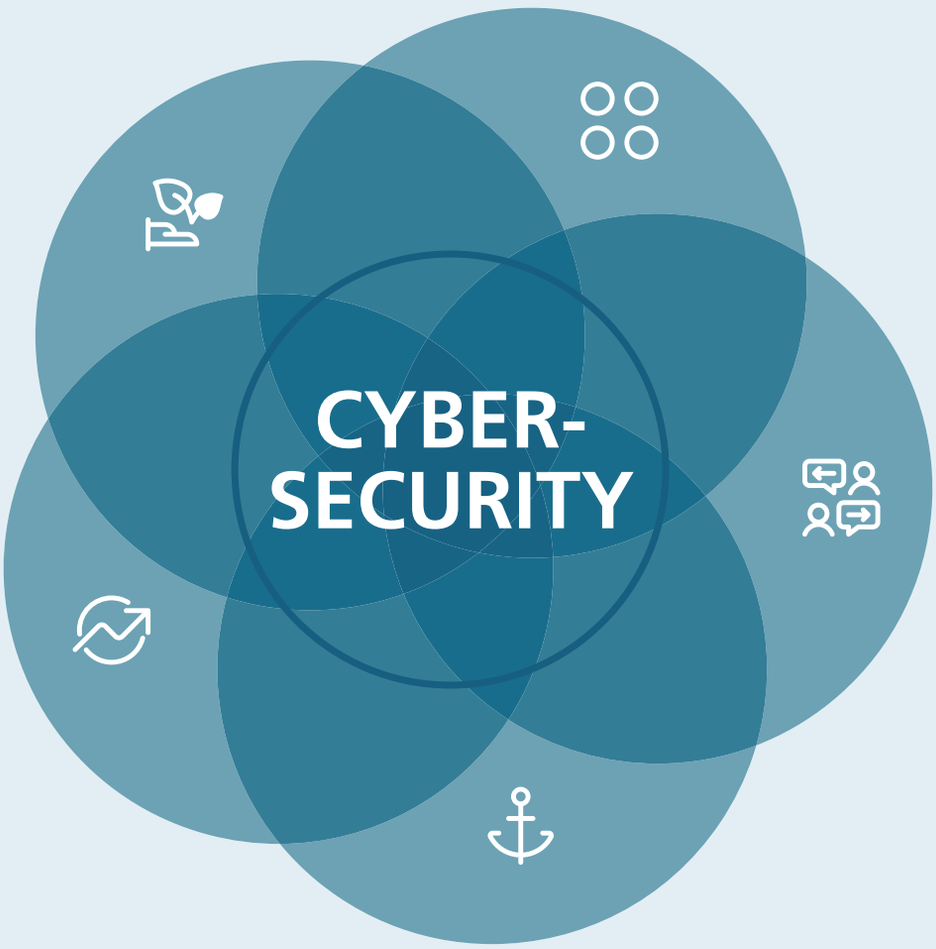
ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN
Hessisches Ministerium
des Innern und für Sport

Fraunhofer
SIT



Das Governance-Framework 5V

Dr. Michael Kreutzer, Kirstin Scheel

Einleitung

Die Digitalisierung durchdringt nicht nur den Alltag aller Bürger*innen, sondern auch Behörden und administrativen Infrastrukturen. Städte und Regionen sollen und wollen sich immer stärker vernetzen und im Rahmen der „Smartification" immer mehr Daten erheben und Wissen nutzen.

Im Schwung des Neuen gerät jedoch manchmal die Cybersicherheit aus dem Blickfeld. Hinzu kommt, dass es in vielen Konstellationen der inter-behördlichen Zusammenarbeit Cybersicherheit strukturelle und organisatorische Hindernisse gibt. Im Bereich der Digitalisierung von Regionen und Städten blendet wiederum die vielfach vorzufindende technokratische Sicht von Smart-City- und Smart-Region-Projekten die komplexe Governance und Interessenslage meist aus.

