1699/AB
vom 16.11.2018 zu 1682/J (XXVI.GP)

Bundesministerium
Bildung, Wissenschaft
und Forschung

bmbwf.gv.at

+43 1 531 20-0
Minoritenplatz 5, 1010 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: BMBWF-10.000/0210-Präs/9/2018

Die schriftliche parlamentarische Anfrage Nr. 1682/J-NR/2018 betreffend „Cybersecurity in der Bildung", die die Abg. Stephanie Cox, BA, Kolleginnen und Kollegen am 17. September 2018 an mich richteten, wird wie folgt beantwortet:

Zu Fragen 1 bis 4:

- *Was sind die Gründe für den Fachkräftemangel im Bereich „Cybersecurity" in Österreich?*
- *Welche Maßnahmen setzen Sie bzw. planen Sie, um der Herausforderung dieses Fachkräftemangels entgegenzuwirken?*
- *Gibt es internationale Best-Practice-Beispiele in diesem Zusammenhang bzw. wie gehen „führende" Länder diese Herausforderung an?*
- *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?*

Zweifelsohne ist die Digitalisierung die größte Veränderung des Wirtschaftens, des Arbeitens und der Kommunikation. Die Herausforderungen für das Bildungssystem reichen von den fachlichen Inhalten bis hin zur Art und Weise der Vermittlung. Das Bundesministerium für Bildung, Wissenschaft und Forschung hat mit den Arbeiten an einem Masterplan für Digitalisierung in der Bildung begonnen. Ziel ist es, die Veränderungen, die sich durch die fortschreitende Digitalisierung ergeben, stufenweise und vor allem flächendeckend in das österreichische Bildungssystem einfließen zu lassen.

Was die geäußerten Vermutungen zum Fachkräftemangel im Bereich „Cybersecurity" anbelangt, so können diese auch aus arbeitsmarktpolitischer Sicht nicht bestätigt werden. Detaillierte Analysen dazu betreffen keinen Gegenstand der Vollziehung des Bundesministeriums für Bildung, Wissenschaft und Forschung.

Jedenfalls trägt das Bundesministerium für Bildung, Wissenschaft und Forschung unter anderem mit seinen zahlreichen Angeboten im Bereich der schulischen und tertiären Ausbildungen als auch thematisch unterstützten Initiativen (vgl. dazu auch die Ausführungen zu den Fragen 5ff) maßgeblich dazu bei, die Voraussetzungen für eine Vielzahl qualitätsvoller und nachgefragter Abschlüsse im IKT-Bereich zu schaffen.

Im laufenden Schuljahr 2018/19 besuchen österreichweit 3.557 Schülerinnen und Schüler die Fachrichtung Informationstechnologie. An den Schülerinnen- und Schülerzahlen der I. und II. Jahrgänge lässt sich ein deutlicher Aufwärtstrend bei der Wahl von Jugendlichen für diese Fachrichtung feststellen.

Im Erweiterungsbereich Digital Business an Handelsakademien wird das Thema (Cyber)-Security mit den Gegenständen Betriebssysteme und Netzwerkmanagement, E-Business und E-Business-Center sowie Office Management und Angewandte Informatik abgedeckt. Insgesamt werden 1.230 Schülerinnen und Schüler an Handelsakademien für Digital Business ausgebildet.

An einschlägigen IT-Security-Studiengängen im Fachhochschul(FH)-Sektor werden im aktuellen Studienjahr 2018/19 rund 240 Anfängerinnen- und Anfänger-Studienplätze angeboten. Darüber hinaus haben Themenfelder wie Netzwerksicherheit, Datensicherheit oder Systemsicherheit aber auch in vielen anderen IT- und Software-Engineering-Studiengängen ihren curricularen Niederschlag gefunden. Durch die starke Berufsfeldorientierung und die vielfach berufsbegleitend studierbare Organisationsform der FH-Studiengänge eignet sich der FH-Sektor besonders, um den Absolventeninnen und Absolventen praxisorientierte und treffsichere Kompetenzen für die unmittelbare Umsetzung in den Unternehmen zu vermitteln.

