September 2023 · Julia Schuetze

Wie sich die Informations-sicherheit von deutschen Städten verbessern lässt

Eine Bedarfsanalyse in 34 Städten

Stiftung Neue Verantwortung

Deutscher Städtetag

Disclaimer:
Diese Analyse wurde von Mitgliedern betroffener Fachausschüsse und Arbeitsgruppen im Deutschen Städtetag durch Online-Zusammenarbeit und Fokusgruppen unterstützt. Die in diesem Dokument geäußerten Ansichten und Meinungen sind die der Autorin und spiegeln nicht unbedingt die Position der Mitglieder der Arbeitsgruppe oder die ihres jeweiligen Arbeitgebers wider.

Die Bedarfsanalyse ist Teil eines Projekts, das von der Stiftung Neue Verantwortung e.V. in Kooperation mit dem Deutschen Städtetag implementiert wurde. Dies erfolgt im Auftrag der Koordinierungs- und Transferstelle Modellprojekte Smart Cities (KTS) und wird durch das Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen finanziert.

Deutscher Städtetag

Liebe Leserinnen, liebe Leser,

der Wert einer Sache zeigt sich oft erst dann, wenn er fehlt. Schmerzhaft mussten die Kommunen das erfahren, die bereits von größeren Cybersicherheitsvorfällen betroffen waren. Wenn eine Stadtverwaltung keine Mails mehr empfangen kann, wenn dringend benötigte Daten nicht mehr greifbar sind oder kein Personalausweis ausgestellt werden kann, zeigt sich die Verwundbarkeit unserer Institutionen. Eine vernetzte Welt bietet viele Angriffspunkte. Was bietet bestmöglichen Schutz? Wie kann die Informationssicherheit von Städten verbessert werden? Diese Fragen haben zu dem Projekt geführt, das der Deutsche Städtetag und die Stiftung Neue Verantwortung in diesem Jahr gestartet haben.

Das Projekt beruht auf einer einfachen Erkenntnis: Die Informationssicherheit von Städten muss auf breiter Basis verbessert werden. Einzelne Fachbereiche der Stadtverwaltung haben verschiedene Anforderungen. Für die IT ist nicht dasselbe entscheidend, wie für die Kommunikationsabteilung. Die Katastrophenschützer blicken anders auf das Thema als die Kolleginnen und Kollegen aus dem Schulamt. Deshalb wurde in mehreren Fokusgruppen diskutiert: Was braucht Ihr? Was würde helfen? Die Antworten hatten einen gemeinsamen Kern. Ein einheitlicher Rahmen ist notwendig. Klare gesetzliche Vorgaben, verbindliche Standards und zentrale Lösungen helfen. Nicht jeder muss immer wieder das Rad neu erfinden. Und es braucht Kooperation. Natürlich die interkommunale Zusammenarbeit, aber auch die Kooperation der Länder. Alle profitieren, wenn gute Ansätze und Lösungen allen zur Verfügung gestellt werden. Deshalb ist das vorliegende Memo auch ein Appell an den politischen Willen zur Zusammenarbeit.

Unser Dank gilt den Mitwirkenden aus den Städten für Ihr Engagement in diesem Projekt, der Stiftung Neue Verantwortung für die gute Zusammenarbeit und dem Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen für die Förderung.

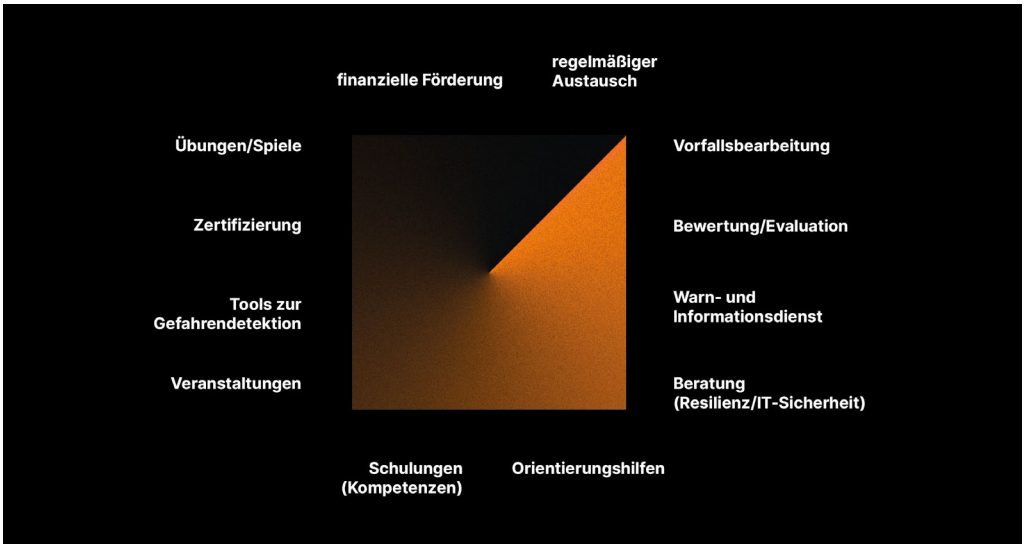
Ich wünsche Ihnen viel Freude beim Lesen!

Helmut Dedy,
Hauptgeschäftsführer des Deutschen Städtetages

Bedarfe bei der Förderung von Informationssicherheit und Resilienz in Städten berücksichtigen

Städte sind dafür verantwortlich, Maßnahmen für ihre Informationssicherheit und Resilienz umzusetzen. Dadurch können sie IT-Sicherheitsvorfälle soweit wie möglich vorbeugen, Gefahren schneller erkennen und den Schaden im Ernstfall zügig minimieren. Aufgaben der Informationssicherheit und Resilienz verteilen sich in Städten auf verschiedene Arbeitsgebiete. Dazu zählen neben den Verwaltungsspitzen etwa Kommunikations- und Presseabteilungen, das Katastrophen- und Krisenmanagement, der Bereich Informationssicherheit und IT-Management, der Querschnittsbereich Digitalisierung, sowie alle Fachbereiche.

Der Cybersicherheitskompass[1] für Kommunen zeigt das aktuelle Leistungsportfolio von Bund und Ländern zur Förderung der Informationssicherheit und Resilienz von Kommunen. **Die folgende Bedarfsanalyse diskutiert, ob die existierenden Leistungen von Bund und Ländern in der Praxis die Bedarfe von Mitarbeiter:innen in Städten tatsächlich adressieren. Sie stellt im zweiten Teil die konkreten Verbesserungsvorschläge vor, die direkt von Mitarbeiter:innen in Städten kommen. In der Untersuchung stand die Erhebung konkreter Bedarfe[2] der Mitarbeiter:innen in den Fokus.**



Unterschiedliche Leistungskategorien für Kommunen von Bund und Ländern (Screenshot von der Website "Cybersicherheitskompass", eine Orientierungshilfe für Mitarbeiter:innen von Kommunen", cybersicherheitskompass.de)

1 Der Cybersicherheitskompass wurde von Stiftung Neue Verantwortung e.V. (SNV) und Deutscher Städtetag im Rahmen dieser Projektförderung im Auftrag von KTS, finanziert von BMWSB, entwickelt. Erhebung und Kategorisierung der Daten wurde finanziert von der Konrad-Adenauer-Stiftung in einem Projekt mit der SNV.

