In der Senatssitzung am 11. April 2023 beschlossene Fassung

Der Senator für Inneres
Der Senator für Finanzen

Bremen, 05.03.2023

Vorlage für die Sitzung des Senats
am 11.04.2023

Verabschiedung der Bremischen Cybersicherheitsstrategie 2023 und Einrichtung einer Zentralstelle für Cybersicherheit

A. Problem

Der Schutz unserer Gesellschaft und unserer Werte in der Freien Hansestadt Bremen, den weiteren Ländern, in Deutschland und den europäischen Mitgliedsstaaten ist eine Grundanforderung an das staatliche Handeln. Die zunehmende Verlagerung des privaten, gesellschaftlichen, wirtschaftlichen und öffentlichen Lebens in den Cyberraum führt dazu, dass sich diese Grundanforderung auch auf den Schutz der dort geschaffenen Werte zu beziehen hat. Cybersicherheit ist die IT-Sicherheit der im Cyberraum auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme. Cybersicherheit ist Teil der Daseinsvorsorge, um die Grundversorgung der hier lebenden Menschen mit Gütern und Dienstleistungen sicherzustellen. Nach der Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) befasst sich Cybersicherheit mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Diese gesamtstaatliche Verantwortung wird mit entsprechenden Gesetzgebungen in der Europäischen Union (EU) und in Deutschland adressiert. Auch die Länder haben entsprechende Vorkehrungen zu treffen, um sich den dynamischen Herausforderungen einer zunehmend digitalisierten und zunehmend vernetzten Gesellschaft zu stellen.

Die im Dezember 2022 erlassene 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) stellt gegenüber der bisherigen Rechtslage auf der Ebene der Europäischen Union sowie der nationalen Gesetzgebung erheblich gesteigerte Anforderungen im Hinblick auf die Identifika-

tion, Erfassung und Kontrolle wesentlicher und wichtiger Dienste dar, sodass bisherige Vorkehrungen zum Schutz Kritischer Infrastrukturen (KRITIS) maßgeblich erweitert und um vielfältige Instrumente zur Stärkung der Cybersicherheit in diesen Diensten erweitert werden müssen.

Derzeit noch offen, aber sehr wahrscheinlich ist, dass die Länder zur Umsetzung der in der NIS-2-Richtlinie geforderten Maßnahmen eigene gesetzliche Grundlagen schaffen müssen, da aktuell nicht absehbar ist, dass der Bund hier von seiner Regelungskompetenz Gebrauch machen wird. Der spätest zulässige Umsetzungszeitpunkt ist Oktober 2024.

Am 04.10.2022 hat der Senat den Senator für Inneres und den Senator für Finanzen gebeten, eine Cybersicherheitsstrategie für das Land Bremen bis zum Ende des ersten Quartals 2023 zu erarbeiten.

B. Lösung

Zur Umsetzung des Auftrags des Senats haben der Senator für Inneres und der Senator für Finanzen mit Unterstützung einer beim Senator für Inneres eingerichteten Projektgruppe eine Arbeitsgruppe mit Beteiligung aller Ressorts sowie des Magistrats der Stadt Bremerhaven eingerichtet, die im Zeitraum von September 2022 bis März 2023 den Entwurf der Bremischen Cybersicherheitsstrategie erarbeitet hat. Auf der strategischen Ebene erfüllt diese bereits alle Verpflichtungen der NIS-2-Richtlinie und stellt die Basis dar, auf der in den identifizierten Handlungsfeldern (Intensivierung der Vernetzung der Cybersicherheitsakteure; Staatliche Verwaltung und Kommunen; Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden; Wirtschaft und KRITIS; Förderung der digitalen Kompetenzen; Awareness und Verbraucherschutz; Fachkräfte; Innovative Forschung und Entwicklung; nationale und internationale Kooperationen) durch die zuständigen Ressorts und Kommunalverwaltungen operative Maßnahmen entwickelt und umgesetzt werden können.

Zentrales Element der Bremischen Cybersicherheitsstrategie ist die Einrichtung einer Zentralstelle für Cybersicherheit. Diese wird die Identifikation der wesentlichen und wichtigen Dienste koordinieren, eine zentrale Ansprechstelle auf Landesebene für die Kooperation mit den anderen Ländern und dem Bund darstellen und zudem den Netzwerkknotenpunkt für die vielfältigen Maßnahmen aller Ressorts und der Stadt Bremerhaven im Bereich der Cybersicherheit darstellen.
Ein weiterer wesentlicher Faktor für die Erhöhung der Cybersicherheit in der Freien Hansestadt Bremen ist eine enge Kooperation mit dem Bundesamt für Sicherheit in der Informati-

onstechnik (BSI), insbesondere in den Bereichen Informationsaustausch, Sensibilisierung und Fortbildung sowie in der gegenseitigen Unterstützung bei der Umsetzung von Cybersicherheitsmaßnahmen. Hierzu soll zwischen der Freien Hansestadt Bremen und dem BSI möglichst zeitnah ein Kooperationsvertrag abgeschlossen werden.

Die Entwicklung einer belastbaren und flexiblen Cybersicherheitsstrategie ist ein fortwährender Prozess, der auf vielfältige Sichtweisen und Impulse angewiesen ist, um eine breitestmögliche Akzeptanz zu erfahren. Diese kontinuierlich bei der Fortschreibung der Bremischen Cybersicherheitsstrategie mit einzuarbeiten unterstreicht das Verständnis, dass Cybersicherheit im Land Bremen nur im Rahmen eines gesamtgesellschaftlichen Ansatzes dauerhaft zu stärken ist. So wird eine Grundlage geschaffen, Innovation und Digitalisierung zu nutzen, während die hiermit einhergehenden Risiken bestmöglich kontrolliert werden. Bei dieser ersten Auflage handelt es sich konzeptionell daher um den Beginn eines langfristig angesetzten Prozesses, der kooperative Bemühungen zur Schaffung eines höchstmöglichen Cybersicherheitsniveaus im Land Bremen anstößt und hierbei kritisch in regelmäßigen Abständen die eigene Zielerreichung hinterfragt. Zu diesem Zweck ist die fortwährende Evaluation und Fortschreibung der Bremischen Cybersicherheitsstrategie vorgesehen. Die erste Evaluation erfolgt zwei Jahre nach der Verabschiedung der Strategie, um das Etablieren notwendiger Strukturen sowie die Umsetzung zentraler Maßnahmen zügig zu bewältigen. Während der Fokus somit zunächst darauf liegt, im Land Bremen schnell arbeitsfähige und belastbare Strukturen zur Bearbeitung von Cybersicherheitsthemen zu schaffen, liegt der Fokus in der Folge auf der Stärkung sowie Erweiterung der Maßnahmen, um Cybersicherheit stetig zu verbessern. Hierfür ist ein vierjähriger Evaluationszeitraum vorgesehen.

C. Alternativen

Der Verzicht auf eine Bremische Cybersicherheitsstrategie hätte zur Folge, dass keine gemeinsame strategische Ausrichtung bestünde und keine Koordination der Maßnahmen zur Stärkung der Cybersicherheit durch die Ressorts und die Stadt Bremerhaven erfolgte.
Es ist in Umsetzung der NIS-2-Richtlinie zu erwarten, dass die Freie Hansestadt Bremen verpflichtet wird, spätestens bis Oktober 2024 eine Cybersicherheitsstrategie vorzulegen.

D. Finanzielle und personalwirtschaftliche Auswirkung; Gender-Prüfung

Angesichts des Handlungsdrucks durch die angespannte Cybersicherheitslage wurde die Bremische Cybersicherheitsstrategie 2023 durch alle Ressorts und den Magistrat der Stadt Bremerhaven mit vorhandenem Personal erarbeitet.

Perspektivisch werden die einzelnen Maßnahmen in den Handlungsfeldern der Bremische Cybersicherheitsstrategie 2023 mit personellen und finanziellen Ressourcen ausgestattet werden müssen. Der konkrete Umfang ist derzeit noch nicht abzusehen.

Auswirkungen auf die Gleichstellung aller Geschlechter ergeben sich durch die Bremische Cybersicherheitsstrategie 2023 nicht unmittelbar. Bei den zu treffenden Maßnahmen werden genderbezogene Auswirkungen jeweils aktiv zu prüfen sein.

E. Beteiligung und Abstimmung

Die Erstellung der Cybersicherheitsstrategie ist unter Beteiligung aller Ressorts sowie des Magistrats der Stadt Bremerhaven erfolgt. Darüber hinaus wurden die Landesbeauftragte für Datenschutz und Informationsfreiheit, der Landesbehindertenbeauftragte und die Zentralstelle zur Verwirklichung der Gleichberechtigung der Frau einbezogen.

Die Vorlage ist mit der Senatskanzlei, der Senatorin für Soziales, Jugend, Integration und Sport, der Senatorin für Klimaschutz, Mobilität, Umwelt, Stadtentwicklung und Wohnungsbau, dem Senator für Kultur, der Senatorin für Wirtschaft, Arbeit und Europa, der Senatorin für Kinder und Bildung, der Senatorin für Wissenschaft und Häfen, der Senatorin für Justiz und Verfassung, der Senatorin für Gesundheit, Frauen und Verbraucherschutz sowie mit dem Magistrat der Stadt Bremerhaven abgestimmt.
Eine Einbeziehung der Landesvertretung erfolgte noch nicht, so dass gegebenenfalls daraus erwachsende relevante Punkte nicht Eingang gefunden haben.

F. Öffentlichkeitsarbeit und Veröffentlichung nach dem Informationsfreiheitsgesetz

Die Senatsvorlage ist nach Beschlussfassung im Senat zur Veröffentlichung geeignet. Einer Veröffentlichung über das zentrale elektronische Informationsregister steht nichts entgegen.

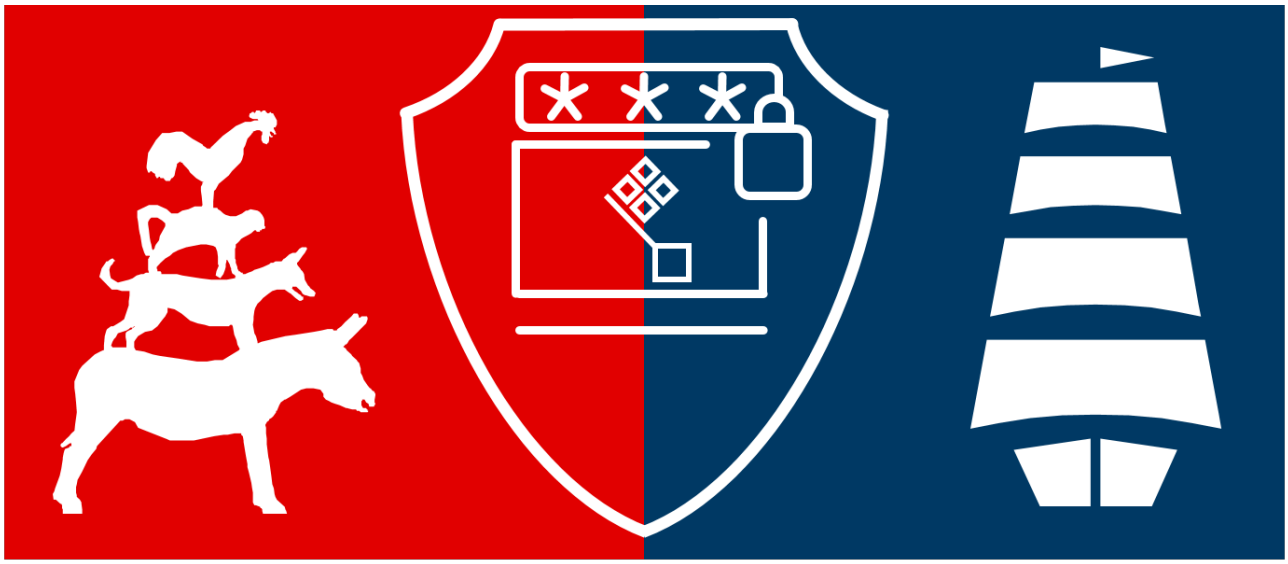
G. Beschlüsse

1. Der Senat beschließt die Bremische Cybersicherheitsstrategie 2023.
2. Der Senat bittet den Senator für Inneres, zum 01.05.2023 eine Zentralstelle für Cybersicherheit einzurichten.
3. Der Senat bittet den Senator für Inneres, in Abstimmung mit allen Ressorts und dem Magistrat Bremerhaven den Entwurf eines Bremischen Cybersicherheitsgesetzes zügig vorzulegen.

4. Der Senat begrüßt die beabsichtigte Kooperationsvereinbarung mit dem Bundesamt für Sicherheit in der Informationstechnik und bittet um Abschluss der Vereinbarung bis September 2023.

Anlage: Bremische Cybersicherheitsstrategie 2023

Freie
Hansestadt
Bremen



Bremische Cybersicherheitsstrategie 2023

Inhaltsverzeichnis

Abkürzungsverzeichnis

AG InfoSic	AG Informationssicherheit
AG ISM	AG Informationssicherheitsmanagement
BakÖV	Bundesakademie für Öffentliche Verwaltung
BCM	Business Continuity Management
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMI	Bundesministerium des Inneren, für Bau und Heimat
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BremCSS	Bremische Cybersicherheitsstrategie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritis-Verordnung
BSKI	Bundesverband für den Schutz Kritischer Infrastrukturen
BVMW	Bundesverband für mittelständische Wirtschaft
CERT	Computer Emergency Response Team
CCSO	Chief Cybersecurity Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DLR	Deutsches Institut für Luft- und Raumfahrt
DSiN	Deutschland sicher im Netz e. V.
EU	Europäische Union
EU CRA	EU Cyber Resilience Act
IFI	Internationaler Frauenstudiengang Informatik (der Hochschule Bremen)
IKT	Informations- und Kommunikationstechnologien
IoT	Internet of Things
ISL	Institut für Seeverkehrswirtschaft und Logistik
IS-LL	Richtlinie für Informationssicherheit in der öffentlichen Verwaltung
ISMS	Informationssicherheitsmanagementsystem(e)
IT-PLR	IT-Planungsrat
KMU	Kleine und mittelständische Unternehmen
KRITIS	Kritische Infrastrukturen
LAG	Länderarbeitsgruppe
LfV	Landesamt für Verfassungsschutz
MABS	Arbeitsgruppe zum Thema Medienkompetenz an Bremerhavener Schulen
NetzDG	Gesetz zur Verbesserung der Rechtsdurchsetzung in den sozialen Netzwerken (Netzwerkdurchsetzungsgesetz)
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsdienstleistungen (Onlinezugangsgesetz)
PG Cybersicherheit	Projektgruppe Cybersicherheit
ReBUZ	Regionales Beratungs- und Unterstützungszentrum Bremerhaven
SEFO	Abteilung Schulentwicklung und Fortbildung des Magistrats der Stadt Bremerhaven
TZI	Technologiezentrum Informatik
UP BUND	Umsetzungsplan BUND
UP KRITIS	Umsetzungsplan KRITIS
VCV	Verwaltungs-CERT-Verbund
VDE	Verband der Elektrotechnik Elektronik und Informationstechnik e. V.
VZHB	Verbraucherzentrale Bremen e.V.
ZAC	Zentrale Ansprechstelle Cybercrime
ZIMT	Zentrum für Informatik und Medientechnologien

1. Cybersicherheit in einer digitalen Welt

Cybersicherheit darf, ebenso wie die stetig fortschreitende Digitalisierung, nicht als selbstverständlich betrachtet werden. Sie ist das Produkt fortwährender Bemühungen, Entwicklungen zu beobachten, Gefahren richtig einzuschätzen und diesen dann mit einer adäquaten Reaktion zu begegnen. Mit der Erstellung der Bremischen Cybersicherheitsstrategie wird daher das Ziel verfolgt, die aktuellen Herausforderungen für staatliche und nichtstaatliche Nutzer:innen, die mit der Digitalisierung einhergehen, zu analysieren und einen belastbaren Schutzrahmen zu entwickeln. Innerhalb dessen tragen vielzählige aufeinander abgestimmte Maßnahmen zu einem hohen Cybersicherheitsniveau bei, das stetig weiterwachsen kann.

1.1 Digitalisierung und Innovation in der heutigen Gesellschaft

In den letzten Jahrzehnten ist die Welt in einem rasanten Tempo technologisiert und digitalisiert worden. Hierzu zählen die Entwicklung neuer Technologien, wie der Künstlichen Intelligenz, die zunehmende Vernetzung elektronischer Geräte über das Internet of Things (IoT) sowie neue Arten der Kommunikation und Interaktion (z. B. durch die Verbreitung von Videotelefonie oder sozialen Netzwerken).

36 Prozent aller Unternehmen in Deutschland mit mindestens 10 Beschäftigten nutzen Geräte oder Systeme, die über das IoT ferngesteuert werden können, so eine Erhebung des Statistischen Bundesamtes.[1] Deutschland liegt hiermit deutlich über dem Durchschnitt der EU-Staaten von 29 Prozent.

Tägliche Arbeitsprozesse werden immer häufiger aus dem Homeoffice erledigt, Arbeitsergebnisse in der Cloud gespeichert oder abgerufen. Dies spiegelt sich auch in den durch Mitarbeitende genutzten digitalen Kommunikationskanälen wider: Die Nutzung von Smartphones, Videokonferenzen, Messenger-Diensten sowie Kollaborationstools (Softwareprogramme zur digitalen Kommunikation und Zusammenarbeit in Teams) gehört mittlerweile zum Alltag vieler Unternehmen, 30 Prozent bedienen darüber hinaus häufig oder sehr häufig Social-Media-Kanäle.[2]

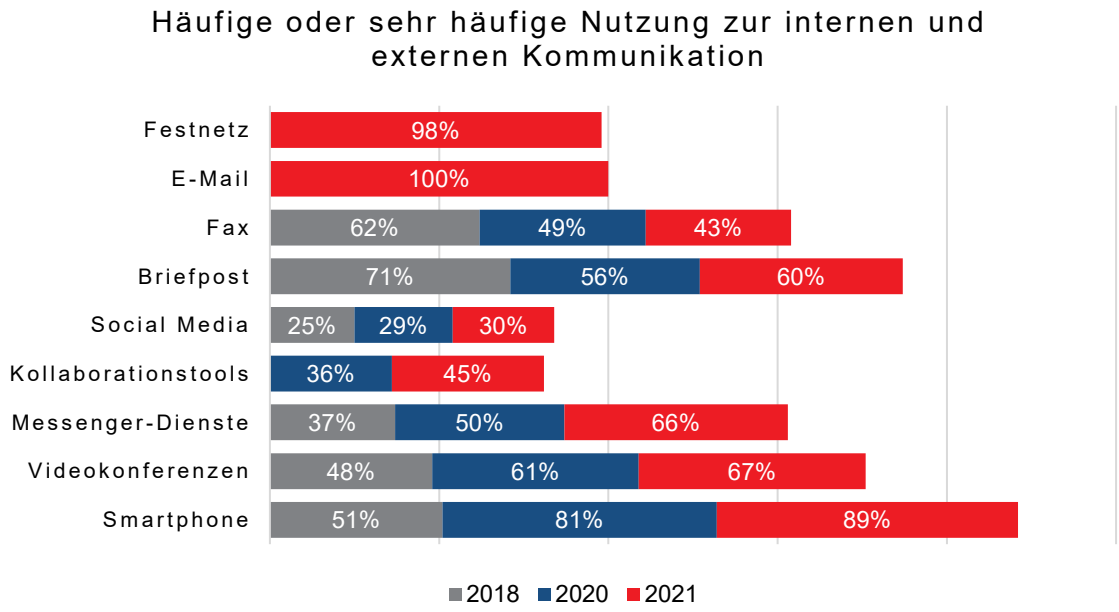


Abbildung 1 - Kanäle digitaler Kommunikation in Unternehmen

Die Corona-Pandemie und die damit verbundenen Beschränkungen und Einschränkungen haben zusätzlich zu einem starken Digitalisierungsschub geführt, der auch zu einem größeren Verständnis vom Potenzial der Digitalisierung geführt hat. Zweifelten 2016 noch 36 Prozent der Unternehmen am wirtschaftlichen Nutzen der Digitalisierung, sank die Zahl im Jahr 2020 auf 27 Prozent, im Jahr 2021 sogar auf 12 Prozent ab.[ebd]

Doch nicht nur Unternehmen erkennen und nutzen das große Potenzial von Digitalisierungsprozessen stärker. Auch im Alltag vieler Menschen wird die Digitalisierung immer greifbarer. So arbeiteten 25 Prozent aller Erwerbstätigen im Jahr 2021 im Homeoffice, im Jahr davor waren es lediglich 13 Prozent.[3]

Darüber hinaus sind digitale Prozesse mittlerweile auch ein fester Bestandteil der privaten Lebensführung vieler Menschen geworden. Heutzutage können wir Überweisungen in Echtzeit mit dem Smartphone autorisieren. Briefträger:innen nehmen an der Haustür auch während unseres Urlaubs Anweisungen zum Abstellort der Pakete über die moderne Klingelanlage entgegen und unser Smart Home tut dank intelligenter Sprachsteuerung alles, was wir wollen. Wir müssen es wortwörtlich nur sagen. Im Jahr 2022 stieg der Anteil der Hausbesitzer:innen, die Smart Home-Anwendungen im Haushalt nutzen, auf 43 Prozent[4].

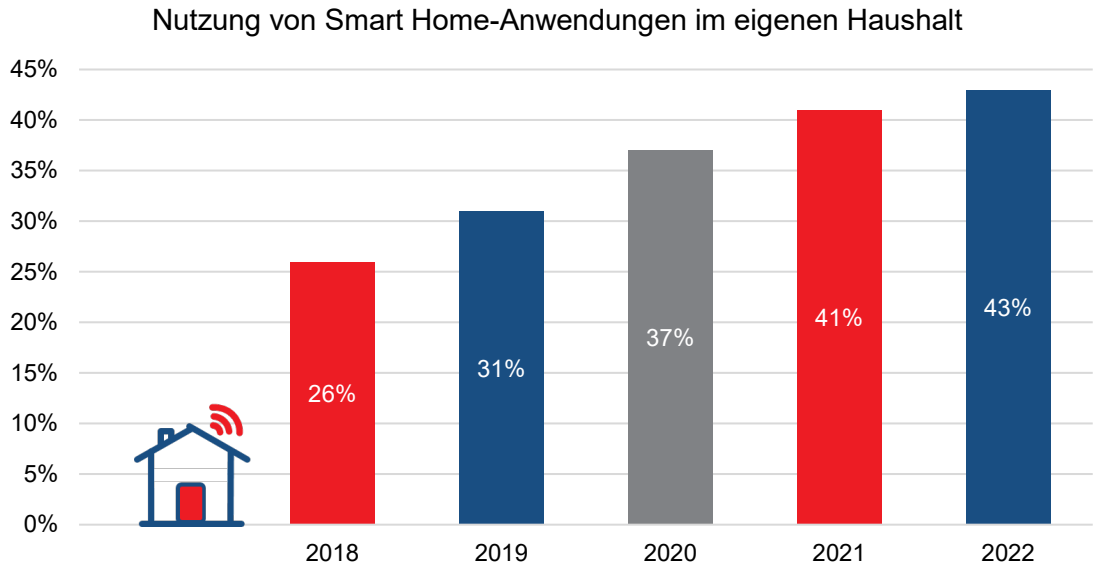


Abbildung 2 - Verbreitung der privaten Nutzung von Smart Home-Anwendungen

Digitalisierung ist technologiegetrieben und daher ein wichtiger Innovationstreiber. Sowohl die wirtschaftliche als auch gesellschaftliche Akzeptanz und Nutzung digitaler Anwendungen und Prozesse steigt stetig. Es ist daher davon auszugehen, dass Digitalisierungsprozesse auch weiterhin rasant fortschreiten, sodass nicht nur die Gegenwart, sondern auch die Zukunft stark durch technische Neuerungen und die zunehmende Vernetzung der digitalen Geräte geprägt sein werden.