Beide Tendenzen wirken sich negativ auf eine erreichbare Cybersicherheit aus.

Bezüglich der Cybersicherheitskollaboration zwischen den Akteuren und hinsichtlich der Prozesse hierfür besteht ein erheblicher Forschungsbedarf. Hier setzte ein vom Hessischen Ministerium des Innern und für den Sport (HMdIS) initiiertes Forschungsprojekt mit dem Fraunhofer-Institut für Sichere Informationstechnologie SIT als Mitwirkender im Forschungszentrum ATHENE an. Im Laufe des Projekts wurde ein Governance-Rahmenwerk entwickelt, welches strategisch das IT-Sicherheitsniveau von öffentlichen Stellen verbessern helfen kann.

Das unten näher erläuterte Konzept der „5V" ist das Kernergebnis des Projekts. Dieses trifft bislang sowohl bei den Praktiker*innen als auch in der akademischen Welt auf positive Resonanz. Das Konzept wurde mit dem zweiten Platz beim eGovernment-Wettbewerb 2022 ausgezeichnet, was die praktische Relevanz von 5V unterstreicht.

Wir hoffen, dass es einen ersten Schritt auf dem Weg in Richtung höhere IT-Sicherheit liefern kann. Wir finden, dass es sich für deutsche Kommunen lohnt, sich in Richtung Erhöhung des Cybersicherheitsniveaus zu bewegen — die 5V können hierzu den entscheidenden Impuls geben. Ist eine Kommune erst einmal auf dem Weg, dann kann und sollte das Ziel der Zertifizierung nach BSI IT-Grundschutz angestrebt werden.

