Deutscher Bundestag **Drucksache 19/13235**

19. Wahlperiode 16.09.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD
– Drucksache 19/12816 –

Private IoT-Geräte am Arbeitsplatz

Vorbemerkung der Fragesteller

Mitarbeiter nehmen immer häufiger ihre eigenen privaten IoT-Geräte wie Laptops, Tablets, Smartphones, Smartwatches, Fitness-Tracker, E-Reader und portable Spielekonsolen oder tragbare Smart-Home-Geräte wie intelligente Kaffeemaschinen mit auf den Arbeitsplatz. Die Mitarbeiter entsprechen damit dem Konzept „Bring Your Own Device“ (BYOD). Diese wurden oder werden oftmals zu beruflichen Zwecken mit dem Netzwerk des Arbeitgebers verbunden, um immer und überall auf die beruflichen Daten zugreifen zu können (www.security-insider.de/private-iot-geraete-im-unternehmen-a-846683/).

Dieser Umstand kann den Arbeitgeber und dessen Netzsicherheit nach Ansicht der Fragesteller vor erhebliche Sicherheitsprobleme stellen und ist generell eine große Herausforderung für die Netzwerkverantwortlichen. Klassische BYOD-Geräte (Tablet, Laptop) werden durch die Security-Verantwortlichen am Arbeitsplatz derzeit schon abgesichert (www.security-insider.de/private-iot-geraete-im-unternehmen-a-846683/).

Die Mitnahme neuerer IoT-Geräte birgt nach Ansicht der Fragesteller enorme Sicherheitsrisiken und Bedrohungen der Arbeitsplatznetzwerke. Angreifer können von außen unter Ausnutzung von Schwachstellen Daten von einem System entwenden, ein Gerät unter ihre Kontrolle bringen, den Anwender ausspionieren oder Daten manipulieren oder löschen. Bei einem Cyber-Angriff auf die Server des DNS-Anbieters Dyn 2016 waren Webseiten von Unternehmen unter anderem von Twitter und Netflix betroffen. Ein Botnet auf Basis des Internet of Things, das über eine Schadsoftware namens Mirai erzeugt wurde, war offenbar dafür verantwortlich (siehe www.allaboutcircuits.com/news/mirai-the-program-that-makes-iot-botnet-zombies/). Selbst der Verlust von privaten IoT-Geräten kann demnach schon eine Schwachstelle für betroffene Arbeitsnetzwerke darstellen.

Auch Hackern könnte hier Tür und Tor über einen Hintereingang geöffnet werden. Über Manipulation bestimmter Funktionen der IoT-Geräte könnten Hacker in ein Netzwerk des Arbeitgebers eindringen. „Gelingt es Angreifern, einmal in das Netzwerk einzudringen, können sie sich dort weiter ausbreiten und beispielsweise nach anderen verwundbaren Geräten suchen, Informationen stehlen, auf Server und Systeme zugreifen oder Geräte fu¨r Botnets ka-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 12. September 2019 übermittelt.

Die Drucksache enthält – in kleinerer Schrifttype – den Fragetext.

pern“ (www.security-insider.de/private-iot-geraete-im-unternehmen-a-846683/).

Selbst der Chef des neuen Cyber-Kommandos der Bundeswehr bestätigt laut einem Medienbericht, dass Fitness-Tracker, IoT und die Nutzung von privaten Smartphones für Soldaten Sicherheitsrisiken bergen (https://diepresse.com/home/techscience/5669079/Deutscher-Cyberkommandant-warnt-vor-Risiken-durch-Smartphones).

Vorbemerkung der Bundesregierung

Die Bundesregierung kann im Rahmen ihrer Zuständigkeit die übermittelten Fragen nur für die Bundesverwaltung (Bundesregierung sowie Bundesministerien und deren Geschäftsbereiche), nicht jedoch für den Bundestag, beantworten.

1. Teilt die Bundesregierung die Meinung der Fragesteller, dass durch die Mitnahme von privaten IoT-Geräten an den Arbeitsplatz große Sicherheitsrisiken bestehen, welche die Netzwerksicherheit von Arbeitgebern gefährden kann?

IoT-Geräte können Sensoren (Audio, Kamera, etc.), Funkkomponenten (WLAN, Bluetooth, etc.) und andere IT-Schnittstellen enthalten. Dadurch besteht grundsätz-lich die Möglichkeit, dass durch private IoT-Geräte Informationstechnik bzw. die Vertraulichkeit von Informationen gefährdet werden könnten.