Als Digitalisierung wird der stetige Veränderungsprozess nahezu aller staatlichen, wirtschaftlichen und gesellschaftlichen Bereiche, der auf dem Einsatz digitaler Technologien beruht, bezeichnet. Sie beschreibt den Wandel der Gesellschaft, der Verwaltung und der Wirtschaft weg von analogen Technologien hin zur Virtualisierung und Vernetzung der realen Welt.[5] Dieses Potenzial hat auch die Freie Hansestadt Bremen erkannt und im Juni 2021 die *Innovationsstrategie für das Land Bremen 2030*[6] beschlossen und als Grundlage künftiger Entscheidungen in der Innovationspolitik vorgestellt. Sie spielt daher eine wichtige Rolle bei aktuellen und künftigen Bemühungen, Cybersicherheit im Land Bremen zu etablieren und Innovationspotenziale sicher auszuschöpfen.

Digitalisierung betrifft nicht nur einzelne Personen oder gesellschaftliche Gruppen, sondern ist eine gesamtgesellschaftliche Herausforderung, der mit einem klug durchdachten Ansatz sowie der Vernetzung der betroffenen Akteur:innen begegnet werden kann. Wie viele Herausforderungen birgt sie, neben viele Chancen und positiven Entwicklungen, auch neue Gefahren und Risiken, die sich insbesondere im Cyber- und Informationsraum manifestieren.

1.2 Cyberraum und Cybersicherheit

Der Cyberraum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme. Ihm liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann. Ebenso dazu gehören IT-Systeme, die über Datenschnittstellen verfügen, ansonsten aber von öffentlich zugänglichen Netzen und dem Internet separiert sind.[7]

Unter Informations- und Kommunikationstechnologien (IKT) versteht man sämtliche technischen Medien, die für den Umgang mit Informationen und zur Unterstützung von Kommunikation genutzt werden, zum Beispiel Hardwarekomponenten und die zugehörige Software. In diesen Netzen werden Daten gesammelt, gespeichert, genutzt und geteilt. Hierbei lassen sich Netze je nach Zugänglichkeit noch einmal näher unterteilen.

Das Clear Web: Das ist der Bereich des Internets, in dem wir shoppen, mit Freunden chatten oder Urlaubsfotos hochladen. Dieser leicht zugängliche Teil des Internets ist jedoch nur ein kleines Fragment des gesamten Netzes.

Das Deep Web: In diesem mit Abstand umfangreichsten Bereich (ca. 90 % des gesamten Internets) befinden sich Firmendatenbanken, Streaming-Server sowie Online-Speicher. Grundsätzlich steht das Deep Web allen offen, viele Inhalte sind jedoch geschützt um bspw. Unternehmensgeheimnisse zu schützen.

Das Darknet: Dieser Raum des Internets ist ein vergleichsweise kleines Teilstück des Deep Webs. Es ist nicht auf herkömmliche Weise auffindbar, die Kommunikation wird verschlüsselt und die Urheber:innen der Inhalte sowie seine Besucher:innen bzw. Konsument:innen wollen möglichst anonym bleiben.

Abbildung 3 - Bereiche des Internets

Aktivitäten im Cyberraum können auch physische Auswirkungen haben. Neben der digitalen Seite des Cyberraums benötigt dieser für seine Funktionsfähigkeit Strom, Infrastrukturen und Menschen. Diese Faktoren müssen bei Maßnahmen, die den Cyberraum betreffen, stets mitgedacht werden. Im Cyberraum handeln somit alle Akteur:innen, wie Einzelpersonen, Wirtschaftsunternehmen, oder staatliche Beteiligte, die auch in der realen Welt handeln.

Der Cyberraum ist unerlässlich für den Fortschritt. Er ist aber auch Angriffspunkt für kritische Verwundbarkeiten. Grund hierfür sind die Komplexität, die Verflechtung, der Quasi-Wegfall zeitlicher und geografischer Grenzen, die Anonymität und die damit verbundene Schwierigkeit, Handlungen bestimmten Akteur:innen zuzuordnen.[8]

Diesen Verwundbarkeiten auf strukturierte Art und Weise zu begegnen und Maßnahmen zu treffen, um das Risiko zu reduzieren, welches sich für unterschiedliche Akteur:innen bei der Nutzung des Cyberraums ergibt, ist Gegenstand der *Cybersicherheit*.

Cybersicherheit umfasst hierbei alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik sowie den Schutz gesellschaftlich relevanter Prozesse vor Cyberangriffen im gesamten Cyberraum. Ebenfalls wird dem Schutz kritischer Infrastrukturen eine besondere Bedeutung zugeschrieben.

1.3 Gefahren und Angriffsmöglichkeiten im Zusammenhang mit dem Cyberraum

Unser Dasein basiert inzwischen in einem bisher nicht bekannten Ausmaß auf funktionierenden, zuverlässigen IKT-Strukturen und Daten im Cyberraum. Dieser hohe Grad an Digitalisierung birgt die Gefahr, dass durch unterschiedliche Ursachen eintretende Schadensereignisse ein erhebliches Ausmaß annehmen können. Hierbei lassen sich kriminelle Handlungen von nicht-vorsätzlichem Verhalten sowie weiteren Schadensfällen nicht immer trennscharf unterscheiden. Dies wird insbesondere vor dem Hintergrund der aktuell präsenten Diskussion um hybride Bedrohungen deutlich.

So ist unter der hybriden Bedrohung einerseits die Bedrohung der Europäischen Union (EU), der Bundesrepublik Deutschland und ihrer Länder durch staatliche Akteur:innen zu verstehen, die unterhalb der Schwelle militärischer Handlungen oder ergänzend zu militärischen Auseinandersetzungen beeinflussend oder schädigend auf die staatlichen Strukturen und auf das Gemeinwesen in demokratischen Staaten einwirken wollen. Hierzu können zum einen manipulative Desinformationskampagnen gehören, die nahezu immer ausschließlich oder überwiegend über elektronische Medien und soziale Netzwerke verbreitet werden, zum anderen aber auch zielgerichtete elektronische Angriffe gegen staatliche oder nichtstaatliche Infrastruktur, gegen Wirtschaftsunternehmen oder gegen die Presse, um die angegriffenen Bereiche vorübergehend oder dauerhaft funktionsunfähig zu machen.

Andererseits kann eine hybride Bedrohung in ihrem eigentlichen Wortsinn bedeuten, dass Gefahren sowohl aus dem Cyberraum heraus als auch auf nicht-digitalen Wegen ein Schadensereignis auslösen können, die Angriffs- bzw. Wirkungswege somit nicht ausschließlich einer Sphäre zuzuordnen sind. Schadensereignisse mit Auswirkungen auf die IT-Infrastruktur gehören, in unterschiedlicher Größenordnung, zum alltäglichen Geschäft der IT-Abteilungen von Unternehmen und der öffentlichen Verwaltung. Sowohl vorsätzliche als auch fahrlässige Handlungen, verbunden mit einer unzureichenden Vorbereitung und der zunehmenden Komplexität und Vernetzung der IKT-Systeme, können schwerwiegende Folgen für die Betreiber:innen der jeweiligen IKT-Infrastruktur haben.

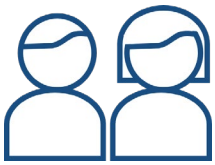
Beispiel: Im März 2021 ging ein französisches Rechenzentrum mit über 100.000 Servern in Flammen auf. In der Folge verloren zahlreiche Nutzer:innen des Clouddienstes ihre Daten.[9] Bisher ist nicht klar, ob die Ursache hierfür in einem technischen Defekt, fahrlässigem oder vorsätzlich kriminellem Verhalten zu finden ist. Die Konsequenzen für die Nutzer:innen sowie das Unternehmen sind jedoch gleichermaßen schwerwiegend: der Datenverlust auf der einen Seite und ein möglicher Vertrauensverlust in das Unternehmen sowie dessen Reputationsschädigung durch dieses Ereignis auf der anderen Seite.

Darüber hinaus wird der Cyberraum durch die große Fülle an vertraulichen Informationen sowie die potenziellen Auswirkungen kompromittierter Netze zu einem attraktiven Angriffsziel für Kriminelle, welche digitale Daten, Dienste oder Infrastrukturen für persönliche Zwecke missbrauchen. Verschiedene Kriterien führen hierbei dazu, dass der Cyberraum für

viele Kriminelle immer attraktiver wird, da sie mit verhältnismäßig geringem Aufwand großen Schaden verursachen können und gleichzeitig kaum noch besondere technische Kenntnisse mitbringen müssen, da Cyberangriffe mittlerweile über das Darknet eingekauft werden können. Ebenfalls wird das Entdeckungsrisiko für Kriminelle im Cyberraum oftmals als sehr gering eingeschätzt.

1.4 Gefährdete Zielgruppen und steigendes Schutzbedürfnis

Die Art und Weise der Durchführung von Cyberangriffen sowie die möglichen Auswirkungen hängen hierbei stark mit der jeweiligen Zielgruppe zusammen, die von Cyberkriminellen in den Blick genommen wird.



Zielgruppe Verbraucher:innen: Während in den Jahren 2019-2021 noch 25 Prozent der Verbraucher:innen angaben, bereits Opfer von Internetkriminalität geworden zu sein, so gaben dies im Jahr 2022 insgesamt 29 Prozent an. Besonders häufig wurden Verbraucher:innen dabei Opfer von Betrüger:innen beim Onlineshopping (25 Prozent) sowie von Fremdzugriffen auf ihr Onlinekonto (25 Prozent). Weitere 24 Prozent waren von einer Infektion mit Schadsoftware, 19 Prozent von Phishing, betroffen.[10]

Zielgruppe Wirtschaft: Die Wirtschaft ist weiterhin einer steigenden Anzahl an Cyberangriffen ausgesetzt. Hierbei handelt es sich bei den meisten Angriffen um sog. Ransomware-Angriffe. Die Professionalität der Angriffe nimmt hierbei stetig zu, sodass das Risiko, Opfer eines erfolgreichen Cyberangriffs zu werden, gleichermaßen steigt. Dieser Tatsache sind sich Unternehmen bewusst, wie eine Umfrage der bitkom zeigte. So gehen 78 Prozent der befragten Unternehmen davon aus, dass die Anzahl der Cyberattacken innerhalb der nächsten 12 Monate „eher“ bzw. „stark“ zunehmen wird.[11] Die Schadenshöhe der durch Cyberattacken verursachten Schäden lag hierbei in den Jahren 2020 bis 2022 regelmäßig bei mehr als 200 Milliarden Euro.[ebd]

Zielgruppe Staat und Verwaltung: Neben gezielten Angriffen auf die öffentliche Verwaltung wird diese auch immer wieder Opfer von Ransomwareangriffen. Hierbei handelt es sich häufig um nicht gezielte Angriffe, die auf Grund ungeschützter oder veralteter Hard- und Software begünstigt werden.

Abbildung 4 - Gefährdete Zielgruppen

Es ist davon auszugehen, dass die Unsicherheiten und Gefahren im Cyberraum weiter steigen werden. Während zu Beginn der globalen Vernetzung der Welt Cybersicherheit lediglich als mühsame Notwendigkeit gesehen wurde, so ist sie inzwischen eine wesentliche Voraussetzung für die sichere und gleichberechtigte Nutzung fortschrittlicher Technologien.

Diese Strategie stellt eine umfassende Grundlage für die gemeinschaftliche Stärkung von Cybersicherheit im Land Bremen bereit. Auf Basis der hier vorgestellten Erkenntnisse können einzelne Maßnahmen entwickelt werden, die unterschiedliche Bedürfnisse adressieren und somit der Vielfältigkeit der Nutzer:innen des Cyberraums gerecht werden, welche von einer Stärkung der Cybersicherheit im Land Bremen profitieren.

1.5 Aktueller Rechtsrahmen

Die Komplexität der Informations- und Cybersicherheit, die historische Entwicklung sowie die zahlreichen Schnittmengen zu anderen Rechtsgebieten haben dazu geführt, dass sehr umfangreiche, teilweise korrespondierende und mitunter sich überschneidende gesetzliche Regelungen auf europäischer, nationaler und subnationaler Ebene bestehen. So können unter dem Oberbegriff der Cybersicherheit Themenfelder der IT-Sicherheit, der Informationssicherheit, der Datensicherheit wie auch des Datenschutzes gefasst werden.[12] Das unter anderem durch das Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt „Cybersecurity Navigator“ der Universität Bremen verdeutlicht die Vielzahl der gesetzlichen Regelungen: So können mit Stand Februar 2023 542 Rechtsvorschriften mit Bezug zur Cybersicherheit auf transnationaler Ebene gefunden werden. Auf Bundesebene sind 617 Regelungen vorhanden, auf Länderebene 1.039.[13] Darüber hinaus gibt es diverse Regelungen auf europäischer Ebene, die noch in nationales Recht überformt werden müssen bzw. sich gerade in diesem Prozess befinden, was das einheitlichen Verständnis des Rechtsrahmens in Bezug auf Cybersicherheit zusätzlich erschwert.

Beispielhafte Regelungen zum Kern der Cybersicherheit sind hier auf europäischer Ebene unter anderem in den NIS-1[14] und NIS-2[15]-Richtlinien sowie dem EU Cyber Resilience Act[16] (EU CRA) zu finden. Auf nationaler Ebene existieren beispielhaft das IT-Sicherheitsgesetz[17], das korrespondierende NIS-Umsetzungsgesetz[18], sowie das IT-Sicherheitsgesetz 2.0.[19] Das IT-Sicherheitsgesetz 3.0 ist bereits in Planung. Darüber hinaus ist der Bund bemüht, der Gefahr durch hybride Bedrohungen im Bereich digitaler Infrastrukturen mit der Erarbeitung eines KRITIS-Dachgesetzes[20] zu begegnen. In diesem Punkt wird die große Schnittmenge zwischen Cybersicherheit auf der einen und dem Schutz kritischer Infrastrukturen auf der anderen Seite deutlich. Harmonisierungen in beiden Bereichen können daher als umfängliches Bemühen verstanden werden, einen digitalen Bevölkerungsschutz zu etablieren und für mehr Transparenz mit Blick auf gültige Regelungen sowie der sich hieraus ergebenden Verpflichtungen zu sorgen.

Eine abschließende Darstellung des Rechtsrahmens mit Bezug zur Informations- und Cybersicherheit ist in dieser Strategie nicht möglich. Vielmehr ist es wichtig, eine hohe Sensibilität für die Komplexität der Rechtsmaterie zu entwickeln und entsprechend zu handeln. So können Maßnahmen getroffen werden, um die verschiedenen relevanten Regelungen, insbesondere für die Fortschreibung der Strategie, in Rücksprache mit unterschiedlichen Expert:innen aus der Wissenschaft sowie der Wirtschaft angemessen zu würdigen. Hierdurch wird sichergestellt, dass sich die Strategie am aktuellen Rechtsrahmen orientiert und gleichermaßen dort, wo aktuell noch Regelungslücken vorhanden sind, Maßnahmen im Sinne zu antizipierender Regelungen gestaltet werden, bis ein verlässlicherer Rechtsrahmen umgesetzt wurde.

Die vom Senat beabsichtigte Erarbeitung eines Cybersicherheitsgesetzes für das Land Bremen wird hierzu ebenfalls einen wesentlichen Beitrag leisten. Die in dieser Strategie vorgenommenen Rechtsbezüge und -bewertungen sind daher vor dem Hintergrund der aktuellen Umsetzungsstände gesetzlicher Regelungen auf unterschiedlichen Ebenen zu bewerten und Gegenstand möglicher Anpassungen, somit als vorläufig zu beurteilen. Eine wichtige Maßnahme, welche jedoch keinem spezifischen Handlungsfeld in dieser Strategie zugeordnet wird, ist daher die fortwährende Prüfung des Rechtsrahmens, um auch künftige rechtliche Entwicklungen bei der Stärkung der Cybersicherheit im Land Bremen zeitnah und umfänglich in die Maßnahmen einzuarbeiten.

2. Methodische Hinweise

Im Folgenden werden zunächst die konzeptuellen Grundlagen und hieraus abgeleiteten zentralen Prämissen beschrieben, bevor in der Folge die Architektur der Bremischen Cybersicherheitsstrategie dargestellt wird. Durch dieses Vorgehen sollen nicht nur die Ziele der Strategie, sondern auch der Weg dorthin, für alle Leser:innen verständlich, transparent und nachvollziehbar gemacht werden.

2.1 Konzeptuelle Anknüpfungspunkte

Damit Maßnahmen zur Erhöhung der Cybersicherheit zielgerichtet geplant und durchgeführt werden können, bedarf es einer vorausschauenden und belastbaren konzeptuellen Grundlage: einer Cybersicherheitsstrategie. Sie dient als Orientierung für alle beteiligten Akteur:innen und bietet darüber hinaus die Möglichkeit, durch regelmäßige Evaluationen überprüft und fortgeschrieben zu werden.

Auf europäischer Ebene wurde im Dezember 2020 die *Cybersicherheitsstrategie der Europäischen Union für die digitale Dekade*[21] verabschiedet und hiermit ein Orientierungsrahmen für die Mitgliedstaaten geschaffen, welche Eckpfeiler eine besondere Bedeutung in den kommenden Jahren bei der Gestaltung der Cybersicherheit einnehmen.

Die Bundesrepublik Deutschland befindet sich ebenfalls seit längerer Zeit in dem Prozess, eine Nationale Cybersicherheitsstrategie zu erstellen und fortzuschreiben, und aktualisiert diese alle fünf Jahre. Nach den Cybersicherheitsstrategien für Deutschland im Jahr 2011[22] und 2016[23] hat die Bundesrepublik mit der *Cybersicherheitsstrategie für Deutschland 2021*[24] an die Cybersicherheitsstrategie der EU angeknüpft. Der Zusammenarbeit zwischen Bund und Ländern fällt hierbei eine besondere Bedeutung zu:

> „Die vielfältigen staatlichen Aufgaben im Cyberraum können nur durch eine gemeinsame Anstrengung von Bund und Ländern erfüllt werden. Eine intensive Verzahnung der Aktivitäten der Bundes- und Landesebene auf dem Wege einer kooperativen und komplementären Zusammenarbeit ist hierbei unumgänglich.“[25]

Um das gemeinsame Vorgehen besser zu koordinieren und um Interoperabilität zwischen den Herangehensweisen der Länder herzustellen, wurde in der Länderarbeitsgruppe (LAG) Cybersicherheit der Ständigen Konferenz der Innenminister und -senatoren der Länder (kurz: Innenministerkonferenz, IMK) die *Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien*[26] entwickelt.

Hierbei handelt es sich um eine Empfehlung zum Aufbau und zur Weiterentwicklung der Cybersicherheitsarchitektur in den Ländern, die Hinweise zum methodischen Vorgehen sowie relevanten Handlungsfeldern anbietet und darüber hinaus länderübergreifend abgestimmte Begriffsdefinitionen bereithält.

2.2 Zentrale Prämissen bei der Strategieerstellung

Bei der Erstellung der *Bremischen Cybersicherheitsstrategie 2023* wurde eng an die methodischen Hinweise der LAG Cybersicherheit angeknüpft, aus denen vier Prämissen abgeleitet wurden:

2.2.1 Cybersicherheit benötigt ein solides Fundament

Für die Strategieerstellung wurden rechtliche Rahmenbedingungen auf europäischer und nationaler Ebene sowie die im Land bereits vorliegenden tatsächlichen Rahmenbedingungen in Bezug auf Informations- und Cybersicherheit ausgewertet und analysiert. Hierdurch wurde ein Verständnis für die besonderen Anforderungen an eine landesspezifische Cybersicherheitsstrategie entwickelt.

Ebenfalls konnten so Anknüpfungspunkte für die Empfehlung von Maßnahmen identifiziert werden, um die bisher geleistete Arbeit im Bereich der Cyber- und Informationssicherheit angemessen zu würdigen. Hierdurch wurde ein tragfähiges Fundament für eine belastbare Cybersicherheitsstrategie geschaffen.

2.2.2 Cybersicherheit braucht Transparenz und Verbindlichkeit

Damit eine Strategie akzeptiert wird und für alle – auch nicht unmittelbar am Erstellungsprozess Beteiligten – verständlich ist, sind eine transparente Herangehensweise bei der Erstellung sowie verbindliche Zielformulierungen erforderlich. Transparenz bei der Erstellung gewährleistet die Bremische Cybersicherheitsstrategie (BremCSS) durch einen klaren Aufbau: Die von der LAG Cybersicherheit identifizierten Handlungsfelder wurden unter Beteiligung aller Ressorts des Senats sowie des Magistrats der Stadt Bremerhaven diskutiert und bewertet. Ebenfalls wurden inhaltliche Schwerpunkte identifiziert und in vielzähligen bi- und multilateralen Gesprächen ausdifferenziert, um den im Land Bremen möglicherweise vorliegenden besonderen Arbeitsweisen sowie technischen oder organisatorischen Rahmenbedingungen Rechnung zu tragen.

Durch diese Herangehensweise wurde zunächst eine Sensibilität für die Herausforderungen des jeweiligen Handlungsfelds erzeugt und ein Sachstand erhoben, bevor in der Folge konkrete Lösungsvorschläge entwickelt wurden.

Wo das Benennen konkreter Lösungsvorschläge zum jetzigen Zeitpunkt noch nicht möglich war, wurden perspektivische Entwicklungen aufgezeigt, die mit der kontinuierlichen Weiterentwicklung und Fortschreibung der Strategie zu messbaren Zielen entwickelt werden. In dieser Strategie entwickelte Maßnahmen sind vor diesem Hintergrund weder als allumfassend noch als abschließend zu betrachten.

2.2.3 Cybersicherheit bedarf gemeinsamer Anstrengungen

Ein hohes Schutzniveau in der Cybersicherheit lässt sich nur durch gemeinschaftliche Anstrengungen erreichen. Die frühzeitige und umfangreiche Einbindung relevanter Akteur:innen im Land Bremen stellte daher einen Grundwert bei der Strategieerstellung dar. Hierdurch war es möglich, eine konsensfähige Cybersicherheitsstrategie für das Land zu entwickeln, welche von der breiten Akzeptanz aller Beteiligten getragen wird und hierüber hinaus eine besondere Sensibilität gegenüber den Besonderheiten des in der Bundesrepublik einzigartigen Zwei-Städte-Staates besitzt.

Die Cybersicherheitsstrategie wurde durch eine Arbeitsgruppe aller Ressorts des Senats sowie des Magistrats der Stadt Bremerhaven unter gemeinsamer Federführung des Senators für Inneres und des Senators für Finanzen erarbeitet. Die Geschäftsführung und Koordination erfolgte durch die beim Senator für Inneres angegliederte Projektgruppe Cybersicherheit (PG Cybersicherheit). Darüber hinaus wurden zahlreiche Ansprechstellen, Personen und Organisationen beteiligt.

Abbildung 5 - Am Strategieerstellungsprozess beteiligte Akteur:innen

Herr Prof. Dr. Dennis-Kenji Kipker, Professor für IT-Sicherheitsrecht an der Hochschule Bremen sowie Mitglied des Vorstands der Europäischen Akademie für Informationsfreiheit und Datenschutz in Berlin, brachte wertvolle Impulse in die Strategieerstellung ein.

Darüber hinaus wurde die Strategieerstellung von einem umfangreichen Informationsprozess begleitet. Zahlreiche Akteur:innen im Land Bremen (eine vollständige Liste befindet sich im Anhang) wurden über die Strategieerstellung informiert. Ihnen wurde Gelegenheit gegeben, Punkte zu benennen, die aus ihrer Sicht für die Stärkung der Resilienz gegenüber Cyberbedrohungen eine besondere Bedeutung einnehmen. Es ist zudem beabsichtigt, sie im Rahmen der zeitnahen Evaluation zu einer Stellungnahme einzuladen.

2.2.4 Cybersicherheit wächst mit stetigen Lern- und Entwicklungsprozessen

Die Entwicklung einer belastbaren und flexiblen Cybersicherheitsstrategie ist ein fortwährender Prozess, der auf vielfältige Sichtweisen und Impulse angewiesen ist, um eine breitestmögliche Akzeptanz zu erfahren. Diese kontinuierlich bei der Fortschreibung der Bremischen Cybersicherheitsstrategie mit einzuarbeiten unterstreicht das Verständnis, dass Cybersicherheit im Land Bremen nur im Rahmen eines gesamtgesellschaftlichen Ansatzes dauerhaft zu stärken ist. So wird eine Grundlage geschaffen, Innovation und Digitalisierung zu nutzen, während die hiermit einhergehenden Risiken bestmöglich kontrolliert werden.