Inhalt

Das Framework

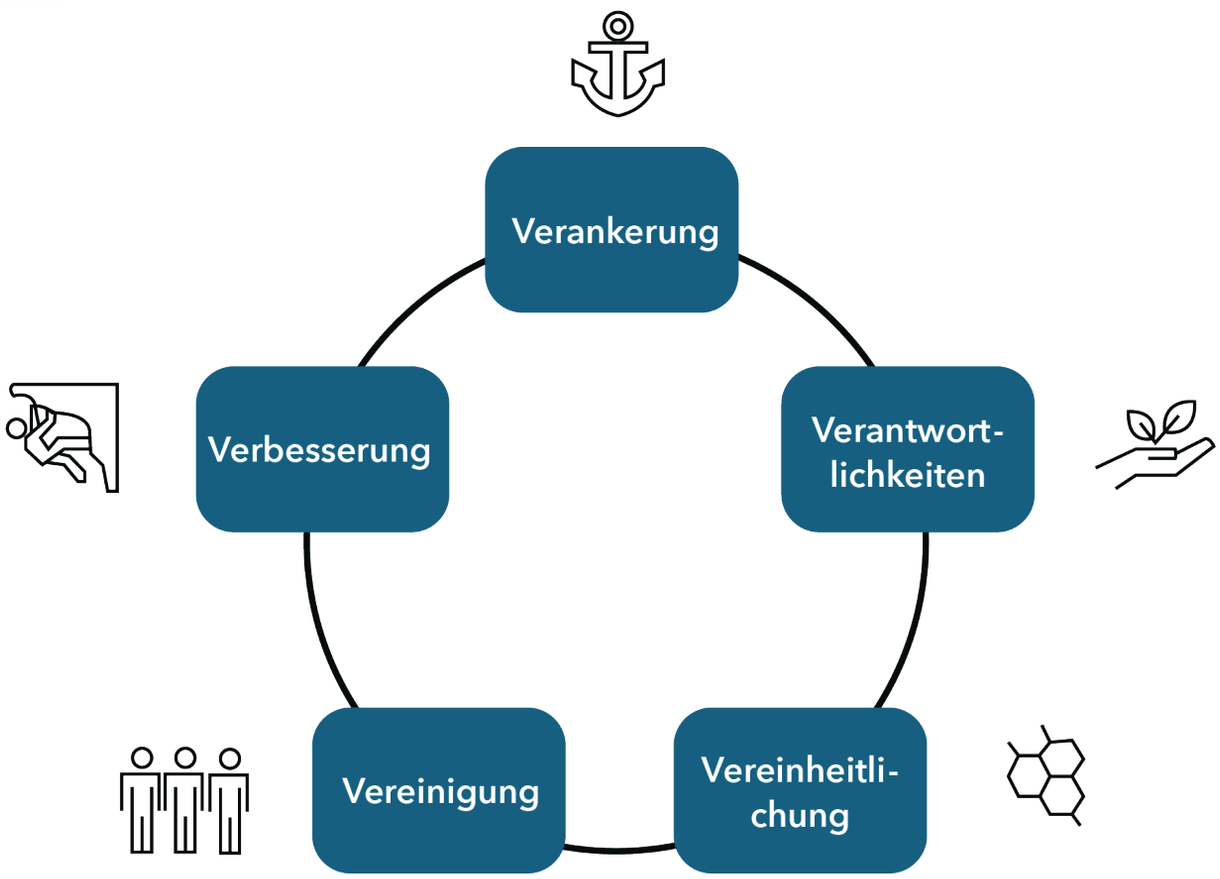


Abbildung 1: Modell der 5V

Aus den Gesprächen mit Stakeholdern aus dem öffentlichen Bereich sowie der Literaturrecherche haben wir das im Folgenden erläuterte Rahmenwerk der 5V entwickelt.

Die öffentlichen Akteure der unterschiedlichen Ebenen haben spezifische Anforderungen an Cybersicherheit, welche im Spannungsfeld begrenzter Ressourcen v.a. auf kommunaler Ebene aktuell z.T. zu einer eher pragmatischen Kooperation und informellen Informationsaustauschen führt. Nicht jede Ebene kann alle fachspezifischen Aufgaben und Verantwortlichkeiten in derselben Form abbilden und ausfüllen (Vgl. kleine ländliche Kommunen vs. Großstädte).

Die öffentliche Hand kann und sollte eine richtungsweisende Funktion in der Cybersicherheit einnehmen. Einerseits ergibt sich diese Funktion aus der Aufgabe der Daseinsvorsorge, andererseits würde diese Rolle strategische Ziele unterstützen, wie einen Zuwachs an digitaler Souveränität und die Erhöhung der Innovationskraft Cybersicherheit.

Wie kann diese Vorreiterrolle der öffentlichen Hand erreicht werden? Dazu stellen wir unsere Idee von 5Vs zur Diskussion.

Die 5Vs sind:

1. die Verankerung von Cybersicherheit auf der jeweils obersten Ebene,
2. die klare Zuordnung von Verantwortlichkeiten,
3. die Vereinheitlichung,
4. die Vereinigung, sprich die Intensivierung von Zusammenarbeit und
5. eine Vorschlags-, Fortentwicklungs- und Fehlerkultur zur kontinuierlichen Verbesserung.

Dabei sei darauf hingewiesen, dass diese nicht als aufeinanderfolgende Schritte zu verstehen sind – alle Punkte bedingen einander und müssen parallel vorhanden sein, um das IT-Sicherheitsniveau zu optimieren.

1. Verankerung

- Die Verankerung von Cybersicherheit auf der jeweils obersten Ebene.
- Als Zukunftsfaktor und Grundlage zukünftiger Relevanz muss IT-Sicherheit strukturell verankert und auf allen Ebenen mitgedacht werden

IT-Sicherheit muss in der Führungsebene als relevanter Zukunftsfaktor strukturell verankert sein (Vgl. [1], [2], [3]). Erst dann kann sie als integraler Bestandteil auf allen Ebenen mitgedacht werden. Denn Cybersicherheit ist kein reines IT-Thema. Die strategisch Verantwortlichen müssen sich der Herausforderung bewusst sein – von der Hausspitze, über die Vergabestellen bis zu den Endanwendenden.

