyberangriffe gehen Unternehmen in Deutschland, Kriminologisches Forschungsinstitut Niedersachsen (KFN) 2020). Kleine und mittlere Unternehmen (KMU) setzen organisatorische Maßnahmen deutlich seltener um als technische Maßnahmen. Nur jedes fünfte KMU in Deutschland hat bereits einmal eine IT-Sicherheitsanalyse durchgeführt, bei größeren Unternehmen ist es immerhin die Hälf-

te (Aktuelle Lage der IT-Sicherheit in KMU, Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH (WIK) 2017).

2. Welche Erkenntnisse liegen der Bundesregierung über den volkswirtschaftlichen Schaden durch Hackerangriffe in Deutschland vor?

Cyber-Angriffe auf Unternehmen in Deutschland verursachen nach einer Untersuchung des Digitalverbands Bitkom aus dem Jahr 2019 Schäden in Milliardenhöhe. Durch Sabotage, Spionage oder Datendiebstahl entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden in Höhe von 100 Milliarden Euro. Damit ist der Verlust durch analoge und digitale Angriffe fast doppelt so hoch wie vor zwei Jahren, als der IT-Branchenverband noch von 55 Milliarden Euro im Jahr ausging.

Für die Erstellung der Studie wurden mehr als 1.000 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Branchen befragt.

3. Inwiefern sind deutsche KMU im Vergleich zu großen Unternehmen in Deutschland nach Kenntnis der Bundesregierung gegen Cyberangriffe gewappnet?

Welchen Handlungsbedarf sieht die Bundesregierung hier vonseiten des Staates?

Die Bedrohungslage für die Cybersicherheit bei Unternehmen ist unabhängig von ihrer Größe heterogen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet nahezu täglich Cyber-Angriffe auf Unternehmen aller Größen und Branchen, demnach sind deutsche KMU ebenso Ziel von Cyber-Angriffen wie Großkonzerne. Gemäß der Cyber-Sicherheits-Umfrage, die das BSI im Rahmen der Allianz für Cybersicherheit im Betrachtungszeitraum 2018 durchgeführt hat, setzen KMU im Vergleich zu großen Unternehmen durchschnittlich weniger Präventionsmaßnahmen um. Dies betrifft zum Beispiel den Einsatz von Managementsystemen. (https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9)

4. Welche Möglichkeiten hat die Bundesregierung, mittelständische Unternehmen bei dem Schutz vor Cyberangriffen zu unterstützen?

Welche Verbesserungsmöglichkeiten sieht die Bundesregierung?

Das BSI hat in der jüngeren Vergangenheit vielfältige Angebote für KMU und andere Unternehmen geschaffen. Hierzu zählt zum Beispiel die Einrichtung von regionalen Verbindungsstellen durch das Nationale Verbindungswesen. So wird, unter anderem für Unternehmen, eine schnelle und direkte Kontaktaufnahme zu festen Ansprechpartnern ermöglicht. Außerdem wurden in Kooperation mit Verbänden branchenspezifische IT-Grundschutz-Profile realisiert, die insbesondere Unternehmen dabei unterstützen, den bewährten BSI IT-Grundschutz in der eigenen Organisation umzusetzen und somit das Cybersicherheitsniveau nachhaltig zu erhöhen.

Mit dem IT-Grundschutz des BSI kann eine Institution ein Managementsystem für Informationssicherheit (ISMS) aufbauen. Die in einem eigenen Leitfaden beschriebene Basis-Absicherung liefert hier einen effektiven und effizienten Einstieg für KMU. Plattform für vielfältige Aktivitäten ist häufig die Allianz für Cybersicherheit, über die das BSI der deutschen Wirtschaft aktuelle, kostenlose Informationen zum Thema Cybersicherheit zur Verfügung stellt. Hierzu

zählen einerseits verschiedene Veröffentlichungen zu Best Practices und aktuellen Bedrohungen, andererseits werden vielzählige Formate zum Austausch mit bzw. unter den deutschen Unternehmen geschaffen.

