Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)119

19.01.2023

Stiftung Neue Verantwortung

Stellungnahme von Julia Schuetze[1], Projektleiterin im Bereich Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e.V., für die öffentliche Anhörung des Ausschusses für Digitales zum Thema "Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

Mittwoch, 25. Januar 2023, 14:00 – 16:00 Uhr, Sitzungssaal Marie-Elisabeth-Lüders Haus (MELH) 3.101

Inhaltsverzeichnis

[1] Stiftung Neue Verantwortung (2023): Expert:innen-Profil von Julia Schuetze.

Einleitung

Deutschlands staatliche Cybersicherheitsarchitektur[2] ist in den vergangenen Jahren zu einem hochkomplexen Gebilde herangewachsen, das hunderte Akteure auf Bundes-, Landes- und kommunaler Ebene umfasst. Dass dieses Konstrukt optimierungsbedürftig ist, um die Cybersicherheit und Resilienz zu erhöhen, zeigt sich an verschiedenen Stellen: Es gestaltet sich zum Beispiel schwierig, ein umfassendes nationales Lagebild zu erstellen[3], es gibt Dopplungen etwa beim Warn- und Informationsdienst[4] und in den Kommunalverwaltungen kommt es vermehrt zu IT-Sicherheitsvorfällen[5]. Der Bedarf ist deshalb groß, sich zum „strukturellen Umbau der IT-Sicherheitsarchitektur“, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) als „zentrale(r) Stelle im Bereich IT-Sicherheit“ und zu der Frage, wie eine Neuordnung oder Bündelung von Kompetenzen auf Bundes-, Länder-, Kommunal- und EU-Ebene aussehen könnte, auszutauschen.

Die Diskussion wird in Deutschland bereits geführt, und es gibt auch schon Lösungsansätze – Beispiele sind die Eckpunkte eines KRITIS-Dachgesetzes, die Umsetzung des IT-Sicherheitsgesetz 2.0 und die Verhandlungen zur Zentralstellenfunktion in Deutschland. In diesem Monat trat außerdem die aktualisierte EU-Richtlinie „Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)“ – kurz NIS-2 – in Kraft. Diese muss bis zum 17. Oktober 2024 von den Mitgliedstaaten – auch Deutschland – umgesetzt werden. 21 Monate sind mit Blick auf die wegweisenden politischen Entscheidungen, die getroffen werden müssen, allerdings nicht viel Zeit.

Die NIS-2 verfolgt dasselbe Ziel wie die Befürworter einer Reform der deutschen Cybersicherheitsarchitektur: die ganzheitliche Stärkung der Cyber-Resilienz und Erhöhung

---

[2]Herpig und Rupp (2022), Deutschlands staatliche Cybersicherheitsarchitektur Impulse, Stiftung Neue Verantwortung e.V., https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur#collapse-newsletter_banner_bottom.

[3]Herpig (2021), Die Beantwortung von staatlich verantworteten Cyberoperationen - Impuls zur deutschen Cybersicherheitspolitik, Stiftung Neue Verantwortung/KAS, https://www.stiftung-nv.de/sites/default/files/snv_kas_-_beantwortung_von_staatlich-verantworteten_cyberoperationen_0.pdf.

[4]Nur einige Beispiele: LSI Bayern, Warn- und Informationsdienst, Accessed 19/01/2023, https://www.lsi.bayern.de/kommunen/warn_und_informationsdienst/index.html. SAKD, Warnmeldungen, Accessed 19/01/2023, https://www.sakd.de/index.php?id=sicherheit_warnmeldungen. EgO-MV, Warn- und Informationsdienst (WID), Accessed 19/01/2023, https://www.ego-mv.de/portal/meldungen/aktuelle-informationen-zur-nutzung-des-cert-m-v-schwachstellenportals-900000744-10044.html?rubrik=900000001. Niedersächsisches Ministerium für Inneres und Sport, 100. Kommune nutzt N-CERT-Angebot des Innenministeriums zur Abwehr von Cyberangriffen, Accessed 19/01/2023 https://www.mi.niedersachsen.de/startseite/aktuelles/presseinformationen/100-kommune-nutzt-n-cert-angebot-des-innenministeriums-zur-abwehr-von-cyberangriffen-174877.html. BSI, Warn- und Informationsdienst, Accessed 19/01/2023, https://wid.cert-bund.de/portal/wid/start. BfV (2022), Informationsblatt "Schutz vor Phishing", https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-05-31-infoblatt-phishing.html. BSI, Phishing & Smishing auf dem Vormarsch, Accessed 19/01/2023, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html.

[5]Kern (2022), Cyberangriffe auf deutsche Kommunen im Jahr, BIGS, 2021 https://www.bigs-potsdam.org/app/uploads/2022/04/2022_BIGS-Essenz-Nr.19-WEB.pdf. Lange, Kommunaler Notbetrieb, Übersicht IT-Sicherheitsvorfälle in Kommunalverwaltungen, Accessed 19/01/2023, https://notbetrieb.hauptsystem.de/uebersichtskarte/.

der Cybersicherheit. Die NIS-2 beinhaltet Vorgaben wie Risikomanagementmaßnahmen und Meldepflichten für so genannte wesentliche und wichtige Einrichtungen[6], worunter erstmals

auch öffentliche Verwaltungen auf “zentraler” und “regionaler” Ebene fallen. Darüber hinaus gibt es Vorgaben, die die institutionelle Struktur betreffen und die zur ganzheitlichen Resilienz beitragen sollen. Diese EU-Vorgaben stehen im Fokus meiner Stellungnahme. Denn diese Anforderungen an Institutionen und Instrumente verlangen eine Optimierung der Architektur. Zum Beispiel soll es mit der Umsetzung der NIS-2 strengere Berichtspflichten geben; außerdem mehr Koordination und Informationsaustausch zwischen Behörden über Cyberbedrohungen, -risiken und Sicherheitsvorfälle. Außerdem sollen geeignete Instrumente für den (freiwilligen) Austausch von Cybersicherheitsinformationen implementiert werden – und zwar nicht irgendwie, sondern in einem Format, das dabei hilft, die “Fähigkeit, Bedrohungsinformationen und -analysen, Warnungen zu Cyberaktivitäten und Reaktionsmaßnahmen schnell und automatisch auszutauschen und zu verstehen”. Von dieser Art des Informationsaustauschs sind wir in Deutschland noch entfernt.

Deutschland sollte die Umsetzung der NIS-2 als Chance zur Optimierung nutzen. Die Richtlinie bietet das Potenzial, vor allem die Ebenen der Architektur (Bund, Land, Kommunen), die Verteilung von Ressourcen und Kapazitäten sowie Formate der Zusammenarbeit zu definieren und im Sinne der Resilienz zu optimieren. Eine Straffung und Bündelung von Kompetenzen tut auch deshalb Not, weil der Fachkräftemangel erschwerend hinzu kommt. Dieser erhöht den Druck, besonders ressourcenschonend zu denken und bei der Verteilung von Zuständigkeiten unnötige Dopplungen zu vermeiden, wodurch Fachkräfte Expertise dort ausbauen und teilen können, wo sie am dringendsten gebraucht wird.

Diese Stellungnahme enthält eine Reihe von Empfehlungen und nimmt zudem Bezug auf die Fragen 1, 6, 11, 12 und 18 (siehe Anhang).

