Deutscher Bundestag **Drucksache 19/17888**

19. Wahlperiode 13.03.2020

Kleine Anfrage

der Abgeordneten Dr. Jens Brandenburg (Rhein-Neckar), Katja Suding, Mario Brandenburg (Südpfalz), Britta Katharina Dassler, Peter Heidt, Dr. h.c. Thomas Sattelberger, Grigorios Aggelidis, Renata Alt, Nicole Bauer, Jens Beeck, Dr. Marco Buschmann, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Manuel Höferlin, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Marcel Klinge, Daniela Kluckert, Pascal Kober, Carina Konrad, Konstantin Kuhle, Ulrich Lechte, Till Mansmann, Alexander Müller, Roman Müller-Böhm, Dr. Martin Neumann, Bernd Reuther, Frank Schäffler, Matthias Seestern-Pauly, Frank Sitta, Judith Skudelny, Dr. Hermann Otto Solms, Bettina Stark-Watzinger, Benjamin Strasser, Linda Teuteberg, Michael Theurer, Stephan Thomae, Dr. Florian Toncar, Dr. Andrew Ullmann, Sandra Weeser, Nicole Westig und der Fraktion der FDP

Cyberangriffe auf deutsche Hochschulen und Wissenschaftsorganisationen

Die Zahl der Angriffe auf IT-Systeme in Deutschland nimmt zu. Im Jahr 2018 erfasste das Bundeskriminalamt insgesamt 87.000 Cyberattacken auf Privatpersonen, Unternehmen und staatliche Organisationen (vgl. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.pdf?__blob=publicationFile&v=3). Die Zahl nicht erfasster Angriffe auf IT-Systeme dürfte jedoch deutlich höher liegen (vgl. https://t3n.de/news/hackerattacken-deutsche-firmen-1175330/). Auch Hochschulen und außeruniversitäre Forschungseinrichtungen sind aufgrund ihres Zugangs zu vertraulichen Forschungsergebnissen einem erhöhten Risiko von Cyberangriffen ausgesetzt (vgl. https://www.deutschlandfunk.de/datenschutz-hochschulen-wollen-sich-gegen-cyberattacken.680.de.html?dram:article_id=448238). Um kritische Infrastrukturen wie Stromnetze, Verkehrswege, Krankenhäuser und Verwaltung zu schützen, fördert das Bundesministerium für Bildung und Forschung drei Kompetenzzentren zur IT-Sicherheitsforschung (https://www.bmbf.de/de/it-sicherheitsforschung-fuer-die-digitale-zukunft-6601.html). Ende 2019 musste die Universität Gießen aufgrund eines Hackerangriffs das gesamte IT-Netzwerk für mehrere Tage offline nehmen – vom WLAN in den Studentenwohnheimen über das Ausleihsystem der Bibliothek bis hin zur Lehrplattform „Stud.IP“. Die Hintergründe des Angriffs blieben unklar (vgl. https://www.faz.net/aktuell/rhein-main/region-und-hessen/uni-giessen-faehrt-nach-cyberangriff-computer-wieder-hoch-16567874.html). Universitätspräsident Prof. Dr. Joybrato Mukherjee sprach in diesem Zusammenhang von einem „digitalen Notstand“ (vgl. https://www.tagesspiegel.de/wissen/nach-cyberangriff-komplett-offline-die-uni-giessen-liegt-lahm/25352288.html).

Wir fragen die Bundesregierung:

1. Wie bewertet die Bundesregierung den Zustand der Sicherheit der IT-Systeme deutscher Hochschulen, außeruniversitärer Forschungseinrichtungen und der übrigen durch den Bund finanzierten Wissenschaftsorganisationen?
2. Wie bewertet die Bundesregierung das Risiko von Angriffen auf die IT-Systeme dieser Einrichtungen?