Trotz größter Bemühungen, die vielfältigen Interessengruppen und Akteur:innen des Landes Bremen adäquat abzubilden, haben vermutlich noch nicht alle besonderen Sichtweisen oder Bedürfnisse Einfluss in diesen Entwurf der Bremischen Cybersicherheitsstrategie finden können. Dies ist insofern unbedenklich, als dass es sich bei dieser ersten Auflage nur um den Beginn eines langfristig angesetzten Prozesses handelt, der kooperative Bemühungen zur Schaffung eines höchstmöglichen Cybersicherheitsniveaus im Land Bremen anstößt und hierbei kritisch in regelmäßigen Abständen die eigene Zielerreichung hinterfragt.

Zu diesem Zweck ist die fortwährende Evaluation und Fortschreibung der Bremischen Cybersicherheitsstrategie vorgesehen. Die erste Evaluation erfolgt zwei Jahre nach der Verabschiedung der Strategie, um das Etablieren notwendiger Strukturen sowie die Umsetzung zentraler Maßnahmen zügig zu bewältigen. Während der Fokus somit zunächst darauf liegt, im Land Bremen schnell arbeitsfähige und belastbare Strukturen zur Bearbeitung von Cybersicherheitsthemen zu schaffen, liegt der Fokus in der Folge auf der Stärkung sowie Erweiterung der Maßnahmen, um Cybersicherheit stetig zu verbessern. Hierfür ist ein vierjähriger Evaluationszeitraum vorgesehen.

Die Evaluationsintervalle sind bewusst kürzer gewählt als die 5-Jahres-Intervalle der Bundesregierung zur Evaluation der Cybersicherheitsstrategie des Bundes, um schneller auf Veränderungen und Regelungsbedürfnisse im Land Bremen reagieren zu können. Gleichzeitig wird so bei allen Akteur:innen ein Verständnis von Dringlichkeit und Verbindlichkeit geschaffen, welches für die Gewährleistung umfassender Cybersicherheit im Land Bremen erforderlich ist.

Letztlich bleibt durch das gewählte Evaluationsintervall genügend Gelegenheit, in einen intensiveren Austausch insbesondere mit den Akteur:innen zu treten, die zunächst nur kursorisch über die Erstellung der Cybersicherheitsstrategie informiert werden konnten. Durch das Benennen einer zentralen Ansprechstelle wurde allen Akteur:innen jedoch die Gelegenheit gegeben, Rückfragen zum Prozess stellen zu können. Dieses Vorgehen wird auch zukünftig beibehalten werden, um die vielfältigen Interessen und Bedürfnisse aller Akteur:innen im Land Bremen angemessen zu berücksichtigen, auf Veränderungen reagieren zu können und den Austausch über die Fortschreibung der Bremischen Cybersicherheitsstrategie niedrigschwellig zu ermöglichen.

2.3 Architektur der Bremischen Cybersicherheitsstrategie

Abgeleitet aus den vier dargestellten Prämissen wurde eine Architektur für die Bremische Cybersicherheitsstrategie entwickelt. Dieses Gerüst dient der Veranschaulichung der Strategie, welche weit mehr als nur die Stärkung von Cybersicherheit zum Ziel hat.

Die Grundsätze der Strategie finden sich in ihrer Methodik wieder: Durch ein transparentes Vorgehen und umfassende Beteiligungsprozesse wird ein solides Fundament geschaffen, welches die Strategie belastbar, anpassungsfähig, verständlich, akzeptiert und somit letztlich auch umsetzbar macht: Nur, wenn alle Akteur:innen an einem Strang ziehen und sich auf die hier entwickelten Maßnahmen verständigen können, ist gemeinschaftliche Cybersicherheitsarbeit möglich.

Die besondere Bedeutung aller beteiligten Akteur:innen aus den Bereichen Staat, Wirtschaft, Wissenschaft und Gesellschaft soll mit der Darstellung vier tragender Säulen betont werden. Gerade weil die Akteur:innen sehr unterschiedliche Kompetenzen, Ansichten, Fachkenntnisse und Ideen mitbringen, bereichern sie den Prozess, an dessen Ende eine Cybersicherheitsstrategie für Alle steht.

Das Vorhandensein eines höchstmöglichen Grades an Cyber- und Informationssicherheit in unserem Alltag ist die Basis, um den Prozess fortschreitender Digitalisierung sicher zu begleiten und durch Kreativität und Innovationen voranzubringen.

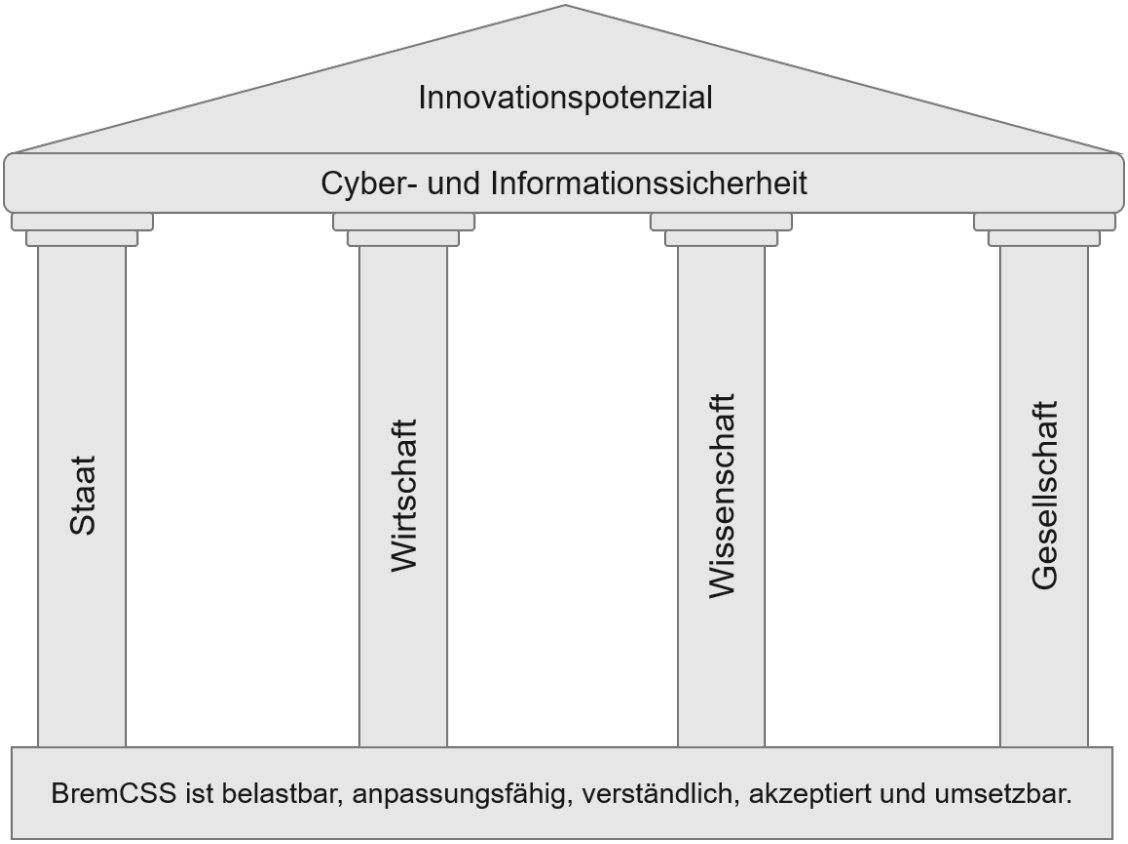


Abbildung 6 - Architektur der Cybersicherheitsstrategie im Land Bremen

3. Handlungsfelder der Bremischen Cybersicherheitsstrategie

In der Leitlinie zur Erstellung föderaler Cybersicherheitsstrategien der LAG Cybersicherheit werden neun Handlungsfelder beschrieben, die ein breites Spektrum relevanter Akteur:innen sowie Anknüpfungspunkte für eine umfassende Cybersicherheitsstrategie anbieten:

1. Intensivierung der Vernetzung der Cybersicherheitsakteur:innen

Nur durch die Identifikation und Vernetzung aller relevanten Cybersicherheitsakteur:innen kann Cybersicherheit in der Freien Hansestadt Bremen stetig gesteigert werden.

2. Staatliche Verwaltung und Kommunen

Die Digitalisierung der Verwaltung und Kommunen birgt Chancen und Herausforderungen. Um ihre Dienstleistungen erbringen zu können, muss die digitale Resilienz aller Bereiche staatlicher und kommunaler Verwaltung gestärkt werden.

3. Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden

Die Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden sind für die Aufrechterhaltung der öffentlichen Sicherheit immanent wichtig. Die personellen und materiellen Voraussetzungen im Umgang mit den neuen Herausforderungen, die sich durch den Cyberraum ergeben, werden fortwährend geprüft.

4. Wirtschaft und KRITIS

Unser Wohlstand beruht auf einer leistungsstarken Wirtschaft. Um diesen zu sichern und zukunftsorientiert weiterzuentwickeln, müssen kritische Infrastrukturen (KRITIS) geschützt und Wirtschaftsunternehmen digital resilient sein.

5. Förderung der digitalen Kompetenzen

Die fortschreitende Digitalisierung erfordert ein lebenslanges Lernen. Damit die Bürger:innen des Landes Bremen sich sicher im Cyberraum bewegen können, müssen ihre digitalen Kompetenzen gefördert werden.

6. Awareness und Verbraucherschutz

Die Digitalisierung fördert die Entwicklung neuer Produkte und Dienstleistungen. Um die Verbraucher:innen vor möglichen Cyberrisiken zu schützen, müssen Regelungen für die Entwicklung dieser geschaffen und die Verbraucher:innen für Cybersicherheit sensibilisiert werden.

7. Fachkräfte

Ein Grundstein der Cybersicherheit sind gut ausgebildete Fachkräfte. Um Cybersicherheit in der Zukunft gewährleisten zu können, muss dem Fachkräftemangel insbesondere im IT-Bereich entgegengewirkt werden.

8. Innovative Forschung und Entwicklung

Um Cybersicherheit auch in der Zukunft gewährleisten zu können, müssen Forschungs- und Entwicklungsinstitute in die Lage versetzt werden, die Herausforderungen von Morgen bereits heute zu erkennen und innovative Lösungen zu entwickeln.

9. Nationale und internationale Kooperationen

Cybersicherheit endet nicht an geografischen oder physischen Grenzen. Um digitale Resilienz zu schaffen, sind nationale und internationale Kooperationen unabdingbar.

Für die Erstellung der Bremischen Cybersicherheitsstrategie wurde die Auswahl und Reihenfolge der in der LAG Cybersicherheit identifizierten Handlungsfelder beibehalten, da sie alle in unterschiedlichem (aber nicht ausschließendem) Maße mit den vier Hauptakteur:innen Staat, Wirtschaft, Wissenschaft und Gesellschaft korrespondieren.

Lediglich das Handlungsfeld 3 wurde um „Strafverfolgungs- und Verfassungsschutzbehörden“ erweitert, um ihrer wichtigen Rolle in der Schaffung eines hohen Cybersicherheitsniveaus gerecht zu werden.

Hierdurch wurden zwei Ziele verfolgt:

Durch die enge Anlehnung an die Struktur der Leitlinie wird erstens eine bewusste Entscheidung gegen eine weitere Fragmentierung der bestehenden Cybersicherheitsarchitektur Deutschlands getroffen. Dem länderübergreifenden Wunsch nach einer stärkeren Harmonisierung sowie der Interoperabilität individueller Bemühungen zur Stärkung der Cyber- und Informationssicherheit wird Rechnung getragen.

Zweitens trägt die individuelle Ausgestaltung und Konkretisierung der Handlungsfelder den landesspezifischen Besonderheiten Rechnung. Auf diese Weise wurde sichergestellt, dass trotz einer einheitlichen Struktur eine Bremische Cybersicherheitsstrategie entwickelt wurde, hinter der sich alle Beteiligten des Landes Bremen sowie der Städte Bremen und Bremerhaven versammeln können.

Die Zuteilung von Handlungsfeldern zu bestimmten Säulen und Akteur:innen, wie in der folgenden Grafik gezeigt, erfolgte in einem ersten Schritt, um die Analysearbeit für die folgenden Handlungsfeldbeschreibungen zu vereinfachen und zu strukturieren. Die Zuordnung ist hierbei keinesfalls als ausschließend zu verstehen und beschreibt darüber hinaus keine alleinigen Verantwortlichkeiten. Auch beinhaltet die Reihenfolge keine Wertung.

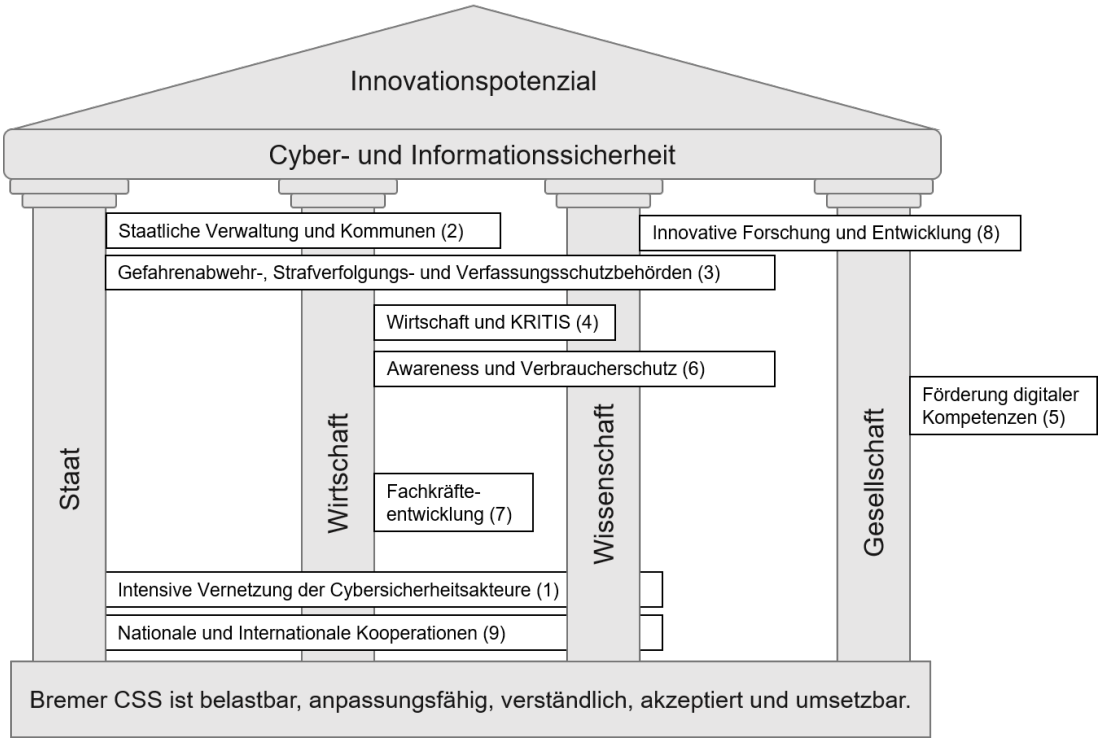


Abbildung 7 - Architektur der Bremischen Cybersicherheitsstrategie mit Handlungsfeldern

Zur besseren Übersichtlichkeit wurde das umfangreiche Kapitel 3 einheitlich strukturiert:

Zu Beginn jedes Handlungsfelds wird eine kurze Zusammenfassung mit Blick auf seine Zielrichtung und Reichweite vorgestellt. Diese Beschreibung ist das Ergebnis eines detaillierten Abstimmungsprozesses aller beteiligten Akteur:innen und beschreibt den Kern des jeweiligen Unterkapitels in wenigen Sätzen.

In der Folge werden zunächst die Herausforderungen des Handlungsfelds skizziert und ein Überblick über die Aktivitäten auf nationaler oder supranationaler Ebene (allgemeiner Sachstand) gegeben, bevor dann ein spezifischer Sachstand für das Land Bremen herausgearbeitet wird. Hierdurch wird der erforderliche Kontext für das aus der Handlungsfeldbeschreibung resultierende Problembewusstsein geschaffen, dem letztlich mit einem Vorschlag von Maßnahmen zur Problembewältigung im Rahmen der Strategieumsetzung begegnet wird.

Wo immer es zum jetzigen Zeitpunkt noch nicht möglich war, spezifische oder messbare Ziele zu definieren, wird dies als Prüfauftrag verstanden, diese im Rahmen der Strategiefortschreibung weiter auszudifferenzieren und zu konkretisieren.

3.1 Intensivierung der Vernetzung der Cybersicherheitsakteur:innen

Ein hohes Cybersicherheitsniveau zu schaffen und stetig zu verbessern ist eine fortwährende Aufgabe, welche nur durch die strategische Vernetzung und enge Kooperation der staatlichen Cybersicherheitsakteur:innen zu erreichen ist. Ein starkes Cybersicherheits-Netzwerk zeichnet sich durch eindeutige Ansprechbarkeiten und einen schnellen und sicheren Informationsfluss über vorab definierte Kommunikationskanäle aus. Durch den regelmäßigen Austausch der staatlichen Cybersicherheitsakteur:innen können Bedrohungen frühzeitig erkannt und Präventionsmaßnahmen gezielt (weiter-)entwickelt werden. Jede:r staatliche Cybersicherheitsakteur:in bringt die eigene besondere Expertise in das Netzwerk ein und profitiert gleichsam von den vielfältigen Kompetenzen der übrigen Netzwerkmitglieder:innen.

3.1.1 Herausforderungen des Handlungsfelds

Cybersicherheit ist ein vielschichtiges Phänomen, welches mit seinen unterschiedlichen Facetten Akteur:innen in Wissenschaft und Wirtschaft und Gesellschaft gleichermaßen beschäftigt. Sie stellt darüber hinaus ein zentrales Element für verschiedene Politikfelder des Staates dar, etwa die Innen- und Außen- sowie die Sicherheits- und Verteidigungspolitik. Für diese wird es immer bedeutsamer, neben der Verteidigung gegenüber klassischen Bedrohungen auch zunehmend Schutzstrategien gegenüber hybriden Angriffen durch staatliche oder nichtstaatliche Akteur:innen zu entwickeln.

Durch die verschiedenen Berührungspunkte zum Thema Cybersicherheit hat sich ein weit verzweigtes Netzwerk unterschiedlicher Akteur:innen gebildet, die verschiedene Interessenschwerpunkte verfolgen. Das Netzwerk der verschiedenen Cybersicherheitsakteur:innen in Deutschland ist über die Jahre hinweg immer weitergewachsen und mittlerweile so komplex geworden, dass eine gewisse Unübersichtlichkeit entstanden ist. Hierdurch wird die Suche nach Ansprechstellen erschwert und die Gefahr von Doppelstrukturen steigt.

Grundvoraussetzung einer funktionierenden Cybersicherheitsarchitektur ist daher die klare Benennung von Akteur:innen und Kommunikationswegen, um einen reibungslosen und verlustfreien Kommunikationsfluss sicherzustellen.

3.1.2 Nationale Cybersicherheitsarchitektur

Mit der Gründung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf Basis des *Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik*[27] im Jahr 1991 wurde ein erster Schritt von der Bundesregierung unternommen, eine zentrale Koordinierungsstelle für Belange der Informationstechnik zu installieren, um „alle Betroffenen und Interessierten […] über Risiken der Informationstechnik und mögliche Schutzmaßnahmen [zu] unterrichten.“[28]

In den folgenden 30 Jahren hat sich nicht nur die Technisierung und Digitalisierung rasant entwickelt; gleichermaßen wuchs auch die Landschaft der Akteur:innen, die sich mit Belangen der Informations- und Cybersicherheit befassten. Das vom Bundesministerium des Inneren, für Bau und Heimat (BMI) im November 2020 herausgegebene *Online Kompendium Cybersicherheit in Deutschland*[29] zeigt in beeindruckender Weise, wie vielfältig, aber auch zersplittert, die Landschaft der Cybersicherheitsakteur:innen in Deutschland heute geworden ist. So zeigte die Recherche zur Erstellung des Kompendiums „über 2.200 Akteur:innen und Initiativen in Deutschland […], die sich thematisch mit Cybersicherheit beschäftigen.“[30]

Neben dieser sehr umfassenden Beschreibung erstellt die Stiftung Neue Verantwortung jährlich eine differenzierte Übersicht über *Deutschlands staatliche Cybersicherheitsarchitektur*[31], die zuletzt im September 2022 aktualisiert wurde. Ein besonderes Augenmerk liegt hierbei auf der Darstellung der Interdependenzen der unterschiedlichen Akteur:innen, sodass das verflochtene Cybersicherheitsnetzwerk erstmals in seiner Komplexität greifbar wird.

Auf jeder Ebene erfüllen Cybersicherheitsakteur:innen besondere Aufgaben, die sich regelmäßig aus unterschiedlichen rechtlichen Rahmenbedingungen sowie dem Selbstverständnis und Aufgabenzuschnitt der jeweils Betroffenen ergeben.

Auf Länderebene ist die Landschaft der Cybersicherheitsakteur:innen gleichermaßen komplex und darüber hinaus von einem sehr unterschiedlichen Harmonisierungsgrad gekennzeichnet. So wurden teilweise die Rollen des Chief Information Officer (CIO) sowie des Chief Information Security Officer (CISO) institutionalisiert und sind in jedem Land einheitlich vorhanden. Gleichermaßen findet sich in jedem Land eine Zentrale Ansprechstelle Cybercrime (ZAC) wie auch ein Anschluss an den oder die Landesdatenschutzbeauftragte:n sowie das Landesamt für Verfassungsschutz (LfV), aus denen sich unterschiedliche Schnittmengen zum Thema Informations- und Cybersicherheit ergeben. Darüber hinaus gibt es zahlreiche Institutionen, die von einzelnen Ländern im Rahmen der Ausgestaltung ihrer Landescybersicherheitsarchitektur errichtet wurden und einmalig sind.

Einheitlichkeit ist vorrangig mit Blick auf den Umgang mit Belangen der Informationssicherheit zu erkennen. Einen wesentlichen Beitrag hierzu leistet der *Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG*.[32]

Im IT-Planungsrat (IT-PLR) sind alle Länder und der Bund vertreten und haben hier die *Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung*[33] erarbeitet. Das Ziel der Leitlinie besteht darin, Informationsmanagementsysteme (ISMS) in den Ländern zu etablieren sowie diese perspektivisch zu vereinheitlichen. Hierdurch soll unter anderem auf die steigenden Anforderungen an Informationssicherheit reagiert werden, die sich aus der zunehmenden Vernetzung verwaltungsübergreifender Bürger:innenportale sowie digitaler Dienstleistungen ergeben.

Auch für die Cybersicherheit wurde ein länderübergreifendes Gremium eingerichtet, welches sich mit strategischen Fragen zur gemeinschaftlichen Stärkung des Cybersicherheitsniveaus in Deutschland befasst: die auf Ebene der Innenministerkonferenz angegliederte LAG Cybersicherheit, in welche auch der Bund eingebunden ist.

Im Gegensatz zum IT-Planungsrat und der hierunter angesiedelten operativen Arbeitsgruppe für Informationssicherheit (AG InfoSic), in welcher die jeweilige CISO der Länder sowie der CIO des Bundes vertreten sind, bestehen jedoch für den Verantwortungsbereich der Cybersicherheit keine einheitlichen Strukturen in den Ländern, wie beispielsweise eine landesverantwortliche Stelle für Cybersicherheit, was durch die unterschiedlich herausgebildeten institutionellen Rahmenbedingungen erklärbar ist.