Außerdem bietet das Bundesministerium für Wirtschaft und Energie (BMWi) mit der Initiative „IT-Sicherheit in der Wirtschaft“ für kleine und mittelständische Unternehmen verschiedene Unterstützungsmöglichkeiten an, um den Schutz vor Cyber-Angriffen zu verbessern. Neben der Transferstelle „IT-Sicherheit im Mittelstand“ (TISiM, siehe Frage 10) werden zahlreiche Projekte gefördert, die das Ziel haben, KMU für die Gefahren und Herausforderungen der IT-Sicherheit zu sensibilisieren und sie dazu befähigen, ihr IT-Sicherheitsniveau realistisch einzuschätzen. Darunter sind Projekte, die sich an bestimmte Branchen richten, wie bspw. das Handwerk sowie Projekte, die mit neuen Ansätzen, wie bspw. Gamification KMU, die systematische Suche nach Risiken vermitteln. Zusammen mit den Fördermaßnahmen Digital Jetzt, Go-Digital, Mittelstand-Digital inkl. der 26 Mittelstand 4.0 Kompetenzzentren existiert ein breitgefächertes Angebot, um insbesondere KMU zu sensibilisieren und zu befähigen, sich besser vor Cyberangriffen zu schützen.

5. Welche politischen Maßnahmen plant die Bundesregierung in naher Zukunft zur Eindämmung von Cyberangriffen auf deutsche Unternehmen, insbesondere KMU?

Um die IT-Sicherheit in Deutschland zu stärken, erarbeitet die Bundesregierung derzeit den Entwurf des IT-Sicherheitsgesetz 2.0, stärkt die Sicherheitsbehörden, um die Abwehr von Cyberangriffen zu verbessern, und baut fortlaufend ihre Beratungsangebote aus (s. a. Antwort zu Frage 4). Zum 01.08.2020 ist zudem ein auf die Belange der KMU zugeschnittenes Referat im BSI eingerichtet worden. Hiermit soll die Durchdringung von Cybersicherheitsmaßnahmen in KMU besonders erhöht werden.

Auf Ebene der Europäischen Union (EU) begleitet die Bundesregierung derzeit die Evaluierung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit(NIS)-Richtlinie.

Im Anschluss an diese Evaluierung wird eine Fortschreibung der NIS-Richtlinie erfolgen, in der nach Vorstellung der Bundesregierung der Schutz von Unternehmen einen besonderen Stellenwert einnehmen wird. Auch setzte sich die Bundesregierung weiter für die Etablierung von Mindestsicherheitsanforderungen an die IT-Sicherheit für vernetze Geräte ein, um das Niveau der IT-Sicherheit insgesamt zu erhöhen.

Durch die angeführten Maßnahmen wird der Schutz von Unternehmen vor Cyberangriffen verbessert. Da sich Methoden und Techniken von Cyberangriffen stetig weiterentwickeln, ist die Fortschreibung von politischen Maßnahmen zur Erhöhung der Cybersicherheit ein stetiger Prozess in der Bundesregierung.

6. Welche Schlussfolgerungen zieht die Bundesregierung aus der Arbeit des „Weisenrats für Cybersicherheit“?

   Inwiefern gibt es Pläne für ein öffentliches Mandat des Weisenrats oder eines ähnlichen Sachverständigenrats für Cybersicherheit?

7. Welche Schlussfolgerungen zieht die Bundesregierung aus den acht Handlungsempfehlungen des „Weisenrats für Cybersicherheit“?

Die Fragen 6 und 7 werden gemeinsam beantwortet. Die Bundesregierung hat den Bericht des „Weisenrats für Cybersicherheit“ zur Kenntnis genommen. Es

gibt derzeit keine Pläne für ein öffentliches Mandat für einen Sachverständigenrat.