2 Der Bedarf ist das Verlangen nach einer bestimmten Dienstleistung, Produkt oder Maßnahme (z.B. politische, technische, organisatorische), die zur Ausgleichung des Mangels beiträgt.

Die Bedarfe der Mitarbeiter:innen in Städten sind sehr unterschiedlich. Mitarbeiter:innen der verschiedenen Arbeitsgebiete ist die Dringlichkeit und Notwendigkeit der Umsetzung verschiedener Maßnahmen bewusst[3]. Allerdings variiert die Priorisierung der Aufgaben. Sie setzen also Maßnahmen in unterschiedlichen Reihenfolgen um. Beispielsweise hat ein:e Mitarbeiter:in in einer Stadt schon eine Cyber-Krisen-Übung durchlaufen, bei der auch die Kommunikationsabteilung einbezogen wurde, während in einer anderen Stadt noch mögliche Szenarien und Zuständigkeiten geklärt werden müssen. Genauso gibt es den:die Informationssicherheitsbeauftragte:n der:die sich gerade mit der Umsetzung eines Informationssicherheitsmanagementsystems beschäftigt, während andere gerade prüfen, welche SIEM-Systeme sie einsetzen können. **Welche Unterstützung gerade benötigt wird, ist direkt davon abhängig, welche Aufgabe konkret bearbeitet wird.** Dies zeigt, dass sich Städte in unterschiedlichen Stadien der Umsetzung von Informationssicherheit befinden. Aus diesem Grund können auch die Informationssicherheit und die Fähigkeiten, sich resilient aufzustellen, variieren. Unterstützungsangebote sollten sich an den unterschiedlichen Praxisbedarfen orientieren, um bestmöglich zu wirken. Bedarfe werden von verschiedenen Faktoren beeinflusst, darunter die Größe der Stadt, die Anzahl der kritischen Infrastrukturen, welche Verwaltungsaufgaben die Stadt übernimmt, Mitarbeiter:innenzahl, Anzahl der Ämter, Grad der Digitalisierung und die IT-Organisation. Die Vielzahl der Faktoren in ihrer unterschiedlichen Ausprägung macht es zu einer Herausforderung, passende Leistungen bereitzustellen. Deswegen erscheint es umso sinnvoller, Leistungen und Maßnahmen gemeinsam und eng mit der Zielgruppe zu evaluieren und zu entwickeln. Einige der schon angebotenen Leistungen, wurden von Mitarbeiter:innen in Städten als besonders nützlich empfunden und gehighlighted. Etwa bieten Bund und Länder momentan Leistungen an, die man als “Hilfe zur Selbsthilfe” bezeichnen kann. Diese sollen Mitarbeiter:innen unterstützen, Kompetenzen aufzubauen oder weiterzuentwickeln. Der Bedarf an Orientierungshilfen und Schulungen zum Aufbau von Kompetenzen und Übungen zum Testen der Kompetenzen ist aber noch nicht gedeckt.

Einige der schon verfügbaren Leistungen, die von Mitarbeiter:innen in Städten als besonders nützlich bewertet wurden:

- Die Orientierungshilfen des Bundesamt für Sicherheit in der Informationstechnik zum Thema Krisenkommunikation und das Projekt „Weg in die Basisabsicherung“ und das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, welche gemeinsam mit den Kommunalen Spitzenverbänden entwickelt wurden
- Unterstützung der Kommunen durch das Landesamt für Sicherheit in der Informationstechnik Bayern, speziell bei der Vorfallsbearbeitung und die aktuelle Schulungs- und Awarenessplattform, die mit einem Rahmenvertrag den Kommunen in Bayern bereitgestellt werden
- Cybersicherheitsberatung einiger Länder (namentlich erwähnt wurden Baden-Württemberg, Bayern, Hessen und Sachsen)
- Die Warn- und Informationsdienste des LSI Bayern und die des Bundesamt für Sicherheit in der Informationstechnik

3 Für eine Übersicht der besprochenen Aufgaben in den verschiedenen Arbeitsgebieten siehe Seite 9

Mitarbeiter:innen wünschen sich Leistungen, die auf sie zugeschnitten sind und das Thema Informationssicherheit und Resilienz in ihrem Arbeitsgebiet adressieren. Beispielsweise benennen Kommunikationsabteilungen den Bedarf nach einem Glossar, welches Begrifflichkeiten aus der Informationssicherheit verständlich aufbereitet oder sehen etwa Zuständige aus dem Krisenmanagement den Bedarf an einem Template, welches abhängig von der jeweiligen Krisensituation die Zuständigkeiten klar abbildet. Da Informationssicherheit bisher häufig nicht formell zum Aufgabenbereich aller Arbeitsgebiete von Mitarbeiter:innen zählt und dementsprechend kaum Zeit zur Verfügung steht, sind Leistungen besonders nützlich, wenn sie auf das Aufgabengebiet der Mitarbeiter:innen und zielgruppenspezifisch zugeschnitten sind (etwa Länge, Material usw.). Wie auch in anderen Bereichen, ist der interkommunale, regelmäßige Austausch wichtig. Bund und Länder stellen zudem bereits Möglichkeiten des regelmäßigen Austauschs bereit. Die Bedarfsanalyse zeigt, dass Städte, die ähnliche Fragen haben und an vergleichbaren Aufgaben arbeiten, dennoch einen Bedarf haben, sich deutschlandweit zu vernetzen. Mitarbeiter:innen könnten erheblich von einem länder- oder sogar sektorübergreifenden Austausch profitieren, da sie andernfalls isoliert versuchen, komplexe Probleme zu bewältigen. Individuen, die mit ähnlichen Herausforderungen, Aufgaben und Fragen konfrontiert sind, sollten Gelegenheit haben, sich zu vernetzen und zu koordinieren. Diese Möglichkeit wird momentan noch nicht ausreichend und zielgruppengerecht angeboten und könnte demnach ausgebaut werden.

