Deutscher Bundestag **Drucksache 19/2252**

19. Wahlperiode 22.05.2018

Kleine Anfrage

der Abgeordneten Jimmy Schulz, Manuel Höferlin, Mario Brandenburg, Frank Sitta, Grigorios Aggelidis, Renata Alt, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Dr. Marco Buschmann, Carl-Julius Cronenberg, Britta Katharina Dassler, Christian Dürr, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Katja Hessel, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Katharina Kloke, Daniela Kluckert, Pascal Kober, Carina Konrad, Konstantin Kuhle, Alexander Kulitz, Ulrich Lechte, Michael Georg Link, Oliver Luksic, Dr. Jürgen Martens, Alexander Müller, Roman Müller-Böhm, Dr. Martin Neumann, Bernd Reuther, Dr. Stefan Ruppert, Frank Schäffler, Matthias Seestern-Pauly, Judith Skudelny, Bettina Stark-Watzinger, Benjamin Strasser, Katja Suding, Michael Theurer, Dr. Florian Toncar, Dr. Andrew Ullmann, Johannes Vogel (Olpe), Sandra Weeser, Nicole Westig und der Fraktion der FDP

Bereitstellung von Erkenntnissen aus dem Hack der Bundesregierung für Wirtschaft und Bevölkerung

Der am 28. Februar 2018 bekanntgewordenen Angriff auf das als sicher geltende Informationsnetzwerk der Bundesregierung, der Informationsverbund Berlin-Bonn (IVBB), hat erneut den Stellenwert aufgezeigt, den IT-Sicherheit in unserem digitalen Zeitalter einnimmt. Sichere IT-Infrastrukturen sind der Grundpfeiler für eine erfolgreiche Digitalisierung unserer Wirtschaft und Gesellschaft.

Um ein hohes Maß an IT-Sicherheit für alle zu gewährleisten, müssen insbesondere Wirtschaft und Staat eng zusammenarbeiten: Einerseits ist die Wirtschaft auf sinnvolle staatliche Regelungen und Standards zur IT-Sicherheit angewiesen, andererseits muss sich der Staat auf Anstrengungen der Wirtschaft verlassen können, beispielsweise durch Schaffung von Software zur Absicherung von informationstechnischen Systemen. Hierbei spielt der Austausch über existierende Sicherheitslücken eine bedeutende Rolle: So existieren zwischen den großen Unternehmen bereits verschiedene Formate, die einen vertraulichen Austausch von Informationen über Cybersicherheitszwischenfälle ermöglichen. In diesem Rahmen ist es nach einem Cybersicherheitszwischenfall innerhalb der Wirtschaft Usus, sich gegenseitig zu informieren, damit Software zur Detektion von Angriffen wie z. B. Firewalls um neue Erkenntnisse, die aus einem solchen Angriff gewonnen wurden, ergänzt werden können. Dies stärkt die IT-Sicherheit aller Beteiligten und erschwert es Angreifern, die gleiche oder eine ähnliche Sicherheitslücke für einen erneuten Angriff zu nutzen, da diese nicht nur im angegriffenen Netzwerk behoben werden kann, sondern auch in allen anderen, bisher nicht angegriffenen Systemen.

Die ausgenutzten Sicherheitslücken und Vorgehensweisen der Angreifer auf die Netze der Bundesregierung fallen unter diese Maßgabe.

Wir fragen die Bundesregierung:

1. Kann die Bundesregierung die Pressemitteilung der „dpa“ vom 28. Februar 2018 bestätigen, dass bei dem Hacker-Angriff auf den IVBB „im Internet verfügbare Software“ genutzt wurde?

   Wenn ja, wann bekamen die betroffenen Behörde Kenntnis über die Hashes oder andere automatisch detektierbaren Kennzeichen dieser Malware?

2. Wenn es eine im Internet verfügbare Software (dpa) war, warum wurde diese dann nicht detektiert?

3. Mit welchen Behörden und zu welchem Zeitpunkt wurden die Informationen über die IOCs (Indicators of Compromise) geteilt?

   Wurde das Cyberabwehrzentrum über die IOCs informiert?

   Zu welchem Zeitpunkt wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Cyberabwehrzentrum über die IOCs informiert?

4. Ist das BSI der Meinung, dass die genutzten Methoden der Angreifer außerhalb der Netze der Bundesregierung auch zur Wirtschaftsspionage oder zur Schädigung einzelner Unternehmen oder Unternehmensnetzwerke genutzt werden könnten?

5. Zu welchem Zeitpunkt beabsichtigt die Bundesregierung, die IOCs mit der Öffentlichkeit zu teilen, damit auch die deutsche Wirtschaft die ausgenutzten Sicherheitslücken beheben kann?

6. Wann hat das BSI eine öffentliche Lageeinschätzung publiziert?

   Wenn bisher nicht erfolgt, wann beabsichtigt das BSI das zu tun?

7. Welche Maßnahmen empfiehlt das BSI den deutschen Behörden und der deutschen Wirtschaft, um sich vor zukünftigen Angriffen, die dem am 28. Februar 2018 bekannt gewordenen technisch ähneln, zu schützen?

8. Welche Erkenntnisse gibt es darüber, ob die Kommunikation zwischen dem Auswärtigen Amt und den deutschen Botschaften im Ausland von dem Angriff betroffen ist?

   Existieren Hinweise darauf, dass die informationstechnischen Systeme der deutschen Botschaften im Ausland ebenfalls kompromittiert sind?

9. In welcher Weise hat das Nationale Cyber-Abwehrzentrum auf die Angriffe reagiert?

   Welche Dienstleistungen und Hilfestellungen kamen von dort?

   Zu welchem Zeitpunkt wurde das Cyber-Abwehrzentrum hinzugezogen?

10. Wann wäre der vorgesehene Zeitpunkt gewesen, um grundlegende Informationen an die Abgeordneten des Deutschen Bundestages weiterzugeben?

11. Wie sieht der Notfallkommunikationsplan für Cyberzwischenfälle dieser oder ähnlicher Art aus?

12. War die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITIS) in die forensische Untersuchung des Angriffs involviert?

    Wenn ja, in welcher Weise?

    Wenn nicht, warum nicht?

13. Hat die Bundesregierung bzw. haben die Sicherheitsbehörden Lehren aus den bekannt gewordenen Hackerangriffen auf das Bundestagsnetzwerk von 2013 und 2015 für digitale Verteidigungsstrategien der Behördennetze gezogen?

    Insbesondere die Folgenden:

    a) Werden regelmäßige Penetrationstests durchgeführt?

       In welcher Frequenz?

    b) Wann war der letzte Pentest der nun betroffenen Systeme?

    c) In welcher Frequenz werden Firewall-Systeme aktualisiert mit aktuellen IOCs (Indicators of Compromise)?

    d) Wird der behördeninterne Netzwerkverkehr mittels DPI (Deep Packet Inspection) fortdauernd überwacht nach Indikatoren für Schadsoftware?

14. Welcher Prozess existiert, um Kenntnisse über identifizierte IOCs, insbesondere solche aus den Fragen 3, 13c und 13d, an die Bevölkerung und die deutsche Wirtschaft weiterzugeben, sodass diese in die Lage versetzt werden, mithilfe dieser Erkenntnisse die eigenen Netzwerke gegen ähnliche Angriffe abzusichern?

Berlin, den 14. Mai 2018

Christian Lindner und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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