Ob diese grundsätzlichen Gefährdungen für eine konkrete Institution (Unternehmen, Behörde, etc.) relevant sind und welche tatsächlichen Risiken daraus gegebenenfalls resultieren, hängt jedoch unter anderem vom Schutzbedarf der jeweils verarbeiteten Informationen sowie von der individuellen technischen und organisatorischen Ausgestaltung der Arbeitsplätze und IT-Systeme ab.

In der Bundesverwaltung werden Risiken beim Einsatz von IT im Rahmen des Informationssicherheits- und Risikomanagements gemäß ISO 27001 BSI IT-Grundschutz bewertet. Die einzelnen Behörden legen auf dieser Basis die jeweils notwendigen Regelungen und Maßnahmen zur Steuerung der Risiken fest.

Zudem hat das BSI für den Einsatz von IoT-Geräten im Rahmen des IT-Grundschutzes Sicherheitsanforderungen formuliert, die einen angemessenen Schutz von Informationen sicherstellen sollen (IT-Grundschutz-Baustein „Sys.4.4 Allgemeines IoT-Gerät“).

2. Hat in diesem Zusammenhang die Bundesregierung Aufklärungs- und Informationsmaßnahmen für Industrie und Wirtschaft und Unternehmen geplant oder durchgeführt, und wenn ja, welche konkreten Maßnahmen in welchem Umfang wurden durchgeführt?

Die Bundesregierung führt regelmäßig Aufklärungs- und Informationsmaßnahmen für die Wirtschaft durch. Unter anderem hat die Allianz für Cybersicherheit mit BSI-Beteiligung eine Vielzahl von Informationen im Rahmen unterschiedlicher Formate (z. B. Informationsveranstaltungen wie Cyber-Sicherheitstage (CST), White-Paper zu BYOD usw.) realisiert. Diese wurden in einem gesamtheitlichen oder spezifischen Kontext thematisiert, so zum Beispiel beim 20. Cyber-Sicherheitstag am 25. Januar 2018 in Berlin mit dem Zentralverband des Deutschen Handwerks zum Thema „Cyber-Sicherheit im

Handwerk“. Fachvorträge waren z. B. „Cyber-Risiken im Handwerk“ und „IT-Sicherheit mit mobilen Endgeräten“.

3. Wie viele Angriffe fanden seit dem Beginn der 19. Wahlperiode nach Kenntnis der Bundesregierung auf die Netzwerke von Bundesbehörden und Bundeseinrichtungen (Bundestag, Bundesregierung, Bundesministerien und deren nachgeordnete Behörden usw.) vor allem über Smartwatches, IoT-Geräte und dergleichen statt, und in welchem Umfang fielen diese aus?

Die Bundesregierung erfasst keine summarischen Zahlen/Gesamtzahl über Angriffe auf die Netzwerke von Bundesbehörden und -einrichtungen. Dies schließt Angriffe über Smartwatches, IoT-Geräte und dergleichen ein.

Bekannt ist dagegen, dass im Zeitraum vom 1. Juli 2017 bis 31. Mai 2018 pro Monat durchschnittlich 28.000 E-Mails mit Schadprogrammen in Echtzeit abgefangen wurden, bevor sie die Postfächer der Empfänger erreichen konnten. Im HTTP-Verkehr wurden im Jahr 2017 durchschnittlich rund 500 Schadprogramme pro Monat erkannt und abgewehrt. Auch hier setzte sich 2018 der Trend fort, dass Schadsoftware immer häufiger in E-Mails nur verlinkt und nicht als Anhang beigefügt ist.

Den automatisierten Antivirus-Schutzmaßnahmen nachgelagert betreibt das BSI ein weiteres System zur Detektion von Schadprogrammen im Datenverkehr der Regierungsnetze, welches auf Grundlage der erweiterten Befugnisse des BSIG betrieben wird (nach § 5 BSIG). Die Analysten des BSI konnten auf diese Weise im Berichtszeitraum über 40.000 Angriffe identifizieren, die von den eingesetzten kommerziellen Schutzprodukten nicht detektiert oder blockiert werden konnten. Zudem wurden über zwei Millionen Zugriffe aus dem Regierungsnetz auf Server unterbunden, die mit Schadcode, Betrug oder Datendiebstahl in Verbindung standen (vergleiche Lagebericht 2018 des BSI – www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf;jsessinid=BEE608FB91515EA09843B338C63EC066.2_cid341?__blob=publicationFile&v=6).