In Fällen spezifischer Aufgaben, bei denen es nicht praktikabel ist, Expert:innen intern aufzubauen oder anzustellen, werden externe Fachleute aus Wirtschaft, Wissenschaft, Zivilgesellschaft sowie von Landes- oder Bundesbehörden auch weiterhin eine bedeutende Rolle spielen. Der Zugang zu externen Expert:innen wird in einigen Bundesländern schon gefördert. Beispielsweise stellen manche Länder Fördermittel bereit, die es Städten ermöglichen, Leistungen wie Pen-Tests abzurufen. Einige Länder bieten sogar selbst solche Leistungen an, indem sie beratend vor Ort sind oder sogar operativ unterstützen. Städte, in denen Länder diese Funktionen bisher nicht anbieten oder übernehmen, müssen sich selbst auf dem Markt orientieren. Insbesondere bei der Bewertung des Standes der IT-Sicherheit und der Vorfallsbearbeitung ist die Nachfrage nach Leistungen und externer Unterstützung besonders hoch und somit ausbaufähig. Um die Förderung von Informationssicherheit und Resilienz effektiver zu gestalten, sollten sich Entscheidungsträger:innen in Bund und Ländern an den im nächsten Abschnitt tabellarisch aufgeführten konkreten Bedarfen orientieren und diese bei der Weiterentwicklung von unterstützenden Leistungen berücksichtigen.

Es wurden allerdings auch Bedarfe identifiziert, die nur durch technische, organisatorische und politische Maßnahmen, die das Miteinander zwischen Städten, Ländern und Bund verändern, adressiert werden können. Beispielsweise fragen Mitarbeiter:innen von Städten nach zentralen Vorgaben. Der aktuelle Zustand, in dem Städte größtenteils von verpflichtenden Maßnahmen ausgenommen sind, führt dazu,

dass Mitarbeiter:innen nicht nur eigenständig Maßnahmen ableiten und priorisieren, sondern auch für die benötigten personellen Ressourcen und finanziellen Mittel Lobbyarbeit betreiben müssen. Diese Aufgabe fällt meist den Mitarbeiter:innen zu, die eigentlich für die Umsetzung der Maßnahmen verantwortlich sind. Somit kommt es vor, dass viel Zeit mit politischer Überzeugungsarbeit verbracht wird, anstatt zu veranlassen, gefährlich veraltete IT-Systeme zu aktualisieren. Gerade Mitarbeiter:innen, die Faktoren wie das Budget oder das stadtinterne Personal nicht (ausreichend) beeinflussen können, profitieren von klaren Leitlinien und Vorgaben oder Bürgermeister:innen, die Informationssicherheit unterstützen und verstehen.

Übergreifende Trends, die Fortschritte bei der Informationssicherheit von Städten erschweren, tun ihr Übriges. Dazu zählt vor allem der Fachkräftemangel im Informationssicherheitsbereich. Da Städte auf diese Faktoren kurz- bis mittelfristig alleine keinen Einfluss haben, ist auch die Bundes- und Länderebene sowie interkommunale Zusammenarbeit gefragt. Hier wird der Wunsch nach intensiverer Zusammenarbeit deutlich, bei der eine Neuverteilung von Zuständigkeiten erfolgen könnte. Solche Vorschläge zur Neuorganisation gehen weit über unterstützende Leistungen von Bund und Ländern hinaus und müssen politisch mitgetragen werden, da sie ggf. gesetzliche Änderungen erfordern. Beispielsweise gibt es Vorschläge, die sich eher darauf konzentrieren, bestimmte Informationssicherheitsaufgaben zu verlagern, um den Prozess effizienter zu gestalten und bestimmte Standards zu erreichen. Ein Beispiel dafür ist die zentrale Organisation der IT-Sicherheitsprüfung von Soft- und Hardware. Diese Umsetzung würde bedeuten, dass nicht jede Stadt bei Ausschreibungen alleine prüfen muss oder die selben Anbieter immer wieder überprüft werden. Andere Vorschläge beziehen sich insbesondere auf das Betreiben der IT-Infrastruktur selbst, da die Art der Organisation der IT und deren Steuerung direkte Auswirkungen auf die Resilienz und Informationssicherheit von Städten haben kann. Vorschläge, wie die Organisation gemeinsamer, zentraler IT-Sicherheitslösungen oder gemeinsamer IT-Infrastruktur, verteilen die Steuerung und die Umsetzung von Informationssicherheit zwischen Bund, Ländern und Städten neu.

Darüber hinaus gab es Bedarfe, die eher Stadt-intern adressiert werden müssten. Insbesondere Informationssicherheitsbeauftragte sind sowohl für die Umsetzung von Maßnahmen als auch für deren Steuerung verantwortlich. Um die Steuerung übernehmen zu können, brauchen sie aber oft die Unterstützung von der Verwaltungsspitze, welche in vielen Verwaltungsorganisationen über die Ressourcen (personell und finanziell) entscheidet. Die Benennung eines Informationssicherheitsbeauftragten kann demnach nur der erste Schritt sein. Um die Organisation der Informationssicherheit zu strukturieren, braucht es die Unterstützung der Verwaltungsspitze und eine klare Strategie, wie verschiedene Mitarbeiter:innen aus den unterschiedlichen Arbeitsgebieten zur Informationssicherheit beitragen. Es ist erforderlich, zusätzliche Mitarbeiter:innen einzubeziehen, nicht nur direkt

im Bereich Informationssicherheit, sondern auch außerhalb davon, um Verantwortung für die Resilienz der Stadt zu übernehmen. Während Mitarbeiter:innen des Arbeitsgebiets Katastrophen- und Krisenmanagement häufig bereits Aufgaben zur Informationssicherheit und Resilienz als Teil ihres Aufgabenbereichs wahrnehmen, setzen sie weitgehend auch unabhängig von Informationssicherheitsbeauftragten Maßnahmen um und bauen Kompetenzen auf. Jedoch fehlen ihnen auch oft personelle und finanzielle Ressourcen. In anderen Bereichen fehlt es an den passenden Koordinations- und Austauschmechanismen. Austausch zum Thema Business Continuity Management (BCM) und Informationssicherheit muss stadt-intern gefördert und ermöglicht werden. Mitarbeiter:innen aus den Fachbereichen sowie dem Querschnittsbereich Digitalisierung muss es ermöglicht werden, ihren Beitrag zu leisten. Mitarbeiter:innen aus Kommunikations- oder Presse-Abteilungen wünschen sich dafür mehr direkten Austausch mit den IT-Abteilungen, um schnell und angemessen reagieren zu können. Ein Vorschlag wäre, gezielte Teil-Kompetenzen für das Thema in diesen Arbeitsgebieten aufzubauen. Hierfür wäre es sinnvoll, Vorlagen zu entwickeln, die erläutern, welche Kompetenzen in jedem Arbeitsgebiet entwickelt werden müssen und wie viel Zeit Informationssicherheits-Aufgaben in den verschiedenen Arbeitsgebieten in Anspruch nehmen würden. Außerdem könnten Städte selbst Formate der internen Zusammenarbeit teilen, die gut funktioniert haben.

Alles in allem zeigt die Bedarfsanalyse, dass Mitarbeiter:innen in Städten eine hohe Anzahl an Bedarfen haben, die adressiert werden sollten, um die Informationssicherheit und Resilienz von Städten zu verbessern. Die konkreten Forderungen der Mitarbeiter:innen sind im folgenden Abschnitt tabellarisch aufbereitet. Entscheidungsträger:innen in Städten, Ländern und Bund sollten diese in politischen Aushandlungsprozesse berücksichtigen.