Im Universitätsbereich sind die Themenfelder Cybersecurity und IT-Security in breiter angelegte und grundlagenorientierte Informatik-Studien an acht Universitäten eingebettet. Darüber hinaus wurde die österreichweite Zahl der Studienplätze im Studienfeld „Informatik" auf 2.800 erhöht.

Für den Verantwortungsbereich des Bundesministeriums für Bildung, Wissenschaft und Forschung wird in diesem Zusammenhang zudem auf die Initiativen zu Digitaler Bildung, die auch bewusstseinsbildende Maßnahmen für Cybersicherheit umfassen, hingewiesen. Die frühe Förderung entsprechender Kompetenzen und altersadäquate Vermittlung von Knowhow im Zuge von Medienbildung und Digitaler Grundbildung schafft eine breite Basis und soll das Interesse bei Schülerinnen und Schülern für eine spätere facheinschlägige Ausbildung fördern.

Das Bundesministerium für Bildung, Wissenschaft und Forschung unterstützt thematisch Initiativen wie z.B. die Cyber-Security-Challenge-Austria und weitere Wettbewerbe zur

Talenteförderung, wie etwa Skills-Austria mit den Kategorie ICT bzw. IKT sowie den weiteren HTL-relevanten Kategorien Mobile Robotics, Mechatronik, Elektronik. Österreichische Schülerinnen und Schüler sowie Studierende nehmen an internationalen Meisterschaften, wie etwa der Europäischen Cyber Security Challenge, teil. Je nach Anlassfall und Thematik erfolgt naturgemäß eine ministeriumsübergreifende Zusammenarbeit.

Zu Fragen 5 und 6 sowie 8 und 9:

- *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 Zusammenhang?
- *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.)*
- *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)?*
- *Planen Sie entsprechende Förderungen (Frage 8) auszubauen bzw. zu erhöhen?*

Für das Bundesministerium für Bildung, Wissenschaft und Forschung ist es wichtig, durch geeignete Formate als Basis frühzeitig das Interesse von Kindern und Jugendlichen für Wissenschaft im Allgemeinen und Technik und Naturwissenschaften im Besonderen zu wecken. Sie sollen auf diese Weise Impulse für die spätere Ausbildungs- und Berufswahl erhalten.

Die Förderung eines reflektierten und sicheren Umgangs mit IKT und digitalen Medien ist Teil des Unterrichtsprinzips Medienbildung, das als Querschnittsmaterie in den Lehrplänen aller Schularten verbindlich verankert ist; auch im derzeit geltenden Lehrplan für die Volksschule. Ziel der Medienerziehung ist Medienkompetenz. Medienkompetenz umfasst vor allem Fähigkeiten wie Selektionsfähigkeit, Differenzierungsfähigkeit, Strukturierungsfähigkeit und das Erkennen eigener Bedürfnisse.

Die mit Beginn des Schuljahres 2018/19 eingeführte verbindliche Übung „Digitale Grundbildung" in der Sekundarstufe I umfasst auch das Thema der IKT- und Cyber-Sicherheit. Beispielsweise weist der Lehrplan folgende Lernziele auf: Schülerinnen und Schüler sind sich der Risiken und Bedrohungen in digitalen Umgebungen bewusst, überprüfen den Schutz ihrer digitalen Geräte und wenden sich im Bedarfsfall an die richtigen Stellen und treffen entsprechende Vorkehrungen, um ihre Geräte und Inhalte vor Viren bzw. Schadsoftware/Malware zu schützen.

In allen Lehrplänen der höheren und mittleren Schulformen der technischen, gewerblichen und kunstgewerblichen Lehranstalten (Sekundarstufe II) sind entsprechende Qualifizierungselemente im Pflichtgegenstandsbereich „Angewandte Informatik" vorgesehen.