NIS-2 - ein Anlass zur Neuordnung

Die staatliche Cybersicherheitsarchitektur[7] Deutschlands besteht aus zahlreichen Akteuren, die auf verschiedenen Ebenen angesiedelt sind. In Deutschland, wie übrigens auch in anderen föderalen Staaten wie Belgien, werden die Ansprechstellen und zuständigen Behörden auf Landesebene immer wichtiger. Sie dienen kleinen, mittelständischen Unternehmen oder Kommunen als Ansprechstellen und bieten oder finanzieren Leistungen, welche die Cybersicherheit und Resilienz fördern. Zu diesen Leistungen gehören etwa

---

[6] “Bei Einrichtungen, die für die Zwecke der Einhaltung von Risikomanagementmaßnahmen und der Meldepflichten im Bereich der Cybersicherheit in den Geltungsbereich dieser Richtlinie fallen, sollten zwei Kategorien unterschieden werden: wesentliche Einrichtungen und wichtige Einrichtungen; zu berücksichtigen ist dabei der Grad ihrer Kritikalität in Bezug auf ihren Sektor oder die Art der von ihnen erbrachten Dienste sowie ihre Größe. In diesem Zusammenhang sollten gegebenenfalls einschlägige sektorspezifische Risikobewertungen oder Leitlinien der zuständigen Behörden gebührend berücksichtigt werden.” Amtsblatt der Europäischen Union (2022), RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555.

[7] Herpig und Rupp (2022), Deutschlands staatliche Cybersicherheitsarchitektur Impulse, Stiftung Neue Verantwortung e.V., https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur#collapse-newsletter_banner_bottom.

Schulungen, Beratungsangebote und Checklisten für Notfallpläne (wobei das Leistungsspektrum von Land zu Land unterschiedlich aussieht). Darüber hinaus geben sie IT-Sicherheitswarnungen heraus, unterstützen bei Vorfällen, stellen Tools für den IT-Sicherheitscheck bereit oder finanzieren den Aufbau von Ressourcen. Leistungen, Ressourcen, Kapazitäten, Zuständigkeiten und auch die Gesetzeslage sehen allerdings in jedem Bundesland und in jeder Kommune anders aus. Die nun umzusetzende NIS-2 macht Vorgaben, wie zuständige Behörden oder auch Computer Security Incident Response Teams (CSIRTs) aufgebaut werden und miteinander agieren sollen. Deswegen könnte die NIS-2 nicht nur einen Harmonisierungs-Effekt innerhalb der Mitgliedstaaten haben, sondern auch innerhalb Deutschlands.

Beitrag der Länder in Deutschland definieren

Mit der NIS-2 stehen einige Grundsatzfragen ins Haus. So muss beispielsweise über die Zentralstellenfunktion des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entschieden werden und welchen konkreten Beitrag diese Stelle in der Architektur leistet. Die NIS-2 macht einige klare Vorgaben für Zuständigkeiten und stellt höhere Ansprüche an Meldeprozesse und den Informationsaustausch zwischen staatlichen, wirtschaftlichen und gesellschaftlichen Akteuren. Dies muss Deutschland bei der Neuordnung der Architektur und Weiterentwicklung bestehender Instrumente mitbedenken. Dennoch gibt es bei der Umsetzung großen Spielraum.

Gerade für eine föderal organisierte Cybersicherheitsarchitektur bringt dies neue organisatorische, rechtliche und politische Herausforderungen bei der Umsetzung mit sich. Entscheidungsträger:innen werden mit wegweisenden Fragen konfrontiert. Denn durch die NIS-2 wird die Anzahl der Einrichtungen, die Vorgaben im Bereich IT-Sicherheit erfüllen müssen und somit aktiv mit der staatlichen Cybersicherheitsarchitektur in den Dialog treten, signifikant erhöht. Dies kann bedeuten, dass Behörden der Landesverwaltungen nicht nur selbst die IT-Sicherheitsanforderungen der NIS-2 als eine wesentliche Einrichtung erfüllen müssen, sondern auch, dass sie für Einrichtungen in den Ländern, zum Beispiel Kommunalverwaltungen, eine größere Rolle im Bereich Informationsaustausch und Aufsicht einnehmen müssen. Deswegen stellt sich die Frage, ob Länder regionale zentrale Ansprechstellen für bestimmte in der NIS-2 regulierte wesentliche und wichtige Einrichtungen und/oder andere Zielgruppen sein sollen. Desweiteren ist zu fragen, welchen Beitrag die Länder konkret in der an NIS-2 angepassten Cybersicherheitsarchitektur leisten müssten.

Die NIS-2 macht eines deutlich: Wenn staatliche Akteure bestimmte Aufgaben übernehmen und somit zuständig dafür sind, am Erreichen der Ziele dieser Richtlinie mitzuwirken (z. B. ganzheitliche Stärkung der Cyber-Resilienz), dann muss es den zuständigen Behörden und den CSIRTs durch angemessene Ressourcen ermöglicht werden, die festgelegten Aufgaben zu erfüllen.

Chancen und Risiken der föderalen Cybersicherheitarchitektur

Die Zuständigkeiten föderal aufzuteilen und dies auch gesetzlich zu verankern, bietet zum einen die Möglichkeit, die Aufgaben auf verschiedene Akteure zu verteilen. Dadurch können

Expertise verteilt und regionale Cybersicherheitsökosysteme[8] in verschiedenen Regionen in Deutschland gefördert werden, ggf. mit unterschiedlichen Schwerpunkten. Nicht alle müssen alles machen, wenn Expertise geteilt wird. Ein anderer Vorteil ist, dass durch die Zuständigkeit auf regionaler Ebene regionale Unterschiede und Schwerpunkte berücksichtigt und dafür passende Angebote geschaffen werden können. Zum Beispiel sollte Beratung zu Resilienzmaßnahmen näher an den Zielgruppen (z.B. Kommunalverwaltungen) organisiert werden, da Vorbeugung den Schaden, der durch IT-Sicherheitsvorfälle entsteht, minimieren kann.

Zum anderen gibt es aber auch Risiken, etwa wenn die Verteilung von Zuständigkeiten und das Erbringen von Leistungen auf eine Art und Weise organisiert ist, die die Zusammenarbeit der Akteure untereinander erschwert oder Prozesse nicht geregelt sind. Problematisch ist auch, wenn Expertise nicht ressourcenschonend geteilt wird und dabei unnötige Dopplungen entstehen. Dies gilt insbesondere bei übergreifenden Zielen, zum Beispiel der Erhöhung der Verfügbarkeit von umsetzbaren ("actionable") Informationen. Diese Informationen können IT-Sicherheitsvorfälle verhindern oder mitigieren. Damit diese Informationen aber überhaupt bei der Zielgruppe ankommen, müssen staatliche Akteure auf verschiedenen Ebenen der Architektur ihren Beitrag leisten. Akteure auf Bundesebene können bisher nur begrenzt Informationen sammeln. Auch eine Einschätzung des Status Quo der IT-Sicherheit oder der Bedrohungslage[9] ist nur begrenzt möglich, denn dafür müssen alle zuständigen Akteure *permanent und strukturiert* Informationen erheben, bewerten und teilen. Die NIS-2 sieht hier die Mitgliedstaaten in der Pflicht, eine verstärkte Koordinierung beim Informationsaustausch sicherzustellen. Es geht vor allem darum, dass zuständige Behörden zusammenarbeiten und unverzüglich Informationen austauschen.