Stiftung Neue Verantwortung

Arbeitsgebiete und ihre Aufgaben für Informationssicherheit und Resilienz in Städten

Mitarbeiter:innen der 34 Städte wurden in fünf Fokusgruppen aufgeteilt, die jeweils ein Arbeitsgebiet repräsentieren.

Die Ergebnisse zeigen die Aufgaben[4] in der Reihenfolge, in der Mitarbeiter:innen Dringlichkeit sehen, sie zu bearbeiten.

4 vor der Bewertung, hat die Autorin konkrete Aufgaben von den bestehenden Standards des Bundesamtes für Sicherheit in der Informationstechnik und Leitlinien abgeleitet und Mitarbeiter:innen zudem befragt, welche Aufgaben sie gerade besonders beschäftigen.

Zu den fünf Arbeitsgebieten zählen:

- **Kommunikation und Presse** (Mitarbeiter:innen aus Bereichen Presse, Kommunikation, Bürgerbeteiligung oder Öffentlichkeitsarbeit)
- **Verschiedene Fachbereiche** (Mitarbeiter:innen aus Ämtern mit Fokus Migration, Soziales, oder Verkehr
- **Krisen- und Katastrophenmanagement** (Mitarbeiter:innen aus Krisenstäben, Feuerwehr, Zivil- und Katastrophenschutz)
- **IT-Management und Informationssicherheit** (Informationssicherheitsbeauftragte, IT-Leiter:innen)
- **Digitalisierung** (Digitalisierungs-Beauftragte, CDOs)

Kommunikation und Presse

1. Vor einem Vorfall: Kommunikation bei Vorfällen vorbereiten (inkl. Template Pressemitteilung, Kontaktliste, Kernbotschaften, Kommunikationswege etc.)
2. Während eines Vorfalls: Mit verschiedenen Zielgruppen wie Bürger:innen oder Presse-Vertreter:innen richtig kommunizieren (inkl. Kommunikationsorte, Notfallkontakt, Kernbotschaften)
3. Vor einem Vorfall: Interne Kommunikation über Maßnahmen oder Cybersicherheitsbedrohungen (in Zusammenarbeit mit Informationssicherheitsbeauftragten)
4. Vor einem Vorfall: Kommunikation zum Thema Cybersicherheit und Resilienz bei Digitalisierungsprojekten
5. Nach einem Vorfall: Erkenntnisse in einer Publikation, einem Blog, einem Vortrag oder einem Seminar mit anderen teilen

Informationssicherheit/ IT-Management | Fokusgruppe 1

1. Implementierung BCM/ISMS: Steuerung/Aufgabenverteilung interner und externer Stakeholder (Dienstleister, Bund, Landesbehörden, Fachabteilungen etc.)
2. SIEM Systeme einführen und organisieren
3. Awareness bei Mitarbeiter:innen schaffen
4. Bedrohungen und Schwachstellen bewerten und anschließend Maßnahmen ableiten
5. Erarbeitung von Notfallszenarien, die in Maßnahmen münden (z. B. Backups), aber auch Verfügbarkeitsanforderungen von Daten & Prozesse validieren
6. Regelmäßige Prüfung und Aktualisierung von Schutzbedarfs- und Risikoanalysen, Überprüfung der Anforderungen, Aktualisierung der Notfallmaßnahmen
7. Anhand der dokumentierten Anforderungen Schutzbedarfe von Daten ermitteln, Sicherheitsmaßnahmen identifizieren und umsetzen.
8. Vorfallbearbeitung inkl. Management, Forensik, Wiederanlauf
9. Beschaffungen inkl. Erstellung von Ausschreibungsunterlagen (Beurteilung Handlungsfähigkeit im Krisenfall, Abhängigkeiten), Prüfung IT-Sicherheit
10. Digitalisierung: Anwendungsfälle und deren sicherheitsbezogene Anforderungen (z. B. organisatorisch, technisch, finanziell, regulatorisch diskutieren und dokumentieren
11. BCM: Prüfung vorhandener Managementsysteme oder Sicherheitsprozesse die Aspekte des BCM enthalten

Stiftung Neue Verantwortung

Informationssicherheit/ IT-Management | Fokusgruppe 2

1. Awareness bei Mitarbeiter:innen schaffen
2. Implementierung BCM/ISMS: Steuerung/Aufgabenverteilung interner und externer Stakeholder z.B. Dienstleister, Bund, Landesbehörden, Fachabteilung etc.
3. Vorfallbearbeitung inkl. Management, Forensik, Wiederanlauf
4. Bewertung von Bedrohungen und Schwachstellen sowie Durchführung von Maßnahmen, Erarbeitung von Notfallszenarien, die in Maßnahmen (z.B. Backups) münden, aber auch Verfügbarkeitsanforderungen von Daten & Prozesse validieren
5. Regelmäßige Prüfungen und Aktualisierungen von Schutzbedarfs- und Risikoanalysen, Überprüfung der Anforderungen, Aktualisierung der Notfallmaßnahmen
6. Digitalisierung: Anwendungsfälle und deren sicherheitsbezogene Anforderungen (z. B. organisatorisch, technisch, finanziell, regulatorisch diskutieren und dokumentieren
7. Beschaffungen inkl. Erstellung von Ausschreibungsunterlagen (Beurteilung Handlungsfähigkeit im Krisenfall, Abhängigkeiten), Prüfung IT-Sicherheit
8. SIEM Systeme einführen, organisieren
9. Anhand der dokumentierten Anforderungen Schutzbedarfe der Daten und Informationen ermitteln, Sicherheitsmaßnahmen identifizieren und umsetzen
10. BCM: Prüfung vorhandener Managementsysteme oder Sicherheitsprozesse, die Aspekte des BCM enthalten

Digitalisierung

1. Entwicklung einer Digitalisierungsstrategie, die Cybersicherheit und Resilienz beinhaltet
2. Zusammenarbeit und Steuerung von internen und externen Stakeholdern bei Digitalisierungsprojekten
3. Regelmäßige Prüfung von z.B. von Schutzbedarfs- und Risikoanalyse, Überprüfung der Anforderungen, Aktualisierung der Notfallmaßnahmen
4. Alle Stakeholder (intern/extern) und ihre Rollen klar benennen und Verantwortlichkeiten identifizieren
5. Erarbeitung von Notfallszenarien, die in Maßnahmen (z. B. Backups) münden sollten, aber auch Verfügbarkeitsanforderungen von Daten und Prozessen validieren
6. Anwendungsfälle und deren sicherheitsbezogene Anforderungen (z. B. organisatorisch, technisch, finanziell, regulatorisch diskutieren und dokumentieren
7. Anhand der dokumentierten Anforderungen Schutzbedarfe der Daten und Informationen ermitteln, um Sicherheitsmaßnahmen zu identifizieren und umzusetzen
8. Planung von Beschaffungen inkl. Erstellung von Ausschreibungsunterlagen (Beurteilung Handlungsfähigkeit im Krisenfall, Abhängigkeiten, Anforderungen)

