Februar 2018 · Julia Schuetze

Warum dem Staat IT-Sicherheits-expert:innen fehlen

Eine Analyse des IT-Sicherheitsfachkräftemangels im Öffentlichen Dienst

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

In Deutschland sind derzeit bis zu 51.000 Stellen für IT-Expert:innen unbesetzt. Neben der Wirtschaft spürt auch der Öffentliche Dienst diesen Fachkräftemangel. Da der Staat zunehmend Aufgaben wie die Unterstützung des Schutzes kritischer Infrastrukturen übernimmt und bei der polizeilichen Aufklärung und der Verteidigung vermehrt technische Mittel eingesetzt werden, manifestiert sich der Fachkräftemangel besonders in der IT-Sicherheit: Der Öffentliche Dienst ist hier momentan nicht attraktiv genug, um bei potentiellen Angestellten im Wettbewerb mit der Wirtschaft zu bestehen. Häufig wird die schlechte Bezahlung als Grund genannt, warum IT-Fachkräfte im Öffentlichen Dienst fehlen. Allerdings ist die Höhe der Gehälter nicht allein ausschlaggebend. Der Öffentliche Dienst ist im Vergleich zur Wirtschaft für IT-Expert:innen aus anderen Gründen nicht attraktiv.

Tatsächlich stellt die Vergütung nur eines von vier Problemfeldern dar, welche dazu führen, dass der Öffentliche Dienst im Vergleich zur Wirtschaft für IT-Expert:innen derzeit nicht reizvoll ist:

1. Die starren Gehaltsstrukturen des TvöD sind insbesondere für Spezialist:innen unattraktiv, die zwar umfassende Berufserfahrung, aber keinen oder nur einen niedrigen akademischen Abschluss vorweisen können. Sie verdienen, trotz Erfahrung, durch geringere Abschlüsse, wie Bachelor oder Berufsausbildung, im Öffentlichen Dienst weitaus weniger als in der Wirtschaft.

2. Die unflexiblen Strukturen wie das hierarchisch organisierte Laufbahnrecht, die Bevorzugung von Generalisten und Juristen und traditionelle Arbeitsformen in nicht-interdisziplinären Teams in der Verwaltung, verhindern eine Karriere für IT-Spezialist:innen innerhalb des Öffentlichen Dienstes attraktiv zu gestalten. Das stellt einen Nachteil gegenüber Arbeitsplätzen in der Wirtschaft dar und führt dazu, dass sich eine klare Laufbahn und angemessene Arbeitsumgebung für Informatiker:innen, vor allem in der Verwaltung, nur schwer etablieren lassen.

3. Es fehlt an flexiblen Weiterbildungsmöglichkeiten, obwohl die konstante Weiterentwicklung im Bereich der IT-Sicherheit essentiell ist. Unkonventionelle Methoden, unabhängige Projekte “Freestyle Coding”, Teilnahme an Konferenzen und Simulationen als auch Hackathons sind in der Wirtschaft als Fortbildung anerkannt. Hier steht der Öffentliche Dienst vor der Heraus-

forderung, die Ansprüche an eine Weiterbildung im IT-Sicherheitsbereich mit internen, teilweise starren Strukturen und Vorgaben zu vereinbaren.

4. Das traditionelle Einstellungsverfahren erschwert die Einstellung von Personen, die zwar über das geforderte Know-How, nicht aber über die entsprechenden formalen Abschlüsse verfügen. Dieses Potential in Form von potentiellen IT-Sicherheitsfachkräften darf der Öffentliche Dienst nicht ungenutzt lassen.

Das Bundesministerium für Verteidigung und das Bundesministerium des Innern haben diese prekäre Situation erkannt und zwei Lösungsansätze entwickelt, die den Fachkräftemangel adressieren sollen: Die "Cyberwehr"[1] und die "Cyber Community". Beides sind so genannte 'Pooling und Sharing' Methoden, die es dem Staat erlauben sollen, externe Expert:innen anzuwerben. Beide Optionen sind erste richtige Schritte, um kurz- bis mittelfristig den Öffentlichen Dienst attraktiver zu machen. Beide Lösungsansätze adressieren vor allem das Problem der mangelnden Weiterbildungsmöglichkeiten. Langfristige Herausforderungen, wie die Arbeitskultur, die fehlenden Karrieremöglichkeiten und die traditionellen Einstellungsverfahren werden nicht adressiert und erschweren es IT-Sicherheitsexpert:innen in den Öffentlichen Dienst zu integrieren und die Arbeitsformen den neuen Herausforderungen anzupassen. Für die tieferen strukturellen Probleme, die zur mangelnden Attraktivität des Öffentlichen Dienstes führen, reichen diese 'Pooling und Sharing'-Methoden also nicht aus.

Parallel zu den genannten Lösungsansätzen muss der Staat daher weitere Konzepte entwickeln, die langfristig funktionieren und den stetig wachsenden Bedarf an Fachkräften decken. Wenn der Öffentliche Dienst nicht modernisiert wird, wird er bei wachsender Zuständigkeit im Bereich IT-Sicherheit bald an seine Belastungsgrenze stoßen: Besonders in Krisensituationen wird ein personell und fachlich unterbesetzter Öffentlicher Dienst die IT-Sicherheit nicht gewährleisten können – oder der Staat muss immer höhere Summen aufwenden, um externe Dienstleister einzukaufen.

1 Die Cyberwehr befindet sich in fortgeschrittener Planungsphase.

Inhalt

Einleitung 5

1. Ursachen des Fachkräftemangels 6
    Hohe Nachfrage in Wirtschaft und Verwaltung trifft auf kleinen Pool von Expert:innen 6
    Fehlende Ausbildungssystematik durch zu kurzfristige Planung 7

2. Warum ist der Öffentliche Dienst im Vergleich zur Wirtschaft kaum attraktiv? 8
    Niedrigere Gehälter und wenig Möglichkeiten anderer Kompensationsformen 8
    Mangelnde Laufbahnmöglichkeiten, traditionelle Arbeitskultur, wenig attraktive Weiterbildungs-möglichkeiten 11
    Formale Einstellungskriterien schließen viele aus 15

3. Ausgewählte Konzepte der Politik gegen den IT-Sicherheits-fachkräftemangel 16
    Lösungsansatz: “Cyberwehr” (Bundesministerium des Innern) 16
    Lösungsansatz: “Cyber-Reserve & Cyber Community” (Bundesministerium der Verteidigung) 19

Fazit 22

Referenzen 24

Impressum 28

Einleitung

Diese Publikation ist im Rahmen der Arbeit des Transatlantic Cyber Forums der Stiftung Neue Verantwortung entstanden. Das Transatlantic Cyber Forum wird durch die William and Flora Hewlett und die Robert Bosch Stiftung gefördert.

Der IT-Sicherheitsfachkräftemangel wird zu einem immer drängenden Herausforderung für Deutschland. Das Problem ist schon länger bekannt. Es ist Teil des wachsenden Mangels an Mathematik-, Informatik-, Naturwissenschaft- und Technik (MINT)-Fachkräften. Die zu besetzenden Stellen übertreffen weit die Anzahl der bereitstehenden und ausgebildeten Fachkräfte in diesem Bereich. Nach einer Bitkom-Studie gab es 2016 insgesamt 51.000 offene Stellen für IT-Expert:innen[1]. Laut dem Bericht der Bundesagentur für Arbeit aus 2016[2] liegt bei Stellen, die Software-Entwickler:innen mit einem abgeschlossenen Hochschulstudium von mindestens vier Jahren suchen, die Vakanzzeit bei 123 Tagen und die Arbeitslosenquote, derjenigen, die diese Voraussetzungen erfüllen, bei nur drei Prozent. Auch wenn es keine konkreten Daten gibt wird deutlich, dass vor allem erfahrene Bewerber:innen besonders gefragt sind. Der IT-Sicherheitsfachkräftemangel betrifft nun nicht mehr allein die Wirtschaft, sondern auch vermehrt den Öffentlichen Dienst. Ein Beispiel dafür ist der Bereich der IT-Sicherheit, in dem der Staat immer mehr Aufgaben übernimmt. Das Bundesamt für Informationstechnik (BSI) unterstützt beispielsweise den Schutz kritischer Infrastrukturen. Außerdem muss sich eine immer digitaler werdende Verwaltung um die Implementierung von IT-Sicherheits(standards) kümmern. Je digitaler die staatliche Leistungen werden, desto mehr wird die Verwaltung selbst zu einer Art IT-Dienstleister. Durch diese Entwicklung steigt die Anzahl der verfügbaren Stellen gerade im Öffentlichen Dienst stetig an. “Stellen bedeutet aber nicht gleich Menschen,” ließ ein ranghoher Vertreter des Bundeskriminalamts im Januar 2018 verlauten. Viele Stellen sind momentan noch unbesetzt. Auch auf Landesebene werden IT-Spezialist:innen gesucht: Zum Beispiel will das

1 Bitkom, 2017 https://www.bitkom.org/Presse/Presseinformation/Bitkom-Branche-schafft-in-diesem-Jahr-21000-neue-Jobs.html.