Aus der Praxis:
In der freien Wirtschaft fällt es der Geschäftsführung oder dem Vorstand zu, ein angemessenes Compliance-System zu implementieren. Im Zweifelsfall prüft die zuständige interne Stelle, ob mit der entsprechenden Sorgfalt vorgegangen und die richtige Organisation eingerichtet wurde. Auch bei öffentlichen Stellen darf es nicht zu einem Organisationsverschulden kommen, daher muss IT-Sicherheit auch hier auf höchster Organisationsebene angesiedelt sein.

Quick Check:
- Ist in Ihrer Organisation Cybersicherheit auf oberster Entscheidungsebene angesiedelt?
- Wird IT-Sicherheit als integraler Bestandteil auf allen Ebenen mitgedacht?

2. Verantwortung und Governance

- Eine klare Zuordnung von Verantwortlichkeiten und eine Ausstattung mit notwendigen Ressourcen ist grundlegend.
- Dazu gehören z.B. Meldewege und festgelegte Reaktionszeiten sowie Übungen.

Auch in einer hierarchisch strukturierten Organisation kann es zu mangelnder Übernahme von Verantwortung kommen. Wer für was zuständig ist, muss zunächst geklärt und dann mit den entsprechenden Ressourcen ausgestattet werden.

Als Teil der Organisationsentwicklung müssen z.B. Meldewege und Reaktionszeiten ebenenübergreifend festgelegt sein, damit im Notfall schnell gehandelt werden kann. Dazu gehört auch, dass diese geübt und gelebt werden (vgl. [4]). Konkret heißt das bei IT- und Cybersicherheit z.B. auch, dass eine einfachere Nutzbarkeit häufig einhergehen kann mit geringerer Sicherheit – und dafür muss Verständnis auf allen Ebenen geschaffen werden ((Bartsch und Frey 2018b), S. 134, [5], S. 306).

Um das Sicherheitsniveau zu erhöhen ist also nicht nur eine Sensibilisierung, sondern auch eine vorausschauende Betrachtung aus organisationspsychologischer Sicht nötig. So können unsichere Gewohnheiten und operative Workarounds wie geteilte Nutzerzugänge oder das Post-it mit dem schwer zu merkenden Passwort unter der Tastatur von vornherein vermieden oder zumindest minimiert werden. (Vgl. [4]). Denn der*die Endanwendende ist in Zeiten von sich ständig verbessernden Angriffsversuchen eine der wichtigsten Verteidigungslinien der Organisation.

Spätestens wenn es zu einem Vorfall gekommen ist, muss klar sein, wer was wann sagt und tut. Krisenkommunikation muss dabei genauso geübt werden, wie das Wiedereinspielen von Backups. Dafür braucht es klare Linien.

Aus der Praxis:
Bei Cyberangriffen kommt es zum Beispiel vor, dass anfangs behauptet wird, es wären keine personenbezogenen Daten betroffen. Leider stellt sich das häufig im Nachhinein als Fehleinschätzung heraus. Das zeigt ein Negativbeispiel aus der Schweiz in der Kleinstadt Rolle im Mai 2021: Zu diesem Zeitpunkt tauchten Daten von Einwohner*innen im Darknet auf. Die offizielle Einschätzung von Seiten der Verwaltung war, dass es sich nicht um sensible Daten handele. Monate später waren die teilweise besonders schützenswerten Daten jedoch immer noch online einsehbar[1]. Hier hatten offensichtlich sowohl die interne als auch die äußere Kommunikation versagt.

Umso wichtiger ist es, gerade am Beginn der Auswirkungen eines solchen Angriffs angemessen zu kommunizieren – und dafür z.B. interne Wege vorab geklärt zu haben.