8. Welche Schlussfolgerungen zog die Bundesregierung aus der Studie „Wirtschaftsschutz in der digitalen Welt“ des Digitalverbands Bitkom?

   Welche Maßnahmen wurden aufgrund der Studie in Angriff genommen?

Die vorbenannte Studie des Digitalverbandes Bitkom deckt sich in der Tendenz mit den Einschätzungen der Bundesregierung aufgrund eigener Erkenntnisse.

Deshalb wurden aus der Studie weder weitergehende, allgemeine Schlussfolgerungen gezogen noch über die bisherigen Sensibilisierungs- und Präventionsmaßnahmen hinausgehende Einzelmaßnahmen veranlasst. Beispielsweise setzt das BSI bereits die Forderung nach mehr konkreter Information und Hilfestellung für die Wirtschaft bereits durch diverse Treffen verschiedener Cybersicherheits-Initiativen mit dem Ziel, Synergieeffekte zu erzeugen und eine bessere Übersichtlichkeit der Angebote zu realisieren, um.

9. Welche eigenen Nachforschungen unternimmt die Bundesregierung, um das Ausmaß von Cyberangriffen auf deutsche Unternehmen zu bestimmen?

   Welche Schlussfolgerungen wurden daraus gezogen?

Die Bundesregierung verfolgt einen kooperativen Ansatz im Bereich der Cybersicherheit, d. h. die jeweiligen Partner tragen insbesondere mit Informationen und Wissen bei. Die Bundesregierung stützt sich bei den Erkenntnissen zu Angriffen und Auswirkungen auf Unternehmen im Wesentlichen auf Umfragen und Studien, die seitens der Wirtschaftsverbände durchgeführt werden. Zusätzlich führt die Allianz für Cybersicherheit regelmäßig eine Umfrage zur Betroffenheit der deutschen Wirtschaft durch Cyber-Angriffe durch. Befragt werden insbesondere Teilnehmer der Allianz für Cybersicherheit. Inhaltlich wurden Angriffsvektoren, die Folgen und auch die Sicherheitsmaßnahmen abgefragt. In diesem Jahr wird eine abweichend gestaltete Umfrage durchgeführt, die im Kern die Pandemie und ihre Auswirkungen auf die Cybersicherheit fokussiert.

Darüber hinaus betreibt das BSI das Nationale IT-Lagezentrum mit dem Auftrag, jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland zu verfügen sowie den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können. Hier gehen Meldungen der Betroffenen von Sicherheitsvorfällen zentral ein.

Aus der Zunahme der Angriffe und der Schäden ist zu folgern, dass die Zahl der Angreifer wächst und dass zusätzliche Anstrengungen unternommen werden müssen, um die Cybersicherheit in den Unternehmen zu erhöhen.

10. Welche Schlussfolgerungen zieht die Bundesregierung aus der Arbeit der von Bundesministerium für Wirtschaft und Energie geförderten Transferstelle IT-Sicherheit im Mittelstand (TISiM)?

    Welche Verbesserungsmöglichkeiten sieht die Bundesregierung?

Die TISiM hat am 1. Januar 2020 ihre Arbeit aufgenommen. Im Laufe des Jahres werden die Angebote und Inhalte weiterentwickelt und ausgebaut. Die Transferstelle hat das Ziel, wirksame Befähigungsstrukturen zur messbaren Erhöhung der Umsetzungsbereitschaft von Maßnahmen der IT-Sicherheit in