2 Bundesagentur für Arbeit, 2016 https://statistik.arbeitsagentur.de/Statischer-Content/Arbeitsmarktberichte/Berufe/generische-Publikationen/Broschuere-Informatik.pdf.

Landeskriminalamt in Baden-Württemberg bis zu 140 IT-Spezialist:innen und das Landesamt für Verfassungsschutz 200 - 300 Personen einstellen.

Auf dem Arbeitsmarkt herrscht ein Mangel an Menschen, die für diese Stellen qualifiziert sind, sodass diejenigen Kandidat:innen, die die Voraussetzungen erfüllen, viele potentielle Arbeitgeber zur Auswahl haben. Diese Situation wird noch zusätzlich dadurch erschwert, dass die Verwaltung mit der Privatwirtschaft um diese Fachkräfte konkurriert. Wenn der Öffentliche Dienst nicht attraktiver wird, um in diesem Wettbewerb besser bestehen zu können, wird sich das Problem vergrößern. Der Mangel hochqualifizierter IT-Fachkräfte auf dem Arbeitsmarkt birgt die Gefahr, dass Deutschland strategisch politische Ziele im Bereich Cybersicherheit nicht umfassend umsetzen kann[3]. Es gibt vorhandene Lösungsansätze aus dem Bundesministerium des Innern und dem Ministerium für Verteidigung, die das Fachkräfteproblem adressieren und den Öffentlichen Dienst attraktiver machen sollen. Inwieweit diese den Fachkräftemangel und die Herausforderungen im Öffentlichen Dienst adressieren, wird in diesem Papier diskutiert.

1. Ursachen des Fachkräftemangels

Hohe Nachfrage in Wirtschaft und Verwaltung trifft auf kleinen Pool von Expert:innen

Der Öffentliche Dienst steht in direkter Konkurrenz mit der Wirtschaft, wenn es um das Werben von IT-Sicherheitsfachkräften geht. Denn IT-Sicherheitsfachkräftemangel ist kein alleiniges Problem des Öffentlichen Dienstes, sondern betrifft ganz Deutschland: Unternehmen sind stark von Cyberangriffen betroffen[4] und benötigen vermehrt spezialisierte Fachkräfte. Die Wirtschaft braucht unter anderem Fachkräfte mit IT-Sicherheitsexpertise, um sichere Software zu entwickeln, die die neuen Technologien von digitalisierten Fahrzeugen zu Smart Home Geräten nutzbar machen. Auch der Staat übernimmt vermehrt Verantwortung für IT-Sicherheit. An vielen Stellen - sowohl auf Landes-, als auch auf Bundesebene, ist die Nachfrage groß. Demnach kon-

3 Zedler, 2016, Seite 151 http://ib.uni-koeln.de/fileadmin/templates/publikationen/aipa/AIPA_2016_2.pdf.

4 Bitkom, 2017 https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf.

BSI, 2018 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber-Angriffe_haben_erhebliche_Konsequenzen_fuer_die_Wirtschaft_31012018.html .

kurriert der Öffentliche Dienst auch mit sich selbst: Das Kommando Cyber- und Informationsraum (KdoCIR) ist ein großer Akteur in diesem Feld, ebenso wie das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Zentrale Stelle für Informationstechnologie im Sicherheitsbereich (ZITiS), aber auch das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA) und der Bundesnachrichtendienst (BND). Sie alle suchen nach IT-Sicherheitsspezialist:innen. Hinzu kommen entsprechende Einrichtungen auf Landesebene: Zum Beispiel sucht die Polizei, der Verfassungsschutz und die Kriminalämter auch auf Länderebene, weil sie durch die vermehrte Nutzung von digitalen Tools ebenfalls auf IT-Sicherheitsexpert:innen angewiesen sind. Zudem sucht die öffentliche Verwaltung spezielle Fachkräfte, die auf dem Markt schwer zu finden sind. Vermehrt wird nach Beschäftigten mit großer IT-Expertise, allerdings nur bedingt nach 100% Informatiker:innen, gesucht. Stattdessen ist vor allem Interdisziplinarität gefragt, um die IT-sicherheitsrelevanten Probleme der öffentlichen Verwaltung zu lösen. Vermehrt wird in Bundes- und Landesbehörden im Bereich E-Government oder der polizeilichen Arbeit sowohl IT-Kenntnisse als auch fachspezifisches Wissen in der Verwaltung verlangt. Für die Umsetzung der Digitalisierung der Verwaltung wird dringend IT-Sicherheitsexpertise benötigt. Auch die Bundeswehr sucht nach Personen, die spezielle Schnittstellenerfahrung haben.

Die Vielzahl der neuen Aufgaben in diesem Bereich übersteigt die Anzahl der Fachkräfte, die passend qualifiziert sind und darüber hinaus eine Karriere im Öffentlichen Dienst in Betracht ziehen, was sich in den vielen freien Stellen manifestiert. Ob Wirtschaft oder Verwaltung – viele Akteure fischen im selben Pool mit wenigen Expert:innen.

Fehlende Ausbildungssystematik durch zu kurzfristige Planung

Da das Themengebiet IT-Sicherheit noch ein relativ neues Aufgabengebiet innerhalb des Öffentlichen Dienst ist, fehlte es an einer Ausbildungssystematik, die den Öffentlichen Dienst rechtzeitig mit eigenem Personal hätte versorgen können. Für den Öffentlichen Dienst zählt letztendlich ein eindeutiges strategisches Mandat, damit danach die Ressourcen eingesetzt werden können oder nicht vorhandenes Potential ausgebildet werden kann. Erschwerend kommt hinzu, dass diese Art von Personalplanung nicht allein in den Zuständigkeitsbereich der Ministerien des Bundes oder Landes fällt, die verantwortlich für IT-Sicherheit sind, sondern es müssen immer auch erst die haushalterischen und finanziellen Voraussetzungen geschaffen werden. Dies erschwert den flexiblen Umgang mit neuen Herausforderungen und Aufgaben für den Öffentlichen Dienst. Da der Öffentliche Dienst deshalb nur

begrenzt selbst ausbilden konnte, ist er nun wie die Wirtschaft auf den Arbeitsmarkt angewiesen. Eine frühe Planung, was der Öffentliche Dienst im Rahmen von IT-Sicherheit leisten soll, ist deswegen auch weiterhin imminent. Die Bundeswehr hadert immer noch damit, was zukünftig ihre Aufgabe im Cyberraum sein soll. Dennoch wird sie sich bewusst, dass sie sich für zukünftige Zuständigkeiten passend aufstellen muss und unternimmt Maßnahmen, um dies, wenn der Zeitpunkt kommt, auch zu können. Die Bundeswehr stellt sich auf – ohne genau zu wissen, "welche Fähigkeiten die Bundeswehr im Bereich Cyber- und Informationsraum benötigt"[5].

Das ersetzt aber ohne genaue politische Vorgaben nicht eine klare Ausbildungssystematik, wie es in anderen Zuständigkeiten der Fall ist. Der unflexible Stellenplan erschwert die vorausschauende Planung und Reaktion auf neue Aufgaben im Öffentlichen Dienst. Der Öffentliche Dienst ist demnach auf eine Zukunft denkende Politik angewiesen, um sich neuen Herausforderungen stellen zu können. Dies wurden in den letzten Jahren versäumt, was sich negativ auf die Ausbildung von IT-Sicherheitsfachkräften auswirkt.