Quick Check:
- Sind in Ihrer Organisation Verantwortlichkeiten bei der Cybersicherheit klar benannt?
- Haben die Verantwortlichen ausreichende Ressourcen zur Ausübung dieser Verantwortung?
- Gibt es eindeutige Meldewege? Gibt es regelmäßig Übungen?

1 Vgl. https://www.heise.de/news/Schweiz-Buerger-und-Gemeindedaten-im-Darknet-veroeffentlicht-6176802.html, abgerufen am 01.09,.2022

3. Vereinheitlichung

- Eine Vereinheitlichung über Organisationseinheiten hinaus kann helfen, eine bessere Nutzung der vorhandenen Mittel darzustellen.

Wenn das Rad an jeder Stelle neu erfunden werden muss (Vgl. [6], [7]), werden Ressourcen nicht effizient genutzt. Eine Vereinheitlichung über Organisationseinheiten hinaus kann helfen, eine bessere Nutzung der vorhandenen Mittel darzustellen.

Konkret kann das z.B. heißen, dass eine kompetent aufgesetzte (beispielsweise korrekt segmentierte) IT-Infrastruktur vor Ausfällen bewahrt, da sich z.B. Schadsoftware nicht im gesamten Netz verbreiten kann. Gut ausgebildete und sensibilisierte IT-Fachleute ebenso wie Endanwendende sind eine absolut notwendige Grundvoraussetzung für Cybersicherheit in einer Organisation.

Die Umsetzung des Onlinezugangsgesetzes (OZG) wird diesen Prozess beeinflussen, doch wenn man bedenkt, dass ein Großteil der operativen Umsetzung auf kommunaler Ebene erfolgen muss, ist auch dort noch Spielraum zu weiterer Kooperation. So sprechen z.B. inzwischen sogar die Rechnungshöfe Empfehlungen für entsprechende IT-Verbünde und IT-Sicherheitsmanagementsysteme aus (Vgl. [8], [9]).

Dass dem öffentlichen Einkauf hier eine besondere Rolle zukommt, sei nur am Rande erwähnt – und bedarf einer gesonderten Betrachtung, die über den Rahmen dieses Papers hinausgeht.

Aus der Praxis:
Auf hessischer Landesebene wurde der HessenPC eingeführt, um auf Landesebene grundlegend vereinheitlichte Rechnerstrukturen zu haben. Der HessenPC wird kontinuierlich weiterentwickelt und trägt somit zu einem höheren Cybersicherheitsniveau bei[2].

Quick Check:
- Gibt es eine einheitliche IT-Strategie, mit Cybersicherheit als relevantem integralem Bestandteil?
- Wird Cybersicherheit von der Ausschreibung, über den Vergabeprozess bis zur täglichen Anwendung mitgedacht?

4. Vereinigung

- Hierbei geht es um die Intensivierung der operativen Zusammenarbeit und bereichsübergreifenden Kooperation
- Eine effizientere und effektivere Nutzung vorhandener Ressourcen kann zu einer höheren IT-Sicherheit beitragen, wenn besser zusammengearbeitet wird.

Eine operative Zusammenarbeit und bereichsübergreifende Kooperation kann für eine effizientere und effektivere Nutzung der Ressourcen sowie ein insgesamt höheres Schutzniveau sorgen. Damit IT-Sicherheit funktionieren kann, ist es notwendig, dass die unterschiedlichen Bereiche zusammenarbeiten und Informationen nicht nur fließen, sondern auch verarbeitet und berücksichtigt werden. Dies gilt bei einer heterogenen Struktur umso mehr: Zusammenarbeit kann zu einer Effizienzsteigerung in der geteilten Ressourcennutzung führen, bei der nicht jeder einzelne Bereiche mit hohem Aufwand dieselben Betriebsmittel bereitstellen muss. Dazu bedarf es einer engeren vertikalen und horizontalen Vernetzung. Angewandte Forschung kann dabei die Rolle einer ideellen Sparringspartnerin und Impulsgeberin übernehmen, um neueste Erkenntnisse anbieterneutral in die Verwaltungspraxis zu integrieren. Insgesamt könnte dadurch die Innovationskraft gestärkt werden.