Einige Länder haben sich bereits eine öffentlich einsehbare Cybersicherheitsstrategie gegeben, etwa die *Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026*[34] oder die *Cybersicherheitsstrategie des Landes Nordrhein-Westfalen*.[35] Darüber hinaus haben manche Länder bereits explizite Cybersicherheitsgesetze erlassen, wie etwa das *Gesetz für die Cybersicherheit in Baden-Württemberg.*[36]

Andere Länder sind aktuell ebenfalls dabei, eigene Cybersicherheitsstrategien zu entwickeln und arbeiten mit unterschiedlichen landesspezifisch ausgestalteten Rechtsrahmen zur Daten- und Informationssicherheit. Gerade im Stadium der Strategieentwicklung ist daher das große Potenzial vorhanden, weiterer Zersplitterung entgegenzuwirken und größere Harmonisierung und Interoperabilität, wie in der Leitlinie der LAG Cybersicherheit vorgesehen, anzustreben.

3.1.3 Cybersicherheitsarchitektur in der Freien Hansestadt Bremen

In der Freien Hansestadt Bremen ist die Funktion des Landes-CIO beim Senator für Finanzen angegliedert und wird vom Staatsrat ausgeübt, der die Freie Hansestadt Bremen im IT-Planungsrat vertritt. Hier ist ebenfalls die Funktion des Landes-CISO verortet, der einen nicht öffentlichen Jahresbericht zur Informationssicherheit in der öffentlichen Verwaltung erstellt. Darüber hinaus besteht die Arbeitsgruppe Informationssicherheitsmanagement (AG ISM), in welcher die Verantwortlichen für Informationssicherheit der jeweiligen Ressorts sowie des Magistrats der Stadt Bremerhaven vertreten sind.

Der Magistrat der Stadt Bremerhaven hat in der Richtlinie zur Informationssicherheit für das Magistratsnetz u. a. die Ziele und Grundsätze für die Informationssicherheit definiert und aufgeführt sowie die Zuständigkeit des IT-Sicherheitsbeauftragten des Magistrats geregelt.

Diese Struktur schafft klare Verantwortlichkeiten und eindeutige Kommunikations- und Informationswege. Diese sind zum Zwecke der Abstimmung wichtig, bei kritischen Vorfällen und Problemen sogar unerlässlich.

Eine zentrale Verantwortung für das Themenfeld Cybersicherheit war im Land Bremen längere Zeit nicht festgelegt. Eine Teilnahme an der LAG Cybersicherheit wurde auf Leitungsebene durch den Staatsrat beim Senator für Inneres gewährleistet. Hiermit war jedoch keine zentrale Verantwortlichkeit für den Themenkomplex Cybersicherheit verbunden, sodass bei Problemen und Fragen anderer Verwaltungsbereiche keine eindeutigen Ansprechbarkeiten gewährleistet werden konnten.

Um hier klare Strukturen zu schaffen, verfügte der Senat der Freien Hansestadt Bremen mit Beschluss vom 04.10.2022[37] eine Änderung der Geschäftsverteilung:

Die bereits bestehenden Kompetenzen des Senators für Finanzen wurden im Feld „Zentrales IT-Management, Digitalisierung öffentlicher Dienste“ mit der Ergänzung des Geschäftsbereichs „Informationssicherheit im Bereich der IT der öffentlichen Verwaltung“ gestärkt und somit auch innerhalb des Verwaltungsaufbaus klar verortet. Da bestehende Zuständigkeiten und Strukturen durch diese Anpassung nicht beeinträchtigt werden, besteht hier zunächst kein Handlungsbedarf.

In der Zuständigkeitszuweisung des Senators für Inneres wurde im Feld „Innere Sicherheit und Ordnungsrecht“ der Geschäftsbereich „Grundsatzangelegenheiten und ressortübergreifende Koordinierung des Handlungsfeldes Cybersicherheit (ohne Informationssicherheit im Bereich der IT der öffentlichen Verwaltung)“ hinzugefügt.

Hierdurch wurde die institutionelle Grundlage für die Umsetzung des Bedürfnisses nach einer zentralen Ansprechstelle einerseits und dem Erfordernis trennscharfer Aufgabenbereiche andererseits entsprochen. In der Konsequenz besteht nun das Erfordernis, den neu angelegten Geschäftsbereich so zu strukturieren und auszugestalten, dass er seiner Zentralstellenfunktion im Land Bremen gerecht werden kann.

3.1.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Zur Gewährleistung eindeutiger Ansprechbarkeiten wird im Land Bremen eine noch näher auszugestaltende Zentralstelle für Cybersicherheit im Geschäftsbereich des Senators für Inneres eingerichtet und von der noch einzurichtenden Position des Chief Cybersecurity Officers (CCSO) geleitet.

Die Zentralstelle für Cybersicherheit wird unter anderem für die Steuerung cybersicherheitsrelevanter Informationen an ein zuvor zu definierendes Netzwerk staatlicher Akteur:innen verantwortlich sein. Darüber hinaus nimmt sie die Zentralstellenfunktion im Sinne eines Single Points of Contact (SPoC) ein, der beispielsweise dem BSI gegenüber benannt werden muss, um Meldeverpflichtungen nachzukommen sowie die Informationssteuerung zwischen der Bundes- und Landesebene sowie in andere Länder hinein zu gewährleisten.

Die Informationsauswertung und -steuerung nimmt somit eine wichtige Rolle in der Zentralstelle für Cybersicherheit ein, welche den Informationsfluss durch ihre aktive Einbindung in die Gremienarbeit des Bundes und der Länder in Sachen Cybersicherheit zusätzlich stärkt. Hierdurch wird es möglich, Expertise und Fachkenntnisse aufzubauen sowie sicherheitsrelevante Informationen zeitnah zu steuern. Ebenfalls erfolgt hier eine zentrale Auswertung rechtlicher Rahmenbedingungen, um Handlungsbedarfe für das Land Bremen mit Bezug auf Cybersicherheit rechtzeitig zu erkennen und Umsetzungsvorschläge zu erarbeiten.

Die Zentralstelle für Cybersicherheit wird somit als Kompetenzknotenpunkt ausgebaut und dann sowohl staatlichen Stellen als auch der Wirtschaft, der Wissenschaft und gesellschaftlichen Akteur:innen als Anlaufpunkt in Fachfragen rund um das Thema Cybersicherheit zur Verfügung stehen. So wird eine Gesamtverantwortlichkeit geschaffen, die gegenüber den vielfältigen Akteur:innen im Land Bremen eindeutige Strukturen und Kommunikationswege bereithält und Zuständigkeitsfragen klar löst.

3.2 Staatliche Verwaltung und Kommunen

Die Handlungsfähigkeit staatlicher Verwaltung hängt in hohem Maß von der Belastbarkeit und Integrität technischer Systeme ab. Mindeststandards für die IKT-Sicherheit werden im Rahmen der Grundwerte der Informationssicherheit definiert. Sie beinhalten die Vertraulichkeit, Integrität und Verfügbarkeit sämtlicher Informationen, Prozesse und Dienstleistungen. Zur Erhöhung der Handlungssicherheit bei den Kommunen sowie der Landesverwaltung ist die Etablierung eines grundschutzkonformen ISMS sinnvoll.

3.2.1 Herausforderungen des Handlungsfelds

Die staatliche Verwaltung und die Kommunen sind eine unverzichtbare Ansprechstelle für Bürger:innen, die Wirtschaft sowie die Wissenschaft im Land Bremen. Sie erbringen wichtige und einzigartige Verwaltungsdienstleistungen von A - wie Anmeldung eines Kindes in der Kindertagesbetreuung bis hin zu Z - wie Zulassung von Kraftfahrzeugen.

Die Aufgabe einer funktionierenden Verwaltung besteht darin, die vielfältigen und für die Betroffenen oft essenziellen Dienstleistungen verlässlich anzubieten und Ausfällen sowie Beeinträchtigungen durch umfangreiche Sicherungsmaßnahmen bestmöglich vorzubeugen. Gerade durch den verstärkten Ausbau des Angebots digitaler Verwaltungsdienstleistungen bedarf es hierzu stabiler informations- und kommunikationstechnischer Infrastrukturen (IKT-Strukturen). Während Anforderungen an die Erreichbarkeit sowie die Datensicherheit schon seit langer Zeit in der technischen Umsetzung von Verwaltungsdienstleistungen mitgedacht werden, ist eine weitere Herausforderung in den letzten Jahren in den Fokus gerückt: die Resilienz gegenüber Cyberbedrohungen. Die Häufung von Cyberangriffen auf Verwaltungsstrukturen in Deutschland in den letzten Jahren zeigt, dass Angriffe ohne Vorwarnung eintreten und zu umfangreichen Ausfällen führen können.

Werden Verwaltungsdaten mithilfe von Schadsoftware verschlüsselt, um beispielsweise im Rahmen eines Ransomware-Angriffs Lösegeld für die Entschlüsselung der Daten zu erpressen, können vielzählige Verwaltungsleistungen nicht mehr ausgeführt werden und stehen somit den Bürger:innen nicht mehr zur Verfügung. Ein besonders schwerwiegender Ransomware-Angriff führte im Sommer 2021 erstmals zum Ausrufen des Digitalen Katastrophenfalls. 207 Tage lang wurde die betroffene Verwaltung lahmgelegt. Gehälter, Wohngeld und BaföG konnten nicht mehr gezahlt, Kraftfahrzeuge nicht mehr angemeldet werden. Zahlreiche Verwaltungsbereiche konnten nicht mehr oder nur mit Unterstützung externer Hilfe arbeiten und ihre Dienstleistungen meist nur noch mit großen Einschränkungen zur Verfügung stellen.

Abbildung 8 - Deutschlands erster digitaler Katastrophenfall

Die Wiederherstellung der Erreichbarkeit von Verwaltungsdienstleistungen kann in schwerwiegenden Fällen mehrere Monate in Anspruch nehmen und zu finanziellen Schäden in Millionenhöhe führen. Hierbei entstehen nicht nur Kosten für den Einsatz von IT-Expert:innen, die Neubeschaffung von IKT-Hardware und, je nach Ausmaß des Schadens, den Aufbau eines neuen Netzwerks. Auch indirekten Kosten eines Cyberangriffs müssen berücksichtigt werden, etwa Beeinträchtigungen und Ausfälle in der Wertschöpfungs- oder Lieferkette, persönliche Auswirkungen auf die individuelle Lebensgestaltung von Bürger:innen sowie Gefahren für die wirtschaftliche Existenz von Unternehmen.

3.2.2 Herausforderungen der öffentlichen Verwaltung durch Digitalisierungsprozesse

Digitalisierungsprozesse haben auch in der Verwaltung Einzug erhalten. Durch das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) wurden der Bund und die Länder verpflichtet, bis Ende 2022 ihre Verwaltungsleistungen über Verwaltungsportale auch digital anzubieten, sodass hierdurch das Angebot digitaler Verwaltungsdienstleistungen stetig wächst. Als Kommunikationsinfrastruktur wird das Internet bereits seit der Jahrtausendwende von der Öffentlichen Verwaltung in wachsenden Umfang benutzt.

Dies stellt eine wichtige Entwicklung der öffentlichen Verwaltung dar, die ihre Dienstleistungen unbürokratischer und flexibler anbieten kann. Im Bundesvergleich sind die Stadtstaaten Hamburg (64 Prozent) und Bremen (60 Prozent) führend bei der Nutzung digitaler Verwaltungsdienstleistungen durch Bürger:innen.[38] Neben der Außenwirkung im Rahmen des Angebots digitaler Dienstleistungen hat die Digitalisierung auch eine Innenwirkung auf die Verwaltung, in der viele Prozesse nur noch als elektronische Akten geführt werden.

In der Folge entsteht jedoch eine Vielzahl von Systemen, Softwarelösungen und benötigten Schnittstellen, die aus dem Cyberraum heraus angegriffen werden können. Ebenfalls wächst die Menge verfügbarer Daten, welche vor unberechtigtem Zugriff, Diebstahl oder Manipulation geschützt werden müssen. Daher ist es erforderlich, dass die Prozesse, Verfahren und IKT-Strukturen auf aktuellem Stand gehalten und entsprechend den gesetzlichen Vorgaben und technisch möglichen Verfahren abgesichert werden, um einerseits die Prozesse abzusichern und andererseits die stetig steigenden Anforderungen an den mit Digitalisierungsprozessen einhergehenden Datenschutz zu erfüllen.

Gem. Art. 91c GG arbeiten Bund und Länder in Fragen der IT zusammen. Auf Basis des hieraufhin erlassenen IT-Netzgesetzes wurde der IT-Planungsrat gegründet. Dieser stellt das zentrale politische Steuerungsgremium zwischen Bund und Ländern in Fragen der Informationstechnik und der Digitalisierung von Verwaltungsleistungen dar. Durch die Beschlüsse des IT-Planungsrats erhalten Bund und Länder eine verbindliche Grundlage für die gemeinsamen föderalen Digitalisierungsaktivitäten.

Im Jahr 2018 hat der IT-Planungsrat eine Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung herausgegeben (Beschluss 2019/04 des IT-Planungsrats). In einem dazugehörigen Umsetzungsplan wurden die Handlungsfelder mit konkreten Maßnahmen und messbaren Zielen unterlegt. Der Umsetzungsstand im jährlichen Berichtswesen der AG InfoSic an den IT-Planungsrat dokumentiert.

Bund und Länder arbeiten somit zwar auf institutioneller Ebene zusammen. Die Umsetzung konkreter Maßnahmen stößt aber in der Praxis auf mehrere Hindernisse. Dazu gehören die Einbeziehung der Kommunen als in der Gesamtschau wichtigster Anbieter von Verwaltungsleistungen, aber auch die Frage nach dem Geltungsbereich der gemeinsam beschlossenen Rahmenregelungen, zum Beispiel beim Verbindungsnetz.

Von großer Relevanz ist daher die kürzlich erlassene EU-NIS-Richtlinie 2022/2555 (NIS-2), welche innerhalb von 21 Monaten von den EU-Staaten in nationales Recht umgesetzt werden muss. Die NIS-2 löst die NIS-1 Richtlinie zum 17. Oktober 2024 ab und legt Mindeststandards in der Europäischen Union für die Regulierung wesentlicher Dienste fest, zu welchen auch die öffentliche Verwaltung zählt. Das Ziel der NIS-2 besteht in der Vertiefung und inhaltlichen Erweiterung der Anforderungen an die Unternehmen und Einrichtungen in definierten wesentlichen und wichtigen Sektoren, um auf wachsende und sich verändernde Cyberbedrohungen angemessen reagieren zu können.

3.2.3 Umsetzung einer resilienten IT-Infrastruktur in der Freien Hansestadt Bremen

Auf supranationaler oder nationaler Ebene bestehende rechtliche Regelungen müssen aufgrund des föderalen Systems der Bundesrepublik Deutschlands auf Landesebene umgesetzt oder konkretisiert werden. Dies wird etwa mit der Umsetzung der NIS-2-Richtlinie deutlich, die gesteigerte Anforderungen an die öffentlichen Verwaltungen als einen identifizierten wesentlichen Sektor stellt, vielfältige Maßnahmen zur Steigerung der Cybersicherheit umzusetzen.

Gleichzeitig besteht im Land Bremen der Anspruch, die bereits sehr positive Nutzung digitaler Verwaltungsdienstleistungen durch Bürger:innen weiter zu steigern und darüber hinaus die Arbeit mit der elektronischen Akte, gestützt auf ein einheitliches Dokumentenmanagementsystem, weiter zu stärken. Diese wurde im Land Bremen bereits Anfang 2022 in der Verwaltung als verpflichtend eingeführt, womit das Land Bremen im Bundesvergleich sehr gut aufgestellt ist.[39]

Zur Erreichung dieser Ziele ist es erforderlich, dass die rechtlichen Rahmenbedingungen auf den unterschiedlichen Ebenen fortwährend analysiert und die Auswirkungen möglicher Veränderungen auf Handlungserfordernisse der Länder geprüft werden. Nur durch die frühzeitige Klärung des Rechtsrahmens kann es gelingen, die stark steigenden Anforderungen an Cybersicherheitsakteur:innen als Land verlässlich zu planen und Strukturen zu schaffen, in welchen diese abgebildet werden können.

Ebenfalls ist es besonders wichtig, die vielfältige und in unterschiedlichen Umsetzungsstadien befindliche bereits geleistete Arbeit im Rahmen der Schaffung resilienter IT-Infrastrukturen in der öffentlichen Verwaltung weiter zu harmonisieren und zu stärken, um die positive Nutzung der elektronischen Akte in der Innenwirkung sowie das Angebot digitaler Dienstleistungen in der Außenwirkung weiter auszubauen.

In der Stadtgemeinde Bremerhaven wird die Nutzung der elektronischen Akte als interne Grundlage des Ausbaus von digitalen Leistungen betrachtet und insoweit stetig erweitert. Zudem bleibt festzustellen, dass aufgrund einer vom Land Bremen abweichenden IT-Infrastruktur trotz der Bemühungen nach einer weiteren Harmonisierung unterschiedliche Lösungswege zur Realisierung von digitalen Angeboten zunächst nicht ausgeschlossen werden können.

Zur Konkretisierung des Umsetzungsplans der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrats hat die AG ISM die Richtlinie für Informationssicherheit in der öffentlichen Verwaltung (IS-LL) herausgegeben, in welcher zwingende Anforderungen an die IT-Sicherheit in der Freien Hansestadt Bremen definiert werden.

Zur Stärkung resilienter IT-Infrastrukturen in der öffentlichen Verwaltung wurden vier Punkte als maßgeblich herausgearbeitet, welche die Umsetzung der Bremischen Cybersicherheitsstrategie prägen und im Folgenden noch näher beschrieben werden:

- Verstärkung der bestehenden Strukturen (dezentrale ISMS, zentrales ISM) im Sinne eines gemeinsamen Informationssicherheitsmanagementsystems
- Stärkung der Analyse- und Reaktionsfähigkeit vor Ort
- Gemeinsame Abwehr von IT-Angriffen
- IT-Notfallmanagement

3.2.3.1 Etablierung von Informationssicherheitsmanagementsystemen (ISMS)

Ein Informationssicherheitsmanagementsystem ist ein Rahmenwerk zur Etablierung und Fortführung eines kontinuierlichen Prozesses zur Planung, Durchführung, Kontrolle und Verbesserung der Konzepte und Aufgaben, die auf die Wahrung der Ziele der Informationssicherheit in einer Institution gerichtet sind. Zur Wahrung der Ziele der Informationssicherheit ist es notwendig, ein angemessenes und ausreichendes Sicherheitsniveau umzusetzen und dieses zu erhalten. Das Informationssicherheitsmanagement dient der Steuerung von materiellen, konzeptionellen und menschlichen Ressourcen mit dem Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen der Verwaltungen und Kommunen des Landes Bremen zu schützen.

Im Land Bremen sind bereits verschiedene ISMS in den Ressorts sowie beim Magistrat der Stadt Bremerhaven etabliert worden beziehungsweise befinden sich gerade in der Planung- oder Implementationsphase. Der Unterstützung aller Akteur:innen bei der zügigen Implementation der ISMS zur Absicherung der IKT-Strukturen der Verwaltungen nimmt einen hohen Stellenwert ein und ist zentral, um das bestehende Angebot an Verwaltungsdienstleistungen noch attraktiver zu gestalten und die Handlungsfähigkeit der Verwaltung selbst bestmöglich abzusichern.

3.2.3.2 Stärkung der Analyse- und Reaktionsfähigkeit vor Ort

Die Verwaltungen von Ländern und Kommunen sind einer gestiegenen Bedrohungslage für informationstechnische Systeme ausgesetzt. Dies gilt auch für die Freie Hansestadt Bremen. Angriffe aus dem Cyberraum geschehen darüber hinaus oft überraschend und mit hoher Geschwindigkeit, sodass Zeit zum kritischen Faktor in der Schadensbegrenzung sowie Lagebewältigung geworden ist. Eine frühzeitige und regelmäßige Information über aktuelle Cybergefahren ist deshalb eine wichtige Grundlage für vorausschauende Sicherheitsplanung und lässt Raum für das Ergreifen möglicher Maßnahmen bei bekannten Gefährdungen. Weitere kritische Faktoren sind die Kenntnis über erforderliche Reaktionsprozesse sowie vorhandene Kapazitäten zur Vor-Ort-Unterstützung, sofern es zu einem Schadensfall gekommen ist. Die Stärkung des Informationsaustauschs sowie der Analyse- und Reaktionsfähigkeit vor Ort fällt im Rahmen der Strategieumsetzung eine wichtige Rolle zu. Insbesondere der Ausbau von landeseigenen Kapazitäten in der IT-Forensik leistet einen wichtigen Beitrag zur Vor-Ort-Unterstützung.

3.2.3.3 Gemeinsame Abwehr von IT-Angriffe

Durch die Einbindung der Freien Hansestadt Bremen in das Computer Emergency Response Team (CERT) Nord des IT-Dienstleisters Dataport sowie den Verwaltungs-CERT-Verbund (VCV) wird ein regelmäßiger Austausch über sicherheitskritische IT-Themen gewährleistet. Die Früherkennung von Sicherheitslücken und zielgerichteten Cyberangriffen ist in Hinblick auf die Zunahme professioneller und gezielter Angriffe auf die IT-Infrastruktur von besonderer Bedeutung. Hinweise auf Sicherheitslücken werden in diesem Zusammenhang als Indicators of Compromise (IoC) bezeichnet. IoC sind technische Informationen, die zur Detektion einer Infektion mit Schadsoftware oder einer anderweitigen Kompromittierung verwendet werden können. Ihr zentral gesteuerter und zeitnaher Versand ermöglicht es allen beteiligten Akteur:innen, frühzeitig Schutzmaßnahmen in den eigenen Netzwerken umzusetzen, sobald IoC bekannt werden. Eine besonders effektive Form der Steuerung von IoC-Listen ist die Bereitstellung über eine sogenannte Malware Information Sharing Platform (MISP). Die Steuerung von IoC wird zukünftig durch die noch auszugestaltende Zentralstelle für Cybersicherheit übernommen werden.

3.2.3.4 IT-Notfallmanagement

Ein vollumfänglicher Schutz von IT-Systemen kann nicht gewährleistet werden. Trotz der Einführung und Umsetzung zahlreicher Schutzmaßnahmen besteht immer ein gewisses Restrisiko, was vor allem darin begründet liegt, dass Angreifer Schwachstellen häufig zuerst entdecken. Umso wichtiger ist es daher, vorhersehbare Szenarien bereits frühzeitig zu beschreiben und abzustimmen, um im Notfall handlungsfähig zu bleiben.

Die bereits bestehenden Arbeitsstrukturen, die bei IT-Notfällen zum Einsatz kommen, werden perspektivisch von der Zentralstelle für Cybersicherheit zentralisiert und ausgebaut, sofern sie nicht den Zuständigkeitsbereich der Fachabteilung des Senators für Finanzen betreffen. In diesen Fällen wird eine enge Kooperation zwischen der Zentralstelle für Cybersicherheit und dem Senator für Finanzen sichergestellt.

Durch die Schaffung klarer Strukturen und die Benennung eines vorab definierten Kontakts in der Zentralstelle für Cybersicherheit erhalten alle staatlichen Akteur:innen in der öffentlichen Verwaltung im Land Bremen eine Ansprechstelle, an die sie sich bei Fragen rund um das IT-Notfallmanagement wenden und auch für ihren Organisationsbereich spezifische Fragen klären können. So wird eine vertrauensvolle Arbeitsbeziehung ermöglicht, in der die jeweiligen Besonderheiten der Ressorts oder des Magistrats der Stadt Bremerhaven bestmögliche Berücksichtigung finden.

Zielführende Aufgaben im Rahmen dieses Handlungsfelds sind beispielsweise die Etablierung von IT-Notfallmanagementsystemen, die Beratung bei der Planung und Durchführung von IT-Notfallübungen sowie die Notfall- und Krisenkommunikation.

Die Reaktionsfähigkeit der von einem Cyberangriff betroffenen Verwaltungsbereiche kann durch den zeitnahen Einsatz von Fachkräften in der IT-Forensik schnellstmöglich wiederhergestellt werden, welche zu diesem Zweck zeitnah verfügbar sein müssen.