2. Warum ist der Öffentliche Dienst im Vergleich zur Wirtschaft kaum attraktiv?

Es gibt formelle und strukturelle Gegebenheiten, die den Öffentliche Dienst weniger attraktiv als die Privatwirtschaft machen: Die Gesetzeslage lässt im Vergleich zur Privatwirtschaft weniger Gestaltungsspielraum – zum Beispiel in Hinblick auf die Vergütung, der Ausgestaltung des Tätigkeitsfeldes oder der Berufsvoraussetzung, wie Bildungsabschlüsse.

Niedrigere Gehälter und wenig Möglichkeiten anderer Kompensationsformen

Ein Problem sind die strikten Vergütungsmodelle, die weniger leistungsorientierte oder flexible Vergütungen zulassen. Dies ist vor allem ein Problem,

5 Mario Hempel, Leiter Reservistenarbeitsgemeinschaft Cyber in der Loyal, p.47 Ausgabe 1/2018

wenn man Spezialist:innen mit mehr als zehn Jahren Berufserfahrung einstellen möchte.

In der Studie des Jobportals StepStone werden Informatiker:innen zwei Jahre nach dem Studium im Durchschnitt mit 46.533[6] Euro pro Jahr vergütet. Bei einem Bachelorabschluss entspricht dies etwa der Gehaltsgruppe E9 - E12 Stufe 1-3 festgelegt im Tarifvertrag im Öffentlichen Dienst (TvöD) Bund[7]. Bei E12 Stufe 2 wäre das zum Beispiel ca. 43.600 Euro[8]. In dieser Gruppe gibt es demnach noch keinen großen Unterschied in der Vergütung von öffentlicher Verwaltung und Privatwirtschaft. Anders sieht es nach längerer Berufserfahrung aus. Erfahrene Software-Entwickler:innen (+10 Jahre) mit und ohne Studium verdienen in der Privatwirtschaft wesentlich mehr: Hier können Expert:innen mit Studium ein Einkommen von durchschnittlich ca. 73.150 Euro erwarten und erfahrene Softwareentwickler:innen mit Berufsausbildung bis zu ca. 59.760 Euro[9]. IT-Sicherheitsexpert:innen bekommen laut einer Studie von Compensation Partners von 2017 am meisten Gehalt mit durchschnittlich 74.600 Euro. Auch IT-Pojektleiter:innen mit mehr als 10 Jahren Berufserfahrung rechnen mit durchschnittlich 76.000 jährlich.[10] Im Öffentlichen Dienst können da nur Erfahrene mit Masterabschluss mithalten, die bis zu ca. 86.000 Euro verdienen können. Dieses Gehalt steht allerdings nur denjenigen zu, die den Großteil ihrer Arbeitsjahre im Öffentlichen Dienst gearbeitet haben. Ein:e IT-Spezialist:in mit Masterabschluss bekommt nicht automatisch die höchste Gehaltsstufe angerechnet. Die Stufen (1-6) werden für bestimmte Zeit in der bestimmten Stellung (E6 - E15Ü) und der jeweiligen Stufe vergeben[11]. Also müsste ein:e Expert:in bei der Bewerbung zumindest beweisen, dass er:sie schon mehrere Jahre Aufgaben der jeweiligen Gehaltsgruppe, zum Beispiel E15 in der Privatwirtschaft übernommen hat, um eine höhere Stufe angerechnet zu bekommen. Ansonsten würde die Person mit einem Gehalt von ca. 52.560 Euro (E15 Stufe 1) beginnen und erst nach entsprechenden Dienstjahren[12] ein Gehalt von ca. 85.000 Euro (E15 Stufe

6 StepStone, 2017 https://entwickler.de/online/development/arbeitsmarkt-entwickler-gehalt-trends-2017-579800476.html.

7 http://www.oeffentlichen-dienst.de/entgelttabelle/tvoed-bund.html.

8 Angaben mit ca. sind gerundet.

9 Siehe Fußnote 6.

10 Der große Gehaltsvergleich in der Informatik, 2017 https://www.computerwoche.de/a/der-grosse-gehaltsvergleich-fuer-it-fachkraefte-2015-6,3218378.

11 http://oeffentlicher-dienst.info/tvoed/bund/stufen.html.

12 http://oeffentlicher-dienst.info/tvoed/bund/stufen.html.

6) erhalten. Um die höchste Stufe (Stufe 6) erreichen zu können, müssen 16 Jahre absolviert werden.

Wenn der:die Expert:in einen Bachelorabschluss hat, endet das Gehalt bei ca. 56.000 Euro (E13 Stufe 6) und Erfahrene mit Berufsausbildung erreichen maximal ein Gehalt von bis zu ca. 39.200 Euro[13]. Das ist problematisch, da IT-Sicherheitsexpertise nicht nur an einem Abschluss gemessen werden kann. Nur in Ausnahmefällen wird (auch) außertariflich bezahlt. Zusammenfassend ist für IT-Expert:innen im gehobenen oder höheren Dienst unter drei Jahren kein wesentlicher Unterschied zur Wirtschaft festzustellen. Auch bei Mitarbeiter:innen im Anwendersupport und in der Administration kann der Öffentliche Dienst durchaus mithalten.[14]

Allerdings wird für Spezialist:innen mit mehrjähriger Berufserfahrung und einem niedrigen / ohne akademischen Abschluss das starre TvöD finanziell sehr schnell unattraktiv.

Zudem kommt, dass im Öffentlichen Dienst leistungsorientierte Vergütung nur in Ausnahmen möglich ist. In der Bundesverwaltung gibt es zum Beispiel drei Arten der leistungsorientierten Vergütung: die Leistungsstufe (Vorziehen der nächsten Dienstaltersstufe bei dauerhaft herausragenden Gesamtleistungen), die Leistungszulage (Anerkennung einer bereits über einen Zeitraum von mindestens drei Monaten erbrachten, auch für die Zukunft erwarteten herausragenden besonderen Einzelleistung) und die Leistungsprämie (bei einer herausragenden besonderen Einzelleistung).[15] Dies ist aber nicht in allen Ländern gleich geregelt. Informatiker:innen können aber gegenüber anderen Berufsgruppen innerhalb des Öffentlichen Dienstes nicht bevorzugt behandelt werden. Da nicht alle IT-Expert:innen im Öffentlichen Dienst außertariflich bezahlt werden können, muss geprüft werden, inwieweit der Öffentliche Dienst in anderen Aspekten attraktiver sein kann.

Neben finanziellen Anreizen sind ist es für den Öffentlichen Dienst ebenso schwierig andere Kompensationsformen, die in der Wirtschaft praktiziert werden und Teil der Unternehmenskultur sind, anzubieten. Nicht-traditionelle Ausgleiche sind zum Beispiel kostenloser Kaffee, kostenlose Snacks und Obst, betrieblich organisierte Veranstaltungen, kostenlose, bzw. ver-

13 Siehe Fußnote 6.

14 Durchschnittlich 42 000 Euro, siehe https://www.computerwoche.de/a/der-grosse-gehaltsvergleich-fuer-it-fachkraefte-2015-6,3218378.

15 DGFP e.V. 10/2004 https://www.fuehrungstraining.de/sm-projekte/129-sm-projekt-tvoed/infos/einstiegsinfo.pdf.

günstigte Mitgliedschaften für Mitarbeiter:innen oder sogar Firmenwagen. Rund 26 Prozent aller IT-Fachkräfte haben in der Wirtschaft zudem eine Prämienregelung und unter den IT-Führungskräften sind es knapp 63 Prozent. Einen Firmenwagen fahren zwölf Prozent und 45 Prozent aller Führungskräfte[16]. Diese Faktoren tragen zur Ungleichheit bei und kreieren einen Nachteil neben dem Gehalt im Vergleich zur Wirtschaft.