Aus der Praxis:
Im Landkreis Gießen haben sich 2022 alle Kommunen zu einem „Interkommunalen Projekt zur Cybersicherheit in öffentlichen Verwaltungen im Landkreis Gießen" zusammengetan[3].

Quick Check:
- Arbeiten Sie bei der Cybersicherheit bereichsübergreifend, womöglich sogar organisationsübergreifend?
- Arbeiten unterschiedliche Bereiche zusammen und fließen Informationen nicht nur, sondern werden sie auch verarbeitet und berücksichtigt?

2 Vgl. https://hzd.hessen.de/medienraum/publikationen/hzd-jahresbericht/geschaeftsjahr-2021/fokusthema-informationssicherheits-management/hessenpc-40-arbeiten-auf-nummer-sicher, abgerufen am 01.09,.2022

3 Vgl. https://www.giessener-anzeiger.de/lokales/kreis-giessen/gemeinsam-gegen-hacker-91511929.html, abgerufen am 01.09,.2022

5. Vorschlags-, Fortentwicklungs- und Fehlerkultur

- Nur dort, wo kontinuierlich aus internen und externen Fehlern gelernt wird, kann mit einem sich dynamisch verändernden Umfeld Schritt gehalten werden.
- Denn Innovation, Weiterentwicklung und Paradigmenwechsel sind normaler Teil der Cyberwelt.

Nur dort, wo kontinuierlich aus internen und externen Fehlern gelernt wird, kann mit einem sich dynamisch verändernden Umfeld Schritt gehalten werden. Dazu gehört auch auf allen Ebenen das Verständnis, dass Innovation, Weiterentwicklung und Paradigmenwechsel normaler Teil der Cyberwelt sind. Nur dort, wo ohne unnötige Schuldzuschreibungen an einem gemeinsamen Verbesserungsprozess gearbeitet wird, kann eine ebenenübergreifende Entwicklung stattfinden.

Solche kontinuierlichen Verbesserungsprozesse betrachtet man im Bereich der IT und IT-Sicherheit im Rahmen von sog. Reifegradmodellen. Auf Basis von fundierten Informationen wird ein System permanent angepasst und der Reifegrad dadurch verbessert. Das gilt auch für die Verbesserung von Cybersicherheit. Dadurch, dass man offen kommuniziert, auch über Fehler, erreicht man eine höhere Effizienz und Effektivität im Betrieb insgesamt und ist gleichzeitig gewappnet für Veränderungen bzw. zukünftige Entwicklungen. Eine gleichzeitige Finanzkontrolle (z.B. Wirkungskontrolle von Investitionen) führt zu Steuerungsfähigkeit und Offenheit für die Zukunft (Vgl. [10]).

Um diesen Prozess auf allen Ebenen zu einem integralen Bestandteil der Organisation werden zu lassen, bedarf es einer kontinuierlichen Weiterbildung nicht nur des Fachpersonals, sondern auch Anwender*innen aus allen anderen Bereichen. Nur durch eine andauernde Sensibilisierung, aber auch Wertschätzung des Beitrags des Einzelnen kann dieses Thema in der Kultur der Organisation verankert werden.

Die IT-Systeme der öffentlichen Hand von morgen werden aus den IT-Systemen von heute heraus entwickelt werden. Es ist nicht davon auszugehen, dass die zukünftige IT-Welt sinnbildlich auf der grünen Wiese gänzlich neu konzipiert wird. Wenn man die angewandte Cybersicherheitsforschung einbinden möchte, dann muss sie Zugang zu den Systemen erhalten, beispielsweise durch die Bereitstellung von Testsystemen. Sie muss auch eingebunden werden in die Konzipierung der Zukunft, hier insbesondere in Überlegungen der Weiterentwicklung der Systemarchitektur sowie organisatorischen Change Managements.