Neben dem Informationsaustausch spielen auch Fragen der Effizienz und Effektivität eine Rolle. Wenn zum Beispiel mehrere staatliche Akteure Tools zur Bildung von Awareness mit derselben Zielgruppe entwickeln, besteht das Risiko, dass unnötige Doppelungen entstehen oder dass Leistungen entwickelt werden, die nicht nachnutzbar sind (siehe deswegen den Vorschlag zum EfA-Prinzip in der Stellungnahme). Gerade im Falle von Fachkräftemangel erscheint diese Vorgehensweise nicht sinnvoll. So wird Expertise gebunden, die an anderer Stelle womöglich dringend gebraucht wird. Wer zum Beispiel Sensibilisierungsmaterialien von Grund auf neu entwickelt, die es womöglich anderswo bereits in guter Qualität gibt, fällt für die Beratung zur Umsetzung von IT-Sicherheitsmaßnahmen aus – eine unnötige Ressourcenverschwendung. Es ist deswegen wichtig, den Beitrag der staatlichen Akteure genau zu definieren, damit u.a. auch der Staat seinen Beitrag leisten kann; damit er also die passenden Fachkräfte einstellen bzw. ausbilden oder Leistungen, die auch nichtstaatliche Akteure übernehmen können, auslagern kann.

[8]ECSO, The Role of the Regions in strengthening the European Union's cyber security Position Paper, Accessed 18/01/2023, (https://www.eurobits.de/wp-content/uploads/20190320_Regions_Position_Paper_approved.pdf

[9]Herpig (2021), Die Beantwortung von staatlich verantworteten Cyberoperationen Impuls zur deutschen Cybersicherheitspolitik, Stiftung Neue Verantwortung/KAS, https://www.stiftung-nv.de/sites/default/files/snv_kas_-_beantwortung_von_staatlich-verantworteten_cyberoperationen_0.pdf.

Gemeinsame Ziele festlegen

Empfehlung: Um die Chancen zu nutzen und die Risiken einer föderalen Cybersicherheitsarchitektur zu minimieren, sollten sich Bund und Länder im Zuge der Umsetzung von NIS-2 *auf die gemeinsamen Ziele einigen,* um auch die Beiträge der jeweiligen Akteure zu definieren. Die Ziele sollten in einer nationalen Strategie gemeinsam mit Ländern münden, damit sie am Ende keine reine Cybersicherheitsstrategie des Bundes bleibt und die Beiträge der Länder zur Erreichung der Ziele und der Zusammenarbeit festgelegt werden. Die gemeinsam abgestimmten Policies zur Zusammenarbeit müssen dann wahrscheinlich nicht nur in Bundesgesetzen, sondern auch in Landesgesetzen verankert werden. Dadurch sollen Regelungslücken geschlossen und Doppelstrukturen vermieden werden.

Im Folgenden liefere ich Anhaltspunkte, wie eine solche Zusammenarbeit zur Verbesserung der Resilienz aussehen und wie methodisch vorgegangen werden könnte. Wichtig ist allerdings, dass weitere nichtstaatliche Akteure strukturiert, zielführend und transparent in diesen politischen Entscheidungsprozess eingebunden werden, denn das Ergebnis hat große Auswirkungen auf die Resilienz ganz Deutschlands.

Mit Übungen Informationsaustausch und Meldewege praxisnah entwickeln und testen

Es ist <u>nicht</u> empfehlenswert, Policies, die auf einen besseren Informationsaustausch und effektivere Meldewege abzielen, alleine in der Theorie zu entwickeln. Zu groß ist

die Gefahr, dass die Prozesse, die daraus entstehen, nicht praxisnah sind. Zudem erhöht sich das Risiko, dass derart entwickelte Policies nicht das erreichen, was sie eigentlich sollen, weil etwa bestimmte Auswirkungen nicht bis ins Detail durchgespielt wurden. Dies kann zur Folge haben, dass das bestehende Problem nicht oder nur teilweise gelöst wird.

Die europäische NIS-2-Richtlinie regt an, die Abstimmung zwischen den für die Aufsicht zuständigen Behörden, also z.B. der zentralen nationalen oder den regionalen Anlaufstellen, der Polizei oder den Datenschutzbeauftragten, zu vereinfachen und zu straffen. So soll der Verwaltungsaufwand für die betreffenden Einrichtungen, die zum Melden von Vorfällen verpflichtet sind, verringert werden. Die NIS-2 gibt aber nur grobe Anhaltspunkte, wie dies genau aussehen kann. Es obliegt Deutschland, die Straffung zu definieren und dabei weitere Ziele im Blick zu behalten, wie zum Beispiel: Wie kann mit einer Straffung oder Verschlankung der Abstimmungsprozesse erreicht werden, dass ein nationales oder regionales Lagebild sowie Informationen zur Prävention, Detektion und Reaktion in angemessener Form geteilt werden? Wie lassen sich freiwillige Meldungen integrieren und sogar fördern? Zudem sollten Vorfälle, die grenzüberschreitende Auswirkungen haben können, über eine zentrale Stelle an die EU gemeldet werden.

Solche Policies entstehen idealerweise nicht am theoretischen Reißbrett, sondern können mithilfe sogenannter Table-Top-Übungen praxisnah und unter Berücksichtigung verschiedener Interessen entwickelt werden. Wenn diese Art von Cybersicherheits-Übung in

der Phase der Policy-Entwicklung angewandt wird, kann die Zuweisung unterschiedlicher Rollen und Verantwortlichkeiten mitsamt ihren Auswirkungen getestet werden. Tabletop-Übungen, aber auch andere Übungsformate[10] eignen sich sehr gut dazu, Vorschläge für eine bestimmte Policy, die Definition politischer Ziele und geeignete Politikinstrumente zu testen. Übungen sind auch sinnvoll, um die politische Machbarkeit zu prüfen und wichtige Details zu klären.

Empfehlung: In der Phase der Policy-Entwicklung sollten Entscheidungsträger:innen verschiedene Handlungsoptionen erarbeiten, um die Auswirkungen der verschiedenen Optionen durchzuspielen. Durch diesen Arbeitsschritt wird deutlicher, welche Policy die vorliegenden Probleme lösen und die gesteckten Ziele erreichen kann. Der diskussionsbasierte Charakter von Tabletop-Übungen kann Entscheidungsträger:innen und Praktiker:innen dabei helfen zu verstehen, wo etwa bei einer Vorfallsmeldung die Rollen und Verantwortlichen liegen könnten, wie die Meldeformulare gestaltet sein und in welchem Format diese dann verwendet und geteilt werden sollten.

Aufschlussreich ist hier ein Blick auf das amerikanische Beispiel: Die USA haben ihr nationales Incident Response Framework mit Hilfe solcher Übungen entwickelt. Entscheidungsträger:innen der Regierung und die von dem Prozess betroffenen Einrichtungen testeten Zuständigkeiten, Formate und Anreize in unterschiedlichen Konstellationen. So konnten die jeweiligen Auswirkungen für verschiedene Vorfallsarten durchgespielt werden[11].