Neben der Prävention von Cyberangriffen ist auch die strafrechtliche Reaktion hierauf ein wichtiges Element der Vorfallsbearbeitung nach einem IT-Sicherheitsvorfall, sofern ein krimineller Hintergrund nicht ausgeschlossen werden kann. Um eine reibungslose Strafverfolgung zu gewährleisten, wird ein enger Austausch zwischen der noch auszugestaltenden Zentralstelle Cybersicherheit, der zuständigen Polizeivollzugsbehörde und der Staatsanwaltschaft etabliert. Hierdurch werden Kommunikationsprozesse optimiert und es wird sichergestellt, dass die forensische Beweismittelsicherung auf dem neuesten Stand der Technik sowie entsprechend gültigen Rechtsvorschriften Anwendung findet.

Auch in diesem Zusammenhang ist die Verabschiedung des beabsichtigten Cybersicherheitsgesetzes für das Land Bremen geboten, um die Handlungskompetenzen und -verpflichtungen aller in diesem Zusammenhang handelnden Akteur:innen klar zu beschreiben.

Das IT-Notfallmanagement ist Teil des ganzheitlichen Notfall- oder Krisenmanagements und kann somit nicht isoliert betrachtet werden. Da sich eine Störung des IT-Betriebs auch auf weitere Bereiche der Verwaltungen von Ländern und Kommunen auswirken kann, ist perspektivisch die Implementation eines ganzheitlichen Business Continuity Management (BCM) in der Verwaltung nach einem zentralen Standard zielführend.

Mögliche Maßnahmen, um ein BCM in den Verwaltungsbereichen der Freien Hansestadt Bremen zu etablieren, werden im Rahmen der Strategiefortschreibung geprüft und konkretisiert.

3.2.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Zur Umsetzung der Ziele in diesem Handlungsfeld sind folgende Maßnahmen geplant:

Etablierung von Informationssicherheitsmanagementsystemen (ISMS)

- Unterstützung der Ressorts sowie des Magistrats der Stadt Bremerhaven beim Aufbau grundschutzkonformer Informationssicherheitsmanagementsysteme unter Berücksichtigung zur Verfügung stehender Vorgehensmodelle sowie des jeweiligen Planungs- und Implementationsstatus der betroffenen Akteur:innen

Stärkung der Analyse und Reaktionsfähigkeit vor Ort:

- Beratung aller Verwaltungsbereiche im Land Bremen über bestehende Strukturen zur Vor-Ort-Unterstützung
- Koordinierung des Ausbaus der bestehenden Strukturen und Kompetenzen in Abstimmung mit den unterschiedlichen Ressorts und Behörden der Freien Hansestadt Bremen durch die Zentralstelle für Cybersicherheit

Abwehr von IT-Angriffen:

- Sammlung und Versand von IoC-Listen durch die Zentralstelle für Cybersicherheit als Single Point of Contact im Land Bremen
- Prüfung der Möglichkeiten, an eine im Bundesgebiet bestehende MISP angeschlossen zu werden oder eine bremische MISP selbst aufzubauen
- Aufbau eines Kompetenznetzwerks bei der Zentralstelle für Cybersicherheit, um Ressourcen zur Unterstützung bei IT-Angriffen abrufen zu können

IT-Notfallmanagement:

- Zentralisierung und Ausbau der bestehenden Arbeitsstrukturen in der Zentralstelle für Cybersicherheit für das IT-Notfallmanagement, sofern diese nicht den Zuständigkeitsbereich der Fachabteilung des Senators für Finanzen betreffen
  - Beratung bei der Planung und Durchführung von IT-Notfallübungen
  - Beratung zur Notfall- und Krisenkommunikation
  - Aufbau eines Fachkräftepools zur IT-Notfallbewältigung
- Ausbau der Kooperation zwischen der Zentralstelle für Cybersicherheit und den zuständigen Stellen der Polizei Bremen, der Ortspolizeibehörde Bremerhaven sowie der Staatsanwaltschaft Bremen, um eine rechtssichere Strafverfolgung bei Cyberangriffen zu gewährleisten

3.3 Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden

Die Funktionsfähigkeit von Gefahrenabwehr-, Strafverfolgungs- sowie Verfassungsschutzbehörden stellt einen wesentlichen Eckpfeiler in der staatlichen Sicherheitsarchitektur dar. Um sich selbst sowie die Bevölkerung vor steigenden Gefahren des Cyberraums zu schützen, bedürfen Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden einer resilienten technischen Infrastruktur, digitaler Fachkompetenzen sowie ausreichender Handlungsbefugnisse. Auch muss der sichere Zugang zu aktuellen und verlässlichen Informationen sichergestellt werden, um angemessene strategische oder operative Entscheidungen im Rahmen der originären Zuständigkeiten treffen zu können.

3.3.1 Herausforderungen des Handlungsfelds

Der verlässliche Schutz der Grundrechte vor Gefahren aus dem In- und Ausland sowie die rechtssichere Verfolgung von Straftaten sowie die Aufrechterhaltung der nichtpolizeilichen Gefahrenabwehr stellen elementare Aufgaben des Staates dar, auf welche Bürger:innen vertrauen können müssen. Zur Erfüllung dieses Auftrags ist es erforderlich, dass der Staat die hierfür notwendigen Strukturen im Bereich der Gefahrenabwehr, der Strafverfolgung und des Verfassungsschutzes schafft.

Die Digitalisierung, Harmonisierung und Modernisierung bieten hierbei erhebliches Potenzial für die Verbesserung der Arbeit der Gefahrenabwehr-, Strafverfolgungs- sowie Verfassungsschutzbehörden.

So ermöglichen die fortschreitende Vernetzung und die Verfügbarkeit von mobilen Netzwerken (WLAN / 5G) neue Lösungsansätze in der Rettung von Menschenleben sowie der Einsatzunterstützung und Lagebewältigung. Neben der erhöhten Vernetzung von Einsatzmitteln und der Leitstelle, durch GPS-Integration und digitalen Funk, können heutzutage unbemannte Luftfahrtsysteme (Drohnen) für die Aufklärung kritischer Bereiche eingesetzt werden, die von Rettungskräften (noch) nicht betreten werden können. Die weitere Einführung von ITK-Systemen sowie ihre Vernetzung kann die Arbeit der o.g. Akteur:innen wesentlich beschleunigen, sodass Entscheidungen schneller getroffen werden können und die Effizienz gesteigert wird. Bereits auf der Anfahrt können Verletzte durch den Rettungsdienst bei den zentralen Notaufnahmen mit einer ersten Anamnese angemeldet werden, Warnmeldungen können schnell und effektiv an Bürger:innen im gefährdeten Bereich verbreitet oder Notrufe durch diese digital abgesetzt werden.

Im Bereich Brandschutz, Rettungsdienst und Katastrophenschutz hat die Transformation zum ganzheitlichen, interdisziplinären Krisenmanagement bereits begonnen. Die Notwendigkeit der Erzeugung von vernetzten aktuellen Lagebildern unter Einbeziehung externer und interner Datenquellen ist Voraussetzung für eine Lagebewältigung und daraus resultierende Einsatzmaßnahmen.

Allerdings ist die Implementierung von digitalen Technologien stets auch mit Risiken verbunden, da diese nicht vollständig abgesichert werden können und somit einen potenziellen Angriffsvektor darstellen.

So müssen die kritischen Prozesse der Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden, die zur Auftragserfüllung immanent wichtig sind, besonders abgesichert und vor Ausfällen geschützt werden. Dies betrifft beispielsweise die Handlungsfähigkeit der Leitstellen von Feuerwehren und Polizeien und des Katastrophenschutzes oder die Sicherstellung einer verschlüsselten Kommunikation und die Verfügbarkeit von Infor-

mationssystemen in der Gefahrenabwehr. Werden für digitale Prozesse keine ausreichende Ausfallsicherung sowie analoge Handlungsalternativen geschaffen, führt ein Ausfall der genutzten Systeme zwangsläufig zur Handlungsunfähigkeit der Akteur:innen.

Weiterhin sind Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden zur Umsetzung der Digitalisierung auf externe Dienstleister angewiesen, woraus sich erhöhte Anforderungen an die Datensicherheit und den Datenschutz ergeben. Bei der Verbesserung der Interoperabilität und Reaktionsfähigkeit müssen daher die fachlichen, technischen und personellen Kompetenzen, unter Beachtung der Zuständigkeiten der verschiedenen Behörden und der föderalen Strukturen, stets wirksam aufeinander abgestimmt werden.

Neben der Gewährleistung der eigenen Handlungsfähigkeit muss sichergestellt werden, dass die Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden auf die hohe Dynamik im Bereich der Cybersicherheit, sowohl präventiv als auch repressiv, national und international, vorbereitet sind und angemessen reagieren können.

Um auf durch den Cyberraum neu aufgetretene Deliktfelder angemessen reagieren zu können, bedarf es sowohl ausreichender materieller als auch personeller Ressourcen. Es muss sichergestellt sein, dass eine resiliente IT-Infrastruktur nicht nur etabliert, sondern von den Mitarbeiter:innen auch bedient werden kann. Darüber hinaus ist ein belastbarer sowie eindeutiger Rechtsrahmen zwingend erforderlich, innerhalb dessen die Gefahrenabwehr- und Strafverfolgungsbehörden agieren. Um sowohl organisatorische Anpassungen an die Arbeit in einer immer stärker digitalisierten Welt vorzunehmen als auch operativ auf aktuelle Cyberbedrohungen reagieren zu können, ist darüber hinaus ein koordinierter Informationsaustausch erforderlich, der alle Beteiligten – im Rahmen der verfassungsrechtlich vorgesehenen Grenzen – mit den für sie notwendigen Informationen versorgt.

3.3.2 Entwicklung von Cyberkriminalität und ihre Bekämpfung

Insbesondere die Strafverfolgungsbehörden werden durch die fortschreitende Digitalisierung vor neue Herausforderungen gestellt. Kriminelle im Cyberraum agieren immer professioneller, während die Fallzahlen seit vielen Jahren stark steigen (s. Abb. 9).

Straftaten, bei denen Kriminelle moderne Informationstechnik nutzen, werden zunächst ganz allgemein als Cyberkriminalität[40] (engl. *cyber crime*) bezeichnet. Cyberkriminalität ist zum Beispiel ein Betrugsversuch, der das potenzielle Opfer via E-Mail statt per Post erreicht. Im engeren Sinne umfasst der Begriff Cyberkriminalität Straftaten, die auf Computersysteme und Netzwerke selbst zielen. Dabei kann es sich auch um Cyber*spionage* oder Cyber*terrorismus* handeln.

Sowohl die stetige Digitalisierung als auch die erhöhte Sensibilisierung der Bürger:innen und die dadurch erhöhte Anzeigebereitschaft haben in den vergangenen Jahren zu einem stetigen Anstieg der Fallzahlen im Bereich der Cyberkriminalität geführt. Trotz dieses Anstiegs müssen Statistiken im Bereich der Cybersicherheit jedoch stets vorsichtig interpretiert werden, da aufgrund von Erfassungsmodi (z. B. keine Erfassung von Auslandsstraftaten), der Definition von Cybercrime (keine Erfassung von Ransomware-Angriffen) und eines erheblichen Dunkelfelds von über 90 Prozent die Aussagekraft der Zahlen stark eingeschränkt ist.

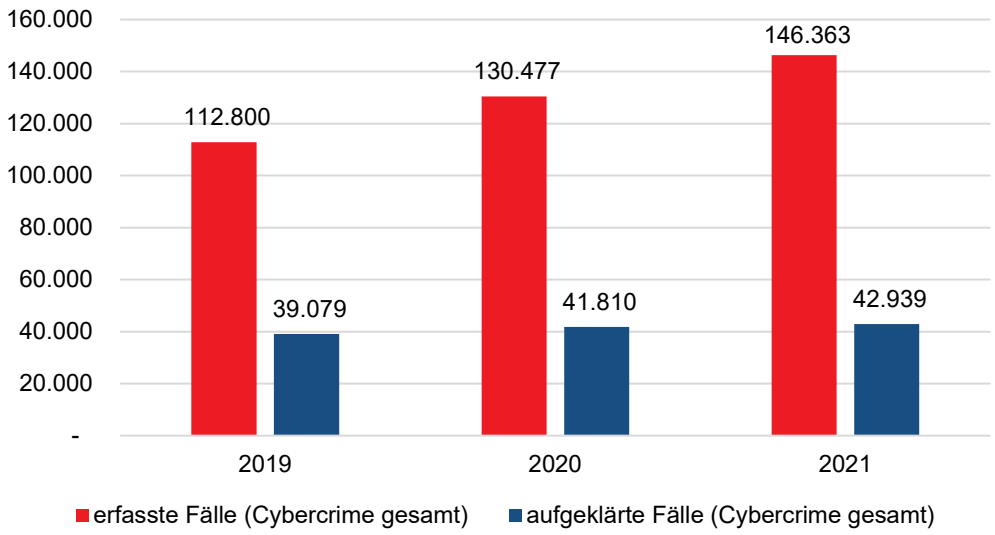


Abbildung 9 - Entwicklung der Fallzahlen im Bereich Cyberkriminalität

Durch den Erlass des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität[41] im Zusammenhang mit neuen Meldepflichten nach dem Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz, NetzDG)[42] ist davon auszugehen, dass Polizei und Justiz eine Vielzahl von im Internet begangenen Straftaten zusätzlich zu bearbeiten haben und die Fallzahlen somit weiter steigen werden.

Mit der professionellen Bekämpfung von Cybercrime steigen auch die Anforderungen an die IT-basierte Beweissicherung und an forensische Labore, die im Rahmen ihrer Arbeit digitale Asservate für eine spätere Auswertung in der Sachbearbeitung aufbereitet.

Die steigenden Fallzahlen und die Komplexität der Ermittlungsverfahren führen, neben der Arbeitsmehrung der Polizei, mittelbar auch zu einer steigenden Arbeitsbelastung der Staatsanwaltschaften und der Gerichte sowie dem Erfordernis, sich technischen Innovationen in immer kürzeren Zeiträumen anzupassen. Ebenfalls steigen die Anforderungen an die Aus- und Fortbildung der Mitarbeiter:innen bei Polizei und Justiz, um auf diese Entwicklungen reagieren zu können.

Um diesen Entwicklungen mit einem ganzheitlichen und flexiblen Bekämpfungsansatz zu begegnen, müssen Gefahrenabwehr- sowie Strafverfolgungsbehörden Hand in Hand arbeiten und Betroffenen eine niedrigschwellige Ansprechbarkeit ermöglichen.

Eine sehr effiziente Struktur hat sich hierfür mit den zentralen Ansprechstellen Cybercrime herausgebildet. Diese wurden bei allen Landespolizeien sowie dem Bundeskriminalamt (BKA) eingerichtet und stehen allen Unternehmen der deutschen Wirtschaft sowohl mit Informationen zur Vermeidung von Cyberangriffen als auch im Falle erfolgter Straftaten im Cyberraum als vertrauensvolle Ansprechstellen zur Verfügung.[43]

Werden Cyberangriffe durch stark organisierte und zum Teil staatlich finanzierte Gruppierungen durchgeführt, sind sowohl die Zielrichtung als auch das mögliche Schadensausmaß häufig deutlich erhöht. Versuchen kriminelle Gruppierungen an Wirtschafts- oder Staatsgeheimnisse zu gelangen, ist von Cyber*spionage* die Rede. Besteht das Ziel lediglich in der Beschädigung von privaten oder staatlichen (IT-)Infrastrukturen, wird in der Regel der Begriff Cyber*sabotage* verwendet.

Für die nachrichtendienstliche Cyberabwehr arbeiten in Deutschland die Landesämter für Verfassungsschutz im Rahmen des Verfassungsschutzverbunds[44] eng mit dem Bundesamt für Verfassungsschutz (BfV) zusammen. Kernaufgaben sind hier die Detektion, die Attribution sowie die Prävention von Cyberangriffen.

Basis und gleichzeitig Ergebnis der sorgfältigen Analysearbeit sind operative sowie strategische Lagebilder, welche fortwährend erstellt und im Rahmen des verfassungsrechtlich abgesicherten Informationsaustauschs zwischen den unterschiedlichen Behörden geteilt werden.

Zu den öffentlichen Lagebildern zählen beispielsweise das jährlich veröffentlichte Bundeslagebild Cybercrime[45] des BKA sowie die „Cyber-Briefe“[46] des BfV. Das BSI gibt ebenfalls jährlich einen Bericht zur Lage der IT-Sicherheit in Deutschland[47] heraus. Darüber hinaus findet innerhalb der etablierten Strukturen und Netzwerke sowie im Rahmen der verfassungsrechtlichen Vorgaben ein Austausch von strategischen und operativen Lagebildern statt, welche Gefahrenabwehr- und Strafverfolgungsbehörden in die Lage versetzen, auf erkannte Entwicklungen zu reagieren.

Ebenfalls wird so eine Grundlage für die gemeinsame Entwicklung von Präventionsansätzen geschaffen, um die Anzahl sowie das Schadensausmaß von Cyberangriffen einzudämmen.

3.3.3 Schutz vor und Bekämpfung von Cyberkriminalität in der Freien Hansestadt Bremen

In der Freien Hansestadt Bremen sorgen die Gefahrenabwehr- und Strafverfolgungsbehörden sowie das Landesamt für Verfassungsschutz täglich für die Sicherheit der Bevölkerung. Auch sie befinden sich in dem Spannungsfeld, Kernaufgaben und Prozesse digital und somit effizient abzubilden und sich gleichzeitig vor den hierdurch entstehenden Risiken durch Cyberkriminalität bestmöglich zu schützen.

Da die Sicherstellung der Handlungsfähigkeit von Gefahrenabwehr- und Strafverfolgungsbehörden mit Blick auf Cyberangriffe vor allem durch hohe Standards in der IT-Sicherheit erreicht werden kann, liegt ein Fokus der Bremischen Cybersicherheitsstrategie auf der Stärkung und dem Ausbau der bisherigen Maßnahmen zur Etablierung von ISMS in den einzelnen Verwaltungsbereichen (s. Kap. 3.3.4.1 sowie Kap. 3.2.3). Der Umsetzungsstand hierbei ist sehr heterogen. Diese Bewertung bezieht sich sowohl auf den Fortschritt bei der Implementierung von ISMS als auch auf die Ausgestaltung des für einen bestimmten Verwaltungsbereich gewählten ISMS selbst. Ein regelmäßiger Austausch findet über die AG ISM beim Senator für Finanzen statt, in welcher die Informationssicherheitsbeauftragten der Ressorts sowie des Magistrats der Stadt Bremerhaven vertreten sind. Aufgrund begrenzter personeller Kapazitäten kann hier jedoch keine umfassende Beratung oder Begleitung der einzelnen Teilnehmenden erfolgen, die perspektivisch jedoch als sehr zielführend erachtet wird.

Bei der Bekämpfung von Cyberkriminalität in der Freien Hansestadt Bremen nehmen vorrangig die Polizeivollzugsbehörden, also die Polizei Bremen, die Ortspolizeibehörde Bremerhaven und das Landeskriminalamt, sowie die Staatsanwaltschaft eine zentrale Rolle ein.

3.3.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Die zwei Hauptziele der Bremischen Cybersicherheitsstrategie für den Bereich der Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden liegen einerseits in der Stärkung ihrer Resilienz gegenüber Cyberbedrohungen sowie anderseits in der Weiterentwicklung eines ganzheitlichen Ansatzes zur Bekämpfung von Cyberkriminalität.

3.3.4.1 Stärkung der Resilienz gegenüber Cyberbedrohungen

Wichtige Maßnahmen zur Stärkung der Resilienz gegenüber Cyberbedrohungen bei staatlichen Stellen sind im Kern bereits in Handlungsfeld 2 beschrieben worden. Die Besonderheit dieses Handlungsfelds besteht daher vor allem in den unterschiedlichen Anforderungen, die teilweise an die betroffenen Akteur:innen dieses Handlungsfelds gestellt werden. So sind diese höchst unterschiedlich organisiert und müssen darüber hinaus verschiedene technische oder organisatorische Standards erfüllen, die sich aus ihren originären Kompetenzen ergeben. Eine individuelle Betrachtung und Betreuung mit Blick auf die Etablierung von IT-Sicherheitsstandards sowie perspektivisch IT-Notfallmanagementkonzepten, in Ergänzung zu den bisher existierenden Strukturen, ist daher unvermeidbar, beispielsweise mit Blick auf Polizei- oder Feuerwehrleitstellen.

Diese Betreuungs- und Beratungsleistung soll, ergänzend zur AG ISM und in enger Absprache mit der Fachabteilung beim Senator für Finanzen, bei der Zentralstelle für Cybersicherheit etabliert werden. So wird eine zentrale Anlaufstelle geschaffen, bei der sich alle Gefahrenabwehr- und Strafverfolgungsbehörden in der Freien Hansestadt Bremen über die Erhöhung ihrer eigenen Resilienz gegenüber Cyberangriffen beraten und unterstützen lassen können. Gleichzeitig wird es so möglich, einen zentralen Überblick über die Umsetzungsfortschritte zu gewinnen.

Da das unbeabsichtigte Fehlverhalten von Mitarbeiter:innen (z. B. durch das versehentliche Ausführen von Schadcode in einer E-Mail) häufig das Einfallstor für einen Cyberangriff darstellt, fällt der Zielgruppe der Mitarbeiter:innen in staatlichen Einrichtungen und Organisationen ein besonderes Augenmerk zu. Ihre gezielte Schulung (vgl. Handlungsfeld 7) leistet einen maßgeblichen Beitrag zur Stärkung der Resilienz der jeweiligen Einrichtung gegenüber Cyberangriffen und stellt somit eine wichtige Ergänzung zu technischen oder organisatorischen Sicherheitsvorkehrungen dar. Die vorhandenen Schulungsangebote sollen zielgruppenorientiert ausgebaut werden.

Um den Erfolg dieser Maßnahmen sicherzustellen, sind ausreichende personelle und technische Ressourcen sowohl bei den beratenden als auch implementierenden Stellen erforderlich. Das umfasst auch die wiederkehrende Schulung der Mitarbeiter:innen sowohl hinsichtlich einer grundsätzlichen Sensibilisierung gegenüber Cybergefahren als auch im Speziellen in Bezug auf das Verhalten bei IT-Notfällen.

Resilienz gegenüber Cyberbedrohungen

- Einführung grundschutzkonformer ISMS sowie perspektivisch der Auf- und Ausbau von IT-Notfallvorsorgekonzepten bei den Gefahrenabwehr- und Strafverfolgungsbehörden sowie dem Verfassungsschutz zur Stärkung der Resilienz gegenüber Cybergefahren
- Flächendeckende Umsetzung größtmöglicher IT-Sicherheitsstandards sowie perspektivisch die Etablierung von IT-Notfallmanagementkonzepten unter Berücksichtigung der jeweiligen Besonderheiten der Gefahrenabwehr- und Strafverfolgungsbehörden sowie des Verfassungsschutzes
- Ergänzende Betreuung und Beratung der in diesem Handlungsfeld betroffenen Akteur:innen durch die Zentralstelle für Cybersicherheit bei der Umsetzung der o.g. Maßnahmen

3.3.4.2 Ganzheitliche Bekämpfung von Cyberkriminalität

Die Bekämpfung von Cyberkriminalität muss stets einen ganzheitlichen Ansatz verfolgen. In diesem fällt der Prävention und Detektion (Entdeckung) eine ebenso große Rolle zu wie der Strafverfolgung.

Prävention und Detektion

Das vorrangige Ziel von Prävention besteht darin, Gefahren abzuwehren, bevor ein Schaden eintritt. Zu diesem Zweck sollen Präventionsmaßnahmen im Bereich der Cyberkriminalität gestärkt und ausgebaut werden. Hierbei stellt die polizeiliche Kriminalprävention nur einen Eckpfeiler einer Präventionsstrategie dar, die eng mit den Ansätzen der Stärkung zur digitalen Kompetenz überlappt. Um bestmögliche Synergieeffekte zu erreichen, sollen die verschiedenen auf diesem Gebiet tätigen Akteur:innen in der Freien Hansestadt Bremen identifiziert und stärker vernetzt werden. So kann beurteilt werden, in welchen Bereichen zusätzliche Maßnahmen erforderlich sind oder weitere Ressourcen benötigt werden.

