Deutscher Bundestag **Drucksache 19/12816**

19. Wahlperiode 29.08.2019

Kleine Anfrage

der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD

Private IoT-Geräte am Arbeitsplatz

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 für Botnets kapern“ (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).

Wir fragen die Bundesregierung:

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?
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?
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?
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?
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?
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?
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?

Berlin, den 15. August 2019

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

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