In den letzten zwei Jahren haben wir in der SNV diese Art von Tabletop-Übung in verschiedenen Ländern umgesetzt, um Verantwortlichkeiten bzw. Rollen zu definieren und um Policies zum Informationsaustausch und Meldeverfahren zu entwickeln. Unsere Erfahrungen zeigen, dass Policies idealerweise mithilfe praxisnaher Methoden entwickelt werden sollten[12]. Daher empfehle ich, auch den Informationsaustausch zwischen Bund, Ländern, wesentlichen und wichtigen Einrichtungen sowie freiwillig meldenden Einrichtungen im Rahmen solcher Übungen zu entwickeln und zu testen.

Im Folgenden werden die einzelnen Entwicklungs- und Testschritte bei einer solchen Übung vorgestellt:

1. Um eine neue Policy zu entwickeln oder zu testen, müssen zunächst klare Ziele definiert werden, zum Beispiel ein nationales Lagebild, ein regionales Lagebild und das Teilen relevanter Informationen für die Prävention, Detektion und Reaktion.

[10] Beigel & Schuetze (2021), Cybersecurity Exercises for Policy Work Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work, Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/cybersecurity.exerises.policy.work__0.pdf.

[11] Siehe auch Seite 19 in: Beigel & Schuetze (2021), Cybersecurity Exercises for Policy Work Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work, Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/cybersecurity.exerises.policy.work__0.pdf.

[12] Schuetze & Beigel (2022), Cybersecurity Policy Exercises in Practice. Learnings from Implementing Tabletop Exercises in Different Countries, Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/sites/default/files/cybersecurity_policy_exercises_in_practice.pdf.

2. Als Nächstes muss der Status Quo erfasst werden – wie sehen der Informationsfluss und die Meldewege momentan aus, welche Akteure sind beteiligt, was läuft bisher gut und was nicht? Eine solche Status-quo-Analyse könnte wie folgt aussehen:
    a. Damit ein nationales Lagebild oder regionale Lagebilder gezeichnet und relevante Informationen für die Prävention, Detektion und Reaktion geteilt werden können, müssen sich viele Akteure der staatlichen Cybersicherheitsarchitektur und viele nicht-staatliche Akteure beteiligen. In unserem politischen System spielen neben Wirtschafts- und zivilgesellschaftlichen Akteuren vermehrt auch verschiedene Akteure in den Ländern eine Rolle. Zum Beispiel wenden sich jetzt schon Akteure, die bisher nicht zur Meldung verpflichtet sind, an Behörden in den Ländern, auch weil einige von ihnen eigene Meldestellen und Warn- und Informationsdienste aufgebaut haben und somit Informationen sammeln. Die Akteure der Länder nutzen diese Meldestellen auch, um auf Vorfälle in ihrer Region reagieren zu können, etwa um zu beraten oder zu ermitteln. Die Trennung ist nicht in allen Ländern gleich scharf, und nicht alle Länder betreiben designierte Meldestellen für IT-Sicherheitsvorfälle. Damit ein nationales Lagebild entstehen kann oder relevante Informationen für die Prävention, Detektion und Reaktion geteilt werden können, ist die Frage, wie und welche Informationen gesammelt und dann auch geteilt werden, ausschlaggebend. Wenn eine Kommunalverwaltung in einem Land betroffen ist und Informationen, die zur Prävention oder Detektion wichtig sind, nicht an andere Kommunalverwaltungen über einen Informationsdienst weitergeleitet werden, können bundesweit Kommunalverwaltungen nicht aus dem Vorfall lernen. Es gibt, so nehme ich an, schon informelle Prozesse, die ggf. sehr gut funktionieren und in denen Informationen nutzbar die Zielgruppe erreichen. Doch möglicherweise ist der Prozess noch nicht permanent, automatisch oder strukturiert, oder die Funktionen der Information – z.B. zur Berichterstattung, Ermittlung von Strafverfolgung oder Prävention und Detektion – werden nicht getrennt. Solche informellen Prozesse unterstützen auf der einen Seite die Zielerreichung und Vertrauensbildung, sind aber auch sehr fragil, da sie nicht selten auf persönlichen Beziehungen beruhen. Sie sind aufgrund der Vertraulichkeit schwer von außen zu analysieren, sollten aber von Entscheidungsträger:innen so gut es geht beschrieben werden. Denn nur dann können sie eine Grundlage zur Entwicklung von Policy-Optionen bieten.

3. Nun können mehrere Policy-Optionen für die Übung entwickelt werden. Welche Optionen entwickelt und im Rahmen einer Übung getestet werden, wird sich natürlich von Fall zu Fall unterscheiden; an dieser Stelle möchte ich exemplarisch eine Option vorstellen, die ich für vielversprechend halte.
    a. Eine sinnvolle Policy-Option könnte es zum Beispiel sein, den schriftlichen, teils verpflichtenden Meldeprozess und den “Notrufprozess” (eigener Arbeitstitel) funktional und operativ zu trennen. Der Meldeprozess dient vornehmlich der Aggregation und Auswertung von Daten, um ein nationales und regionales Lagebild zu erstellen. Außerdem sollten dabei Vorfälle, die grenzübergreifende Auswirkungen haben, identifiziert werden. Die Analyse der Meldungen sollte auch die Basis dafür sein, dass wichtige Informationen zur

Prävention und Detektion aggregiert und anonymisiert an Wirtschaftsakteure oder Bürger:innen weitergegeben werden, zum Beispiel mittels eines Informationsdienstes, wo Zielgruppen ggf. nach Informationen filtern können. Der “Notrufprozess” ist der passende Kommunikationsweg, wenn schnell auf einen Vorfall reagiert werden muss. Er dient dazu, unverzüglich operative Unterstützung, telefonische oder persönliche Beratung oder auch eine rasche forensische Untersuchung des Vorfalls sicherzustellen. Demnach sollte die betroffene Einrichtung den Vorfall nur an einer Stelle schriftlich melden müssen, in einem einzigen Formular – was die Aufsichtsverfahren harmonisiert (Vorschlag NIS-2). Die Trennung beider Kommunikationswege – der schriftliche, teils verpflichtende Prozess und der Notfallprozess – würde auch dazu führen, die von der NIS-2 angeregte Trennung zwischen den Einrichtungen und den CSIRTs zu stärken. So wäre gewährleistet, dass es, falls ein CSIRT Teil einer zuständigen Behörde ist, eine funktionale Trennung zwischen den operativen Aufgaben der CSIRTs und den Aufsichtstätigkeiten der zuständigen Behörde gäbe. Die NIS-2 spricht hier von den CSIRTs als “trusted intermediary”.