Aus der Praxis:
Cybersicherheit ist grundsätzlich ein Prozess, kein einzelnes Projekt. Die Bedrohungslandschaft entwickelt sich kontinuierlich weiter, und somit auch die Möglichkeiten der Verteidigung und des Schutzes. In Hessen unterstützen zum Beispiel das Hessische Cyberabwehrausbildungszentrum Land/Kommunen (HECAAZ L/K) und das Kommunale Dienstleistungszentrum Cybersicherheit (KDLZ-CS) öffentliche Einrichtungen bei der kontinuierlichen Weiterbildung[4].

Quick Check:
- Lernen Sie aus eigenen Fehlern und den Fehlern anderer?
- Suchen Sie gezielt Mitstreitende, um sich als Organisation in der Cybersicherheit weiterzuentwickeln?
- Gibt es das Verständnis, dass Innovation, Weiterentwicklung und Paradigmenwechsel normale Teile besonders auch der Cyberwelt sind?

Abbildung 2: Einige Angebote zur Cybersicherheit in Hessen

4 Vgl. https://www.ekom21.de/infocenter/einfo21-digital/2022/juni/hecaaz/, abgerufen am 01.09.2022

Fazit und Ausblick

Auf übergreifender Ebene scheinen sich drei Bereiche abzuzeichnen, welche für eine weitere Betrachtung von Interesse sein können:

1. Der fundamentale Ressourcenengpass im Bereich qualifizierten Personals

2. Die grundlegenden Herausforderungen der öffentlichen Beschaffung und Vergabe im Bereich IT, vor allem auch im Zusammenhang mit sicherheitsrelevanter Beschaffung

3. Das Ideal einer kontinuierlichen Weiterentwicklung einer ebenenübergreifenden Kooperation.

Cybersicherheit ist kein Thema, das in absehbarer Zeit an Relevanz verlieren wird – es ist schon lange keine Frage mehr, ob es die eigene Organisation treffen wird, sondern nur noch wann. Gerade deshalb ist es wichtig, sich proaktiv damit zu befassen – und sich Verbündete und Partner*innen zu suchen, im Haus wie extern. Denn nur, wenn alle Bereiche von der Ausschreibung, Beschaffung bis zum Betrieb zusammenarbeiten und alle Beteiligten auf jeder Ebene entsprechend sensibilisiert sind und sich stetig weiterentwickeln, kann Cybersicherheit gelingen.

Literaturverzeichnis

1. Guhr, N., Lebek, B., Breitner, M.H.: The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. Info Systems J, vol. 29, 340–362 (2019). doi: 10.1111/isj.12202

2. Bruijn, H. de, Janssen, M.: Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly, vol. 34, 1–7 (2017). doi: 10.1016/j.giq.2017.02.007

3. Norris, D.F., Mateczun, L., Joshi, A., Finin, T.: Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. Journal of Urban Affairs, vol. , 1–23 (2020). doi: 10.1080/07352166.2020.1727295

4. Jäger, T., Daun, A., Freudenberg, D. (eds.): Prävention auf kommunaler Ebene. Lehrbuch, vol. / Thomas Jäger, Anna Daun, Dirk Freudenberg (Hrsg.) ; Band 2. Springer VS, Wiesbaden, Germany (2018)

5. Reuter, C. (ed.): Sicherheitskritische Mensch-Computer-Interaktion. Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement. Lehrbuch, vol. . Springer Vieweg, Wiesbaden (2018)