Gleichermaßen ist es bedeutsam, Gefahren früh im Rahmen der Detektion zu erkennen, da ein Schadenseintritt so häufig frühzeitig bemerkt oder sogar abgewendet werden kann. Gleichermaßen stellt die dann folgende Attribution, also die Zuordnung von Angriffen zu kriminellen Gruppierungen, einen wesentlichen Baustein in der Strafverfolgung dar. Hier arbeiten Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden innerhalb verfassungsrechtlicher Schranken Hand in Hand. Ein wichtiger Baustein für die erfolgreiche Prävention und Detektion sowie Attribution von Cyberangriffen ist das Erstellen aktueller operativer sowie strategischer Lagebilder.

Strafverfolgung

Die Ermittlung in Fällen von Cyberkriminalität stellt hohe Anforderungen an die Fachkenntnisse sowie die technischen Möglichkeiten, auf welche Ermittler:innen für eine beweissichere Strafverfolgung zurückgreifen müssen. Modi Operandi von Cyberkriminellen verändern sich schnell. Ebenso wird täglich neue Schadsoftware entdeckt, welche von Cyberkriminellen programmiert (oder über Dritte eingekauft) wird. Gleichzeitig finden Kriminelle immer wieder neue Wege, ihre digitalen Spuren zu verschleiern. In der Konsequenz müssen Ermittler:innen mit den gleichen technischen Möglichkeiten ausgestattet sein und über ausreichende Fachkenntnisse verfügen, um erfolgversprechende Ermittlungen im digitalen Raum aufzunehmen.

Um den stetig wachsenden technischen Möglichkeiten krimineller Aktivitäten im Internet zu begegnen und von diesen nicht abgehängt zu werden, müssen Strafverfolgungsbehörden mit ausreichenden personellen sowie technischen Ressourcen ausgestattet sein. Ein wichtiger Schritt zur effektiven Bekämpfung der Cyberkriminalität besteht daher in der regelmäßigen Prüfung, ob den Anforderungen des Deliktsbereichs mit den aktuellen Strukturen begegnet werden kann, sowie einer konsequenten Bereitstellung der erforderlichen Ressourcen in Form von besonderer Expertise, wenn Defizite erkannt werden.

Ganzheitliche Bekämpfung von Cyberkriminalität

Prävention und Detektion

- Identifikation der auf den verschiedenen Gebieten der Prävention tätigen Akteur:innen und deren Vernetzung unter Federführung der Zentralstelle für Cybersicherheit unter Berücksichtigung von möglichen Synergieeffekten sowie einem effektiven Ressourceneinsatz

- Identifikation und Bewertung der bestehenden Schulungsangebote für Mitarbeitende in staatlichen Einrichtungen durch die Zentralstelle für Cybersicherheit

    - Prüfung, inwieweit ein zielgruppenorientierter Ausbau der Schulungsangebote erforderlich und möglich ist

- Regelmäßige Bewertung der personellen und technischen Kapazitäten beim Landesamt für Verfassungsschutz für die Detektion und Attribution von Cyberangriffen um eine frühzeitige Reaktion an sich ändernde Bedarfe zu ermöglichen.

Strafverfolgung

- Regelmäßige Bewertung g der personellen und technischen Kapazitäten der Strafverfolgungsbehörden zur effektiven Bekämpfung der Cyberkriminalität, um eine frühzeitige Reaktion an sich ändernde Bedarfe zu ermöglichen.

3.4 Wirtschaft und KRITIS

Cyberangriffe stellen sowohl für kleine und mittelständische Unternehmen (KMU) als auch für große Unternehmen ein herausragendes Sicherheitsrisiko dar. Angriffe auf die IT-Struktur des Unternehmens können zu existenzbedrohenden wirtschaftlichen Folgen führen. Gleichermaßen besteht bei Cyberangriffen auf ein Unternehmen das Risiko von Produktions- oder Dienstleistungsausfällen, die Nutzer:innen empfindlich treffen können. Insbesondere Unternehmen, die gemäß BSI-KritisVerordnung (BSI-KritisV) als Betreibende kritischer Infrastrukturen einzustufen sind, fällt hier eine besondere Bedeutung zu. Doch auch unterhalb der gesetzlich definierten KRITIS-Schwelle existieren systemrelevante Unternehmen mit herausragender Bedeutung für die Daseinsvorsorge oder für die Wirtschaftsstandorte Bremen und Bremerhaven, deren Ausfall zu erheblichen Beeinträchtigungen des Alltags in der Bevölkerung führen kann, etwa die für die Wirtschaftsregion NordWest besonders relevanten Hafenanlagen in der Freien Hansestadt Bremen. Für diese systemrelevanten Unternehmen existiert jedoch aktuell kein Standard unterhalb der KRITIS-Definition des BSI, sodass eine einheitliche Identifikation bisher nicht möglich war.

3.4.1 Herausforderungen des Handlungsfelds

Die Zukunft des Wirtschaftsstandortes Deutschland und somit auch des Landes Bremen wird in einem hohen Maße durch die Digitalisierung beeinflusst. Hierbei sind funktionsfähige und sichere IKT-Systeme und Dienstleistungen eine wesentliche Voraussetzung, sowohl für den Betrieb kritischer Infrastrukturen als auch die Wertschöpfung bei kleinen und mittleren Unternehmen.

Welche Einrichtungen, Anlagen oder Teile wegen ihrer Bedeutung für die Versorgung der Bevölkerung und damit für das Funktionieren des Gemeinwesens als Kritische Infrastrukturen im Sinne des BSI-Gesetzes (BSIG) gelten, wird durch die BSI-KritisV definiert. Ob ein bedeutender Versorgungsgrad vorliegt, ist vom Erreichen oder Überschreiten von in der BSI-KritisV aufgeführten Schwellenwerten abhängig. Werden diese Schwellenwerte erreicht oder überschritten, gelten für KRITIS-Betreiber die gesetzlichen Melde- und Nachweispflichten des BSIG.[48]

Um ihre jeweiligen Dienstleistungen zu erbringen, setzen KRITIS-Betreibende hochkomplexe und stark vernetzte Infrastrukturen ein. Sie sind hierbei in besonderem Maße auf störungsfrei arbeitende IKT-Systeme angewiesen. Eine Störung oder der Ausfall kritischer Infrastrukturen kann längerfristig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder anderen negativen Auswirkungen zur Folge haben.

Doch auch Unternehmen und Betriebe, welche die Schwellenwerte der BSI-KritisV nicht überschreiten und somit nicht unter die KRITIS-Regulierung fallen, können essenziell für die (regionale) Daseinsvorsorge sein und müssen vor Cyberangriffen geschützt werden.

Nach Angaben des Bundesverbands für mittelständische Wirtschaft (BVMW) sind 99,3 Prozent aller Unternehmen in Deutschland kleine und mittelständische Unternehmen. Der jährliche Exportumsatz von mittelständischen Unternehmen beträgt über 200 Milliarden Euro, darüber hinaus entfallen 60 Prozent der Nettowerkschöpfung auf KMU.[49] Viele KMU sind hochspezialisiert und Weltmarktführer auf ihrem Gebiet, auf deren Produkte oder Dienstleistungen Großunternehmen angewiesen sind. Sie leisten somit einen wesentlichen Beitrag zu weltweiten Lieferketten.

Aufgrund geringerer finanzieller und personeller Ressourcen ist die digitale Verwundbarkeit von KMU jedoch häufig noch höher als die großer Unternehmen. Dies hat zur Folge, dass die Gefahr von erfolgreichen Cyberangriffen gegenüber KMU steigt.

Gleichzeitig ist es möglich, dass der Schaden in Folge eines Cyberangriffs nicht immer und nicht unmittelbar ersichtlich wird. Letztlich fehlt KMU häufig das Wissen, an wen sie sich im Fall eines Cyberangriffs wenden können.

Der Umgang mit Cyberangriffen stellt für Unternehmen immer eine besondere Herausforderung dar, da mit Bekanntwerden des Cyberangriffs das Vertrauen der Kund:innen in das Unternehmen oder seine Reputation beschädigt werden.

Cyberangriffe gegenüber Unternehmen können verschieden motiviert sein. So kann der Angriff auf kritische Infrastrukturen das Ziel verfolgen, gesamtgesellschaftlichen Schaden zu verursachen oder politische Instabilität hervorzurufen. Breite Angriffe mit zufällig ausgewählten Zielen und dem Einsatz von Ransomware zielen hingegen regelmäßig auf wirtschaftlichen Profit, etwa durch das Zahlen von Lösegeldern („Ransom“), ab. Darüber hinaus können die IT-Systeme von Unternehmen im Rahmen der Wirtschaftsspionage oder -sabotage infiltriert werden, um Firmengeheimnisse zu stehlen oder Dateien zu beschädigen. Die Bandbreite verantwortlicher Akteur:innen reicht von Einzelpersonen über kriminelle Gruppierungen bis hin zu staatlichen oder staatlich unterstützten Akteur:innen.

Mit ihren begrenzten personellen oder finanziellen Ressourcen stellen KMU darüber hinaus attraktive Einfallstore für Cyberkriminelle dar, die sich über die IT-Systeme des KMU an ihr eigentliches Ziel vorarbeiten, etwa einen durch technische Systeme verbundenen Großunternehmer, welchem das KMU zuliefert.

Eine zentrale Herausforderung für Unternehmen und Einrichtungen des KRITIS-Sektors sowie für KMU ist daher die Steigerung ihrer Cyberresilienz. Hierzu bedarf es sowohl präventiver Sicherheitsmaßnahmen wie auch der Kapazitäten und des Know-hows, auf Cyberangriffe zu reagieren, um die Funktionsfähigkeit zentraler Prozesse und Infrastrukturen selbst unter außergewöhnlichen Umständen aufrecht zu erhalten und zu sichern.

3.4.2 KRITIS-Regulierungen auf Bundesebene und perspektivische Entwicklung

KRITIS-Betreiber, die gem. BSI-KritisV einen bedeutenden Versorgungsgrad erreichen, sind gesetzlich verpflichtet, Maßnahmen zur Prävention (§ 8a BSIG) und zur Bewältigung von IT-Sicherheitsvorfällen oder IT-Störungen (§ 8b BSIG) zu implementieren. Auch sind sie dazu verpflichtet, bestimmte Informationen an das BSI melden und Registrierungspflichten nachzukommen.

Dies führt in der Konsequenz dazu, dass alle Unternehmen, welche zwar kritische Dienstleistungen im Sinne der Definition erbringen, jedoch die definierten Schwellenwerte nicht erfüllen, keinen Meldeverpflichtungen nachkommen müssen.

Sie können jedoch freiwillig an der Kooperation „Umsetzungsplan KRITIS“ (UP KRITIS) teilnehmen.

Bei UP KRITIS handelt es sich um eine öffentlich-private Kooperation zwischen KRITIS-Betreibenden, deren Verbänden und den zuständigen staatlichen Stellen. Die Mitglieder des UP KRITIS erarbeiten strategisch-konzeptionelle Ziele und Projekte. Dies geschieht durch die Teilnahme an brancheninternen bzw. branchenübergreifenden Arbeitskreisen. Das Ziel des UP KRITIS besteht darin, die Versorgung mit Dienstleistungen Kritischer Infrastrukturen in Deutschland aufrechtzuerhalten. Hierbei werden acht von neun Sektoren adressiert. Ausgenommen ist der Sektor „Staat und Verwaltung“, welcher durch den Umsetzungsplan BUND (UP BUND) sowie Aktivitäten auf Länder- und Kommunalebene abgedeckt wird.[50]

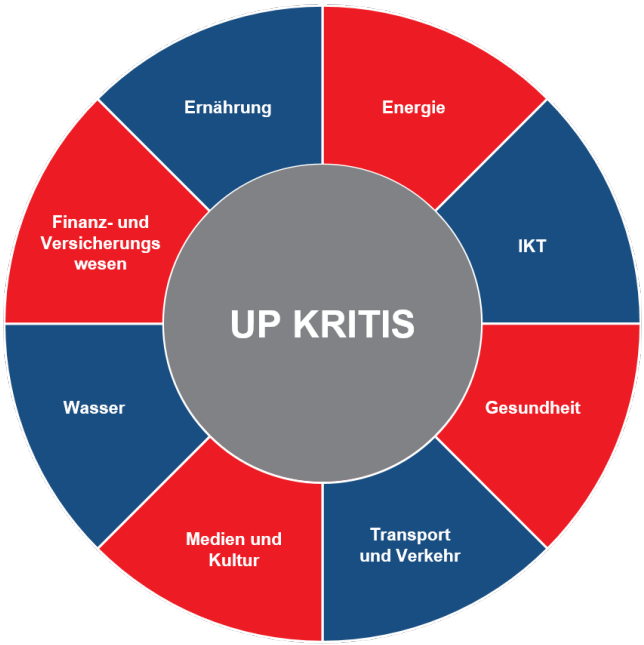


Abbildung 10 - UP KRITIS Sektoren

Eine neue Herausforderung im Umgang mit kritischen Infrastrukturen ergibt sich durch die NIS-2-Richtlinie der Europäischen Union. Im Dezember 2022 haben der Rat und die Europäische Kommission die „*Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union*“ verabschiedet, die von den Mitgliedstaaten bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden muss.

Die sogenannte NIS-2-Richtlinie löst die bisherige NIS-Richtlinie aus dem Jahr 2016 ab und soll zu einem einheitlichen Sicherheitsniveau in der Union beitragen. Hintergrund ist die erhöhte Bedrohungslage und die damit einhergehenden besonderen Anforderungen an die Cybersicherheit.

Wesentlichen Neuerungen sind unter anderem Mindestanforderungen an das IT-Sicherheitsmanagement betroffener Einrichtungen, wie die Pflicht zur Schaffung von Risikoanalyse- und Sicherheitskonzepten, die Pflicht zur Nutzung von Systemen zur Angriffserkennung und umfangreiche Meldepflichten bei Sicherheitsvorfällen. Daneben wurde der Anwendungsbereich erheblich erweitert, sodass nun nicht mehr Einrichtungen kritischer Infrastruktur von der Richtlinie erfasst werden, sondern auch KMU, welche vorab definierte Schwellenwerte nicht erreicht hatten, sobald sie sogenannten „wesentlichen“ oder „wichtigen“ Sektoren zugeordnet werden können. Insbesondere ist nun erstmals auch die öffentliche Verwaltung auf zentraler und regionaler Ebene von der Richtlinie betroffen.

Die NIS-2-Richtline unterscheidet zwischen „wesentlichen“ und „wichtigen“ Sektoren. Insgesamt handelt es sich hierbei um 18 Sektoren, die als kritische Infrastruktur eingestuft werden (S. Tab. 1). Weiterhin werden in der NIS-2-Richtlinie neue Schwellenwerte festgelegt, ab denen Unternehmen oder Betreiber der o.g. Sektoren Cybersicherheitsmaßnahmen implementieren und umsetzen müssen. Diese Schwellenwerte sind weitaus geringer als die der BSI-KritisV. Somit wird die Anzahl der Unternehmen und Betriebe, die gesetzlich dazu verpflichtet sind Cybersicherheitsmaßnahmen zu implementieren, ansteigen.

Tabelle 1 - Wesentliche und wichtige Sektoren gem. NIS-2

Wesentliche Sektoren	Wichtige Sektoren
▪ Energie ▪ Transport ▪ Banken ▪ Finanzmärkte ▪ Gesundheit ▪ Trinkwasser ▪ Abwasser ▪ Digitale Infrastruktur ▪ ICT Service Management (Unterstützung von Geschäftsprozessen durch IT) ▪ Öffentliche Verwaltung ▪ Raumfahrt (Bodeninfrastruktur)	▪ Post und Kurier ▪ Abfallwirtschaft ▪ Chemikalien ▪ Ernährung ▪ Industrie ▪ Digitale Dienste ▪ Forschung (Forschungsinstitute)

Für die Umsetzung der NIS-2-Richtlinie sind die EU-Mitgliedstaaten nicht nur verpflichtet, eine nationale Cybersicherheitsstrategie zu erlassen, sie müssen daneben weitere Maßnahmen treffen. Unter anderem sollen zuständige nationale Behörden benannt oder eingerichtet werden, die mit diversen Befugnissen ausgestattet sein sollen. Diese Behörden sollen die Umsetzung und Einhaltung der Richtlinie überwachen, kontrollieren und bei Nichtbeachtung auch die entsprechenden Einrichtungen sanktionieren.

3.4.3 Sachstand in der Freien Hansestadt Bremen

Unklar ist bislang, wie die neuen Anforderungen der NIS-2-Richtlinie in föderalen Mitgliedstaaten wie der Bundesrepublik Deutschland umgesetzt werden. Jedoch ist damit zu rechnen, dass neben einer bundesweiten zentralen Anlaufstelle auch in den Ländern zuständige Behörden eingerichtet werden müssen. Bislang existiert in der Freien Hansestadt Bremen eine solche Behörde nicht.

Daneben sieht die Richtlinie eine weitere Verpflichtung vor, die Auswirkungen auf die Landesebene hat. In der Richtlinie werden die betroffenen privaten und öffentlichen Einrichtungen in *wesentliche* Einrichtungen (hohe Kritikalität) und *wichtige* Einrichtungen (sonstige kritische Sektoren) unterteilt. In diesem Zusammenhang sollen die Mitgliedstaaten bis zum 17.05.2025 eine Liste der wesentlichen und wichtigen Einrichtungen übermitteln. Diese Liste soll sodann mindestens alle zwei Jahre kontrolliert und gegebenenfalls aktualisiert werden. Sie soll nach ersten Informationen zwar bei dem Bundesamt für Sicherheit in der Informationstechnik geführt werden, allerdings müssen die Länder die entsprechenden Informationen an das BSI melden. Im Ergebnis wird damit auch die Freie Hansestadt Bremen die wesentlichen und wichtigen Einrichtungen identifizieren müssen.

Im Land Bremen fallen derzeit 15 Betriebe und Einrichtungen unter die BSI-KritisV. (Die Liste dieser Unternehmen ist als „Verschlusssache – Nur für den Dienstgebrauch“ eingestuft). Weitere 13 Betriebe erreichen zwar formal nicht die Schwellenwerte, haben aber eine so große lokale Bedeutung, dass ein Ausfall schwerwiegende Auswirkungen hätte. Weiterhin sind die Häfenstrukturen im Land Bremen hervorzuheben. Gemessen am jährlichen Containerumschlag belegte Bremerhaven im europäischen Ranking der größten Häfen im Jahr 2021 Platz 6.[51] Die Bedeutung der Häfenanlagen im Land Bremen, nicht nur für die Wirtschaftsregion, sondern für den gesamten europäischen Bereich, wird so deutlich.

Hinzu kommen zahlreiche weitere Betriebe und Einrichtungen, die eine wichtige Bedeutung für das staatliche Gemeinwesen haben und bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen in der Freien Hansestadt Bremen oder der Wirtschaftsregion Nordwest eintreten würden.

Das durch die NIS-2-Richtlinie ausgelöste Erfordernis, eine zentrale Stelle im Land zu schaffen und einen deutlich erweiterten Kreis von Unternehmen und Einrichtungen zu identifizieren, die im Sinne der Richtlinie identifiziert werden müssen, deckt sich mit dem bereits existenten Bedarf einer umfassenderen Übersicht im Land über Unternehmen und Einrichtungen, die bisher von der BSI-KritisV nicht erfasst wurden. Durch den in der NIS-2-Richtlinie vorgeschriebenen Lieferkettenschutz, welchen der Bund nur mithilfe der Länder umsetzen können wird, wird dieser Notwendigkeit zusätzliches Gewicht verliehen.

Neben der allgemeinen Melde- und Kontrollverpflichtung aufgrund europäischen und nationalen Rechts besteht im Land Bremen der Anspruch, in einen konstruktiven Austausch über das Thema Cybersicherheit mit Unternehmen und Einrichtungen aller Größenordnungen zu gehen.

Zur Orientierung der Bremerhavener Wirtschaft in diesem Themenfeld ist die Einstellung eines Digital-Lotsen zum 01.02.2023 bei der Wirtschaftsförderungsgesellschaft BIS erfolgt. Die Aufgabe des Digital-Lotsen ist die Unterstützung von IT-anwendenden Unternehmen in allen Fragestellungen der Digitalisierung, das heißt Aufbau von Online-Shops, Hardware-Anwendungen und auch Cyber-Sicherheitsfragen.

Um diese Ziele zu erreichen, ist die Gründung eines IT-Kompetenznetzwerks in Bremerhaven vorgesehen. In diesem Netzwerk sollen sowohl IT-Unternehmen, aber auch die für die IT in Dienstleistungs- und verarbeitenden Unternehmen zuständigen Personen (Administratoren) zusammengeführt werden, um unter anderem die Bedarfe der Anwendungsunternehmen zu ermitteln, aber auch die Kompetenz der IT-Unternehmen in Bremerhaven sichtbarer werden zu lassen.

Es sollen Arbeitsgruppen zu verschiedenen Themenstellungen einberufen werden, so zum Beispiel auch zum Thema Cybersicherheit. Hier sollen Beratungsangebote durch hiesige Unternehmen, aber gegebenenfalls auch durch externe Expert:innen etabliert werden. Dieses Netzwerk wird auch den wissenschaftlichen Einrichtungen Bremerhavens zur Verfügung stehen.

Darüber hinaus existieren weitere Strukturen, die Beratungs- und Informationsangebote zum Thema Cybersicherheit und digitale Transformation anbieten. Eine (nicht abschließende) Auswahl möglicher Ansprechstellen im Land Bremen umfasst:

- Zentrale Ansprechstelle Cybercrime (ZAC) des LKA Bremen
- Transferstelle IT-Sicherheit im Mittelstand (TISiM)
- Mittelstand 4.0-Kompetenzzentrum Bremen
- Maritimes Cluster Norddeutschland e. V.
- Freies Institut für IT-Sicherheit (ifit) e. V.
- Bremerhavener Gesellschaft für Investitionsförderung und Stadtentwicklung mbH (BIS)

Auch im Rahmen des Maßnahmenpakets „Bremen Digital 2019 bis 2021“ wurde das Thema Cybersicherheit durch den Senat berücksichtigt. So wurden in diesem Rahmen diverse Veranstaltungsformate, wie Live-Hackings, Innovationsforen und Informationsveranstaltungen, mit dem Schwerpunkt „Cybersicherheit in der Wirtschaft“ geplant, um das

Know-how von Instituten und Unternehmen in Bremen und Bremerhaven zur IT- und Datensicherheit zugänglich zu machen.[52]

Ein wichtiges Ziel besteht darin, den bereits sehr guten Austausch zwischen staatlichen Stellen und Wirtschaftsunternehmen im Land Bremen zu stärken und weiter auszubauen, etwa durch die Organisation themenspezifischer Veranstaltungen, Symposien, digitaler Stammtische oder Innovationsforen. Die noch auszugestaltende Zentralstelle für Cybersicherheit wird hier perspektivisch den Auf- und Ausbau des landesweiten Netzwerks unterstützen.