b. In diesem Meldeverfahren sollten dann alle drei Kategorien, die die NIS-2 vorgibt, integriert werden: Meldungen innerhalb von 24 Stunden, Meldungen nach 72 Stunden und ein Abschlussbericht nach einem Monat. Alle Fälle sollten an die nationale Zentralstelle weitergeleitet werden. Über Formulare und Einverständniserklärungen sollten die Informationen an die berechtigten Stellen weitergegeben werden können. Dieser Informationsaustausch muss rechtlich verankert sein; es könnte z.B. eine Vorgabe geben, dass Informationen zu Vorfällen aus einer bestimmten Region an die regionalen Anlaufstellen weitergeleitet werden. Dies könnte aber durchaus kontrovers sein. Genauso stellt sich die Frage, welche Informationen ggf. über so eine Trennung verloren gehen oder über andere informelle Formate ausgetauscht werden sollten, zum Beispiel sektorspezifische Verbünde von CSIRTs. Daran sieht man, warum es wichtig ist, verschiedene Policy-Optionen zu entwickeln. Es handelt sich nicht nur um organisatorische und technische, sondern vor allem auch um politische Entscheidungen.
c. **Empfehlung: Um weitere Policy-Optionen zu entwickeln, wäre die Einbindung verschiedener Akteure möglich, zum Beispiel in einem Workshopformat.**
d. **Empfehlung: Für deutsche Akteure wäre es sinnvoll, sich über Policy-Optionen mit anderen föderalen EU-Mitgliedstaaten auszutauschen.** Andere föderal organisierte Mitgliedstaaten stehen vor denselben Herausforderungen und stellen sich aktuell diese Fragen bei der Umsetzung von NIS-2 (z.B. Belgien). Daher empfehle ich, in den Austausch mit anderen föderalen Staaten zu treten und eine Arbeitsgruppe zu bilden. Da NIS-2 zahlreiche Anforderungen und teils völlig neue Fragen mit sich bringt, gibt es für die Umsetzung wahrscheinlich noch keine Good Practices. Es bietet sich dennoch an, schon vor der Umsetzung mit anderen EU-Staaten in den Austausch zu gehen, gemeinsam Ideen zu entwickeln und dabei die Vor- und Nachteile verschiedener Optionen durchzuspielen.

4. Als Nächstes müssen passende Szenarien entwickelt werden. Es bietet sich hier an, Vorfälle nach Typus zu kategorisieren: Welche Einrichtungen betreffen sie, welche freiwilligen und/oder verpflichtenden Meldevorschriften gibt es und ist eine Hilfeleistung erforderlich? Ist es ein grenzübergreifender Vorfall

5. Dann sollten für die verschiedenen Policy-Optionen passende Aufgaben entwickelt werden, zum Beispiel standardisierte maschinenlesbare Meldeformulare für alle drei Kategorien (24 Stunden, 72 Stunden und Monatsbericht). Nur einige Informationen, die im Meldeprozess abgefragt werden, gibt die NIS-2 vor. Deutschland hat hier also die Möglichkeit, die Abfragen von Informationen mitzugestalten, und kann dabei durch Übungen die betroffenen Einrichtungen einbeziehen.

6. Für die Organisation der Übung ist es wichtig, dass (potenziell) zuständige Akteure, ggf. Entscheidungsträger:innen sowie von der Policy betroffene Akteure, z.B. meldende Einrichtungen, beteiligt sind.
    a. Je nach Vertrauensgrad sollten die Übungen in einem “Safe Space” durchgeführt werden, denn die zuständigen Akteure sollten sich idealerweise selbst spielen.
    b. Da viele Policies im Falle ihrer Umsetzungen ggf. gesetzliche Änderungen nach sich ziehen, sollten Jurist:innen die Übung begleiten, um nach der Übung die erarbeiteten Policy-Optionen mit geltendem Recht abzugleichen.
    c. Hilfreich ist ein sogenanntes „Hot Wash“-Szenario: Hier verändert sich das Szenario schnell, und unmittelbar nach der Übung können mit allen Teilnehmer:innen die Auswirkungen und “Learnings” erfasst werden – nicht nur die Daten, sondern auch die ungefilterten Emotionen.
    d. Aus dem US-amerikanischen Modell hat man vor allem gelernt, dass neutrale Dritte die Übung begleiten sollten, um Notizen zu machen, in einem Hot-Wash-Szenario Fragen zu stellen oder auf Überraschungen hinzuweisen.
    e. Auch wenn dies wie ein eher softes Kriterium erscheinen mag: Wichtig für den Erfolg einer solchen Übung ist auch ein offenes Mindset. Zum Beispiel sollten Teilnehmer:innen nicht mit der vorgefassten Meinung antreten: „Ich bin mir sicher, dieser Prozess funktioniert besser". Es gibt kein richtig oder falsch bei solchen Übungsformaten – zumindest wenn die Übung der Entwicklung von Prozessen und dem Testen der Auswirkungen dienen soll. Sollte es schon einen Prozess geben, können Übungsformate auch dazu eingesetzt werden, diesen zu testen und zu prüfen, ob alle mit dem Prozess vertraut sind und ihn in der Praxis auch wirklich anwenden können[13].

Bei den hier aufgeführten Empfehlungen und Voraussetzungen für den erfolgreichen Einsatz von Übungen handelt es sich um eine Auswahl. Zu den zahlreichen weiteren Aspekten, die

[13]Vgl. Schuetze & Beigel (2022), Cybersecurity Policy Exercises in PracticeLearnings from Implementing Tabletop Exercises in Different Countries, Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/sites/default/files/cybersecurity_policy_exercises_in_practice.pdf. Und Beigel & Schuetze (2021), Cybersecurity Exercises for Policy Work Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work, Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/cybersecurity.exerises.policy.work__0.pdf.

berücksichtigt werden sollten, gibt es eine Fülle an Fachliteratur, die ggf. bei der Entwicklung konsultiert werden sollte[14].

Empfehlung: Es sollte geprüft werden, inwiefern Policy-Optionen zur Vereinfachung und Straffung des Informationsaustauschs in der für 2023 geplanten Lükex (Länder- und Ressortübergreifende Krisenmanagementübung)[15] aufgenommen und getestet werden könnten. Da die Vorbereitungen laut Website des Bundes noch in diesem Monat beginnen sollen, ist es sinnvoll, hier Fragestellungen der NIS-2 soweit möglich mit aufzugreifen und die Umsetzung der Richtlinie als Gelegenheit zu nutzen, verschiedene Policy-Optionen zu testen.

Zentralstelle - ja oder nein?

Schon die oben vorgestellte Policy-Option zeigt, dass gemeinsame Technologien genutzt werden müssten, um den Informationsaustausch permanent, automatisch und strukturiert zu organisieren. Um Ziele wie ein nationales Lagebild zu erreichen oder potenziell grenzüberschreitende Vorfälle zu identifizieren, werden höchstwahrscheinlich Datensätze entstehen, die das BSI zum Informationsknotenpunkt machen. Dies würde, soweit ich es beurteilen kann, über die jetzige, eher punktuelle Zusammenarbeit mit den Ländern hinausgehen. Sollten sich Bund und Länder auf diese Policy-Option einigen, halte ich eine Zentralstellenfunktion des BSI für unterstützenswert.

NIS-2 und Kommunalverwaltungen

In den vergangenen Jahren kam es vermehrt zu IT-Sicherheitsvorfällen[16], zum Beispiel durch Ransomware, bei denen die kommunale Verwaltung in Deutschland betroffen war. Der Bund, die Länder und die Kommunen selbst entwickeln momentan unterschiedliche Modelle und Ansätze, wie Kommunen ihre Resilienz[17] stärken können und wie die Kooperation bei einem Vorfall aussehen sollte. Denn für Teile der Vorfallsbearbeitung sind Deutschlands Kommunen selbst zuständig.