KMU zu schaffen. Mit Hilfe der Transferstelle erhalten KMU Zugang zu einem breiten Spektrum an bestehenden Initiativen und Angeboten zur Verbesserung der IT-Sicherheit und dem Schutz von Daten, das anhand ihrer Schutzbedarfe passgenau aufbereitet sowie niedrigschwellig und nachhaltig zur Verfügung gestellt wird. Mit einem von der TISiM derzeit entwickelten auf Künstlicher Intelligenz basierten Werkzeug („SecOmat“) können sich KMU passgenaue IT-Sicherheitslösungen vorschlagen lassen. Die Nutzung wird via Internet, App und in den regionalen Anlaufstellen (Schaufenstern) möglich sein. Hinzu kommt zukünftig die Möglichkeit, KMU vor Ort mit einem sogenannten Tourenbus zu erreichen, um auch in den Regionen das Angebot der TISiM zur Verfügung zu stellen. Im Rahmen der Allianz für Cyber-Sicherheit des BSI besteht Austausch zu den Projektträgern der Transferstelle, sodass Schnittstellen zu vorhandenen und geplanten Angeboten identifiziert, geschaffen und genutzt werden.

11. Wie bewertet die Bundesregierung die Arbeit des Nationalen Cyber-Abwehrzentrums?

Das Nationale Cyber-Abwehrzentrum (Cyber-Az) ist eine Informations- und Koordinierungsplattform zu dessen teilnehmenden Kernbehörden derzeit das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), der Militärische Abschirmdienst (BAMAD), die Bundespolizei (BPOL), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Kommando Cyber- und Informationsraum der Bundeswehr (KdoCIR) zählen.

Zielsetzung des Cyber-Az ist der Informationsaustausch zu Cyber-Vorfällen im Rahmen der den teilnehmenden Behörden gesetzlich eingeräumten Befugnisse sowie die Abstimmung von Maßnahmen der Behörden bei Cyber-Vorfällen. Das Cyber-Az sorgt so für den Informationsfluss zwischen den Behörden und verbessert die Koordination und Abstimmung von Maßnahmen der teilnehmenden Behörden bei Cyber-Vorfällen im Rahmen der bestehenden Zuständigkeiten und Befugnisse. Die Bundesregierung bewertet die Arbeit des Cyber-Az als zielführend und positiv.

12. Welche Bedeutung hat das Nationale Cyber-Abwehrzentrum beim Schutz der deutschen Wirtschaft, insbesondere von mittelständischen Unternehmen?

Die Cybersicherheitsarchitektur in Deutschland beruht auf verschiedenen Pfeilern. Zunächst sind Unternehmen für die Gewährleistung der Sicherheit der von ihnen genutzten IT selbst verantwortlich. Unterstützt wird diese Eigenverantwortung durch das BSI, das technische Richtlinien und weiteres Wissen zur Gewährleistung von Cybersicherheit allen Bereichen in Deutschland zur Verfügung stellt. Den Polizeien kommt im Rahmen der ihnen gesetzlich eingeräumten Befugnisse – neben eigenen Sensibilisierungs- und Unterstützungsangeboten für die Wirtschaft – die Aufgabe der Gefahrenabwehr und der Unterstützung der Justiz bei der Strafverfolgung zu. Durch den engen Austausch der am Cyber-Az beteiligten Behörden, wird der Informationsfluss verbessert, was in Folge dazu führt, die gesetzlich zugewiesene Aufgabenwahrnehmung jeder einzelnen Behörde zu verbessern und somit mittelbar auch der Wirtschaft und ihren Unternehmen bei Cyber-Vorfällen hilft.

13. Welche Schlussfolgerungen zieht die Bundesregierung aus der negativen Einschätzung des Nationalen Cyber-Abwehrzentrums durch netzpoliti k.org?

Die Bundesregierung geht davon aus, dass sich die Frage auf den Gastbeitrag von Sven Herpig vom 20. Juni 2020 bezieht.

Die Einschätzung wird seitens der Bundesregierung nicht geteilt. Das Cyber-Abwehrzentrum ist bewusst eine flexible Zusammenarbeitsplattform, die die zuständigen Akteure zusammenführt und nicht – durch Verselbständigung – neue Zuständigkeiten schafft.

Der dortige Informationsaustausch erfolgt im Rahmen des bestehenden Rechts auf der Grundlage der Übermittlungsvorschriften in den einschlägigen Fachgesetzen.

