1682/J
vom 17.09.2018 (XXVI.GP)

Anfrage

der Abgeordneten Stephanie Cox, Kolleginnen und Kollegen

an den Bundesminister für Bildung, Wissenschaft und Forschung

betreffend „Cybersecurity in der Bildung"

BEGRÜNDUNG

Cyberkriminalität auf globaler Ebene

Laut McAfee und dem „Center for Strategic and International Studies" (CSIS)[1] ist Cyberkriminalität an dritter Stelle, wenn es um kriminelle Handlungen mit globalen Auswirkungen geht.[2] Laut Schätzung von CSIS hat Cyberkriminalität 2014 für die globale Wirtschaft Kosten idHv. 500 Mrd. Dollar verursacht.

Cyberkriminalität in Österreich

Auch in Österreich ist die Lage ernst. Eine Studie von KPMG[3] (September 2017) kam zu folgenden Erkenntnissen: 72 % aller Unternehmen in Österreich waren zwischen September 2016 und September 2017 Opfer einer Cyberattacke (im Jahr davor waren es „nur" 49%); 78% der Industrieunternehmen wurden angegriffen; 50% der Unternehmen litten als Folge unter einer Unterbrechung der Geschäftsprozesse und 36% wissen gar nicht, welche Auswirkungen der Angriff hatte.

Die Risiken, die von Cyberkriminalität ausgehen, werden durch neue technologische Entwicklungen sogar noch verstärkt, z.B. durch „Machine Learning" oder das „Internet of Things" („IoT"). Fast alle von KPMG befragten Unternehmen (99 Prozent) haben Bedenken im Hinblick auf „IoT".

Fachkräftemangel

Laut einer aktuellen Studie von KPMG (Mai 2018)[4] bleibt Fachkräftemangel nach wie vor eine der größten Herausforderungen im Zusammenhang mit Cybersecurity. Mehr als zwei Drittel der Unternehmen (67%) beklagen einen Mangel an Cybersecurity-Expert_innen am heimischen Markt.

Die unterfertigenden Abgeordneten stellen daher folgende

---

[1] Economic Impact of Cybercrime – No Slowing down, Februar 2018 (abrufbar unter: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf).

[2] Die Bewertung erfolgte nach „dollar value".

[3] https://home.kpmg.com/content/dam/kpmg/at/images/sujets/cyber-security-2017/FS_CyberSecurity2017_D_screen.pdf .

[4] https://home.kpmg.com/at/de/home/media/press-releases/2018/05/kpmg-cyber-security-in-oesterreich-2018.html .

Anfrage

1. Was sind die Gründe für den Fachkräftemangel im Bereich „Cybersecurity" in Österreich?

2. Welche Maßnahmen setzen Sie bzw. planen Sie, um der Herausforderung dieses Fachkräftemangels entgegenzuwirken?

3. Gibt es internationale Best-Practice-Beispiele in diesem Zusammenhang bzw. wie gehen „führende" Länder diese Herausforderung an?

4. Gibt es bereits oder planen Sie mit anderen Ministerien eine Zusammenarbeit, um das Problem des Fachkräftemangels im Bereich „Cybersecurity" zu lösen? Wie sehen diese Kooperationen aus und zu welchen Ergebnissen führten sie?

5. Welche Maßnahmen setzen bzw. planen Sie, um Kinder, Jugendliche und Studierende für das Thema Cybersecurity zu begeistern, damit diese eine Karriere im Cybersecurity-Bereich beginnen? *(Im Unterschied zu Frage 6. geht es hier nicht nur um „Sicherheitsbildung", sondern darum, potentielle Fachkräfte für das Thema zu begeistern.)*

    a. Aus welchen Mitteln und in welcher Höhe sind diese Maßnahmen finanziert?

    b. Gibt es internationale Best-Practice-Beispiele in diesem Zusammenhang?

6. Welche Maßnahmen setzen Sie bzw. planen Sie, um Kinder und Jugendliche in der i) Volksschule und ii) Sekundarstufe zu „Sicherheit" (im Allgemeinen) und „Sicherheit im Internet" (im Speziellen) zu bilden? (Bitte um getrennte Beantwortung für Volksschulen und Sekundarstufen, sowie beide Bereiche.)

7. Da Jede/r von Cyberkriminalität betroffen sein kann: Welche Maßnahmen setzen Sie bzw. planen Sie, um Erwachsenen die wichtigsten Grundzüge des Themas „Cybersecurity" bzw. „Sicherheit im Internet" beizubringen?

8. Welche Initiativen und Organisationen, die im Bildungsbereich das Thema „Sicherheit (im Internet)" sowie verwandte Themen fördern (z.B. Safer Internet), unterstützt Ihr Ministerium und in welcher Form bzw. Höhe (in EUR)?

9. Planen Sie entsprechende Förderungen (Frage 8) auszubauen bzw. zu erhöhen?

Angesichts der Tatsache, dass Lehrer_innen derzeit keine besondere Ausbildung im Bereich „Sicherheit" bzw. „Cybersecurity" und verwandten Feldern erhalten:

10. Planen Sie Themen wie „Sicherheit" bzw. „Cybersecurity", „Gesamtsystemverständnis" (als Gegensatz zur reinen „Anwendungskompetenz") verpflichtend in der Lehrer_innenausbildung zu verankern?

11. Wie bzw. mit welchen konkreten Maßnahmen unterstützen Sie Schulen und Lehrer_innen dabei, Expert_innen aus entsprechenden Bereichen in den Unterricht zu bringen, um diese Kenntnisse zu vermitteln?

12. Welche Partnerschaften (z.B. mit der Privatwirtschaft) gibt es, um entsprechende Expert_innen in Schulen zu bringen, und wie erfolgreich sind diese?

13. Sind Maßnahmen geplant, um für Studierende einschlägiger Studienbereiche (z.B. Informatik) Anreize zu schaffen bzw. diesen zu ermöglichen, an Ausbildungseinrichtungen ihr Wissen zu teilen? Falls ja, welche? *(Beispielsweise durch die Einführung entsprechender Lehrveranstaltungen und/oder die Vergabe von ECTS für solche Leistungen über die Leistungsvereinbarungen mit den Universitäten.)*

14. Sind Maßnahmen geplant, um für im Berufsleben stehende sowie pensionierte Expert_innen und für Unternehmen Anreize zu schaffen bzw. diesen zu ermöglichen, an Ausbildungseinrichtungen ihr Wissen zu teilen? Falls ja, welche?

15. Wie viele Lehrstühle gibt es an österreichischen Universitäten, die relevant für den Bereich „Cybersecurity" sind, und welche sind das? (Bitte auch Art bzw. rechtliche Einordnung der Professur anführen.)

16. Ist geplant, weitere Lehrstühle im Bereich „Cybersecurity" zu schaffen? Falls ja, welche Arten von Professuren, an welchen Universitäten und in welchen Bereichen?

17. Gibt es besondere Vereinbarungen mit den Universitäten bzgl. der Finanzierung relevanter Lehrstühle, Forschungsprogramme oder Institute?

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2018-09-17T13:56:25+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	