Anwendung von NIS-2 auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene

Die NIS-2 ist bindend für "öffentliche Verwaltung auf regionaler Ebene". Im deutschen Diskurs, noch lange bevor der Text der NIS-2 im Amtsblatt veröffentlicht wurde, war man sich einig, dass die Richtlinie ausschließlich für Landesverwaltungen, nicht aber für die Kommunen verpflichtend sein werde. Die NIS-2 macht nun ausdrücklich klar, dass die Mitgliedstaaten bei der Definition von “Einrichtungen öffentlicher Verwaltung auf regionaler Ebene” einen

---

[14]Zum Beispiel: Österreich Projekt Cursor (https://www.kiras.at/gefoerderte-projekte/detail/cursor) ENISA Cyber Exercises (https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises) oder auch Estland Cyber Range Exercises (https://e-estonia.com/solutions/cyber-security/cyber-range-exercises/)

[15]BBK Bund, LÜKEX Aktuell, BBK Bund, Accessed 18/01/2023, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Aktuell/aktuell_node.html.

[16]Kern (2022), Cyberangriffe auf deutsche Kommunen im Jahr, BIGS, 2021 https://www.bigs-potsdam.org/app/uploads/2022/04/2022_BIGS-Essenz-Nr.19-WEB.pdf. Lange, Kommunaler Notbetrieb, Übersicht IT-Sicherheitsvorfälle in Kommunalverwaltungen, Accessed 19/01/2023, https://notbetrieb.hauptsystem.de/uebersichtskarte/.

[17]Herpig (2023), Mehr Resilienz für Deutschlands IT-Systeme, Tagesspiegel Background Cybersecurity, https://background.tagesspiegel.de/cybersecurity/mehr-resilienz-fuer-deutschlands-it-systeme.

gewissen Spielraum haben. Sie dürfen ihre eigene Verwaltung nach nationalem Recht gestalten und somit auch die Einteilung selbst vornehmen. Zudem überlässt die NIS-2 den Mitgliedstaaten die Verantwortung, die NIS-2 auch auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene anzuwenden.

Empfehlung: Deutschland sollte zuerst, zum Beispiel im Umsetzungsgesetz, diese Ebenen genauer definieren und diskutieren, inwiefern könnten zum Beispiel Landkreise in die regionale Ebene im Sinne der IT-Sicherheit zählen und/oder könnte die Umsetzung der NIS-2 auch Einrichtungen der lokalen öffentlichen Verwaltung betreffen? Die NIS-2 enthält verschiedene Vorgaben, die ganz oder auch nur teilweise, z.B. über ein Stufenmodell, für lokale öffentliche Verwaltungen verpflichtend sein können, zum Beispiel Berichtspflichten, CSIRT Leistungen. Die Richtlinie ist eine so genannte "Mindestharmonisierung" und hindert Mitgliedstaaten ausdrücklich nicht daran, "Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau gewährleisten"[18]. Meiner Einschätzung nach wäre es mehr als angemessen, den Spielraum, den die NIS-2 den Mitgliedstaaten lässt, zu nutzen und auch die lokalen öffentlichen Verwaltungen in die Umsetzung mit einzubeziehen.

Anwendung auf kommunale Rechenzentrumsdienste

Empfehlung: Es sollte ebenfalls geprüft werden, ob und welche "Rechenzentrumsdienste" der Kommunen als wesentliche oder wichtige Einrichtung registriert werden sollten. Kommunen betreiben selbst die von der NIS-2 ausgenommenen "interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden". Jedoch könnte es auch Fälle geben, wo Dritte, in diesem Fall Kommunalverwaltungen, einen Rechenzentrumsdienst nutzen und dabei keine Kontrolle über technische und organisatorische Einzelheiten haben. Für diese Art von Rechenzentrumsdienst gibt es besonderen Regelungsbedarf. Ein solcher Rechenzentrumsdienst könnte durch die NIS-2 Umsetzung reguliert werden.

Beispiel für die Anwendung von NIS-2: Ausbau von CSIRTs

Empfehlung: Nicht alle Kommunen haben bisher ein designiertes CSIRT, was bedeutet, dass die Kommunen in Deutschland momentan mit unterschiedlichen Ressourcen und Kapazitäten unterstützt werden. Welche Organisationsform und Finanzierung sich anbietet, kommt auf die jeweiligen Formate in den Ländern an. Um ressourcenschonend auszubauen, bieten sich die Andockung oder Erweiterung von bestehenden Organisationsformen an, z. B. eine Anbindung an Länderverwaltungs-CSIRTs oder eine Erweiterung von Leistungen der IT-Dienstleister oder des kommunalen Zweckverbands. Deutschland ist hier sehr heterogen organisiert, weshalb unter Umständen hier eine Harmonisierung schwierig ist. Wichtig wäre allerdings, dass sich die zuständigen CSIRTs in ihrer Arbeitsweise, Anforderungen und im Aufbau an den

[18]Vgl. NIS-2 Artikel 5 Amtsblatt der Europäischen Union (2022), RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555.

bestehenden Good Practices von CSIRTs orientieren und ggf. auch dazu verpflichtet werden. Da CSIRTs mit der Verarbeitung großer Mengen teils sensibler Daten betraut sind, macht die NIS-2 in diesem Zusammenhang auf einige Vorgaben für CSIRTs aufmerksam, zum Beispiel:

- Nutzung des Traffic Light Protocol zur Informationsanalyse und -weitergabe
- Verfügbarkeit einer Infrastruktur für den Informationsaustausch und die Verarbeitung von Informationen
- Gut ausgestattetes Personal

Die CSIRTs, die für Kommunalverwaltungen zuständig sind, sollten auch an Informationsaustauschformate angebunden sein, z.B. den Verwaltungs-CERT-Verbund.

EfA-Prinzip[19] auch für Cybersicherheits-Leistungen

Die NIS-2 regt die Förderung von Maßnahmen an, zum Beispiel die "Bereitstellung kostenfreier Dienste oder Instrumente für bestimmte Einrichtungen, einschließlich Selbstbedienungskontrollen (self-service checks), Detektionswerkzeugen und Bereinigungsdiensten"[20]. Auch jetzt schon stellen manche Länder solche Leistungen für Kommunen bereit. Zudem werden andere Leistungen zur Prävention von IT-Sicherheitsvorfällen entwickelt, wie etwa Sensibilierungsmaßnahmen, Schulungen und Checklisten. Bisher entstehen dabei nicht selten verschiedene Produkte, die dasselbe wollen. Die Entwicklung der Leistungen wird nicht immer proaktiv koordiniert oder explizit nachnutzbar gemacht, wie es zum Beispiel bei OZG-Leistungen[21] angeregt wird. Die Koordination hängt noch zu sehr von Einzelpersonen ab – ob z.B. ein Austausch stattfindet und Leistungen gemeinsam entwickelt oder von anderen übernommen werden. Es gibt hier ein erhöhtes Risiko, dass dadurch Ressourcen und Expertise verschwendet werden und unnötige Dopplungen entstehen, was sich Deutschland mit Blick auf den gravierenden Fachkräftemangel in diesem Bereich nicht leisten kann.

Empfehlung: Cybersicherheits-Leistungen zur Prävention, zum Beispiel Fortbildungen oder Sensibilisierungsmaßnahmen oder auch Detektionswerkzeuge für Kommunalverwaltungen und Landesverwaltungen, sollten auch im Cybersicherheitsbereich nach dem "Einer für Alle"-Prinzip (EfA-Prinzip) entwickelt und geteilt werden. Dabei sollte das BSI eine Konformität mit BSI-Standards oder die Anpassung nach einem Stufenmodell für verschiedene Zielgruppen sicherstellen. Außerdem sollte regelmäßig Austausch zu Fortbildungsinhalten zwischen Bund und Ländern und den jeweiligen Zielgruppen stattfinden, etwa den Kommunalverwaltungen. Zudem könnte so – wie beim OZG – genau definiert werden, welche Kriterien eine Leistung

---

[19] BMI, Einer für Alle – Einfach erklärt, Accessed 18/01/2023, https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/nachnutzung/efa/efa-node.html

[20] VGl. (57) In Amtsblatt der Europäischen Union (2022), RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555.