Angemerkt wird, dass das Thema Cyber-Security – allem voran in den Fachrichtungen der „Höheren Lehranstalt für Informationstechnologie", der „Höheren Lehranstalt für Informatik" sowie der „Fachschule für Informationstechnik" – in die fachtheoretischen Pflichtgegenstände als integraler Bestandteil in den Unterricht einfließt. Darüber hinaus wird festgehalten, dass von HTL-Schulstandorten im Rahmen von schulautonomen Vertiefungsmöglichkeiten modulare Wahlmöglichkeiten, gegenstandsbezogene Schwerpunktsetzungen sowie Workshops im Bereich der Netzwerk-Security angeboten werden. Im Freigegenstandsbereich werden von den HTLs ebenfalls standortspezifisch individuelle Schwerpunktsetzungen zu „IT-/Cyber-Security" vorgesehen.

Um vermehrt Kinder für technische Ausbildungen zu begeistern, setzen die technischen, gewerblichen und kunstgewerblichen Schulstandorte (HTL) auf Kooperationen mit den Zubringerschulen, wie etwa im Rahmen folgender Projekte: Kindergarten- und Volksschulkinder können von den HTL-Schülerinnen und -Schülern mitgebrachte Anschauungsmaterialien ausprobieren, Information der Beratungslehrpersonen der Zubringerschulen über das Ausbildungsangebot der HTL, Einladung der Eltern der Schülerinnen und Schüler der Zubringerschulen über das Ausbildungsangebot der HTL. Im Rahmen des Projekts „NÖ-Kids go HTL" wurde zwischenzeitlich für über 12.000 Volksschulkinder aus 370 Volksschulen die Möglichkeit eröffnet, an den niederösterreichischen HTLs einen Workshop zu besuchen und im Rahmen dessen, ihre technischen Fähigkeiten und Interessen zu erproben. Dieses Projekt wurde in der Zwischenzeit auch vom Bundesland Steiermark übernommen.

Über die Plattform „Safer Internet" stehen zielgruppenspezifische Angebote für Pädagoginnen und Pädagogen sowie für Schülerinnen und Schüler zur Verfügung. Unterrichtsmaterialien zu verschiedenen Themen und für alle Schularten geben Impulse und zeigen Lehrenden Beispiele auf, wie sie Cybersicherheit und damit im Zusammenhang stehende Themen wie z.B. Datenschutz, Schutz der Privatsphäre u. a. in ihren Unterricht einbeziehen und an die Schülerinnen und Schüler vermitteln können. Der jährliche „Safer Internet Aktionsmonat" im Februar lädt alle Bildungseinrichtungen ein, Projekte zu IKT- und Cybersicherheit durchzuführen. Die Angebote von Saferinternet.at werden regelmäßig an Schulen kommuniziert. Das Österreichische Institut für angewandte Telekommunikation (ÖIAT) wurde mit Leistungen im Bereich von Contententwicklung, Broschürenservice sowie Vermittlung von Trainerinnen und Trainern beauftragt.

Der MOOC „Das Internet im Unterricht – aber sicher" bietet Lehrenden, Lehramtsstudierenden sowie Multiplikatorinnen und Multiplikatoren einen Überblick über die

sichere Nutzung von digitalen Medien sowie Internet und gibt Impulse zur pädagogischen Vermittlung im Unterricht. Über das Netzwerk innovativer Schulen „eEducation Austria" werden unter anderem spezifische Fortbildungsangebote zur Förderung einschlägiger Kompetenzen der Lehrenden unterstützt.

Das Bundesministerium für Bildung, Wissenschaft und Forschung hat es sich auch im Rahmen des gesamtösterreichischen Universitätsentwicklungsplans 2019-2024 zum Ziel gesetzt, Jugendliche vermehrt für ein Studium im Bereich Technik/Informatik zu interessieren. Daher ist vorgesehen, mit Universitäten im Rahmen der Leistungsvereinbarungen für die kommende Periode 2019-2021 auch Outreach-Maßnahmen und innovative Formate zu vereinbaren, die die Maßnahmen der regulären Studieninformation und Studienberatung entsprechend ergänzen sollen. Die Entwürfe der Universitäten für die Leistungsvereinbarungen 2019-2021 beinhalten entsprechende Vorhaben.