3.4.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Um die beschriebenen Herausforderungen zu bewältigen, wurden folgende Maßnahmen bei der Erstellung der Bremischen Cybersicherheitsstrategie 2023 identifiziert:

- Übernahme der Zentralstellenfunktion für das Land Bremen durch die Zentralstelle für Cybersicherheit
- Enger Austausch der noch auszugestaltenden Zentralstelle für Cybersicherheit mit Arbeitskreisen und Netzwerken der Betreiber:innen kritischer Infrastrukturen
- Prozessentwicklung bezüglich der sich aus der NIS-2-Richtlinie ergebenden Anforderungen
    - Identifikation der durch die NIS-2 Richtlinie betroffenen Einrichtungen
    - Hiernach Einstufung der Einrichtungen in wesentliche und wichtige Einrichtungen gemäß der NIS-2 Richtlinie
    - Benennung und / oder Schaffung zuständiger Stellen zur Umsetzung und Überwachung der betroffenen Einrichtungen
- Erarbeitung eines Bremischen Cybersicherheitsgesetzes zur Regelung der behördlichen Zuständigkeiten, welche sich aus der NIS-2-Richtlinie ergeben
- Ausbau von Ansprechstellen und Beratungsangeboten zum Thema Cybersicherheit für KMU im Rahmen eines IT-Kompetenznetzwerks für Bremen und Bremerhaven
- Förderung der Vernetzung von Akteur:innen aus Staat und Wirtschaft, etwa durch die Etablierung bewährter moderner Kommunikationsformate, zum Beispiel „digitaler Stammtische“

3.5 Förderung der digitalen Kompetenzen

Die fortschreitende Digitalisierung hat Einzug in viele Lebensbereiche erhalten. Während digitale Anwendungen und Endgeräte von vielen Nutzer:innen positiv betrachtet und gerne genutzt werden, sind sie sich der hiermit einhergehenden spezifischen Risiken häufig nicht oder nur unzureichend bewusst. Hierdurch steigt die Gefahr, dass Anwender:innen zu Opfern im oder im Zusammenhang mit dem Cyberraum werden. Das erfolgreiche Navigieren durch eine digitale Welt stellt erhöhte Anforderungen an die digitalen Kompetenzen der Nutzer:innen. Je nach Alters- und Zielgruppe existieren spezifische Risiken, vor denen sich Nutzer:innen gezielt schützen müssen. Hierbei gilt es, besonders verwundbare Zielgruppen zu identifizieren und diese mit besonderen Maßnahmen im Rahmen einer geschlechter- und vielfaltssensiblen Förderung ihrer digitalen Fähigkeiten zu kompetenten Nutzer:innen digitaler Anwendungen und Endgeräte zu machen. Einen Orientierungsrahmen für die Ausrichtung sämtlicher Maßnahmen zur Förderung der digitalen Kompetenzen stellt hier der Bericht zur „Medienkompetenzförderung in Bremen und Bremerhaven – Gesamtstrategie und Bestandsaufnahme“ dar, welcher die Stärkung der „Medienkompetenz von der Kita bis ins hohe Alter“ zum Ziel hat.

3.5.1 Herausforderungen des Handlungsfelds

Die Digitalisierung durchdringt alle Lebensbereiche bis hinein ins Private und ist daher kaum mehr aus der täglichen Alltagsgestaltung hinwegzudenken. Insgesamt nutzen inzwischen 95 Prozent der Bevölkerung Deutschlands das Internet. 48 Prozent der Bevölkerung nehmen an sozialen Netzwerken teil, 61 Prozent der Bevölkerung suchen nach Informationen über Waren und Dienstleistungen und 49 Prozent nutzen Online-Banking. Allerdings gibt es hierbei große Unterschiede zwischen den Altersgruppen.[53]

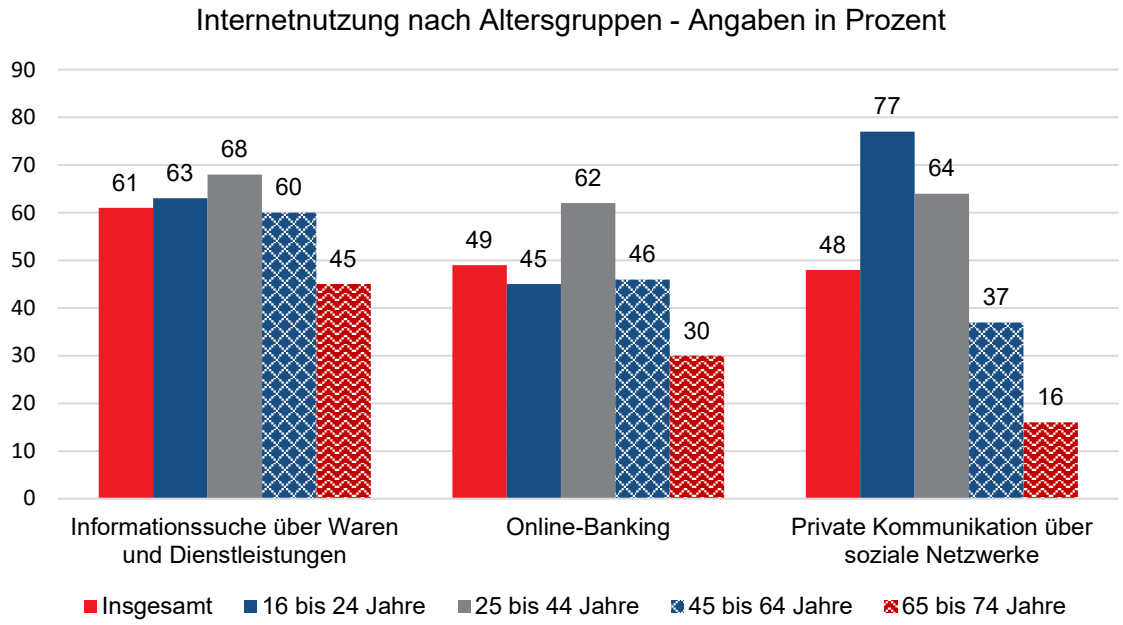


Abbildung 11 - Internetaktivitäten zu privaten Zwecken 2022 nach Alter

Die fortschreitende Digitalisierung und die intensivere Nutzung des Cyberraums führen allerdings auch zu einem Anstieg der Gefahren in diesem. Die Entwicklung neuer Phänomene in der realen Welt spiegelt sich anhand der wachsenden Gefahren im Cyberraum wider. Darüber hinaus entstehen Gefahren, die überhaupt erst durch die Nutzung digitaler Medien ermöglicht werden.

Zu einem sicheren Umgang mit dem Cyberraum bedarf es eines sicheren Rechtsrahmens, der Schutz und die Möglichkeit der Strafverfolgung durch die entsprechenden Behörden im Falle von Straftaten bietet. So ist der Cyberraum kein „rechtsfreier Raum“, denn auch in diesem gelten die Vorschriften des Strafrechts sowie zivilrechtlicher Gesetze. Der Gesetzgeber steht hierbei im Spannungsfeld der schnell fortschreitenden Entwicklung des Cyberraums sowie den Anforderungen an Gesetzgebung.

Es passiert jedoch immer wieder, dass Lebensbereiche nicht abschließend gesetzlich geregelt werden können oder sich Kriminelle diesen Regelungen entziehen. Von Teilen der Gesellschaft wird der Cyberraum als rechtsfreier Raum wahrgenommen, was kriminelle Handlungen in diesem motivieren kann. Trotz bestehender Regelungen ist es daher immer unabdingbar, dass Nutzer:innen über die Gefahren und Risiken im Umgang mit dem Cyberraum informiert sind und ihr Verhalten entsprechend anpassen.

Zur sicheren und gleichberechtigten Nutzung des Cyberraums benötigen Nutzer:innen gut ausgeprägte digitale Kompetenzen sowie eine persönliche digitale Resilienz. Die Kompetenz der Nutzer:innen ist allerdings unterschiedlich stark ausgeprägt. Dies wiederrum führt dazu, dass manche Nutzer:innen nicht alle Chancen des Cyberraums nutzen können und ein erhöhtes Risiko haben, den Gefahren im Cyberraum ausgesetzt oder sogar Opfer einer Straftat zu werden.

Um zu gewährleisten, dass alle Bevölkerungsgruppen von der Digitalisierung und den gesellschaftlichen Entwicklungen profitieren, die gleichen Chancen haben und einzelne Gruppen nicht abgehängt werden, müssen diese den Cyberraum sicher und angstfrei nutzen können. Neben einem sicheren Rechtsrahmen muss hierfür die digitale Kompetenz der Nutzer:innen gesteigert werden.

3.5.1.1 Gestiegene Gefahren für Nutzer:innen des Cyberraums

Die Gefahren, denen Nutzer:innen im Cyberraum ausgesetzt sind, sind vielfältiger Natur. Straftaten können psychische, physische wie auch finanzielle Schäden verursachen. Teilweise sind Nutzer:innen auch Verhaltensweisen ausgesetzt oder werden zu Verhalten motiviert, welches keine unmittelbaren Straftatbestände erfüllt, jedoch zu physischen oder psychischen Beeinträchtigungen führen kann.

Tabelle 2 - Beispiele für Gefahren im Cyberraum

Gefahren finanzieller Art	Psychische / physische Gefahren
▪ Phishing ▪ Fake-Shops ▪ Scamming ▪ Sextortion ▪ u.v.m.	▪ Cybermobbing ▪ Cybergrooming ▪ Hungergruppen ▪ Challenges ▪ u.v.m

Hierbei sind die Nutzer:innen einigen Gefahren in gleichem Maße ausgesetzt. So kann jede:r Nutzer:in einem professionell gestalteten Fake-Shop zum Opfer fallen. Auch können persönliche Daten aller Nutzer:innen mittels Phishing durch Kriminelle erbeutet werden. Andere Gefahren hingegen betreffen nur einzelne Nutzer:innengruppen.

Da Kinder, Minderjährige und junge Erwachsene im Vergleich der Altersgruppen zudem die meiste Zeit im Cyberraum verbringen, sind sie auch den vielfältigen Gefahren in einem erhöhten Maße ausgesetzt.[54]

Weiterhin sind einige Gefahren eng mit neuen sozialen Medien verbunden, die hauptsächlich durch Kinder, Minderjährige und junge Erwachsene genutzt werden. Gefahren, denen

hauptsächlich Kinder- und Minderjährige ausgesetzt sind, stehen häufig im Zusammenhang mit der sexuellen Selbstbestimmung. So werden etwa ein Viertel aller Kinder Opfer von sogenanntem Cybergrooming, bei welchem ältere Kriminelle versuchen, einen sexuell motivierten Kontakt zu dem Kind aufzubauen.[55]

Behinderte Menschen ziehen teilweise einen besonders hohen Nutzen aus digitalen Angeboten, wie Smart-Assistant-Anwendungen, und sind daher einem höheren Risiko ausgesetzt.

Ältere Nutzer:innen hingegen werden häufig Opfer von sogenanntem „Scamming“, bei dem sie mittels unterschiedlicher Vorgehensweisen dazu verleitet werden, hohe Geldsummen an Unbekannte zu senden. Insbesondere das „Love-Scamming“, das Erschleichen eines finanziellen Vorteils mittels Vortäuschung einer Liebesbeziehung, ist hierbei mit hohem emotionalem Stress für die Opfer verbunden.

3.5.1.2 Gestiegene Anforderungen an die Digitale Kompetenz von Nutzer:innen

Um die Risiken und Gefahren einschätzen und bewältigen zu können, welche mit der Nutzung des Cyberraums einhergehen, bedarf es digitaler Kompetenz. Digitale Kompetenz beschreibt die Fähigkeit, konstruktiv mit den durch die Digitalisierung auftretenden Herausforderungen umzugehen. Durch die zunehmende Verlagerung des analogen Lebens in den Cyberraum steigen auch die Anforderungen an die digitale Kompetenz der Nutzer:innen.

Digitale Kompetenz kann hierbei in fünf Punkte gegliedert werden, die durch den europäischen Referenzrahmen für digitale Kompetenzen definiert werden.[56]

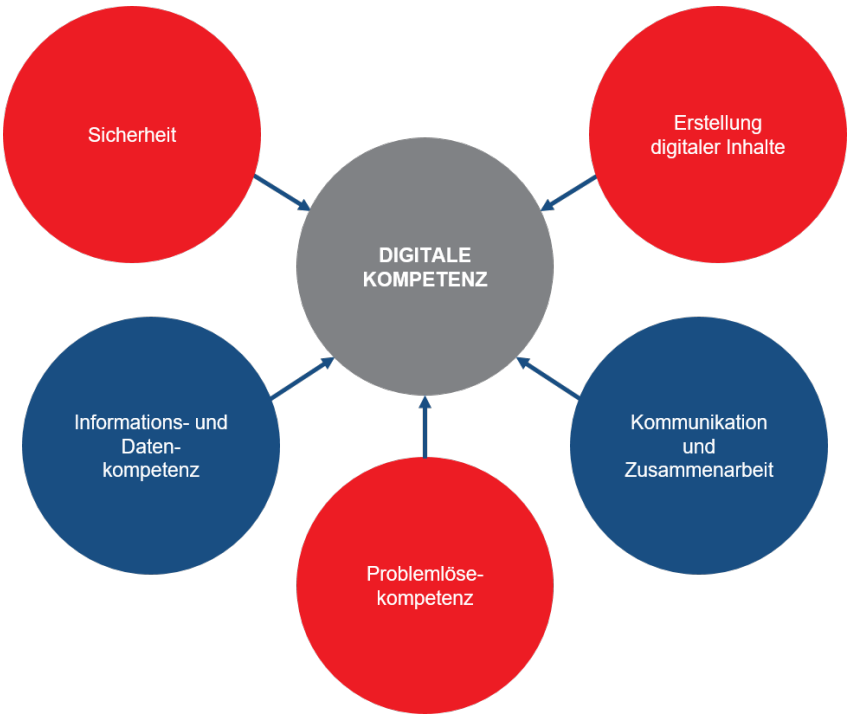


Abbildung 12 - Die fünf Felder der digitalen Kompetenz

Anhand dieser fünf Punkte kann die allgemeine digitale Kompetenz der Nutzer:innen eingeschätzt werden. Neben einer reinen Nutzungskompetenz ist für die fortschreitende Digitalisierung die Vermittlung eines tieferen Verständnisses technologischer und digitaler Entwicklungen unabdingbar.

Insgesamt befindet sich das digitale Kompetenzniveau der deutschen Bevölkerung im mittleren Bereich. Basiskompetenzen im Umgang mit digitalen Medien sind weit verbreitet, wohingegen eine komplexere digitale Kompetenz hingegen häufig nur bei sehr digitalaffinen Gruppen vorhanden ist. Hierbei beeinflussen Alter, Bildung, Gesellschaft und Art der Berufstätigkeit die digitale Kompetenz.[57]

Insbesondere Menschen mit niedriger Bildung und hohem Alter drohen durch den sogenannten „Digital Skills Gap“, also unterschiedlich stark ausgeprägte Fähigkeiten in den digitalen Kompetenzfeldern, abgehängt zu werden. Dies kann bei einer weiteren Verlagerung des beruflichen und gesellschaftlichen Lebens dazu führen, dass diese Gruppen den Anschluss verlieren und gleichzeitig ein höheres Risiko haben, Opfer einer Straftat im digitalen Raum zu werden.

So werden durch Nutzer:innen mit einer geringen formalen Bildung seltener digitale Schutzmaßnahmen ergriffen und Anzeichen für problematisches Medienkonsumverhalten weniger häufig erkannt als durch Nutzer:innen mit einer mittleren oder höheren formalen Bildung. Gleiches gilt für junge Nutzer:innen, die die digitalen Medien gut bedienen und anwenden können, bei denen Schutzmaßnahmen allerdings keinen besonders hohen Stellenwert haben.[58] Zur Steigerung der Cyberresilienz ist es allerdings erforderlich, dass alle Nutzer:innen, die sich im Cyberraum bewegen, über angemessene digitale Kompetenzen verfügen, um diesen sicher nutzen zu können.

Darüber hinaus zeigt der seit 2020 erhobene Digital-Index, dass Frauen im Durchschnitt geringere digitale Kompetenzen als Männer aufweisen. Sie haben seltener Zugang zu digitalen Technologien und weisen eine geringere Affinität hinsichtlich digitalisierungsbezogenen Fragestellungen auf. Mit der aktuellen Erhebung 2022/2023 wird zudem ersichtlich, dass Frauen sich als weniger resilient gegenüber der digitalen Transformation einstufen. Dieser Sachverhalt wird auch als „Digital Gender Gap“ bezeichnet.[59,60]

Neben der digitalen Kompetenz ist auch Medienkompetenz ein wichtiger Baustein der individuellen Resilienz. Medienkompetenz hat zum Ziel, zu einem reflektierten, angemessenen, verantwortungsbewussten, sinnvollen und sicheren Umgang mit Medien zu befähigen, der unabhängig von Alter, Behinderung, Geschlecht oder Bildung eine reflektierte Teilhabe am sozialen Leben ermöglicht.

Ohne digitale Kompetenz und Medienkompetenz hingegen werden bestimmte Personengruppen von der digitalen Entwicklung abgehängt und können somit nicht an gesellschaftlichen Prozessen teilnehmen. Dies kann soziale und berufliche Nachteile zur Folge haben und sich nachteilig auf die Teilhabe an öffentlichen Meinungsbildungsprozesse auswirken. Es ist daher wichtig, bereits frühzeitig alters-, geschlechts- und vielfaltssensible Angebote zu unterbreiten, um die digitale Kompetenz von Nutzer:innen nachhaltig zu steigern, denn „auch wenn eine umfassende Risikoeliminierung nie möglich ist, beginnt der Schutz vor zunehmendem Datenmissbrauch in den Köpfen und an den Endgeräten der Anwender.“[61]

3.5.2 Digitale Kompetenzförderung auf Bundesebene

Auf internationaler sowie nationaler Ebene existieren zahlreiche Initiativen, die sich mit der Thematik digitaler Kompetenz sowie Medienkompetenz befassen. Schwerpunkte sind hierbei die Stärkung des kompetenten und kritischen Umgangs mit Medien, die Veröffentlichung von Publikationen zu Cybersicherheitsthemen sowie Vorträge und Schulungen zur Steigerung der Awareness und der Sensibilisierung zum Thema Cybersicherheit.

Auf Bundesebene setzt sich das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) dafür ein, dass alle Bürger:innen digitale Technologien selbstbestimmt und sicher nutzen können. Hierfür schafft das BMFSFJ zielgruppen- und bedarfsspezifische Angebote, wie die digitalen Engel, die ältere Bürger:innen vor Ort oder digital beraten[62] bzw. die Initiative „Gutes Aufwachsen mit Medien“[63], deren Mitarbeiter:innen zu Medienerleben und Medienerziehung aufklärt, lokale Netzwerke berät und Fachkräfte qualifiziert.

Ähnlich engagiert sich der Verein „Deutschland sicher im Netz e.V. (DSiN)“[64], der Verbraucher:innen im sicheren und souveränen Umgang mit der digitalen Welt unterstützt. Ebenso haben die EU-Initiative „klicksafe“[65] und die Initiative „SCHAU HIN! Was Dein Kind mit Medien macht“[66] zum Ziel, die digitale Kompetenz und Medienkompetenz zu fördern. Unter anderem sollen hier die sozialen Komponenten der Cybersicherheit, zum Beispiel durch eine Sensibilisierung in Bezug auf Cybermobbing und Sextortion, gestärkt werden.

3.5.3 Digitale Kompetenzförderung in der Freien Hansestadt Bremen

Der Senat der Freien Hansestadt Bremen hat im Februar 2022 eine Gesamtstrategie für die Medienkompetenzförderung in Bremen und Bremerhaven vorgestellt.[67] Bei dieser Gesamtstrategie handelt es sich um einen Orientierungsrahmen, an dem die einzelnen Ressorts, der Magistrat der Stadt Bremerhaven sowie weitere Institutionen ihre Arbeit zur Medienkompetenz ausrichten können. Hierdurch können Synergieeffekte genutzt und Überschneidungen vermieden werden, während individuelle Ansätze ein gemeinsames Ziel verfolgen. Die Strategie verfolgt das Ziel, die Medienkompetenz der Bürger:innen in Bremen und Bremerhaven von der Kita bis ins hohe Alter zu stärken. Neben diversen anderen Themenfeldern wird in dieser Gesamtstrategie auch auf Präventionsangebote zum Thema Cybersicherheit (im weiteren Sinne) hingewiesen.

In der Freien Hansestadt Bremen informieren mehrere Akteur:innen zu den Themen digitale Kompetenz sowie Medienkompetenz. Hierbei werden unterschiedliche Formate bedient. Eine Angebotsübersicht kann auf der Website der Bremischen Landesmedienanstalt (www.bremische-landesmedienanstalt.de/medienkompetenz) eingesehen werden.[68]

Durch das Präventionszentrum der Polizei Bremen sowie die Präventionsabteilung der Ortspolizeibehörde Bremerhaven werden Beratungen für Bürger:innen angeboten. Neben Handlungsempfehlungen zum generellen Verhalten im Netz, beziehungsweise zu Vorgehensweisen von potenziellen Täter:innen, werden zusätzlich zu den Vorträgen weitere Präventionsmedien angeboten. Auf Anfrage werden die Vorträge auch zielgruppenspezifisch im Rahmen von Netzwerkkooperationen, etwa mit der Verbraucherzentrale, der Handwerkskammer oder der Universität Bremen, gehalten. Auch gibt es auf Anfrage in zielgruppenorientiertem Rahmen für Jugendliche oder Heranwachsende abgestimmte Vorträge in Betreuungseinrichtungen, Bildungseinrichtungen außerhalb der gesetzlichen Schulen und in Jugendfreizeiteinrichtungen. Darüber hinaus werden alternativ Onlinevorträge, zum Beispiel in Kooperation mit der Verbraucherzentrale oder der Bremischen Landesmedienanstalt, angeboten. Darüber hinaus ist eine aktive Pressearbeit und das regelmäßige Veröffentlichen von Handlungsempfehlungen ein wichtiger Baustein aktiver Cybersicherheitsprävention.

Beim Magistrat der Stadt Bremerhaven gibt es ein Beratungsangebot beim Amt für Jugend, Familie und Frauen als Fachstelle für „Jugendschutz im Internet“. Das Angebot ist angegliedert an den Internet-Treff im Dienstleistungszentrum Grünhöfe und ist stadtweit aktiv. Durch Informationsmaterialien, -veranstaltungen, Schulungen und Workshops sollen Kinder und Jugendliche, Eltern und Multiplikator:innen präventiv für die Risiken des Mediums Internet sensibilisiert werden.

Zusätzlich bietet die Fachstelle Institutionen der Stadt Hilfe zu Fragen des Jugendschutzes im Internet und Unterstützung an und berät z. B. bei der Auswahl der passenden Schutzsoftware. Eltern und Erziehungsbeauftragte können sich in den Sprechstunden ebenfalls zu diesen Themen informieren und Informationsmaterialien vor Ort erhalten. Bei der Beratung können sowohl technische als auch pädagogische Fragen geklärt werden.

Die Fachstelle wird stadtweit von Kooperationspartnern für Vorträge, Schulungen und Informationsveranstaltungen angefragt. Das Angebotsspektrum variiert von referierenden Vorträgen bei Elternabenden über offen gestaltete Projekttage „Gefahren im Internet“ mit Schüler:innen. Ziel ist es, stets für die Zielgruppe angepasste Angebote vorzuhalten, damit die Themen „gefährliche Inhalte im Internet“ und „riskante Mediennutzung“ bei den Zielgruppen ankommt.

Um beispielsweise Jugendliche für die Problematik Cyber-Mobbing flächendeckend in Bremerhaven zu sensibilisieren, wurde vom Präventionsrat Bremerhaven, auf Initiative der Fachstelle Jugendschutz im Internet und der Kriminalprävention der Ortspolizeibehörde Bremerhaven, Mitte 2011 eine Arbeitsgruppe zum Thema Medienkompetenz an Bremerhavener Schulen (MABS) eingerichtet, die zur Zeit Teilnehmer:innen aus folgenden Bereichen umfasst: Regionales Beratungs- und Unterstützungszentrum Bremerhaven (ReBUZ), Abteilung Schulentwicklung und Fortbildung des Magistrats der Stadt Bremerhaven (SEFO), Fachstelle Jugendschutz im Internet des Amtes für Jugend, Familie und Frauen, Präventionsrat, Medienzentrum sowie Zentrale Kriminalprävention der Ortspolizeibehörde Bremerhaven. Hervorgegangen aus dieser Arbeitsgruppe ist das Kooperationsprojekt „Cyber-Mobbing“, in dem Student:innen des Studiengangs „Soziale Arbeit“ der Hochschule Bremerhaven durch Mitarbeiter:innen der Arbeitsgruppe ausgebildet werden, um jedes Jahr in allen Bremerhavener 6. Klassen Workshops über den sicheren Umgang mit sozialen Netzwerken, insbesondere zum Thema Cyber-Mobbing, zu leiten.