Krisen- und Katastrophenmanagement

1. Prozesse und Zuständigkeiten bestimmen – z.B. Rolle Krisenstab bei IT-Krisen Unterschiede der Prozesse und Ansprechpersonen bei einer IT-Krise versus anderer Krisen oder Notfall versus einer IT-Krise
2. Entwicklung eines Krisenkommunikationskonzepts
3. Schutz der eigenen IT (Feuerwehr, Rettungsstellen usw.)
4. Basis-Q&A, Kontaktlisten, Antizipieren der wichtigsten Fragen
5. Entwicklung eines Wiederanlaufplans
6. Entwicklung von Szenarien für eine IT-Krise: Welche Angriffe könnten auftreten? Welche Systeme könnten betroffen sein?
7. Testen der möglichen Szenarien, um Prozesse, Zuständigkeiten und Equipment zu prüfen (z.B. durch Übungen)

Fachbereiche

1. Maßnahmen zur IT-Sicherheit identifizieren und mit den zentralen Stellen koordinieren
2. Unterstützung bei der Entwicklung von Notfallplänen (Kontaktpersonen, Fall-Back Optionen)
3. Unterstützung bei der Entwicklung von Wiederanlaufplänen bei einer IT-Krise z.B. Auswirkungen auf Fachbereiche einschätzen
4. Unterstützung bei der Identifizierung wichtiger Daten und Prozesse (z.B. Definition der Verfügbarkeitsanforderungen)
5. Sensibilisierung für das Thema Informationssicherheit und Bedrohungen speziell für Fachbereichsleiter:innen
6. Zusammenarbeit mit relevanten internen und externen Akteuren organisieren

Stiftung Neue Verantwortung

Vorschläge für weitere unterstützende Leistungen, die Bedarfe adressieren

Bund und Länder stellen verschiedene Leistungen bereit, die Mitarbeiter:innen von Städten unterstützen können.[5] In den Fokusgruppen wurden Mitarbeiter:innen aus den verschiedenen Arbeitsgebieten befragt, welche dieser Leistungen ihnen bei der Umsetzung der von ihnen priorisierten Aufgaben noch Unterstützung bieten würden.

5 Alle öffentlich nachvollziehbaren Leistungen finden sich auf dem Cybersicherheitskompass für Kommunen, cybersicherheitskompass.de

01 Kommunikation und Presse

Leistungskategorien	Vorgeschlagene Leistungen zur Unterstützung
Vorfallsbearbeitung	• Notfall-Kommunikationsmittel (Satelliten-Telefone) • Ein Krisen-Backbone für die Kommunikation • Dezentrale (autarke) Kommunikations-Standorte • Mehrsprachig verfasste Informationen bzw. Echtzeit-Übersetzung mit KI • Krisenfeste Kommunikationsleitungen auch in Zusammenarbeit mit Länderbehörden
Orientierungshilfen	• Glossar von Fachbegriffen vs Kommunikation für Öffentlichkeit
Übungen/Spiele	• Übungen wichtiger (gravierender) Szenarien • Regionale Übungen, die über den Stadtkreis hinausgehen, sind sehr wertvoll, weil der Informationsfluss und die Verantwortlichkeiten anders liegen

02 Informationssicherheit/IT-Management

Leistungskategorien	Vorgeschlagene Leistungen zur Unterstützung
Bewertung/Evaluation	• Förderung oder Bereitstellung von Penetrationstests inkl. Berichterstattung an die Leitungsebene
Warn- und Informationsdienst	• Informationen zu Schwachstellen und Bedrohungen, aktuelle Taktiken und Techniken, aktuelle Angriffsmuster, IoC mit relevantem Kontext zur Bewertung. • Informationen zu allgemeinen Gefahren, die auf die Organisation gemünzt sind
Beratung (IT-Sicherheit und Resilienz)	• ISMS-Beratung (auch extern inkl. Interviews bei Fachbereichen/Dienststellen) • Beratung Umsetzung BCM auch inkl. Beteiligung aller Arbeitsgebiete
Orientierungshilfen	• Informationen zu Gesetzgebungen und zukünftigen Maßnahmen teilen • Grundschutzprofile für Kommunen/Es braucht weitere IT-Grundschutz-Profile speziell für Kommunen • Unterstützung bei der Bemessung von Personal für die Umsetzung von Informationssicherheit - etwa Tool zur Einschätzung (siehe ähnliche Forderung von Fachbereichen)
Schulungen (Kompetenzen)	• Angebot Awareness Schulungsmaßnahme, etwa Nutzung von Schulungssoftware und Trainings via Rahmenverträge
regelmäßiger Austausch	• Austausch mit Personen, die dieselben Aufgaben und Fragen bearbeiten • Best Practices, Stand vergleichbarer Kommunen zum interkommunalen Austausch
finanzielle Förderung	• Personelle/Monetäre Unterstützung • Finanzielle Mittel zur Sicherstellung erforderlich • Finanzen für die Umsetzung von Maßnahmen

Stiftung Neue Verantwortung

03 Digitalisierung

Leistungskategorien	Vorgeschlagene Leistungen zur Unterstützung
Vorfallsbearbeitung	• Unterstützung im Notfall / Bei Sicherheitsvorfall
Bewertung/Evaluation	• Überprüfung IT-Sicherheit von Digitalisierungsprojekten, oder Soft- und Hardware
Orientierungshilfen	• Musterverträge, -strategien, -anforderungslisten, die viele Verwaltungen betreffen
Schulungen (Kompetenzen)	• Schaffung einer Sicherheitskultur: Es sollte eine Kultur der Sensibilisierung und des Bewusstseins für IT-Sicherheit in der gesamten Organisation gefördert werden - gemeinsame Verantwortung • Schulungen zur Sensibilisierung von allen Organisationseinheiten
regelmäßiger Austausch	• Best Practices & ehrlichen Erfahrungsaustausch in geschütztem Rahmen ermöglichen • Fachaustausch, um mit anderen zu netzwerken und Erfahrungen sowie Herangehensweisen auszutauschen