Das Bundesministerium für Bildung, Wissenschaft und Forschung fördert im Programm Sparkling Science seit 2007 Forschungsprojekte, in welchen Schülerinnen und Schüler aller Schulstufen aktiv in den Forschungsprozess einbezogen werden. In diesen Projekten unterstützen Schülerinnen und Schüler die Forschenden bei der wissenschaftlichen Arbeit und bei der Vermittlung der gemeinsamen Forschungsergebnisse an die Öffentlichkeit.

Zu Frage 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?*

Im Universitätsbereich gilt es, den Studierenden die Grundzüge des Themas „Cybersecurity" bzw. „Sicherheit im Internet" im Rahmen von Angeboten zu digitalen Grundkompetenzen zu vermitteln. Es gibt für die Studierenden bereits an einigen Universitäten die Möglichkeit, im Rahmen eines spezifischen Studienangebots (z.B. Erweiterungscurriculum „Computational Thinking" an der Universität Wien) entsprechende digitale Grundkompetenzen zu erwerben. In den Leistungsvereinbarungen 2019-2021 werden mit weiteren Universitäten solche Zusatzangebote vereinbart. So wird beispielsweise die Universität Innsbruck einschlägige Studienergänzungen (30 ECTS) oder Erweiterungsstudien entwickeln, an der Universität Klagenfurt ist die Einrichtung eines Erweiterungsstudiums zu „Digitalen Kompetenzen" vorgesehen. Die Universität Graz wird ein Angebot zur Basiskompetenzvermittlung „Digitalisierung" etablieren, das digitale Kompetenzen in praktischer Anwendung und Erfahrung sowie Informationsbeurteilung beinhaltet. Die Universität Salzburg wird ihre Studienergänzungen in Richtung digitale Grundkompetenzen ausbauen. Die Universität für Bodenkultur Wien plant die Schaffung von „Computational Thinking"-Modulen in ihren Curricula und die Implementierung einer Lehrveranstaltung „Computational Thinking".

Über die derzeit eingerichteten, breit angelegten Studienangebote im Studienfeld Informatik (15 Bachelorstudien, 25 Masterstudien) hinaus werden mit Universitäten in den Leistungsvereinbarungen 2019-2021 neue Studienangebote vereinbart, die sich auch mit dem Thema IT-Sicherheit – aus spezifischem Blickwinkel – beschäftigen sollen, beispielsweise ein interdisziplinäres Bachelorstudium „Digitalisierung – Information – Gesellschaft" an der Universität Salzburg.

An den Fachhochschulen (FH) widmen sich im Wintersemester 2018/19 etliche Studiengänge, wie „Sichere Informationssysteme" (Bachelor- und Masterstudiengang, beide Vollzeit) oder „Information Security Management (Masterstudiengang, berufsbegleitend) an der Fachhochschule Oberösterreich, „IT-Security (Masterstudiengang, berufsbegleitend) an der Fachhochschule Technikum Wien bzw. „IT & Mobile Security" (Masterstudiengang, berufsbegleitend) an der Fachhochschule Joanneum, thematisch explizit dem Thema Cyber-Security, wobei hervorgehoben werden muss, dass Lehrveranstaltungen oder Vertiefungen zum Thema IT-Sicherheit auch in anderen Informatik- und Software-Engineering-Studiengängen curricularer Bestandteil sind. Hinzuweisen ist noch auf den Umstand, dass viele der angebotenen FH-Studiengänge berufsbegleitend studierbar sind. Auf Doktoratsebene kann auf das aufgrund einer institutionellen Kooperation zwischen der Technischen Universität Wien und der FH Technikum Wien eingerichtete gemeinsame Doktoratskolleg „Resilient Embedded Systems" hingewiesen werden, welches erstmals im Wintersemester 2018 den Studienbetrieb aufnimmt.