6. Deutscher Städtetag: Digitale Souveränität von Kommunen stärken - Diskussionspapier des Deutschen Städtetages (2020)

7. BMWi: Digitalisierung in Deutschland – Lehren aus der Corona-Krise (2021)

8. Rechnungshöfe des Bundes und der Länder: Handreichnung IT-Verbünde und IT-Kooperationen, vol. (2020)

9. Rechnungshöfe des Bundes und der Länder: Grundsatzpapier Informationssicherheitsmanagement, vol. (2020)

10. Stöwer, M., Kraft, R.: Sicherheit messen! Kennzahlensysteme zur Überwachung der Informationssicherheit. In: Sowa, A. (ed.) IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit. Neue Ansätze für die IT-Revision, pp. 97–116. Springer Vieweg, [S.l.] (2020)

11. IT-Planungsrat: Leitfaden IT-Personal für die öffentliche Verwaltung gewinnen, binden und entwickeln (2017)

12. Schuetze, J.: Warum dem Staat IT-Sicherheitsexpert:innen fehlen. Eine Analyse des IT-Sicherheitsfachkräftemangels im Öffentlichen Dienst (2018)

13. Thapa, B.E.P.: Strategische Beschaffung in der IT-Konsolidierung (2019)

14. Eßig, M., Glas, A., Deimling, C. von: Beschaffung für Einsatzorganisationen. In: Kern, E.-M., Richter, G., Müller, J.C., Voß, F.-H. (eds.) Einsatzorganisationen. Erfolgreiches Handeln in Hochrisikosituationen, pp. 181–203. Springer Fachmedien Wiesbaden GmbH; Springer Gabler, Wiesbaden (2020). doi: 10.1007/978-3-658-28921-8_10

15. Puhl, P., Stuck, J., Schäfer, S., Hillebrand, A.: Vertrauen in Datenverarbeitung (2021)

16. Winkler, F.: Abschlussbericht Voruntersuchung Spezialistenebene IT-WBS. 2.2.349 - Voruntersuchung der ersten Fortbildungsebene des IT-Fortbildungssystems im Rahmen der Vorbereitung zur Novellierung der Verordnung über die berufliche Fortbildung im Bereich der Informations und Telekommunikationstechnik (Voruntersuchung IT-Fortbildungsverordnung, Teil 2) (2021)

17. Mertens, A., Ahrend, K.-M., Kopsch, A., Stork, W.: Smart Region. Die digitale Transformation einer Region nachhaltig gestalten. Springer Fachmedien Wiesbaden; Imprint: Springer Gabler, Wiesbaden (2021)

18. Münchhausen, G., Schmitz, S., Schönfeld, G.: Betriebliche Weiterbildung, Lernformen und Kompetenzanforderungen. Ergebnisse der Betriebsfallstudien der CVTS5-Zusatzerhebung in Deutschland (2021)

19. Ausgestaltung der Informationssicherheitslinie in Kommunalverwaltungen. Handreichung (2017)

20. BMI: Nationaler Pakt Cybersicherheit. Online Kompendium Cybersicherheit in Deutschland (2020)

21. Seckelmann, M., Brunzel, M. (eds.): Handbuch Onlinezugangsgesetz, vol. . Springer Berlin Heidelberg, Berlin, Heidelberg (2021). doi: 10.1007/978-3-662-62395-4

Impressum

Herausgeber
Fraunhofer-Institut für Sichere Informationstechnologie

www.sit.fraunhofer.de

Hinweise
Die in diesem Dokument enthaltenen Arbeitsergebnisse sind sorgfältig und unter Zugrundelegung des bekannten Standes der Wissenschaft erstellt worden, stellen jedoch Forschungsansätze dar. Eine Haftung oder Garantie dafür, dass die Arbeitsergebnisse bzw. Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird aus diesem Grund nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, sodass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse bzw. Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Kontakt

Dr. Michael Kreutzer
Tel. +49 6151 869-348
michael.kreutzer@athene-center.de

Nationales Forschungszentrum für
angewandte Cybersicherheit ATHENE
Rheinstraße 75
64295 Darmstadt