04 Krisen- und Katastrophenmanagement

Leistungskategorien	Vorgeschlagene Leistungen zur Unterstützung
Bewertung/Evaluation	• Finanzierung oder Durchführung von Risikoanalysen
Warn- und Informationsdienst	• Ausbau der Informationsplattform des Bundesamt für Sicherheit in der Informationstechnik
Beratung (Resilienz/ IT-Sicherheit)	• Beratung zu verschiedenen Themen von Landesbehörden, aber auch Möglichkeit der Nutzung von externer Beratung
Orientierungshilfen	• Aufbereitung der Unterscheidung von Prozessen und Umgang in der Katastrophe, Notfall, Krise sowie Prozesse in unterschiedlichen Krisenszenarien • Bereitstellung eines Templates für einen Masterablaufplan, welche Dienststelle muss wann miteinbezogen werden
Schulungen (Kompetenzen)	• Welche Kompetenzen braucht es bei einer IT-Sicherheitskrise?
Übungen/Spiele	• Übungen der Reaktionen im Krisenstab
regelmäßiger Austausch	• kommunale Expert:innen-Netzwerke schaffen
finanzielle Förderung	• Finanzielle Förderung, um sich auf Krisen vorzubereiten, zum Beispiel Finanzierung des Ausbaus einer IT-Krisen-Infrastruktur

05 Fachbereiche

Leistungskategorien	Vorgeschlagene Leistungen zur Unterstützung
Orientierungshilfen	• Templates für Stellenprofile mit klaren Aufgaben und Kompetenzen, einheitlicher und vergleichbarer Qualifizierungen auf kommunaler Ebene

Stiftung Neue Verantwortung

Vorschläge für technische, organisatorische und politische Maßnahmen, die Bedarfe adressieren

Neben konkreten Vorschlägen für weitere Leistungen wurden in den Fokusgruppen technische, organisatorische und regulatorische Maßnahmen benannt, die die Umsetzung von Informationssicherheit und Resilienz fördern könnten. Des Weiteren wurde von der Autorin eine erste Einschätzung gegeben, wer in der Cybersicherheitsarchitektur so eine Maßnahme umsetzen könnte.

Diese Maßnahmen würden vor allem die unterschiedlichen Faktoren, die trotz Bewusstsein für Aufgaben ein Stagnieren der Umsetzung verursachen, ansprechen. Zum Beispiel könnten fehlende Zeit durch effizientere Umsetzung der Maßnahme oder ein Mangel an Fachkräften durch zentralere Umsetzung der Maßnahme adressiert werden.

01 Kommunikation und Presse

Umsetzbar von	Art der Maßnahme	Vorgeschlagene Maßnahmen
Städten	Organisatorisch	• Hausintern: Klärung unterschiedlicher Szenarien und welche Ressourcen/Kommunikationsmöglichkeiten dann jeweils zur Verfügung stünden bzw. stehen müssten • Vorherige Abstimmung und Koordinierung mit den Partnern in den Kommunen • Appell: Nutzen Sie auch die Kommunikations-Expertise. Bei IT-Sicherheitsvorfällen die Kommunikationsabteilung frühzeitig einbinden.
Bund	Technisch, organisatorisch	• Einbindung der Kommunen in die Bundes-Cloud, Behörden-Cloud

02 Informationssicherheit/IT-Management

Umsetzbar von	Art der Maßnahme	Vorgeschlagene Maßnahmen
Städten	Organisatorisch, politisch	• Das Thema muss von der Stadtspitze und der Verwaltungsleitung unterstützt und vermittelt werden. Informationssicherheit und BCM benötigen dieses Engagement.
Bund	Technisch, politisch	• Einbindung/Zutritt der Kommunen in die Behörden Cloud des Bundes (ggf. Nutzung von Office DSG konform). • Abschluss EU-USA-Vereinbarung zur datenschutzrechtlichen Thematik bei Cloud, Outsourcing oder Beschleunigung Gaia-X.
Bund und/ oder Ländern	politisch	• Gesetzliche Pflichten und Rechte zur Informationssicherheit für Kommunen • Gesetzliche Pflichten (Klare Regelungen und Anforderungen) an die Kommunen und deren Gesellschaften. • Verbindliche Standards, an denen man sich orientieren kann
Ländern		• klare Regelung für alle Schulen • Sicherstellung Personal und Finanzen

03 Digitalisierung

Umsetzbar von	Art der Maßnahme	Vorgeschlagene Maßnahmen
von allen Stakeholdern zu koordinieren	Politisch	• Ressourcenbereitstellung: Es ist wichtig, angemessene Ressourcen in Form von Budgets, Personal und Technologie für die Umsetzung von IT-Sicherheitsmaßnahmen bereitzustellen. Digitalisierungsförderung sollte Informationssicherheitsmaßnahmen berücksichtigen.
Städten	Organisatorisch	• Trennung des Betriebs (Administration) und der IT-Sicherheitskonzeption innerhalb der Stadt
	Technisch	• Mobiles Arbeiten mit städtischen Geräten organisieren • Empfehlenswert wäre es, wenn Kommunen gemeinsam an Software arbeiten → Entwicklungsgemeinschaften
Bund und/ oder Ländern	Technisch, organisatorisch, politisch	• Mehr verbindliche Standards (von Land/Bund veranlasst) wären hilfreich • IT-SEC für Webapplikationen (Smart City bringt diese zu großen Teilen hervor) ist aktuell noch nicht ausgereift
	Technisch, politisch	• Beschaffung zentral organisieren • Überprüfung der IT-Sicherheit von Digitalisierungsprojekten sowie Hard- und Software zentral oder regional organisieren • Organisation von Entwicklungsgemeinschaften • Vorgaben von Bund und Land, um Einheitlichkeit zu schaffen • Zurverfügungstellung von Demilitarisierter Zone • Vorgaben besser kommunizieren bzw. darauf achten, dass Umsetzungsempfehlungen der übergeordneten Behörden sich nicht widersprechen • Mindeststandards, die für Verwaltungen verbindlich sind per Gesetz, um das Thema auch auf Leitungsebene deutlich zu machen • Festplattenverschlüsselung bereitstellen und sog. "Schleusen-PCs" einrichten

04 Krisen-Katastrophenmanagement

Umsetzbar von	Art der Maßnahme	Vorgeschlagene Maßnahmen
Städten	Organisatorisch	• Definition der eigenen Zuständigkeiten, Entwicklung eines Ablaufplans (welche Dienststelle muss wann mit einbezogen werden) inkl. der Stadtspitzen
Bund	Politisch	• Mehr Kompetenz des Bundes für Länder, aber auch für Kommunen erwägen
Ländern	Technisch, organisatorisch, politisch	• Ausbau des EfA-Prinzip - gemeinsame Entwicklung und Nutzung von Software

05 Fachbereiche

Umsetzbar von	Art der Maßnahme	Vorgeschlagene Maßnahmen
Städten	Organisatorisch	• Stabsstelle IT-Sicherheit bei der Fachbereichsleitung • Zusammenarbeit von den Beauftragten, Identifizieren wichtiger Prozesse • Abbildungen der Aufgaben in den Fachbereichen (mit mind. 5 %) - damit die Zeit auch eingepreist ist, die es braucht, um sich mit Informationssicherheit und Resilienz zu beschäftigen.