Bezahlung Öffentlicher Dienst versus Privatwirtschaft[17]

Erfahrung	TvÖD	Privatwirtschaft
Bachelorstudium+ 2 Jahre Arbeitserfahrung	ca . 43.200 Euro (E12, 2/ 2 J.)*	46.533 Euro
Berufsausbildung + 10 Jahre Arbeitserfahrung	max. ca. 37.800 Euro (E9a, 4/ 10 J.)*	59.754 Euro
Bachelor + 10 Jahre Arbeitserfahrung	max. ca. 55.100Euro (E12, 4/ 10 J.)*	73.143 Euro
Master + 10 Jahre Arbeitserfahrung	max . ca. 68.000 Euro (E15, 4/ 10 J.)*	73.143 Euro

** (Tarifvertrag Öffentlicher Dienst, Stufe/Anzahl Dienstjahre, nach der diese Stufe in der Regel erreicht wird)*

Mangelnde Laufbahnmöglichkeiten, traditionelle Arbeitskultur, wenig attraktive Weiterbildungsmöglichkeiten

Wichtiger als das Geld ist zumindest angehenden Informatiker:innen und damit potenziellen Mitarbeiter:innen des Öffentlichen Dienstes, die Unternehmenskultur, die Aufgaben und ihre Entwicklungschancen[18]. “Zwei Drittel würden einen Job ausschlagen, wenn die Unternehmenskultur des Arbeit-

16 https://www.computerwoche.de/a/der-grosse-gehaltsvergleich-fuer-it-fachkraefte-2015-6,3218378.

17 Alle Angaben ergeben sich aus den genannten Studien.

18 laut einer Umfrage des Meinungsforscher Trendence.

gebers nicht zu ihnen passt", erläutert Jörn Klick von Trendence[19]. Die Kultur des Öffentlichen Dienstes wirkt sich durchaus hinderlich auf die Gewinnung von Fachkräften aus. Die Kultur bildet außerdem einen starken Gegensatz zu Unternehmenskulturen von IT-Firmen, die auch um IT-Sicherheitsspezialist:innen werben.

Durch die neuen Aufgaben und den entstehenden Fachkräftemangel wird der Öffentliche Dienst mehr denn je gezwungen, sich mit den seit jahrzehnten gefestigten Strukturen zu beschäftigen.

"Im Zuge gesellschaftlicher und politischer Veränderungsprozesse sprechen viele Wissenschaftler:innen von einem ausgeprägten Reform- und Modernisierungsbedarf der öffentlichen Verwaltung, insbesondere aufgrund nachlassender Leistungsfähigkeit und zunehmender Komplexität der Verwaltungsaufgaben"[20] Verwaltungsaufgaben werden digitalisiert, was sie komplexer als je zuvor macht. Zum Beispiel in dem Bereich E-Government, wird zukünftig vermehrt mit persönlichen Daten oder personenbezogenen Daten von Bürger:innen umgegangen. Neu ist auch, dass Tätigkeitsfelder interdisziplinärer werden, indem sie digitaler werden. Um bei der zunehmenden Digitalisierung Sicherheitsaspekte nicht zu vernachlässigen, sollte IT-Sicherheit ein wesentlicher Faktor sein. Teams müssen dabei bereichsübergreifend zusammenarbeiten. Völlig neue Aufgaben, wie zum Beispiel die Gewährleistung der IT-Sicherheit eines Bürgerportals, verlangt neue Expertise in der öffentlichen Verwaltung. Allerdings tut sich traditionelles Personalmanagement mit Interdisziplinarität und weiteren neuen Anforderungen rund um IT-Sicherheit noch schwer. "Die restriktiven gesetzlichen Bedingungen – insbesondere das Beamtenrecht und das komplizierte Tarifrecht – prägen das Personalmanagement in öffentlichen Verwaltungen"[21].

Mangelnde Laufbahnmöglichkeiten und traditionelle Arbeitskultur

Die lange Tradition des Berufsbeamtentums, welche über die Jahre eine eigene Kultur mit tief verwurzelten Verhaltensweisen und einer spezifischen

19 Weigner, 2015 https://www.computerwoche.de/a/arbeiten-wie-ein-beamter-verdienen-wie-ein-manager,3099407.

20 vgl. hierzu u.a. Becker et al. 2009; Schedler 2006; Budäus 1994; Naschold/ Begumil 1998) https://www.uni-muenster.de/imperia/md/content/ifpol/sic/abschlussarbeiten/ba_stegemann.pdf.

21 DGfP e.V., 2004 https://www.dgfp.de/fileadmin/user_upload/DGFP_e.V/Medien/Publikationen/Praxispapiere/200410_Praxispapier_oeffentlich.pdf.

Mentalität hervorgebracht hat[22], ist schwierig mit dieser neuen Berufsgruppe zu vereinbaren. Zudem sind Rechtssicherheit und Kontinuität wichtige Grundlagen für die Arbeitsweisen des Öffentlichen Dienstes. Als Antwort auf diese Erwartungen haben sich festgefügte Strukturen mit einer klaren Linienorganisation herausgebildet. "Dadurch, dass von Verwaltungen zunehmend Flexibilität und Veränderungen erwartet werden, stehen sie mehr und mehr in einem Spannungsfeld sich widersprechender Anforderungen" das ergab eine Studie der Deutsche Gesellschaft für Personalführung, e.V. im Jahr 2004.[23] Für die Personalentwicklung in öffentlichen Verwaltungen spielen traditionell Gleichstellungspläne und das Laufbahnrecht eine wichtige Rolle. Auch der Gedanke der Jobrotation mit dem Ziel, die Mitarbeiter:innen mit möglichst vielen Abteilungen und Tätigkeiten vertraut zu machen, ist typisch für Personalentwicklungskonzepte im öffentlichen Dienst. Besonders in der öffentlichen Verwaltung ist dies eine Herausforderung, weil dort in der Regel Generalist:innen und nicht Spezialist:innen angestellt werden. Ein:e IT-Sicherheitsspezialist:in muss allerdings in einem sehr speziellen Aufgabenbereich immer besser werden, da sich IT-Sicherheit von Natur aus ständig neuen Herausforderungen stellen muss. Zudem braucht der Öffentliche Dienst Personen, die flexibel auf neue Herausforderungen, wie IT-Sicherheit reagieren können und Ideen ausprobieren können ohne langwierige hierarische Abläufe zu durch laufen. In den starren Strukturen des Öffentlichen Dienstes fällt es immer noch schwer, eine klare Laufbahn und angemessene Arbeitsumgebung für Informatiker:innen zu skizzieren. Informatiker:innen, die nicht im Öffentlichen Dienst sind, fehlt ein Einblick darüber, was ihre konkreten Aufgabenfelder wären[24] und wie diese sich entwickeln könnten[25]. Persönliche Erfahrungsberichte von Informatiker:innen in einer Landesverwaltung bestätigen, dass sie zum Beispiel nur schwer Führungspositionen erreichen können, da der Öffentliche Dienst von Jurist:innen geprägt ist und ihnen die Vorstellung einer Laufbahn im öffentlichen Sektor fehlt.[26] Diese eher anektdotische Evidenz sollte man durch Erhebungen quantitativ anreichern. Welche möglichen Karrieremöglichkeiten für Informatiker:innen innerhalb des Öffentlichen Dienstes bestehen oder zukünftig bestehen könnten, sollte evaluiert und dann auch kommuniziert werden, um die entsprechenden Zielgruppen zu erreichen. Praktische Hürden, wie die dreijähri-

22 Siehe Fußnote 14.

23 Siehe Fußnote 14.

24 IT-Sicherheitsexpert:in im Workshop.

25 Ausnahme BSI, da IT-Sicherheitsbehörde und Laufbahn innerhalb BSI klarer zu skizzieren.

26 https://www.forum-3dcenter.org/vbulletin/archive/index.php/t-550136.html.

ge Probezeit für Fachkräfte, die im gehobenen Dienst arbeiteten, dann aber ihren Masterabschluss absolviert haben, um in den höheren Dienst aufsteigen zu können, sollten überdenkt werden.

Der deutsche Öffentliche Dienst ist zudem auch speziell, da es nicht so einfach ist, wie in anderen Ländern, nur für bestimmte Zeit in den Staatsdienst einzutreten und dann nach einer Zeit wieder zurück in die Privatwirtschaft, Zivilgesellschaft oder Wissenschaft zu wechseln. Das ist in Deutschland weder vorgesehen noch leicht möglich und birgt sogar Nachteile, zum Beispiel würden Beamte ihre Beamtenpensionsansprüche verlieren und müssten Sozialversicherungsbeiträge, die man für die Beamtenjahre bekommt nachzahlen. Hier geht wichtige Expertise und Erfahrung verloren, die ein Wechsel zwischen verschiedenen Sektoren mitbringt. Es ist auch ein Hemmnis, gute Spezialist:innen, wenn auch nur auf Zeit, in die Verwaltungen zu bekommen.