   Für wie wahrscheinlich hält die Bundesregierung Angriffe auf die IT-Systeme dieser Einrichtungen, und mit welchen Folgen solcher Angriffe rechnet die Bundesregierung?
3. Wie begründet die Bundesregierung ihre Auffassung, dass mit Blick auf potenzielle Angriffe auf die IT-Systeme von Hochschulen und Wissenschaftseinrichtungen keine „Bedrohungslage von bundesweiter Bedeutung für die deutsche Wissenschafts- und Hochschullandschaft“ vorliege (vgl. die Antwort der Bundesregierung auf die Schriftliche Frage 93 des Abgeordneten Kai Gehring auf Bundestagsdrucksache 19/16761)?
4. Wie viele und welche Angriffe auf die IT-Systeme deutscher Hochschulen, außeruniversitärer Forschungseinrichtungen und übriger aus Mitteln des Bundes finanzierter Wissenschaftsorganisationen gab es nach Kenntnis der Bundesregierung jeweils in den Jahren von 2010 bis 2019 (bitte nach Jahren, Ländern sowie Hochschulen, Forschungseinrichtungen und übrigen Wissenschaftsorganisationen aufteilen)?
5. Bei wie vielen und welchen dieser Angriffe wurden nach Kenntnis der Bundesregierung Daten der Hochschulen bzw. Forschungseinrichtungen durch die Angreifer entwendet (bitte nach Jahren – 2010 bis 2019 –, Ländern sowie Hochschulen, Forschungseinrichtungen und übrigen Wissenschaftsorganisationen aufteilen)?
6. In welchem Umfang wurden bei diesen Angriffen nach Kenntnis der Bundesregierung Daten welches Vertraulichkeitsniveaus jeweils entwendet (bitte nach Jahren – 2010 bis 2019 –, Ländern, und verschiedenen Vertraulichkeitsniveaus – öffentlich, vertraulich, streng vertraulich – aufteilen und in Gigabyte ausweisen)?
7. In welchem Umfang wurden bei diesen Angriffen nach Kenntnis der Bundesregierung vertrauliche Daten entwendet, insbesondere

   a) persönliche Daten, wie Namen und Adressen von Hochschulangehörigen;

   b) Noten und Ergebnisse von Prüfungsleistungen von Studierenden und Doktoranden;

   c) Prüfungsleistungen von Studierenden;

   d) bisher unveröffentlichte und vertrauliche Forschungsdaten bzw. Forschungsergebnisse (bitte jeweils nach Jahren – 2010 bis 2019 – und Ländern aufteilen)?
8. Wie hoch schätzt die Bundesregierung den durch Cyberangriffe entstandenen Schaden bei Hochschulen sowie insbesondere bei außeruniversitären Forschungseinrichtungen und übrigen aus Mitteln des Bundes finanzierten Wissenschaftsorganisationen (bitte nach Jahren – 2010 bis 2019 –, Ländern sowie Hochschulen, Forschungseinrichtungen und übrigen Wissenschaftsorganisationen aufteilen)?

   Wie kommt die Bundesregierung zu dieser Schätzung?

9. In wie vielen und welchen Fällen waren potenzielle Angriffe auf die IT-Systeme deutscher Hochschulen, außeruniversitärer Forschungseinrichtungen und übriger aus Mitteln des Bundes finanzierten Wissenschaftsorganisationen nach Kenntnis der Bundesregierung zuvor dem Bundesnachrichtendienst, dem Bundesamt für Verfassungsschutz, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder nachgelagerten Behörde des Bundesregierung bekannt?

   Wie viele potenzielle Angriffe konnten aufgrund von Aktivitäten dieser Behörden bereits vor Realisierung abgewehrt werden (bitte nach Jahren – 2010 bis 2019 – und Ländern aufteilen)?

10. In wie vielen und welchen Fällen erfolgreicher bzw. abgewehrter Angriffe auf die IT-Systeme deutscher Hochschulen, außeruniversitärer Forschungseinrichtungen und übriger aus Mitteln des Bundes finanzierten Wissenschaftsorganisationen nahmen nach Kenntnis der Bundesregierung die Ermittlungsbehörden (insb. der Generalbundesanwalt und das Bundeskriminalamt) Ermittlungen auf (bitte nach Jahren – 2010 bis 2019 – und Ländern aufteilen)?

    In wie vielen und welchen Fällen konnten die Angreifenden identifiziert werden?

11. In wie vielen und welchen Fällen unterstützte das Bundesamt für Sicherheit in der Informationstechnik nach Kenntnis der Bundesregierung gemäß § 5a Absatz 7 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) von Angriffen auf die IT-Systeme betroffene Hochschulen bzw. Wissenschaftseinrichtungen bei der Wiederherstellung ihrer IT-Systeme (bitte nach Jahren – 2010 bis 2019 –, Ländern sowie Hochschulen, Forschungseinrichtungen und übrigen Wissenschaftsorganisationen aufteilen)?