4. Teilt die Bundesregierung die Meinung der Fragesteller, dass generell die Mitnahme von privaten IoT-Geräten hohe Sicherheitsrisiken in Bundesbehörden und Bundeseinrichtungen (Bundestag, Bundesregierung, Bundesministerien und deren nachgeordnete Behörden usw.) mit sich bringen kann?

Auf die Antwort zu Frage 1 wird verwiesen.

5. Ist in Bundesbehörden und Bundeseinrichtungen (Bundestag, Bundesregierung, Bundesministerien und deren nachgeordneten Behörden usw.) die Mitnahme von privaten IoT-Geräten im Sinne des BYOD generell gestattet, und wenn ja, können sich die Mitarbeiter mit ihren privaten IoT-Geräten auch mit dem Arbeitsnetzwerk verbinden?

Die Bundesregierung verfolgt aufgrund der mit BYOD verbundenen Sicherheitsrisiken grundsätzlich keine BYOD-Strategie.

Das Mitbringen privater IoT-Geräte ist in der Bundesverwaltung mit Ausnahme einiger Sicherheitsbereiche nicht generell verboten. Das Verbinden dieser privaten Geräte mit den Netzen der Bundesverwaltung ist aber nicht zulässig und wird durch geeignete technische Mittel auf Basis der Empfehlungen des BSI verhindert. Abgesichert durch den Einsatz einer BSI zertifizierten Sicherheits-

lösung kommen im Rahmen der mobilen Arbeit in einem Bundesministerium – in begrenztem Umfang – auch bekannte private Endgeräte zum Einsatz.

Zum Teil existieren in der Bundesverwaltung spezielle WLAN-Netze (beispielsweise für den Internetzugang von Gästen); diese sind allerdings von den internen/schützenswerten Netzen separiert.

6. Sind nach Kenntnis der Bundesregierung die Netzwerke von Bundesbehörden und Bundeseinrichtungen (Bundestag, Bundesregierung, Bundesministerien und deren nachgeordnete Behörden usw.), vor allem aber hoch sensible Einrichtungen des Bundesnachrichtendienstes (BND), Bundesministeriums des Innern, für Bau und Heimat (BMI) und der Bundeswehr ausreichend und letztaktuell vor Angriffen über IoT-Geräte geschützt?

Ja. Die Netze der Bundesregierung werden auf der Grundlage der Anforderungen des „Umsetzungsplan Bund 2017“ (Leitlinie für Informationssicherheit in der Bundesverwaltung) und der „Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA)“ durch modernste IKT-Systeme und entsprechend den Empfehlungen des BSI vor potenziellen Angriffen geschützt. Die Sicherheitskonfigurationen werden im Bedarfsfall (z. B. bei Bekanntwerden neuer Angriffsmuster) unverzüglich angepasst.

Für hoch sensible Bereiche werden gesonderte Sperrzonen eingerichtet, in denen das Einbringen privater und dienstlicher mobiler IT untersagt ist.

Im Übrigen wird auf die Antwort zu Frage 5 verwiesen.

7. Welche konkreten Maßnahmen haben die einzelnen Bundesbehörden und Bundeseinrichtungen (Bundestag, Bundesregierung, Bundesministerien und deren nachgeordnete Behörden usw.) gesetzt, um das Abhören, Transkribieren und Auswerten von Mitschnitten von Sprachsoftware (zum Beispiel auf Smartphones oder Kaffeemaschinen) zu verunmöglichen und somit den Schutz sensibler Daten zu gewährleisten?

Die Maßnahmen werden grundsätzlich auf Basis des für das jeweilige Netzwerk geltenden Schutzbedarfes abgestimmt und zur Verhinderung verschiedenster Angriffsszenarien umgesetzt.

Auf dienstlichen Endgeräten existieren verschiedene Sicherheitsmaßnahmen, wel-che Abhör- und Spionagefunktionalität verhindern sollen (Virenscanner, Gruppen-richtlinien, Software Restriction Policies, Application Whitelisting etc.). In Besprechungen mit eingestuften VS-Inhalten ist die Mitnahme von privaten Endgeräten (z. B. Smartphones, Smartwatches oder anderer IoT-Geräte, die über Mikrophone verfügen) untersagt. Mitarbeiter werden hinsichtlich des Aspekts „Vertraulichkeit von Informationen“ geeignet sensibilisiert (z. B. Schulungen zur Verschlusssachenanweisung).

Im Übrigen wird auf die Antworten zu den Fragen 5 und 6 verwiesen.

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