14. Welche Pläne gibt es vonseiten der Bundesregierung, das Nationale Cyber-Abwehrzentrum zu reformieren?

Wie in der Antwort zu Frage 11 angeführt, wurde die Zusammenarbeit im Cyber-Az in 2019 deutlich intensiviert. Dennoch prüft die Bundesregierung fortlaufend die Notwendigkeit einer Fortentwicklung.

15. Wie sieht die Bundesregierung staatliche Stellen in der Abwehr von Cyberangriffen auf mittelständische Unternehmen aufgestellt?

Zunächst liegt die Verantwortung für die Sicherheit der von Unternehmen genutzten IT-Systemen bei den Unternehmen selbst. Staatliche Stellen unterstützen die Unternehmen hierbei durch Beratungsangebote, um sich erfolgreich vor Cyber-Angriffen schützen zu können. Im Übrigen wird auf die Antwort zur Frage 12 verwiesen.

16. Inwiefern sind staatliche Behörden nach Auffassung der Bundesregierung ausreichend vorbereitet und ausgestattet, um Unternehmen bei Fragen der IT-Sicherheit zu unterstützen?

Welche Verbesserungsmöglichkeiten sieht die Bundesregierung?

Nach Einschätzung der Bundesregierung sind die staatlichen Behörden für die Unterstützung in Fragen IT-Sicherheit bei Unternehmen gut aufgestellt. Beispielsweise wurde das BSI in den vergangenen Jahren personell deutlich gestärkt. Das Bundeskriminalamt und das Bundesamt für Verfassungsschutz haben in den vergangenen Jahren Abteilungen und Organisationseinheiten aufgestellt, die sich mit Cybercrime und staatlich gesteuerten Cyber-Angriffen im jeweiligen Zuständigkeitsbereich beschäftigen.

Aufgrund des technischen Wandels und Veränderungen in den Tatmodalitäten prüft die Bundesregierung fortlaufend Anpassungsbedarf, um Unternehmen in Fragen IT-Sicherheit noch besser zu unterstützen und setzt die identifizierten Bedarfe zeitnah um.

17. Welche Förderungen der Mitarbeiterschulungen durch Bundesmittel im Bereich der Cybersicherheit existieren für kleine und mittlere Unternehmen?

Mitarbeiterschulungen bzw. Qualifizierungsmaßnahmen im Bereich IT-Sicherheit werden insbesondere durch das Projekt KMU Aware (awareness-im-mittelstand.de) sowie die Förderprogramme „go-digital“ und „Digital Jetzt“ angeboten bzw. gefördert. Zudem werden auch von dem Mittelstand 4.0-Kompetenzzentren.Mitarbeiterschulungen sowie auch andere Sensibilisierungsmaßnahmen im Bereich Cybersicherheit angeboten.

18. Wann plant die Bundesregierung, einen Entwurf für das IT-Sicherheitsgesetz 2.0 vorzulegen?

Welche zentralen Maßnahmen sind im Rahmen des Gesetzes aus Sicht der Bundesregierung von zentraler Bedeutung?

Der Entwurf für das IT-Sicherheitsgesetz 2.0 befindet sich in der Ressortabstimmung. Die Bundesregierung äußert sich nicht zu in der Ressortabstimmung befindlichen Gesetzentwürfen.

19. Inwiefern könnte das geplante IT-Sicherheitsgesetz 2.0 zur Sicherheit von mittelständischen Unternehmen beitragen?

Unter Bezugnahme auf die Antwort zur Frage 18, äußert sich die Bundesregierung grundsätzlich nicht zu in der Ressortabstimmung befindlichen Gesetzentwürfen.

Es kann aber davon ausgegangen werden, dass die vorgesehenen Maßnahmen auch einen Beitrag zur Sicherheit von mittelständischen Unternehmen leisten können.

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