[21] "Der Begriff OZG -Leistung beschreibt ein Leistungsbündel bestehend aus bis zu mehreren Hundert einzelnen Verwaltungsleistungen aus dem "Leistungskatalog der öffentlichen Verwaltung" (LeiKa), die thematisch aus Nutzersicht zusammenhängen." BMI, Glossar OZG-Leistung, Accessed 18/01/2023, https://www.onlinezugangsgesetz.de/Webs/OZG/DE/service/glossar/functions/ozg-lexikon.html?cms_lv3=13074320&cms_lv2=12998324#doc13074320

erfüllen muss, um tatsächlich nachnutzbar im Sinne des EfA-Prinzips zu sein. Es ist hier allerdings wichtig, die Lehren aus der Umsetzung des EfA-Prinzips im OZG mitzubedenken, um ggf. bestimmte Probleme schon von vorneherein zu verhindern oder zumindest verringern[22].

Bei den hier aufgeführten Empfehlungen handelt es sich wohlgemerkt nur um eine aussagekräftige Auswahl, die Liste könnte fortgeführt werden. Die genannten Punkte unterstreichen, dass die NIS-2 ein willkommener Anlass und eine Chance ist, das Zusammenspiel von Bund, Ländern und Kommunen im Bereich der Cybersicherheit zu verbessern. Alle diese Ebenen müssen einen Beitrag leisten, um das gemeinsame Ziel – die Resilienz von Kommunalverwaltungen – zu erreichen. Besonders wichtig sind dabei eine enge Zusammenarbeit, aber auch klare Zuständigkeiten, um unnötige Doppelungen zu vermeiden.

Fachkräftemangel begegnen – Anknüpfungspunkte

Berücksichtigung der zwölf Profile im Bereich Cybersicherheit

Empfehlung: Cybersicherheit ist ein interdisziplinäres Gebiet. Das macht es schwieriger, Kompetenzen zu entwickeln oder einzuschätzen. Um sicherzustellen, dass Deutschland Fachkräfte sowohl ausbildet als auch anzieht, sollten Arbeitgeber und Ausbildungseinrichtungen sich an den zwölf Profilen der Cybersicherheit, die die europäische Agentur ENISA mit Expert:innen für Cybersicherheit entwickelt hat, orientieren[23]. Die Profile helfen dabei, Personen im Bereich Cybersicherheit besser zu beurteilen.

Es sollte geprüft werden, inwiefern Deutschland diese Profile nutzen könnte, um den aktuellen Fachkräftemangel besser zu analysieren. So könnten zum Beispiel die Profile in Datenerhebungen zu Angebot und Nachfrage eingesetzt werden, um nachzuvollziehen, welche Profile besonders benötigt oder ausgebildet werden müssen[24]. Weitere Anwendungsbeispiele entwickelt demnächst eine Ad-hoc-Arbeitsgruppe der ENISA.

Arbeitskultur, fehlende Karrieremöglichkeiten und traditionelle Einstellungsverfahren

Pooling- und Sharing-Methoden sind hilfreich, um kurz- bis mittelfristig den Mangel an IT-Sicherheitsfachkräften auszugleichen[25] oder in schweren Fällen eine Aufstockung oder Unterstützung durch externe Fachkräfte zu ermöglichen.

Empfehlung: Bei einer IT-Sicherheitsfachkräfte-Initiative sollten außerdem die strukturellen Probleme, die den öffentlichen Dienst so vergleichsweise unattraktiv für viele Arbeitnehmer:innen machen, angegangen werden. Hier muss sich der Blick unter anderem auf die Arbeitskultur, fehlende Karrieremöglichkeiten und traditionelle

---

[22] Kommune 21 (2022), Einer-für-Alle-Prinzip in der Praxis, Kommune 21, https://www.kommune21.de/meldung_37899_Einer-f%C3%BCr-Alle-Prinzip+in+der+Praxis.html.

[23] ENISA (2022), European Cybersecurity Skills Framework Role Profiles, ENISA, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles.

[24] ENISA (2022), European Cybersecurity Skills Framework (ECSF) - User Manual, ENISA, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.

[25] Schuetze (2018), Warum dem Staat IT-Sicherheitsexpert:innen fehlen - Eine Analyse des IT-Sicherheitsfachkräftemangels im Öffentlichen Dienst, Stiftung Neue Verantwortung e.V., https://www.stiftung-nv.de/sites/default/files/it-sicherheitsfachkraeftemangel.pdf.

Einstellungsverfahren richten. Sicherlich gibt es Orte in Deutschland, wo für diese Herausforderungen schon Lösungen gefunden wurden, die also als Vorbilder dienen könnten. Es wäre hilfreich, diese Good Practices sichtbar zu machen, um dann auch gezielt ihre Anwendung auszuweiten.

Einbindung nicht-staatlicher Akteure im Aufbau von regionalen Trainings-Hubs

Empfehlung: Beim Auf- oder Ausbau von Fort- und Weiterbildungen von staatlichen Akteuren können Kooperationen zwischen wissenschaftlichen, zivilgesellschaftlichen, privaten und staatlichen Akteuren hilfreich sein, um einen Austausch von Expertise und Erfahrung zu gewährleisten. Hier könnten bestehende Formate im In- und Ausland als Inspiration dienen und zielgerichtet ausgebaut werden, wie zum Beispiel der neu gegründete französische Cyber-Campus, die Ohio Cyber Range, der BCM-Workshop des HECAAZ und der CyberSecurity Verbund Sachsen-Anhalt.

Prüfung von Bildungsinitiativen anderer EU-Staaten

Empfehlung: Im Einklang mit dem Europäischen Gesetz zur Cybersicherheit, Artikel 102, hat ENISA den Auftrag, die Mitgliedstaaten auch beim Thema Cybersicherheit auf allen Bildungsebenen zu unterstützen. In diesem Kontext hat ENISA eine engere Koordinierung und den Austausch von Good Practices unterstützt. Deutschland sollte diesen Bericht zum Anlass nehmen, vielversprechende Ansätze[26] anderer Länder zu prüfen. Es wäre durchaus denkbar, hier Ideen aufzugreifen.

[26] ENISA (2022), Cybersecurity Education Initiatives in the EU Member States, ENISA, https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states.