Nicht angemessene Weiterbildungsmaßnahmen

IT-Sicherheitspezialist:innen müssen ständig dazulernen, um sich zu spezialisieren und auf dem neuesten Stand zu bleiben. In der jetzigen Verwaltungsfachausbildung spielen die Vermittlung von digitalen Fähigkeiten noch keine große Rolle[27]. Dies wirkt sich auch auf das vorhandene Weiterbildungsangebot innerhalb des Öffentlichen Dienstes aus, was für IT-Sicherheitsfachkräfte nicht angemessen und flexibel genug ist.

Im Öffentlichen Dienst gibt es Fortbildungsangebote, zum Beispiel zur Weiterbildung von Fachwissen wie dem Beamtenrecht oder für die Entwicklung von Führungs- und Sozialkompetenzen, welche für Personalverantwortung wichtig sind. Bei den Qualifizierungsangeboten zur Weiterentwicklung der Führungskompetenzen handelt es sich um eine bewusste Abgrenzung gegenüber dem „Konzept der besten Fachkraft“[28]. Für IT-Sicherheitsspezialist:innen sind Weiterbildungen sehr wichtig. In der Wirtschaft gehören zu Weiterbildungen Dienstreisen zu Konferenzen, wie die Black Hat, eine der größten Konferenzen für IT-Sicherheit, Seminaren oder auch Zeit für persönliche Weiterentwicklung, wie eigene Projekte a la freies Forschen oder „Freestyle Coding“. Weiterbildungsmöglichkeiten sind in dem Sinne ein Zusatz zum Gehalt, und sie dienen auch dazu IT-Sicherheit zu erlernen oder zu vertiefen. Das Studium ist im Bereich der IT-Sicherheit nicht allumfassend

27 http://www.langkabel.de/die-blinden-stellen-bei-der-suche-nach-der-digitalen-verwaltung-teil-1/.

28 Siehe Fußnote 14; Seite 17.

und die immer neuen Entwicklungen setzen weitere Bildung und praktische Kenntnisse voraus.

Allerdings bedeutet Weiterbildung nicht gleich offizielle Weiterbildung – das Können und die Freiheit, sich selbst etwas beizubringen und unabhängig zu lernen, muss auch berücksichtigt werden können, denn der:die ideale Kandidat:in, denn der:die ideale Kandidat:in weist entscheidende Fähigkeiten nicht schon bei der Bewerbung vor, sondern erlernt diese erst durch gezielte Weiterbildungen und Praxiserfahrungen. Unkonventionelle Methoden, wie Simulationen, Bug Bounty Programme, Hackathons oder Cyber Security Challenges, sind dabei auch eine wichtige Komponente. Denn konstante Weiterentwicklung ist essentiell im Bereich IT-Sicherheit.

Hier hat der Öffentliche Dienst die Herausforderung, die Ansprüche an eine Weiterbildung mit internen teilweise starre Strukturen und Vorgaben zu vereinbaren.

Formale Einstellungskriterien schließen viele aus

Ein elementarer Bestandteil der Herausforderungen im Personalmanagement ist zudem der Bewerbungsprozess. Im öffentlichen Sektor werden Zertifikate und Abschlüsse stark berücksichtigt, diese unterscheiden sich im IT-Bereich sehr von anderen Bereichen. Der Bewerbungsprozess obliegt der Personalabteilung, welche oft wenig mit spezifischen Zusatzzertifikaten, wie Certified Information Systems Security Professional (CISSP) und praktischen Erfahrungen (Teilnahme an Cyber Exercises, etc.) anfangen kann. Im IT-Sektor wird nicht nur formelle Voraussetzungen, wie Zertifikate geachtet, sondern auch Wissen und Können anders getestet, zum Beispiel werden im Privatsektor öfters neue Wege genutzt, um die Eignung von Bewerber:innen zu testen. Ein Beispiel dafür ist die Plattform Hackerrank, auf der die Bewerber:innen zunächst Aufgaben lösen müssen, um ihr Können zu testen oder das so genannte ‘Pair-Coding’, wo ein:e Mitarbeiter:in mit der:dem Bewerber:in zusammen programmiert. Erst danach werden sie eingeladen und zum Beispiel auf Teamfähigkeit getestet. Hier steht also das Testen von Fähigkeiten gleichberechtigt zu bestimmten theoretischen Abschlüssen. Im öffentlichen Sektor hingegen entscheidet häufig zunächst die Papierlage, dann das Gespräch. Ein:e IT-Sicherheitsspezialist:in kann allerdings gelernte:r Elektrotechniker:in und dann in den Beruf IT-Sicherheit gewechselt sein. Einstellungen von Personen ohne bestimmte Abschlüsse ist Potential, das genutzt werden muss. Allein bestimmte Studiumsanerkennungen zu bekommen, kann schwierig sein und ist meist Voraussetzung, um bestimm-

te Gehaltsstufen erreichen zu können (siehe Seite 3). Nach wie vor ist ein Master-Abschluss zur Befähigung im höheren Dienst notwendig. Um verbeamtet werden zu können, müssten auch Informatiker eine 18-monatige Ausbildung, die Laufbahnausbildung im gehobenen Dienst, durchlaufen. Beim BND werden hierbei erforderliche Kenntnisse und Fähigkeiten im Bereich der Fernmelde- und elektronischen Aufklärung des Bundes sowie allgemeine Rechts- und Verwaltungsgrundlagen[29], vermittelt – viel Zeit, in der anderes IT -Fachwissen vernachlässigt werden kann.

3. Ausgewählte Konzepte der Politik gegen den IT-Sicherheitsfachkräftemangel

Derzeit gibt es auf Bundesebene zwei ‘Pooling und Sharing’ Lösungsansätze, die den IT-Sicherheitsfachkräftemangel adressieren sollen. ‘Pooling und

29 BND, 2017 http://www.bnd.bund.de/DE/Karriere/Ausbildungen%20-%20Studium/Flyer/Laufbahnausbildung%20im%20gehobenen%20Dienst%20der%20Fernmelde_%20und%20Elektronischen%20Aufklaerung.pdf?__blob=publicationFile&v=5.

Sharing' Optionen ermöglichen eine Bündelung von Fähigkeiten und Expert:innen.

Die vom Bundesministeriums des Innern und vom Verteidigungsministerium auf Bundesebene geplanten Lösungsansätze[30] sollen sektorübergreifenden Einsatz der Arbeitskräfte ermöglichen[31].

Lösungsansatz: "Cyberwehr" (Bundesministerium des Innern)

Der Lösungsansatz der "Cyberwehr" des Bundesministeriums des Innern ist angesiedelt im Bundesamt für Sicherheit in der Informationstechnik (BSI). Zunächst einmal ist festzuhalten, dass der nun verbreitete Begriff "Cyberwehr", nur eine interne Benennung eines Konzepts war und verfrüht nach außen gedrungen ist.[32] Tatsächlich ist der Name irreführend, denn er beschreibt nicht wirklich das Konzept. Bei der Cyberwehr des BSI plant man eine Spezialist:innengruppe, durch einen Kooperationsvertrag geregelte Noteinsätze mit dem BSI zusammen ausführt. Es kommt allerdings nur zum Einsatz, wenn die entsprechende Expertise im BSI selbst nicht ausreichend vorhanden ist, beispielsweise in extremen oder besonderen Fällen wie bei einem Angriff auf eine kritische Infrastruktur. Dafür prüft das BSI, in welchen Bereichen intern bestimmte Expert:innen fehlen, die in einem konkreten Einsatzfall abgefragt werden könnten. Es soll kein Alternativmodell zur Personalgewinnung des BSI sein. Die Überlegung dabei ist, dass das BSI seine gesetzlich geregelten IT-Sicherheitsaufgaben weiterhin aufbaut und ausführt und dazu selbst eigene Kompetenzen hat, es aber besondere Notfälle gibt, wo spezielle Expertise aktuell im BSI nicht vorhanden ist. In diesen speziellen Fällen wird dann Expertise von außen mit herangezogen. Diese Personen können zum Beispiel hauptberuflich bei einer großen Softwarefirma angestellt sein. Zusammen mit dem BSI Team, zum Beispiel einem Mobile

30 Die Cyberwehr befindet sich in fortgeschrittener Planungsphase.

31 Auf Landesebene gibt es 'Pooling und Sharing' Methoden innerhalb der öffentlichen Verwaltung, zum Beispiel hat das Land Brandenburg, wie auch andere Länder (z.B. Saarland), einen zentralen IT-Dienstleister entwickelt, der Brandenburgische IT-Dienstleister (ZIT-BB). Dieser übernimmt für die Landesverwaltung Brandenburg, dem Zentraldienst der Polizei und die Rechenzentren, die Systembetreuung der Server und der Clients sowie die Benutzerbetreuung für alle Verfahren, die nicht polizeiliche Fachverfahren mit erhöhten Sicherheitsanforderungen sind übernimmt.