Im Rahmen der Initiative Erwachsenenbildung spielt die Vermittlung der digitalen Kompetenz im Programmbereich Basisbildung eine wesentliche Rolle.

Zu Frage 10 (einschließlich vorangestelltem Satz):

- *Angesichts der Tatsache, dass Lehrer_innen derzeit keine besondere Ausbildung im Bereich „Sicherheit" bzw. „Cybersecurity" und verwandten Feldern erhalten:*
- *Planen Sie Themen wie „Sicherheit" bzw. "Cybersecurity", „Gesamtsystemverständnis" (als Gegensatz zur reinen „Anwendungskompetenz") verpflichtend in der Lehrer_innenausbildung zu verankern?*

Das Thema IT-Sicherheit bzw. Cyber-Sicherheit ist in den Curricula der Lehramtsstudien in unterschiedlichen Ausprägungen enthalten. Explizite Medienschwerpunkte sind in einigen Curricula der Primarstufe verankert. Die Ausbildung für das Lehramt in der Sekundarstufe Allgemeinbildung enthält eine Auseinandersetzung mit verschiedenen Aspekten der Digitalisierung. In der Sekundarstufe Allgemeinbildung wird der Gegenstand Informatik in gemeinsam eingerichteten Studien zwischen Universitäten und Pädagogischen Hochschulen geführt. IT-Sicherheit bzw. Cyber-Sicherheit wird in Lehrveranstaltungen zur allgemeinen „Netzwerksecurity" thematisiert.

Die Lehramtsausbildungen im Unterrichtsfach „Informatik und Informationsmanagement" sehen in allen vier Verbundregionen (Nordost, Südost, West und Mitte) eine Auseinandersetzung mit rechtlichen und sicherheitstechnischen Belangen beim Umgang mit Daten, Software und Medien vor. Im Verbund West wird die Spezialisierung Medienpädagogik angeboten, deren Zielsetzungen unter anderem in der Qualifizierung zur Evaluation und Kritik von Medien und Informationstechnologien gelegen sind.

In den Curricula der Sekundarstufe Berufsbildung für das Studienfach Information und Kommunikation, das an Pädagogischen Hochschulen alleine geführt wird, sind vielfach die Themen IT-Security, Safer Internet, Websecurity u.a. enthalten.

Weiters wird auf das Model für digitale Kompetenzen von Pädagoginnen und Pädagogen (digi.kompP) hingewiesen, das unter anderem auch den reflektierten und sicheren Umgang mit digitalen Technologien, Datenschutz und Datensicherheit umfasst. Ausgehend vom Kompetenzmodell digi.kompP bündelt die Maßnahme „digi.folio" alle thematischen Fortbildungsangebote der Pädagogischen Hochschulen. „digi.folio" als modulares Ausbildungsangebot zur Weiterentwicklung der digitalen Kompetenzen steht prinzipiell allen Pädagoginnen und Pädagogen offen, richtet sich aber insbesondere an neu in den Dienst eintretende Lehrkräfte. Dabei setzen sich Lehrpersonen mit Themen wie z.B. Sicherheit im Netz, Cybermobbing, Hetze, Hass und Fake News auseinander und sind aufgefordert, diese in den Unterricht einzubringen, um Schülerinnen und Schüler zu einem kompetenten und kritischen Auftreten in der digitalen Welt zu befähigen.

Digitalisierung, neue Möglichkeiten der Vermittlung von Inhalten bzw. Möglichkeiten, sich diese anzueignen, sollen im Rahmen des zur Zeit in Entwicklung befindlichen Masterplans zur Digitalisierung im Bildungswesen systematisch in der Ausbildung bzw. Fort- und Weiterbildung von Pädagoginnen und Pädagogen verankert werden.