Danksagungen

Diese Analyse wurde von Mitgliedern betroffener Fachausschüsse und Arbeitsgruppen im Deutschen Städtetag durch Online-Zusammenarbeit und Fokusgruppen unterstützt. Die in diesem Dokument geäußerten Ansichten und Meinungen sind die der Autorin und spiegeln nicht unbedingt die Position der Mitglieder der Arbeitsgruppe oder die ihres jeweiligen Arbeitgebers wider.

Die Autorin dankt folgenden Personen für die Teilnahme an den Fokusgruppen, entscheidende Denkanstöße und den offenen Austausch:

- Mate Čović, IT-Systemadministrator, *Stadt Frankfurt am Main*
- Dr Stephanie Dinkelaker, Referentin für Digitale Transformation, *Frankfurt am Main*
- Andreas Franke, Amt für Kommunikation und Stadtmarketing, *Nürnberg*
- Adrian Foitzik, Kommunikation, *Braunschweig*
- Tilo Gläser, Abteilungsleiter IT-Infrastruktur, *Stadt Chemnitz*
- Martin Götzke, Leiter Stabsstelle Zivil- und Katastrophenschutz, *Oberhausen*
- Sabine Griebsch, Senior Advisor Cyber Resilience, *GovThings*
- Holger König, Informationssicherheit/Digitalisierung, *Mühlhausen*
- Volker Kühn, Abteilung Einsatz, Organisation und Bevölkerungsschutz, *Nürnberg*
- Jens Lange, Informationssicherheitsbeauftragter, *Kassel*
- Marco Majert vom Regionalverband *Ruhr*
- Tobias Scherbaum, IT-Sicherheit, *Oberhausen*
- Sabine Meigel, Abteilung Digitale Agenda, *Stadt Ulm*
- Frank Menninger, Informationssicherheitsbeauftragter, Amt für Brand- und Katastrophenschutz Sachgebiet 2 Information und Kommunikation, *Kempten (Allgäu)*
- Marlene Müller, Öffentlichkeitsarbeit und Repräsentation, *Stadt Ulm*
- Andrea-Julia Reichl-Streich, Informationssicherheitsbeauftragte, *Ingolstadt*
- Joachim Roesner, Bereich Stadtentwicklung, *Ludwigshafen am Rhein*
- Dipl.-Ing. Adrian Röhrle, Feuerwehrkommandant, *Stadt Ulm*
- Uwe Schulz, Feuerwehr, Abteilung Zivil- und Katastrophenschutz, *Stadt Chemnitz*
- Thomas Sprenger, Referat für politische Gremien, Bürgerbeteiligung und Kommunikation, *Bochum*
- Matthias Zehender (Sachbearbeiter Katastrophenschutz) *Stadt Regensburg*
- Mitarbeiter:innen von *ITK Rheinland*

- (Weitere) Mitarbeiter:innen aus den Städten:
  - Bochum
  - Bonn
  - Celle
  - Chemnitz
  - Essen
  - Frankfurt am Main
  - Gelsenkirchen
  - Hannover
  - Heidelberg
  - Iserlohn
  - Kempten (Allgäu)
  - Lutherstadt Wittenberg
  - Lübeck
  - Magdeburg
  - Metropole Ruhr
  - Neubrandenburg
  - Neu-Ulm
  - Nürnberg
  - Oberhausen
  - Oldenburg
  - Regensburg
  - Wiesbaden
  - Solingen
  - Speyer
  - Witten

Ein besonderer Dank gilt Peter Adelskamp aus Essen, Heiko Hußmann, Benjamin Stein und Volker Schreinert aus Hannover, Jens Lange aus der Stadt Kassel, Sabine Meigel aus Ulm, Dr. Tom Reeg aus München und Andrea-Julia Reichl-Streich aus Ingolstadt, die sich Zeit nahmen, die Analyse eng zu begleiten und wichtige Impulse zur Methodik und/oder Aufbereitung gaben.

Die Autorin bedankt sich außerdem bei Frauke Janßen vom Deutschen Städtetag für die exzellente Zusammenarbeit, die diese interdisziplinäre Arbeit möglich gemacht hat.

Die Autorin bedankt sich bei Dr. Sven Herpig für wichtige, inhaltliche Impulse, Martha Reinicke für die Redigatur und Alina Siebert für das Design des Layouts.

Glossar

Begriffe	Beschreibung
Informations-sicherheit	"Informationssicherheit ist ein Zustand von technischen oder nicht-technischen Systemen zur Informationsverarbeitung, -speicherung und -lagerung, der die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen soll. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken. In der Praxis orientiert sich die Informationssicherheit im Rahmen des IT-Sicherheitsmanagements unter anderem an der internationalen ISO/IEC-27000-Reihe. Im deutschsprachigen Raum ist ein Vorgehen nach IT-Grundschutz verbreitet. Im Bereich der Evaluierung und Zertifizierung von IT-Produkten und -systemen findet die Norm ISO/IEC 15408 (Common Criteria) häufig Anwendung."[6]
Resilienz-Fähigkeiten	IT-Sicherheitsvorfälle zu antizipieren, im entscheidenden Moment die richtigen Schutzmechanismen anzuwenden, zentrale Prozesse und Infrastrukturen und damit Dienstleistungen aufrechtzuerhalten, aus Vorfällen zu lernen und Systeme entsprechend anzupassen.[7]
BCM	"Betriebskontinuitätsmanagement (BKM; englisch business continuity management (BCM)) bezeichnet in der Betriebswirtschaftslehre die Entwicklung von Strategien, Plänen und Handlungen, um Tätigkeiten oder Prozesse, deren Unterbrechung der Organisation ernsthafte Schäden oder vernichtende Verluste zufügen würden (etwa Betriebsstörungen), zu schützen bzw. alternative Abläufe zu ermöglichen.[1] Ziel ist somit die Sicherstellung des Fortbestands des Unternehmens im Sinne ökonomischer Nachhaltigkeit im Angesicht von Risiken mit hohem Schadensausmaß."[8]
IoC	"Ein Indicator of compromise (IoC) ist in der IT-Forensik ein Artefakt, das mit hoher Wahrscheinlichkeit auf einen unberechtigten Zugriff auf einen Computer hinweist."[9]
ISMS	"Ein Information Security Management System (ISMS, englisch für „Managementsystem für Informationssicherheit") ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.[10] Beispielsweise definiert der BSI -Standard 200-1 allgemeine Anforderungen an ein ISMS."