32 Netzpolitik.org, 2016 https://netzpolitik.org/2016/tatue-tata-cyberwehr-fuer-hilfe-bei-it-sicherheitsvorfaellen-geplant-unternehmen-sollen-kostenlos-mitmachen/.

Incident Response Team (MIRT), werden sie dann bei kritischen Infrastrukturen und herausgehobenen Fällen vor Ort akut Hilfe leisten[33]. Das BSI versteht sich hierbei als Partner der Wirtschaft, daher entstand gemeinsam mit Wirtschaftsvertreter:innen die Überlegung, die Freistellung von Mitarbeiter:innen für Notfälle zu vereinbaren. Es soll auch gemeinsam trainiert werden.

Der Begriff "Cyberwehr" beschreibt das Konzept allerdings nicht passend, denn er lässt vermuten, dass das BSI nun bei jeder Art von IT-Sicherheitsproblem diese 'Cyberwehr' ruft. Hierfür gibt es andere Maßnahmen, wie das Bürgerportal oder länderspezifische Hilfsportale und Teams, wie zum Beispiel in Baden Württemberg[34].

Ähnlich zur Freiwilligen Feuerwehr ist eigentlich nur, dass es einen Lohnfortzahlungsanspruch während des Auftrags gibt, um die Mitarbeiter:in freizustellen. Die Teilnahme an dem Einsatz ist vollkommen freiwillig und muss mit den Mitarbeitenden und Arbeitgebern abgesprochen sein.

Zudem gibt es schon konkrete Überlegungen darüber, wie Reaktionen auf die Reaktion, Aufwand und Zusammenarbeit bei Angriffen gehandhabt werden, bei denen ein:e Expert:in aus der Notfallgruppe gerufen wird, um einen Fall bei Firma Y zu unterstützen, er:sie allerdings beim Konkurrenten Firma X angestellt ist. Hier sollte transparent gemacht werden, wer für den jeweiligen Einsatz vorgesehen ist, sodass das betroffene Unternehmen final entschei-

33 Es gelten die Einsatzvoraussetzungen §5a http://www.gesetze-im-internet.de/bsig_2009/__5a.html.

34 Staatsministerium Baden-Württemberg, 2017 https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/landesregierung-initiiert-cyberwehr-baden-wuerttemberg/.

den kann, wen sie zur Unterstützung zulässt. Hinzu kommt natürlich eine Geheimhaltungsvereinbarung.

Zusammenfassende Details der Cyberwehr

Zielgruppen: IT-Sicherheitsspezialist:innen in Wirtschaft/KRITIS-Unternehmen in fester Anstellung
Art und Weise: punktueller Einsatz in Ausnahmefällen, in denen BSI-Expertise nicht ausreicht, netzwerken, gemeinsames üben, planen
Gehalt: N/A wird vom Arbeitgeber gestellt
Stellen: je nach Bedarf und Können und Bereitschaft des entsendenden Unternehmens
Gründe: Expertise in Notfällen verfügbar, Institutionalisierung des Wissenstransfers

Bewertung des Lösungsansatzes

Das Problem, dass in der Wirtschaft und im Öffentlichen Dienst dieselben Personen gefragt sind – vor allem IT-Sicherheitsspezialist:innen, umgeht dieser Lösungsansatz, indem eine Festanstellung nicht nötig wird. Genauso müssen die Expert:innen nicht nach dem TvöD bezahlt werden, sondern erhalten weiter ihr normales Gehalt bei ihrem festen Arbeitgeber. Dieser Lösungsansatz adressiert die Nachfrage nach qualitativ hochwertigen und flexiblen Weiterbildungen, welche durch Wissenstransfer und praktischen Übungen geboten werden sollen. BSI-internen Angestellten wird durch den Austausch mit anderen Expert:innen die Möglichkeit der gemeinsamen Weiterbildung gegeben.

Das Problem der strategischen Planung wird kurzfristig bis mittelfristig umgangen, da das BSI seinen schon festgelegten Aufgaben weiterhin nachgehen wird, und darüber hinaus im Notfall auf die erweiterte Expertise zugreifen kann. Sollten sich allerdings Notfälle häufen, muss auch darüber nachgedacht werden, wie eine Ausbildungsystematik aussehen kann. Das traditionelle Personalmanagement bleibt weiterhin ein Hindernis für BSI-interne Angestellte, wird aber in dem Lösungsansatz umgangen, da die Expert:innen durch das Personalmanagement des jeweiligen Arbeitgebers eingestellt werden.

Wird der IT-Sicherheitsfachkräftemangel durch die Cyberwehr adressiert?

Problematik	Ja	Umgangen	Nein
Fischen im selben Pool		X	
Erfahrene Spezialist:innen sind teuer		X	
Traditionelles Personalmanagement		X	
Weiterbildungen	X		

Lösungsansatz: "Cyber-Reserve & Cyber Community" (Bundesministerium der Verteidigung)

Die Cyber Community, bestehend zum Teil aus der "Cyber-Reserve"[35] unter Schirmherrschaft des Bundesministeriums für Verteidigung, soll Möglichkeiten bieten, punktuell bei der Bundeswehr Aufgaben zu übernehmen und die Bundeswehr für zukünftige Aufgaben zu befähigen. Die Cyber Community ist eine Bündelung von Spezialist:innen, welche den Erfahrungsaustausch und Wissenstransfer zwischen den Mitgliedern der Community fördern soll. Innerhalb der Community soll es auch die Cyber Reserve geben, welche mit Hilfe des Reservistenverbandes aufgebaut wird. Die Reservistenarbeitsgemeinschaft (RAG) Cyber wurde von Mario Hempel, Cyberbeauftragter des Reservistenverbandes und Tobias Zech, Stellvertreter des Präsidenten des Reservistenverbandes, gegründet. Die Cyber Reserve soll der gesamtstaatliche Sicherheitsvorsorge und dem Wirken des Kommando Cyber Informationsraum zur Verfügung gestellt werden und bei der Identifizierung von geeigneten Reservist:innen die Bundeswehr unterstützen. Über die Reservist:innen hinaus sollen durch die Cyber Community auch anderen Mitgliedern, welche nicht unbedingt eine militärische Laufbahn haben müssen, Arbeits - und Weiterbildungsmöglichkeiten geboten werden. Das Ziel ist es, durch diese Art von Community den Zugang zu Fachkräften zu erleichtern und dementsprechend so dem internen Fachkräftemangel entgegenzuwirken. Dieses Konzept enthält Möglichkeiten der Bildung, Weiterbildung und richtet sich eben auch an verschiedene Zielgruppen, wie Professor:innen, Chief Information Officers, Sozialwissenschaftler:innen oder Architekt:innen. So soll auch Quereinsteiger:innen ermöglicht werden, die Fortbildungen zu nutzen. Zum Beispiel haben Reservist:innen mit Expertise aus verschiedenen Bereichen daran mitgewirkt eine komplexe Cyberübungsumgebung zu erarbeiten

35 https://www.bmvg.de/de/aktuelles/cyber-reserve-bundeswehr-oeffnet-sich-fuer-it-community-11166.

– eine Art Truppenübungsplatz im Internet. In den virtuellen Raum wurden ungefähr 60 Prozent der kritischen Infrastrukturen modelliert[36]. Diese Übungen sollen dazu dienen, auch gemeinsam mit Unternehmen und anderen Bundesministerien, für einen Ernstfall zu üben.