Zu Fragen 11 und 12:

- *Wie bzw. mit welchen konkreten Maßnahmen unterstützen Sie Schulen und Lehrer_innen dabei, Expert_nnen aus entsprechenden Bereichen in den Unterricht zu bringen, um diese Kenntnisse zu vermitteln?*
- *Welche Partnerschaften (z.B. mit der Privatwirtschaft) gibt es, um entsprechende Expert_innen in Schulen zu bringen, und wie erfolgreich sind diese?*

Grundsätzlich ist darauf hinzuweisen, dass es den einzelnen Lehrpersonen im Rahmen ihrer eigenständigen und eigenverantwortlichen Gestaltung des Unterrichts nach Maßgabe der §§ 14, 17 und 56 des Schulunterrichtsgesetzes frei steht, außerschulische Personen in den Unterricht, z.B. zu speziellen Themen wie etwa Cyber-Sicherheit, einzubinden.

Forschende können beispielsweise im Rahmen von Sparkling Science-Projekten in Schulen ihr Wissen vermitteln. Besonders im Rahmen dieses Vermittlungsformats wurde ein Fokus

auf langfristige Kooperationen zwischen Schule und Wissenschaft gelegt. Die Forschungseinrichtungen liefern Themenanregungen für vorwissenschaftliche Arbeiten, halten regelmäßig Workshops und Vorträge in den Schulen, laden die Schülerinnen und Schüler an ihre Einrichtungen zu Laborbesuchen, Vorlesungen etc. ein oder bieten Sommerpraktika an.

Weitere Kooperation bestehen mit „Safer Internet", aber auch im Rahmen der kriminalpräventiven Angebote zur sicheren Nutzung digitaler Technologien im Zuge des Projekts Cyberkids, die Schulen abrufen können, ergeben sich entsprechende Kooperationen mit außerschulischer Expertise.

Etwa 125 Forscherinnen und Forscher besuchen als Young Science-Botschafterinnen und -Botschafter ehrenamtlich Schulen in ganz Österreich und erzählen von ihrem Forschungsfeld und ihrem beruflichen Werdegang. Schülerinnen und Schüler haben so die Möglichkeit, Fragen direkt an Forschende zu stellen und Einblicke in deren Arbeitsalltag zu erhalten.

Zu Frage 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.)*

Die Curricula der Bachelorstudien im Studienfeld Informatik sehen in der Regel Lehrveranstaltungen oder Module zum Thema Cyber-Security/IT-Sicherheit vor. Diese Lehrveranstaltungen sind prinzipiell auch für Studierende anderer Bereiche – als Wahlfächer oder frei wählbare Fächer – zugänglich. So beinhalten die Curricula der Bachelorstudien der Informatik an der TU Wien Module zu „Security" oder „Security und Recht", z.B. mit Lehrveranstaltungen, die in Themenstellungen wie „Security", „Privacy Enhancing Technologies" oder „Modern Cryptography" einführen. Das Bachelorstudium „Informatik" an der Universität Salzburg beinhaltet ein Modul „Netze und Sicherheit", mit Vorlesung bzw. Lehrveranstaltung zur „Einführung Kryptographie und IT Sicherheit". Auch das Bachelorstudium der Informatik an der TU Graz beinhaltet eine Einführung in IT-Sicherheit („Introduction to Information Security").

Die meisten Masterstudien im Informatikbereich enthalten weiterführende Pflichtlehrveranstaltungen zu IT-Sicherheit oder ermöglichen Wahlmodule (z.B. „IT Sicherheit", „Multimedia und Sicherheit", „Media Security"), Spezialisierungen oder Vertiefungen zum Bereich IT-Sicherheit. Beispielsweise ermöglicht das Masterstudium Computer Science an der Universität Linz eine Spezialisierung in „Networks and Security".