12. In wie vielen Fällen handelte es sich, sofern die Identität der Angreifenden geklärt werden konnte, dabei nach Kenntnis der Bundesregierung um

    a) inländische Unternehmen;

    b) inländische Privatpersonen;

    c) inländische Gruppen privater Personen;

    d) ausländische staatliche Organisationen (insbesondere Geheimdienste);

    e) ausländische Unternehmen;

    f) ausländische Privatpersonen;

    g) ausländische Gruppen privater Personen (bitte jeweils nach Jahren – 2010 bis 2019 – und Ländern aufteilen)?

13. Welche Erkenntnisse hat die Bundesregierung jeweils über die Absichten der Angriffe auf die IT-Systeme deutscher Hochschuleinrichtungen, Forschungseinrichtungen und Wissenschaftseinrichtungen?

14. Inwiefern betrachtet es die Bundesregierung als ihre (Teil-)Zuständigkeit, die Angriffe auf die IT-Systeme deutscher Hochschuleinrichtungen, Forschungseinrichtungen und Wissenschaftseinrichtungen zu erkennen, zu verhindern und so die IT-Sicherheit zu gewährleisten bzw. die Einrichtungen dabei zu unterstützen?

15. Wie, und über welche nachgelagerten Behörden unterstützt die Bundesregierung

    a) die Länder und die Hochschulen,

    b) die außeruniversitären Forschungseinrichtungen,

c) übrige aus Mitteln des Bundes finanzierte Wissenschaftsorganisationen bei der Sicherung ihrer IT-Systeme und sensibler Daten vor Angriffen durch Hacker?

16. In welchem Umfang stellt die Bundesregierung Personal für diese Unterstützungsleistungen zur Verfügung?

17. Hat die Bundesregierung gemeinsam mit allen außeruniversitären Forschungseinrichtungen und allen übrigen aus Mitteln des Bundes finanzierten Wissenschaftsorganisationen Notfallpläne ausgestaltet, um Angriffe auf die IT-Systeme der genannten Einrichtungen frühzeitig zu erkennen und Schäden zu minimieren?

    Wenn ja, wann wurden diese Pläne erarbeitet und abgeschlossen?

    Welche Maßnahmen sind in diesen Plänen vorgesehen?

    Wenn nein, für wie viele Organisationen fehlen solche Pläne bisher, und aus welchen Gründen?

18. In welchem Umfang stand die Bundesregierung den Hochschulen und Ländern bei der Entwicklung solcher Pläne beratend zur Verfügung?

19. In welcher Form unterstützte die Bundesregierung, beispielsweise über das Bundesamt für Sicherheit in der Informationstechnik, die Universität Gießen beim Erkennen, Reagieren und Entfernen der Schadsoftware auf den Hochschulservern?

20. Welche Konsequenzen hat die Bundesregierung aus den Angriffen auf die IT-Systeme der Universität Gießen im Dezember 2019 gezogen, und welche Maßnahmen hat sie seitdem ergriffen?

21. Ist der Bundesregierung der Fall des Verdachts auf (Forschungs-)Spionage durch den ehemaligen chinesischen Leiter des Konfuzius-Instituts Brüssel bekannt (vgl. https://www.zeit.de/news/2019-10/30/leiter-von-chinesischem-kulturinstitut-aus-schengen-raum-verbannt)?

    Wenn ja, wie bewertet die Bundesregierung diesen Fall mit Blick auf die Aktivitäten der chinesischen Konfuzius-Institute an deutschen Hochschulen?

    Welche Konsequenzen zieht sie aus dieser Einschätzung?

22. Wie bewertet die Bundesregierung das Risiko potenzieller Forschungsspionage über die Zugänge zu den IT-Systemen deutscher Hochschulen durch chinesische Konfuzius-Institute?

    Liegen der Bundesregierung Erkenntnisse vor, ob das von der chinesischen Regierung ins Ausland entsandte Lehrpersonal der Konfuzius-Institute neben einer „stärkeren ideologischen Vorbereitung“ (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/15560) auch Vorbildung auf dem Gebiet der Informationstechnologie aufweist und/oder über berufliche Erfahrungen bzw. Ausbildung auf dem Gebiet geheimdienstlicher bzw. militärischer Aktivitäten besitzt?

    Mit welchen Ländern und Hochschulen hat die Bundesregierung diese Risiken und mögliche vorbeugende Maßnahmen erörtert?

Berlin, den 12. Februar 2020

Christian Lindner 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