Durch eine individuelle Bedarfsanalyse sollen Projektverträge aufgesetzt werden können, welche dann den Einsatz und Umfang des Cyber-Community-Mitgliedes in einem temporär begrenzten Einsatz bestimmen. Das bedeutet auch, dass zum Beispiel nicht immer eine Sicherheitsprüfung nötig ist, denn diese wird abhängig von der Arbeit des/der Einzelnen durchgeführt, was den Zugang zur Expertise in Einzelfällen verschnellern kann.

Momentan handelt es sich um eine sehr geringe Zahl an Cyber Community Mitgliedern (10-12), allerdings sollen es bis 2020 bis zu 300 werden können[37]. Es soll auch möglich sein, darüber Spezialkräfte punktuell außerhalb des TvöD zu bezahlen. Durch fachliche Weiterbildung in Kombination mit unkonventionelle Praxisaufgaben und spielerischer Arbeit, wie zum Beispiel Simulationen oder Red Teaming, einem zielgerichteten Penetrationstest, soll sich auf zukünftige Herausforderungen vorbereitet werden.

Bei der Erstellung der Mitgliederdatenbank[38] ist es für den Reservistenverbund hinderlich, dass es noch keine konkreten Vorstellungen gibt, welche Fähigkeiten die Bundeswehr genau brauchen wird.

Zusammenfassende Details der Cyber Community

Zielgruppen: Top-Führungskräfte, ausscheidende BW-Angehörige, Quereinsteiger:innen, Freiwillige, Reservist:innen
Art und Weise: Gemeinsames Üben, “Spielen”, Planen
Gehalt: Bis zu 120.000€ p.a. Gehalt möglich; auch unentgeltlich/ freiwillig möglich für extra Einsätze
Stellen: Aktuell nur geringe Zahl benötigt (rund 10), da CIR noch nicht steht → exklusive Projekte einzelner Personen, größere Rolle für Cyberinnovationhub

36 Eicker, 2018 in Loyal 2/18 Seite 44.

37 Quelle: anonymes Hintergrundgespräch.

38 Mario Hempel, Leiter Reservistenarbeitsgemeinschaft Cyber in der Loyal, p.47 Ausgabe 1/2018.

(Kooperation von Technologie/Startup Szene und BW, Entwicklung von spannenden Innovationen) → final werden rund 200-300 benötigt bis 2021
Gründe: Institutionalisierung des Wissenstransfer, Austausch, Aufbau eines Fachkräftepools

Bewertung des Lösungsansatzes:

Die Cyber Reserve soll dem Militär die Möglichkeit geben, mit IT-Fachkräften zu arbeiten, die die in der Wirtschaft angestellt sind. Außerdem ist es ein Instrument der Weiterentwicklung der Reserve und ermöglicht zusätzlich den Zugang zu einer breiteren Community an interdisziplinären Expert:innen. Das Modell schafft neue Weiterbildungsangebote, die auch neuere Formen von Vermittlung von Expertise berücksichtigen. Das traditionelle Personalmanagement wird nicht direkt adressiert, aber umgangen. Flexible Verträge erlauben mehr Freiheit in dem Umgang mit Expert:innen von außen, welche Vollzeit woanders eingestellt sind. Je nach zukünftiger, strategisch politischer Aufgabe der Bundeswehr im Cyberraum, muss aber auch hier darüber nachgedacht werden, wie die Fähigkeiten langfristig erhalten bleiben und demnach auch wie man dann mit Konzepten wie dem Laufbahnrecht oder der Tarifverordnung des Öffentlichen Dienstes umgeht. Ein Problem, was der Lösungsansatz schafft zu adressieren, ist 'Fischen im selben Pool'. Da der Lösungsansatz darauf angelegt ist, Menschen erst einmal nur kurzzeitig aus-oder weiterzubilden oder punktuell in Aufgaben der Bundeswehr einzubinden, steht die Bundeswehr nicht mehr in direkter Konkurrenz mit der Wirtschaft. Demnach gehen die Beteiligten hauptberuflich anderen Tätigkeiten nach. Dass Expert:innen zu teuer sind, kann durch spezielle Verträge adressiert werden. Indem Expert:innen außertariflich Verträge vermittelt werden, kann auch vereinzelt mehr als der TvöD vorgibt, gezahlt werden. Demnach werden die Probleme im Zusammenhang des traditionellen Personalmanagements nicht unbedingt adressiert.

Das größte Problem, die strategisch politische Planung, die wichtig ist, um eine längerfristige Ausbildungsystematik zu schaffen, kann die Cyber Community nicht adressieren. Einen Expertenpool aufzubauen, aus dem auch in Notfällen geschöpft werden kann, ist kurz- bis mittelfristig allerdings hilfreich, um den Zugang, falls die Aufgaben für die Bundeswehr im Cyberraum steigen sollten, zu erleichtern. Trotzdem muss darüber nachgedacht werden, inwieweit Expert:innen sich dann spontan binden können. Der Wissenstransfer und die Erweiterung von Expertise gerade in Verbindung mit interdisziplinären Weiterbildungen könnte allerdings der Politik helfen, zukünftige politische Aufgaben klarer zu definieren.

Wird der IT-Sicherheitsfachkräftemangel durch die Cybercommunity adressiert?

Problematik	Ja	Umgangen	Nein
Fischen im selben Pool		X	
Erfahrene Spezialist:innen sind teuer	X **		
Traditionelles Personalmanagement		X	
Weiterbildungen	X		

*** nur kurzfristig durch Zeitverträge*

Fazit

IT-Sicherheitsfachkräftemangel betrifft zunehmend auch den Öffentlichen Dienst. Die Lösungsansätze "Cyberwehr" und "Cyber Community" haben das Potenzial, einige der Herausforderungen in diesem Bereich zu adressieren.

Eine Herausforderung, die durch die aktuellen Lösungsansätze adressiert wird, sind die Weiterbildungswünsche der IT-Sicherheitsfachkräfte. IT-Sicherheit benötigt ständige und vor allem unkonventionelle Weiterbildungsmöglichkeiten, die der Öffentliche Dienst bisher nicht in seinem Repertoire hatte. Beide Lösungsansätze ermöglichen auch eine angemessenere Fortbildung.

Weitere dringende Herausforderungen, die den IT-Sicherheitsfachkräftemangel im Öffentlichen Dienst begünstigen, werden von den Lösungsvorschlägen umgangen und teilweise gar nicht adressiert. Der Öffentliche Dienst steht in starker Konkurrenz mit der Wirtschaft und sich selbst. Beide Lösungen setzen auf das Teilen der vorhandenen Expertise in Deutschland, was kurz- bis mittelfristig wirksam ist, aber keine längerfristige Lösung sein kann, weil IT-Sicherheitsaufgaben und Stellen sowohl in der Wirtschafts als auch im öffentlichen Sektor steigen. Der Öffentliche Dienst kann vor allem Spezialist:innen längerfristig nicht so hohe Gehälter zahlen, wie die Wirtschaft. Zudem behindert das starre Gehaltssystem, was auf traditionelle Qualifikationen setzt, die Einstellung von Expert:innen mit Erfahrung aber ohne Hochschulabschluss. Weiterhin muss die Politik konkrete Aufgaben für die öffentliche Verwaltung definieren, damit eine allgemeine Umstrukturierung von IT-Berufen in verschiedenen Ebenen der Verwaltung geplant und umgesetzt werden kann. Dies ist notwendig, damit langfristige Karrieremöglichkeiten geschaffen werden. Die Lösungsansätze adressieren auch

nicht das traditionelle Personalmanagement, was die Integration von IT-Expert:innen behindert.