Kernaussagen

- Ansprechestellen und zuständige Behörden auf Landesebene werden immer wichtiger. Dies ermöglicht es, Maßnahmen wie z.B. Beratung zu Resilienzmaßnahmen näher an den Zielgruppen (etwa Kommunalverwaltungen) zu organisieren.
- Die NIS-2 könnte durch ihre Vorgaben nicht nur einen Harmonisierungs-Effekt innerhalb der EU, sondern auch innerhalb Deutschlands haben, indem die Beiträge der Länder genauer definiert werden.
- Trotz Vorgaben der NIS-2 bleiben den Mitgliedstaaten bei der Umsetzung große Spielräume. Für eine föderal organisierte Cybersicherheitsarchitektur wie der Deutschen bringt dies neue organisatorische, rechtliche und politische Herausforderungen bei der Umsetzung mit sich.
- Um den Beitrag verschiedener staatlicher Akteure genau zu definieren, sollte eine nationale Cybersicherheitsstrategie gemeinsam mit den Ländern erarbeitet werden. Darin sollten die Zuständigkeiten und Beiträge der Länder zur Erreichung der Ziele festgelegt werden.
- Ein Risiko der föderalen Struktur ist, dass Expertise nicht ressourcenschonend geteilt wird und unnötige Dopplungen entstehen.
- Empfehlung ist deshalb, mit Cybersicherheitsübungen Informationsaustausch und Meldewege, die im Rahmen der NIS-2 vereinfacht und gestrafft werden sollen, praxisnah zu entwickeln und zu testen.
- Cybersicherheits-Leistungen zur Prävention, zum Beispiel Fortbildungen oder Sensibilisierungsmaßnahmen für Kommunalverwaltungen und Landesverwaltungen, sollten auch im Cybersicherheitsbereich nach dem "Einer für Alle"-Prinzip (EfA-Prinzip) entwickelt und geteilt werden.
    - Bei Cybersicherheitsleistungen sollte das BSI eine Konformität mit BSI-Standards oder die Anpassung nach einem Stufenmodell für verschiedene Zielgruppen sicherstellen können.
- Das BSI könnte durch Nutzung gemeinsamer Technologien zum Informationsaustausch oder Meldeverfahren und Datensätze zum Knotenpunkt der Bund-Länder-Zusammenarbeit werden.
- NIS-2 macht klar, dass die Mitgliedstaaten bei der Definition von “Einrichtungen öffentlicher Verwaltung auf regionaler Ebene” Spielraum haben.
- Mitgliedstaaten können daher über die Anwendung von NIS-2 auf lokaler Ebene eigenständig entscheiden.
- Es empfiehlt sich, die öffentliche Verwaltung auf lokaler Ebene in die Umsetzung der NIS-2 einzubeziehen. Zum Beispiel sollte jede Kommunalverwaltung auf CSIRT-Leistungen Zugriff haben und in Informationsaustausch und Meldeverfahren eingebunden werden.
- Es muss geprüft werden, ob und welche “Rechenzentrumsdienste” der Kommunen als wesentliche oder wichtige Einrichtung registriert werden sollten.
- Mit Blick auf den Fachkräftemangel sollten die zwölf Profile der Cybersicherheit, die die europäische Agentur ENISA mit Expert:innen entwickelt hat, bei der Analyse von Ursachen und Lösungen genutzt werden.
- Pooling- und Sharing-Methoden sind hilfreich, um kurz- bis mittelfristig den Mangel an IT-Sicherheitsfachkräften in der Verwaltung auszugleichen.

- Im Rahmen einer IT-Sicherheitsfachkräfte-Initiative sollten strukturelle Aspekte wie z.B. die Arbeitskultur, fehlende Karrieremöglichkeiten und traditionelle Einstellungsverfahren adressiert werden.
- Die Einbindung nicht-staatlicher Akteure beim Aufbau regionaler Trainings-Hubs ist ein guter Anreiz für den Austausch von Expertise und Erfahrung.
- Weitere Lösungsansätze könnten sich nach einer Prüfung von Bildungsinitiativen anderer EU-Staaten ergeben.

Danksagungen

Für die sprachliche und strukturelle Überarbeitung bedanke ich mich bei Luisa Seeling.
Ich bedanke mich außerdem für den fachlichen Austausch zur Stellungnahme bei Carolin Kemper, Deutsches Forschungsinstitut der öffentlichen Verwaltung zum Thema NIS-2-Anwendung und Dr. Sven Herpig zur Rolle des Bundes in der Architektur. Impulsgebend waren für mich außerdem Recherchen und Gespräche mit Expert:innen im Rahmen des SNV-Projekts “Policy Good Practices für die Zusammenarbeit von Bund, Bundesländern und Kommunen zur Verbesserung der Vorfallsbearbeitung” [27], das Design von Übungen im SNV-Projekt "länderspezifische Cybersicherheitspolitik-Übungen"[28] und der von SPIRI und ORF organisierte Workshop zu “Cyber Postures der EU, USA, China und Russland”[29].

[27] SNV, Resilienzfähigkeiten von Kommunalverwaltungen stärken, Accessed 18/01/2023, https://www.stiftung-nv.de/de/unterprojekt/resilienzfaehigkeiten-von-kommunalverwaltungen-staerken.
[28] SNV, Cybersecurity Policy Exercises, Accessed 18/01/2023, https://www.stiftung-nv.de/en/publication/cybersecurity-policy-exercises.
[29] SNV, How the Cyber Resilience Act could change EU’s Cyber Posture, Accessed 18/01/2023, https://www.stiftung-nv.de/de/veranstaltung/how-cyber-resilience-act-could-change-eus-cyber-posture.

Anhang

Fragen des Ausschusses

In der Stellungnahme beziehe ich mich auf folgende Fragen des Ausschusses:

Frage 1: Im Koalitionsvertrag haben die Regierungsparteien vereinbart, dass sie „einen strukturellen Umbau der IT-Sicherheitsarchitektur“ einleiten und das „Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger“ aufbauen und es als „zentrale Stelle im Bereich ITSicherheit“ ausbauen wollen. Wie sollte die Cybersicherheitsarchitektur auf nationaler und europäischer Ebene ausgestaltet werden, um effektiver, wirksamer und widerspruchsfreier aufgestellt zu sein und wo bedarf es einer Neuordnung oder auch Bündelung der Kompetenzen zwischen Bund, Ländern und der Europäischen Union und bedarf es auch angesichts der aktuellen Herausforderungen einer Diskussion über innere und äußere Sicherheit und der diesbezüglichen Kompetenzen und Grenzen? Welche anderen Akteure neben dem BSI (also etwa Cyber-Abwehrzentrum, Nationaler Cyber-Sicherheitsrat, ZITiS), die in Deutschland für Cybersicherheit zuständig sind, sollten reformiert werden und wie?

Frage 6: Was kann die Bundesrepublik Deutschland in ihrer nationalen und internationalen Cybersicherheitspolitik von anderen Ländern und internationalen best practices konkret lernen, insbesondere im Hinblick auf staatliche Stellen, Governance, verfügbare Instrumente, Fokus
und Kapazitäten?

Frage 11: Wie bewerten Sie die Lage von IT-Fachkräften – insbesondere für Cybersicherheit – auf dem Arbeitsmarkt und was müssten staatliche (Sicherheits)-Behörden verbessern, um noch mehr kompetente IT-Fachkräfte zu gewinnen?

Frage 12: 12) Wie könnte die Ausbildung von IT-Cyberfachkräften sowohl in quantitativer als auch in qualitativer Hinsicht in Deutschland weiter verbessert werden?

Frage 18: Wer bzw. was muss alles in den Blick genommen werden, wenn wir über Zuständigkeiten und Instrumente zur Verbesserung der IT-Sicherheit nachdenken, wo liegen die jeweiligen Defizite sowie Verbesserungsmöglichkeiten und wie bewerten Sie die Effektivität aktueller Informations- und (Weiter-)Bildungsmaßnahmen?