6 Seite „Informationssicherheit". In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 9. August 2023, 13:51 UTC. URL: https://de.wikipedia.org/w/index.php?title=Informationssicherheit&oldid=236259245 (Abgerufen: 23. August 2023, 12:19 UTC)

7 Herpig (2023), Mehr Resilienz für Deutschlands IT-Systeme, https://background.tagesspiegel.de/cybersecurity/mehr-resilienz-fuer-deutschlands-it-systeme (Zuletzt abgerufen 18.08.2023)
Abgeleitet aus BSI-Standard 200-4, the BCI, ENISA, NIST-SP 800-172, MITRE Working Group
Tiirmaa-Klaar & Skierka (2022), Germany's National Security Strategy: A Chance to Pivot to Adaptive Cyber Resilience https://fourninesecurity.de/2023/01/17/germanys-national-security-strategy-a-chance-to-pivot-to-adaptive-cyber-resilience (Zuletzt abgerufen 18.08.2023)

8 Seite „Betriebliches Kontinuitätsmanagement". In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 11. Mai 2023, 12:49 UTC. URL: https://de.wikipedia.org/w/index.php?title=Betriebliches_Kontinuit%C3%A4tsmanagement&oldid=233637018 (Abgerufen: 23. August 2023, 12:17 UTC)

9 Seite „Indicator of compromise". In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 5. August 2023, 18:39 UTC. URL: https://de.wikipedia.org/w/index.php?title=Indicator_of_compromise&oldid=236146894 (Abgerufen: 23. August 2023, 12:21 UTC)

10 Seite „Information Security Management System". In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 8. Juli 2023, 07:24 UTC. URL: https://de.wikipedia.org/w/index.php?title=Information_Security_Management_System&oldid=235286442 (Abgerufen: 23. August 2023, 12:16 UTC)

Begriffe	Beschreibung
SIEM	"Security Information and Event Management (SIEM) kombiniert die zwei Konzepte Security Information Management (SIM) und Security Event Management (SEM) für die Echtzeitanalyse von Sicherheitsalarmen aus den Quellen Anwendungen und Netzwerkkomponenten. SIEM dient damit der Computersicherheit einer Organisation und ist ein Softwareprodukt, das zentral installiert oder als Cloudservice genutzt werden kann."[11]
Pen Tests oder Penetrationstests	"Penetrationstest, kurz Pentest(ing), ist der fachsprachliche Ausdruck für einen umfassenden Sicherheitstest einzelner Rechner oder Netzwerke jeglicher Größe. Ein Penetrationstest prüft die Sicherheit von Systembestandteilen und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden, die tauglich sind, um unautorisiert in das System einzudringen (Penetration). Penetrationstests können Sicherheitslücken aufdecken, aber nicht ausschließen. Werkzeuge bilden bei Penetrationstests Angriffsmuster nach, die sich aus zahlreichen bekannten Angriffsmethoden ableiten lassen."[12]
IT-Grundschutz-Profile	"IT-Grundschutz-Profile sind Schablonen für die Informationssicherheit von Anwendern für Anwender.Unternehmen oder Behörden können IT-Grundschutz-Profile für bestimmte Anwendungsfälle erstellen und im Anschluss weiteren Interessierten zur Verfügung stellen. Anwender, die ähnliche Sicherheitsanforderungen haben, können anhand dieser Vorlage ressourcenschonend das Sicherheitsniveau überprüfen oder damit beginnen, ein Managementsystem für Informationssicherheit (ISMS) nach IT-Grundschutz aufzubauen."[13]
EfA-Prinzip	"Das Motto "Einer für Alle" – oder kurz: "EfA". Sprich, jedes Land sollte Leistungen so digitalisieren, dass andere Länder sie nachnutzen können und den Online-Prozess nicht nochmal selbst entwickeln müssen. Das spart Zeit, Ressourcen und Kosten. Der Grundgedanke hinter EfA ist also, dass Länder und Kommunen nicht jedes digitale Verwaltungsangebot eigenständig neu entwickeln, sondern sich abstimmen und die Arbeit aufteilen."[14]
Gaia-X	"Gaia-X ist ein Projekt zum Aufbau einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur für Europa, das von Vertretern aus Wirtschaft, Wissenschaft und Verwaltung aus Deutschland und Frankreich, gemeinsam mit weiteren, vorwiegend europäischen Partnern getragen wird. Der Name des Projektes leitet sich von einer der ersten aus dem Chaos entstandenen griechischen Gottheit Gaia ab, die in der Mythologie als personifizierte Erde für die Gebärerin steht. Der breiten Öffentlichkeit wurde das Projekt beim Digital-Gipfel 2019 in Dortmund vorgestellt und wird seitdem kontinuierlich weiterentwickelt."[15]

11 Seite „Security Information and Event Management". In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 3. Juli 2023, 10:35 UTC. URL: https://de.wikipedia.org/w/index.php?title=Security_Information_and_Event_Management&oldid=235143746 (Abgerufen: 23. August 2023, 12:15 UTC)

12 Seite „Penetrationstest (Informatik)". In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 19. Januar 2023, 16:31 UTC. URL: https://de.wikipedia.org/w/index.php?title=Penetrationstest_(Informatik)&oldid=230007964 (Abgerufen: 23. August 2023, 12:13 UTC)

13 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzprofile, Abgerufen 23. August 2023, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/it-grundschutz-profile_node.html

14 Bundesministerium für des Innern und für Heimat, Einer für Alle – Einfach erklärt, Abgerufen 23. August 2023 https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/nachnutzung/efa/efa-node.html

15 Seite „Gaia-X". In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 19. Mai 2023, 12:24 UTC. URL: https://de.wikipedia.org/w/index.php?title=Gaia-X&oldid=233859283 (Abgerufen: 23. August 2023, 12:31 UTC)

Über die Stiftung Neue Verantwortung

Die Stiftung Neue Verantwortung (SNV) ist ein gemeinnütziger Think Tank für die aktuellen politischen und gesellschaftlichen Fragen neuer Technologien. Unsere Veröffentlichungen, Veranstaltungen und Beratungsangebote richten sich nicht nur an Regierungen und Parlamente, sondern an alle, die sich informieren und beteiligen wollen. Unsere Expert:innen arbeiten unabhängig von Interessengruppen und Parteien.

Die SNV ist im deutschen Lobbyregister und im europäischen Transparenzregister eingetragen.

Über die Autorin

Julia Schuetze ist Projektleiterin für Cybersicherheitspolitik und -resilienz bei der Stiftung Neue Verantwortung e.V. Seit 2017 leitet sie verschiedene Projekte für die SNV, die sich auf vergleichende Cybersicherheitspolitik, europäische Cybersicherheitspolitik, Cyberoperationen gegen Wahlprozesse und die Cyberresilienz lokaler Regierungsstellen konzentrieren. Außerdem konzipiert und implementiert sie Übungen zur Cybersicherheitspolitik, an denen mehrere Interessengruppen beteiligt sind.

So erreichen Sie die Autor:in

Julia Schuetze
Projektleiterin "Cybersicherheitspolitik und Resilienz"
jschuetze@stiftung-nv.de
twitter.com/juschuetze
info@cybersicherheitskompass.de

Impressum

Think Tank für die Gesellschaft im technologischen Wandel

Stiftung Neue Verantwortung e.V.
Ebertstraße 2
10117 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:
Alina Siebert