Zudem schaffen die Lösungsansätze nur kurz- bis mittelfristig Abhilfe. Sie adressieren nicht die langfristigen Herausforderungen, IT-Sicherheitsexpert:innen in den Öffentlichen Dienst zu integrieren und die Arbeitsformen den neuen Herausforderungen anzupassen. Die tieferen strukturellen Probleme (mangelnde Attraktivität des Öffentlichen Dienstes) können diese 'Pooling und Sharing'-Methoden nicht lösen. Die kurzfristigen Lösungen dürfen nicht von den langfristigen Problemen ablenken oder entsprechenden Lösungsansätzen entgegenlaufen. Wenn die Aufgaben in der öffentlichen Verwaltung digitaler werden, muss erkannt werden, dass die Struktur und Arbeitsform des Öffentlichen Dienstes angepasst werden müssen, damit der Staat seine Aufgaben in der modernen Gesellschaft effektiv wahrnehmen kann. Parallel zu den genannten Lösungsansätzen muss der Staat daher weitere Lösungsansätze entwickeln, die sich auf die langfristige Behebung fokussieren und den Bedarf, der im Öffentlichen Dienst immer größer wird, decken. Hierbei geht es vor allem darum, Personal zu gewinnen und zu halten. Dies setzt eine Erneuerung des Öffentlichen Dienst in seiner Gesamtheit voraus, was die Attraktivität und die Leistung des Staatsdienstes steigern würde. Außerdem sollte zumindest sichergestellt werden, dass die nicht adressierten oder umgangenen Herausforderungen, die aktuellen Lösungsansätze nicht behindern oder die Umsetzung erschweren. Dies könnte den IT-Sicherheitsfachkräftemangel verschlimmern.

Zudem gilt es darauf zu achten, dass der Öffentliche Dienst sich nicht selber im Weg steht – gerade in Zeiten, wo der IT-Sicherheitskräftemangel sehr akut ist. Die knappe personelle und technischen Ressourcenausstattung darf die Einsatzfähigkeit von wenig verfügbarem Fachpersonal in Notfällen nicht behindern. Hier sollte der Öffentliche Dienst genau überlegen, wo welche Expertise gebraucht wird. Wie eine Studie zur Organisation der Cybersicherheitspolitik auf Bundesebene bestätigt, gibt es "insbesondere Verbesserungsbedarf bei der Zusammenarbeit der Bundesministerien und Bundesämter untereinander".[39] Die Herausforderung bei wenigem Personal, bestehen darin, besonders in Krisenfällen IT-Sicherheit gewährleisten zu können. Dies sollte auch bei der Entwicklung von Lösungsansätzen berücksichtigt werden.

39 http://ib.uni-koeln.de/fileadmin/templates/publikationen/aipa/AIPA_2016_2.pdf (Zedler, 2016:151).

Referenzen

Biselli (2016). Tatü, tata: „Cyberwehr“ für Hilfe bei IT-Sicherheitsvorfällen geplant – Unternehmen sollen kostenlos mitmachen, https://netzpolitik.org/2016/tatue-tata-cyberwehr-fuer-hilfe-bei-it-sicherheitsvorfaellen-geplant-unternehmen-sollen-kostenlos-mitmachen/.

Bitkom (2017). Bitkom-Branche schafft in diesem Jahr 21.000 neue Jobs, https://www.bitkom.org/Presse/Presseinformation/Bitkom-Branche-schafft-in-diesem-Jahr-21000-neue-Jobs.html.

Bitkom (2017). Wirtschaftsschutz in der digitalen Welt, https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf.

BMVg (2017). Cyber-Reserve: Bundeswehr öffnet sich für ITInformationstechnik-Community, https://www.bmvg.de/de/aktuelles/cyber-reserve-bundeswehr-oeffnet-sich-fuer-it-community-11166.

BND (2017). Laufbahnausbildung beim Bundesnachrichtendienst, http://www.bnd.bund.de/DE/Karriere/Ausbildungen%20-%20Studium/Flyer/Laufbahnausbildung%20im%20gehobenen%20Dienst%20der%20Fernmelde_%20und%20Elektronischen%20Aufklaerung.pdf?__blob=publicationFile&v=5.

BSI (2018). Cyber-Angriffe haben erhebliche Konsequenzen für die Wirtschaft, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber-Angriffe_haben_erhebliche_Konsequenzen_fuer_die_Wirtschaft_31012018.html.

Bundesministerium Justiz und Verbraucherschutz (2009). Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) § 5a Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen, http://www.gesetze-im-internet.de/bsig_2009/__5a.html.

Bundesagentur für Arbeit (2017). Berichte: Blickpunkt Arbeitsmarkt | April 2017 IT-Fachleute, https://statistik.arbeitsagentur.de/Statischer-Content/

Arbeitsmarktberichte/Berufe/generische-Publikationen/Broschuere-Informatik.pdf.

DGFP e.V. (2004). Personalmanagement in öffentlichen Verwaltungen. Experteninterviews zu Status quo und Herausforderungen, https://www.dgfp.de/fileadmin/user_upload/DGFP_e.V/Medien/Publikationen/Praxispapiere/200410_Praxispapier_oeffentlich.pdf.

Eicker (2018). Cyber-Reserve: Übung macht den Meister, Loyal Das Magazin für Sicherheitspolitik 2/18:44.

Guofu (2014). Erfahrungsbericht eines Informatikers im Öffentlichen Dienst, https://www.forum-3dcenter.org/vbulletin/archive/index.php/t-550136.html.

Klose (2017). IT-Arbeitsmarkt und Gehalt: Die Trends 2017, https://entwickler.de/online/development/arbeitsmarkt-entwickler-gehalt-trends-2017-579800476.html.

Königes (2017). IT-Gehälter 2017/2018 Der große Gehaltsvergleich in der Informatik, https://www.computerwoche.de/a/der-grosse-gehaltsvergleich-fuer-it-fachkraefte-2015-6,3218378.

Langkabel (2017). Die blinden Stellen bei der Suche nach der Digitalen Verwaltung – Teil 1, http://www.langkabel.de/die-blinden-stellen-bei-der-suche-nach-der-digitalen-verwaltung-teil-1/.

Öffentlicher Dienst Info (2017). TVöD - Stufen, http://oeffentlicher-dienst.info/tvoed/bund/stufen.html.

Staatsministerium Baden-Württemberg (2017). Landesregierung initiiert „Cyberwehr Baden-Württemberg", https://www.baden-wuerttemberg.de/de/header-und-footer/impressum/.

Stegemann (2010). Probleme der öffentlichen Verwaltung und Lösungsansätze im Lichte der Bürokratietheorie von Niskanen. Eine Untersuchung am

Beispiel der Bundeswehr, https://www.uni-muenster.de/imperia/md/content/ifpol/sic/abschlussarbeiten/ba_stegemann.pdf.

Vorhölter (2018). So hilft die RAG Cyber bei der Suche nach IT-Experten, Loyal Das Magazin für Sicherheitspolitik 1/18:46-47.

Wegener (2018). TVöD Bund und die Entgelttabelle 2017/ 2018 Tabelle, Stufen und Stufenzugehörigkeit, http://www.oeffentlichen-dienst.de/entgelttabelle/tvoed-bund.html.

Weidner (2015). Arbeiten wie ein Beamter, verdienen wie ein Manager, https://www.computerwoche.de/a/arbeiten-wie-ein-beamter-verdienen-wie-ein-manager,3099407.

Zedler (2016). Zur strategischen Planung von Cyber Security in Deutschland, Lehrstuhl International Politik Universität zu Köln, http://ib.uni-koeln.de/fileadmin/templates/publikationen/aipa/AIPA_2016_2.pdf.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über die Autorin

Julia Schuetze

Julia Schuetze, M.A. ist Projektmanagerin des Transatlantischen Cyber Forums und beschäftigt sich in diesem Zusammenhang mit internationaler Cybersicherheitspolitik. Im Rahmen des Euromasters an der University of Bath mit Austauschen an der UW Seattle und HU Berlin schrieb sie ihre Masterarbeit über Cybersicherheitsarchitektur in den USA am Beispiel von Cyberangriffen gegen die politische IT-Infrastrukturen. Zuvor arbeitete sie bei Wikimedia Deutschland e.V. und forschte am Berkman Klein Center der Harvard Universität.

Sie ist Fellow der Atlantic Expedition und engagiert sich ehrenamtlich bei Polis180 e.V., im Arbeitskreis OGP und im Steering Committee des Internet Governance Forums Deutschland.

So erreichen Sie die Autorin

Julia Schuetze, M.A.
Projektmanagerin Transatlantic Cyber Forum
jschuetze@stiftung-nv.de
+49 (0) 30 81 45 03 78 82

Impressum

stiftung neue verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de