Zu Frage 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?*

Neben der bereits zu Fragen 11 und 12 genannten Möglichkeit der Einbeziehung von außerschulischen Expertinnen und Experten in den Unterricht, wurden insbesondere durch das neue Lehrpersonendienstrecht „Pädagogischer Dienst" attraktivere Bedingungen für Quereinsteigerinnen und Quereinsteiger geschaffen. Die Anrechnung von bis zu 12 Jahren einschlägiger Vordienstzeiten und der neue Kurvenverlauf ermöglichen auch bei späterem Berufseinstieg attraktive Einstiegsgehälter. Zusätzlich besteht seit dem Schulrechtsänderungspaket 2016 als Teil der Bildungsreform die Erleichterung des Einsatzes von externen Expertinnen und Experten im Wege von Lehrbeauftragungen.

Zu Fragen 15 bis 17:

- *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.)*
- *Ist geplant, weitere Lehrstühle im Bereich „Cybersecurity" zu schaffen? Falls ja, welche Arten von Professuren, an welchen Universitäten und in welchen Bereichen?*
- *Gibt es besondere Vereinbarungen mit den Universitäten bzgl. der Finanzierung relevanter Lehrstühle, Forschungsprogramme oder Institute?*

Universitäre Lehre und Forschung zu Cyber-Security, IT-Sicherheit, Security and Privacy u.ä. ist an Universitäten verortet, an denen Studien aus dem Bereich Informatik/Wirtschaftsinformatik eingerichtet sind. Lehre und Forschung zu diesem Feld ist allerdings nicht unbedingt an das Vorhandensein eines spezifischen „Lehrstuhls" bzw. einer Professur mit dieser spezifischen Widmung geknüpft. Auch ohne einen solchen bzw. eine solche findet diesbezügliche Lehre und Forschung statt, insbesondere im Rahmen von thematisch einschlägigen oder breiter definierten Forschungsgruppen. Hinter Überbegriffen wie Cyber-Security, Information Security, IT-Sicherheit, Security and Privacy u.ä. steht dabei ein breites Feld von spezifischen Themenstellungen: Formal Methods for Design and Verification, Security Issues in Software Systems, Secure Crypto-implementations, Secure e-Government, Trustworthy Systems, Kryptography, e-Identity, Trusted Computing, RFID Security, Secure Hardware Implementations of Cryptographic Algorithms, Side-channel Analysis, Network Security, Media Security, Digital Identities, Secure Code, Security Infrastructures, Information Security Management, Systems Security, Application Security, Web (application) Security, Database Security, Privacy, Malware, IT Risk Management etc.

Einige Universitäten sehen in ihrem aktuellen Entwicklungsplan, der die beiden Perioden 2019-2021 und 2022-2024 abdeckt, in Zusammenhang mit ihrer Profilbildung die Einrichtung einer Professur mit Widmung im Bereich IT-Security vor. Im Rahmen der neuen Universitätsfinanzierung wird das Bundesministerium für Bildung, Wissenschaft und

Forschung über die Leistungsvereinbarungen 2019-2021 zusätzliches hochqualifiziertes Personal (Professuren und äquivalente Verwendungen) finanzieren, um die Betreuungsrelationen zu verbessern und die Forschungsbereiche zu stärken. Dabei wird unter anderem ein Fokus auf dem Ausbau des Informatikbereichs liegen.

Die Universität Wien, die Technische Universität Wien, die Technische Universität Graz und die Wirtschaftsuniversität Wien sind darüber hinaus wissenschaftliche Partner im Kompetenzzentrum „Secure Business Austria (SBA)", das durch das COMET-Programm („COMET Competence Centers for Excellent Technologies") gefördert wird und auf vier Schwerpunkt-Forschungsbereiche von IT-Sicherheit fokussiert: (1) Governance, Risk and Compliance, (2) Data Security and Privacy, (3) Secure Coding and Code Analysis und (4) Hardware and Network Security.

Wien, 16. November 2018
Der Bundesminister:

Univ.-Prof. Dr. Heinz Faßmann eh.

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR BILDUNG, WISSENSCHAFT UND FORSCHUNG @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Bildung, Wissenschaft und Forschung
	Datum/Zeit	2018-11-16T09:44:31+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	285175223
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at. Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bmbwf.gv.at/verifizierung.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2018-11-16T09:53:03+01:00
	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.	