Darüber hinaus hat der IT-Planungsrat unter der Federführung der Freien Hansestadt Bremen das Bundesprojekt Qualifica Digitalis für die Qualifizierung des digitalisierten öffentlichen Sektors beauftragt. Im Rahmen der Projektlaufzeit (01.01.2020 – 30.09.2022) wurden geeignete und praxisnahe Lösungen für die „Qualifizierung 4.0“ und die Vermittlung digitaler Kompetenzen für Beschäftigte im öffentlichen Sektor entwickelt. Ergebnisse des Projektes sind umfassende Handlungsempfehlungen für den Bereich der Förderung digitaler Kompetenzen unteranderem im Rahmen der Fort- und Weiterbildung in der öffentlichen Verwaltung, wie z. B. der Weiterentwicklung von lernförderlicher IT-Infrastrukturen und Lernsystemen oder der Berücksichtigung der Fortbildungs- und Lernbedarfe in übergeordneten Digitalstrategien. Das Projekt bietet auch einige Praxisergebnisse, wie z. B. das auf der Qualifikationsebene „Bachelor“ für Studium und Fort- und Weiterbildung unmittelbar zu verwendende Curriculum zum Themenfeld E-Government, welches mit 17 Modulen (zukünftige) Verwaltungsmitarbeiter:innen dazu befähigen soll, Digitalisierung staatlichen Handelns mitzugestalten und einen wesentlichen Beitrag zur digitalen Daseinsvorsorge leisten zu können.[69]

3.5.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Um die digitale Kompetenz der Nutzer:innen zu steigern, müssen sie in ihrer Lebenswelt abgeholt und begleitet werden. Nur so können Lernen und Kompetenzerwerb effektiv und nachhaltig umgesetzt werden.

Ein wichtiger Baustein zur Verbesserung der digitalen Kompetenz ist die Stärkung des formalen sowie des informellen Lernens. Hierbei ist es notwendig, dass die vielfältigen Bildungsangebote zielgruppenorientiert, vielfalts- sowie geschlechtersensibel gestaltet werden. So kann sichergestellt werden, dass digitale Sicherheitskompetenzen in das lebenslange Lernen integriert werden.

Da das Einstiegsalter in den Cyberraum immer weiter sinkt, müssen Mitarbeiter:innen in Kitas und Schulen befähigt werden, digitale Kompetenzen und die damit einhergehende Cyberresilienz ihrer Schützlinge so früh wie möglich zu stärken. Hierdurch werden an Erzieher:innen und Lehrer:innen hohe Anforderungen gestellt, da diese zusätzlich zu den bestehenden Aufgaben eine fachliche Expertise in dem Bereich Cybersicherheit erlangen müssen, um die Lehrinhalte überzeugend vermitteln zu können.

Eine besondere Herausforderung bei der Stärkung der digitalen Kompetenz besteht daher nicht nur darin, vielfalts- und geschlechtersensible Bildungsangebote zu erstellen, die barrierefrei bereitgestellt werden (insb. in Deutscher Gebärdensprache sowie Leichter Sprache). Vielmehr müssen zunächst die personellen Kapazitäten geschaffen werden, um Lerninhalte in unterschiedlichen Kontexten (Schule, Kita, Arbeitsplätze, etc.) zu vermitteln.

Um die beschriebenen Herausforderungen zu bewältigen, wurden folgende Maßnahmen bei der Erstellung der Bremischen Cybersicherheitsstrategie 2023 identifiziert:

- Stärkung des formellen sowie des informellen Lernens durch die Berücksichtigung vielfalts- und geschlechtssensibler Bildungsbedürfnisse für die unterschiedlichen Zielgruppen bei der Konzeption und Durchführung von Schulungsmaßnahmen.
- Befähigung der Mitarbeiter:innen in Kitas und Schulen, um die digitalen Kompetenzen sowie die Cyberresilienz so früh wie möglich zu stärken.

3.6 Awareness und Verbraucherschutz

Die fortschreitende Digitalisierung stellt nicht nur ein Risiko für Verbraucher:innen dar. Bei unbedachter Nutzung digitaler Endgeräte und Anwendungen wird der Mensch zur Schwachstelle jeder ITK-Infrastruktur. Um die Integrität von ITK-Infrastrukturen zu schützen sowie die Sicherheit und Vertraulichkeit besonders schützenswerter Informationen zu gewährleisten, müssen Mitarbeitende in Unternehmen durch gezielte Awareness-Strategien im sicheren Umgang mit der verwendeten Technik geschult werden. Darüber hinaus können technische Vorkehrungen im Rahmen von *security-by-design*-Ansätzen zur Minimierung von Sicherheitsrisiken durch Verbraucher:innen beitragen.

3.6.1 Herausforderungen des Handlungsfelds

Während die Stärkung digitaler Kompetenzen einen sehr breiten Ansatz verfolgt, um Menschen zu kompetenten Nutzer:innen des Cyberraums zu machen, liegt der Fokus des Handlungsfeld Awareness und Verbraucherschutz speziell auf Gefahren, welche sich durch oder bei der Nutzung von ITK-Hard- und Software ergeben können, und Strategien, um diese zu reduzieren.

Wer spezifische Risiken kennt und richtig einschätzt, kann sein Verhalten entsprechend anpassen und somit die Gefahr von Schäden sowohl für sich selbst (durch kompromittierte persönliche Daten) als auch die genutzten Systeme (etwa durch unbeabsichtigtes Ausführen von Schadcode auf dem Arbeitsplatz-PC) reduzieren. Einen wesentlichen Beitrag hierzu leisten darüber hinaus technische Ansätze, in denen Sicherheitsrisiken für Anwender:innen bereits bei der Konzeption digitaler Produkte und Anwendungen mitgedacht und durch eine vorrausschauende Entwicklung bestmöglich reduziert werden.

3.6.1.1 Gestiegene Herausforderungen an den Verbraucherschutz

Eine wichtige Aufgabe des Verbraucherschutzes besteht darin, die potenziellen Risiken, welche durch die Nutzung neuer Produkte oder Dienste entstehen, frühzeitig zu identifizieren und Strategien zu finden, um diese zu reduzieren oder zu beseitigen. Auch hierbei beeinflussen Alter, Bildung, Geschlecht und Art der Berufstätigkeit entscheiden die digitale Kompetenz und Resilienz.

Die Vernetzung digitaler Geräte ist für Verbraucher:innen sehr bequem und wird immer einfacher, macht sie jedoch auch zunehmend angreifbar. Sind Geräte nicht ausreichend gesichert, können Kriminelle sich Zugriff auf das gesamte Netzwerk mit allen hieran angeschlossenen Geräten verschaffen und hierüber an vertrauliche Daten der Nutzer:innen gelangen. Auch können sie weitere Systeme kompromittieren und diese nutzen, um ihre kriminellen Taten zu verschleiern.

Die Anzahl entdeckter Schwachstellen in Softwareprodukten (13 Prozent davon kritisch) wuchs im Jahr 2021 auf 20.174 (10 Prozent mehr als im Vorjahr) an.[70] Mit sogenannten „exploits“ können Kriminelle diese Schwachstellen ausnutzen, um beispielsweise Daten auszuspähen oder kleine Schadprogramme in die Software einzuschleusen. Jede nicht abgesicherte Videoüberwachungsanlage, selbst das Babyfon mit integrierter Kamera, wird so zur Möglichkeit für Kriminelle, Verbraucher:innen in ihrem höchstpersönlichen Lebensbereich unbemerkt auszuspionieren. Darüber hinaus können neben voyeuristischen Absichten solche Eingriffe als Vorbereitungshandlungen weiterer krimineller Taten dienen, etwa zum Ausspähen einer Wohnung zum Zwecke eines Einbruchs.

Durch die wachsende Anzahl an Schwachstellen in Software-Produkten steigt das Risiko für Verbraucher:innen immer mehr, Opfer eines Cyberangriffs zu werden. Auch fehlt häufig

das technische Wissen, um ein kompromittiertes Gerät oder einen kompromittierten Dienst zu erkennen, sodass Angriffe oftmals erst mit eintretendem Schaden bemerkt werden.

Es ist daher besonders wichtig, dass Geräte und Dienste technisch definierte Standards erfüllen, und den Verbraucher:innen die Möglichkeit gegeben wird, sich vor dem Kauf über die Sicherheitseigenschaften der Geräte und Dienste neutral zu informieren. Standards müssen hierbei verständlich und transparent sein, damit Verbraucher:innen die Sicherheitseigenschaften eines Produkts in ihre Kaufentscheidungen mit einbeziehen können.

Neben der Sensibilisierung von Verbraucher:innen kommt Security-by-Design-Ansätzen eine immer größere Bedeutung zu. Hierbei werden Sicherheitsaspekte bereits in alle Phasen der Softwareentwicklung integriert und sollen somit einen bestmöglichen „eingebauten“ Schutz für Verbraucher:innen gewährleisten.

3.6.1.2 Gestiegene Anforderungen an Awareness

Werden Verbraucher:innen an ihrem Arbeitsplatz Opfer eines Cyberangriffs, kann ein eintretender Schaden weitreichende Folgen für das Unternehmen haben. Plötzlich werden nicht mehr nur persönliche Mails oder das eigene Bankkonto kompromittiert, sondern die Geschäftsgeheimnisse des beschäftigenden Unternehmens. Werden Daten verschlüsselt oder gelöscht, ist das Unternehmen gegebenenfalls nicht mehr handlungsfähig. Das Bekanntwerden von Angriffen kann in der Folge zu einem erheblichen Reputationsverlust des Unternehmens führen.

Auch für Verbraucher:innen kann ein solcher Cyberangriff schwerwiegende Konsequenzen haben, etwa wenn dieser durch die unberechtigte Nutzung von privaten Geräten am Arbeitsplatz oder eigenes Fehlverhalten verursacht wurde und sich in der Konsequenz haftungsrechtliche Fragen stellen.

Um sowohl sich selbst als auch Mitarbeiter:innen zu schützen, sollten Arbeitgeber:innen daher stets bemüht sein, das eigene Personal umfangreich über die digitalen Gefahren ihres eigenen Arbeitsplatzes aufzuklären. Darüber hinaus können sie ihre Mitarbeiter:innen mit Schulungen dazu befähigen, Sicherheitsrisiken zu erkennen und zu vermeiden.

Auch im Bereich der öffentlichen Verwaltung gibt es im Zuge der Verwaltungsmodernisierung eine Vielzahl von Anwendungen, die durch unbeabsichtigtes Fehlverhalten einer Mitarbeiterin oder eines Mitarbeiters kompromittiert oder schlimmstenfalls lahmgelegt werden könnten. So kann das Klicken eines unscheinbaren Links oder das Ausführen einer unbekannten Datei im schlimmsten Fall zu einer Verschlüsselung der gespeicherten Daten führen und Teile der Verwaltung für längere Zeit handlungsunfähig machen – abhängig von der ITK-Infrastruktur sowie dem Grad der Vernetzung unterschiedlicher Systeme und Anwendungen.[71]

Obwohl viele Schadprogramme bereits durch technische Vorkehrungen abgefangen werden, gelangen immer wieder einzelne Schadmails an Mitarbeiter:innen. Je professioneller diese erstellt wurden, desto geringer ist die Chance für Mitarbeiter:innen, diese als solche zu erkennen. Wird in der Folge ein Link in der Mail angeklickt oder ein Programm ausgeführt, können Cyberkriminelle so über die Mitarbeiter:innen Zugang zu IT-Systemen der Verwaltung erhalten und großen Schaden verursachen.

Cyberkriminelle machen sich hierbei häufig die Strategie des Social Engineerings zunutze, bei welcher die Opfer über die Identität der/des Kriminellen sowie ihre/seine Absichten getäuscht werden. Können Mitarbeiter:innen Phishing-Mails häufig noch als solche erken-

nen, wird es bei der Vorgehensweise des sogenannten Spear-Phishings schon schwieriger: Hier recherchieren Kriminelle erst persönliche Informationen über ein zielgerichtet ausgewähltes Opfer, um den Angriff auf dessen Persönlichkeit abzustimmen.[72]

Die Verwaltungen der Länder sind wesentliche Einrichtungen im Sinne der NIS-2-Richtlinie, in denen eine Vielzahl von Daten verarbeitet und gespeichert wird. Sie stellen daher ein besonders lohnendes Ziel für Cyberkriminelle dar. Neben zielgerichteten Angriffen, die die Infiltration der Systeme und den Abfluss von Daten zum Ziel hat, können diese auch Opfer von ungerichteten Ransomwareangriffen werden.

Damit Cyber-Kriminelle nicht erfolgreich sind müssen, neben dem technischen und organisatorischen Schutz der ITK-Systeme, auch die Mitarbeiter:innen der Verwaltungen von Ländern und Kommunen befähigt werden, die verfügbaren digitalen Infrastrukturen und Instrumente sicher zu nutzen.

3.6.2 Verbraucherschutz auf europäischer und nationaler Ebene

Im September 2022 wurde durch die EU der *Cyber Resilience Act*[73] verabschiedet. Das Ziel des Cyber Resilience Act ist es, grundlegende Anforderungen an die Gestaltung, Entwicklung und Herstellung von Produkten mit digitalen Elementen, wie Hard- oder Software, einzuführen. So soll die Cybersicherheit dieser Produkte über den gesamten Lebenszyklus aufrechterhalten werden. Da diese Vorgehensweise auch den Security-by-Design-Ansatz verfolgt, wurde der Cyber Resilience Act bisweilen informell auch als Security-by-Design-Act bezeichnet.

Auf Bundesebene wurde das BSI im Mai 2021 im Rahmen des IT-Sicherheitsgesetzes mit der Aufgabe des digitalen Verbraucherschutzes betraut. Zudem soll das BSI den gesamtgesellschaftlichen Dialog zur Cybersicherheit verstetigen.

Ziele des digitalen Verbraucherschutzes sind hierbei:

- Schutz der Verbraucher:innen vor Sicherheitsrisiken im Cyber-Raum,
- Sensibilisierung der Verbraucher:innen über die geeignete Auswahl, den sicheren Einsatz und die sichere Nutzung von marktgängigen, vernetzten IT-Systemen und Online-Diensten, Hardware und Software,
- Warnung vor strukturellen und aktuellen Sicherheitsrisiken dieser marktgängigen, internetfähigen IT-Systeme und Online-Dienste.

Als eine weitere Maßnahme des Verbraucherschutzes hat das BSI mit dem *Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)*[74] den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen einzuführen.

Trägt ein internetfähiges Gerät dieses IT-Sicherheitskennzeichen, so verspricht der Hersteller, dass es grundsätzliche, vom BSI definierte, Sicherheitseigenschaften besitzt.

3.6.3 Awareness und Verbraucherschutz in der Freien Hansestadt Bremen

Sowohl der gesundheitliche als auch wirtschaftliche Verbraucherschutz wurde im Land Bremen in einem eigenen Ressortbereich bei der Senatorin für Gesundheit, Frauen und Verbraucherschutz zusammengeführt, um Voraussetzungen zu schaffen, die Interessen der Verbraucher:innen im Land Bremen bestmöglich zu vertreten. Hier wird die Rechtsetzung zum Thema Cybersicherheit mit Bezug zu Verbraucher:innen über den Bundesrat sowie die Verbraucherschutzministerkonferenz eng begleitet.

Von dort aus wird auch die Verbraucherzentrale Bremen e.V. (VZHB), neben anderen Themen, auch zum Thema Digitales gefördert, um die Verbraucher:inneninformation und -beratung in diesem Bereich sowie die Verbraucherrechtsarbeit zu diesem Thema zu stärken.

Zur Stärkung der Verbraucher:innen im Land Bremen werden durch die Senatorin für Gesundheit, Frauen und Verbraucherschutz, in Kooperation mit der VZHB, der Polizei Bremen sowie der Bremischen Landesmedienanstalt, angeboten. So werden in der Veranstaltungsreihe „Dialog Verbraucherschutz“ wiederholt interdisziplinäre Vorträge zum Thema „Internet-Abzocke und Cybercrime: Wie schütze ich mich?“ angeboten.[75] Neben dieser Veranstaltungsreihe bietet die Polizei Bremen, durchgeführt durch die Mitarbeiter:innen des Präventionszentrums, verschiedene Vorträge an, um über Gefahren im Internet aufzuklären und Tipps zum Schutz zu geben. Weiterhin informiert die Polizei Bremen auf der Website „Rund ums Internet - Polizei Bremen. Bremen Aber sicher!“ über aktuelle Themen im Bereich Cybersicherheit.

Zur Steigerung der „Awareness“ der Mitarbeiter:innen der öffentlichen Verwaltung finden regelmäßig Aufklärungsveranstaltungen zu den Themen IT-Sicherheit / Cybersicherheit, wie z. B. „die Hacker kommen“, statt. Diese werden in Zusammenarbeit mit der Bundesakademie für Öffentliche Verwaltung (BAköV) durchgeführt.

Weitere Maßnahmen, durch die die Awareness gesteigert werden soll, sind die Erstellung und Bereitstellung von themenbezogenen Publikationen zu Informations- und Cybersicherheit, die Aus- und Fortbildung von IT-Sicherheitsbeauftragten sowie die Schaltung von Hinweisen zum Umgang mit aktuellen IT-Bedrohungslagen im Intranet der bremischen Verwaltung.

Zudem haben alle Mitarbeiter:innen der öffentlichen Verwaltung Zugriff auf das Selbstlernprogramm „BITS“ (Behörden IT Sicherheitstraining), in welchem Themen und Ziele der IT-Sicherheit behandelt werden.

3.6.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Der Schutz der Verbraucher:innen und der Arbeitnehmer:innen ist ein besonderes Anliegen des Senats der Freien Hansestadt Bremen. Ein wichtiges Ziel ist es, Verbraucher:innen in ihrer Eigenverantwortung und Entscheidungsfindung zu stärken, entsprechend der vielfalts- und geschlechtssensibler Bildungsbedürfnisse für die unterschiedlichen Zielgruppen.

Basierend auf den Zielstellungen des digitalen Verbraucherschutzes sollen die Verbraucher:innen im Land Bremen befähigt werden, die Gefahren, die durch den Einsatz von Hard- und Software ausgehen können, eigenständig zu erkennen und diesen gegenüber resilienter zu werden.

Durch die Koordination und Ergänzung der bisherigen Aktivitäten sollen die Verbraucher:innen darin unterstützt werden, die Risiken, die bei der Nutzung von internetfähigen Geräten ausgehen können, besser beurteilen und vorhandene Lösungen besser nutzen zu können.

Ein wichtiges Ziel besteht deshalb darin, die vielfältigen Akteur:innen des Verbraucherschutzes im Bereich Cybersicherheit auf Landesebene zusammenführen, eine Schnittstelle für neue Akteur:innen zu bilden und diese nach Möglichkeit zu unterstützen. Diese Rolle kann perspektivisch über die auszugestaltende Zentralstelle für Cybersicherheit in enger Kooperation mit dem Landesverbraucherschutz wahrgenommen werden. Hierdurch

sollen Synergien genutzt und möglichst viele Verbraucher:innen zum Thema Cybersicherheit erreicht werden. So kommt die Zentralstelle für Cybersicherheit nicht nur ihrer Rolle als zentrale Koordinierungsstelle nach, sondern leistet auch einen wichtigen Beitrag zur Präventionsarbeit im Land Bremen.

Verbraucher:innen sollen auf die Möglichkeiten der Nutzung sicherheitskonformer IT-Produkte und Dienste hingewiesen werden. Während insbesondere die Verbraucherzentrale Bremen, das Präventionszentrum der Polizei Bremen und die Bremische Landesmedienanstalt als Ansprechstellen für die Verbraucher:innen im Land Bremen zur Verfügung stehen, wird die Zentralstelle für Cybersicherheit perspektivisch als Ansprechstelle für Sensibilisierungskampagnen aller Verwaltungs- und Behördenmitarbeiter:innen im Land Bremen fungieren. Weiterhin ist die Zentralstelle für Cybersicherheit bestrebt, einheitliche Kampagnen zu entwickeln und diese den Verwaltungen und Kommunen zur Verfügung zu stellen.

Um die beschriebenen Herausforderungen zu bewältigen, wurden folgende Maßnahmen bei der Erstellung der Bremischen Cybersicherheitsstrategie 2023 identifiziert:

- Stärkung der Verbraucher:innen in ihrer Eigenverantwortung und Entscheidungsfindung bei der Produktauswahl unter Berücksichtigung vielfalts- und geschlechtssensibler Bildungsbedürfnisse für die unterschiedlichen Zielgruppen
- Befähigung der Verbraucher:innen, Gefahren im Zusammenhang mit dem Einsatz von Hard- und Software eigenständig zu erkennen und resilienter diesen gegenüber zu werden unter Berücksichtigung vielfalts- und geschlechtssensibler Bildungsbedürfnisse für die unterschiedlichen Zielgruppen
- Zusammenführung der vielfältigen Akteur:innen des Verbraucherschutzes im Bereich Cybersicherheit auf Landesebene durch die auszugestaltende Zentralstelle für Cybersicherheit, um Synergien sowie eine größtmögliche Reichweite zu schaffen und einen Beitrag zur Präventionsarbeit im Land Bremen zu leisten
- Förderung des Designansatzes „Security by Design“ durch Hinweise auf sicherheitskonforme IT-Produkte und Dienste in enger Zusammenarbeit mit den weiteren Akteur:innen des Verbraucherschutzes
- Einrichtung der auszugestaltenden Zentralstelle für Cybersicherheit als zentrale Ansprechstelle für Sensibilisierungsmaßnahmen aller Verwaltungs- und Behördenmitarbeiter:innen im Land Bremen

3.7 Fachkräfte

Der Bedarf an qualifizierten Fachkräften im Bereich Cybersicherheit / IT ist sowohl in der Wirtschaft als auch in der Verwaltung gleichermaßen hoch. Die Gewinnung und Bindung dieser Fachkräfte stellt eine zentrale Herausforderung dar. Die Hebung des Fachkräftepotenzials im Kreislauf von Schule, Wissenschaft und Wirtschaft ist dabei von herausragender Bedeutung. Besondere Beachtung fällt hierbei der Steigerung des Frauenanteils unter Beschäftigten in der IT-Branche zu. Ebenfalls gilt es, Interessierten bereits frühzeitig einen niedrigschwelligen Einstieg in die IT- und Cybersicherheit zu ermöglichen und durch aufeinander aufbauende Ausbildungs- und Studienmöglichkeiten zu qualifizierten Fachkräften auszubilden. Durch die Weiterentwicklung der Freien Hansestadt Bremen zum attraktiven Standort für IT-Fachkräfte wird die Fachkräftegewinnung und -bindung unterstützt.

3.7.1 Herausforderungen des Handlungsfelds

Mit zunehmender Digitalisierung steigt auch der Bedarf an IT-Fachkräften, welche diese begleiten und weiter vorantreiben. IT-Fachkräfte sind essenziell, um Innovation und Wettbewerbsfähigkeit, Wachstum und Beschäftigung, Wohlstand und Lebensqualität zu sichern.

Hierbei existiert schon jetzt in bestimmten Regionen und Branchen ein Mangel an ausreichend qualifizierten Kräften, so dass nicht immer alle offenen Stellen besetzt werden können. Der Fachkräftemangel betrifft die Wirtschaft und die öffentliche Verwaltung gleichermaßen, da diese um qualifiziertes Personal konkurrieren. Insbesondere die Absolvent:innen in den sogenannten MINT-Fächern (Mathematik, Informatik, Naturwissenschaft und Technik) und somit auch der Themenbereich der Cybersicherheit sind hiervon betroffen.

Zusätzlich zu dem bereits bestehenden Fachkräftemangel ist der demografische Wandel eine weitere Herausforderung der Sicherung des Fachkräftebedarfs, die in den kommenden Jahrzenten durch alle Akteur:innen in Politik, Wirtschaft und Wissenschaft gemeinsam gemeistert werden muss.

3.7.1.1 Auswirkungen des Fachkräftemangels

Im Jahr 2021 fehlten in Deutschland knapp 350.000 qualifizierte Arbeitskräfte in allen Berufsgattungen. Durch diese sogenannte „Fachkräftelücke“ konnten rund 34 Prozent aller offenen Stellen nicht besetzt werden, weil es kein:e ausreichend qualifizierte:r Arbeitslose:n für diese gab.[76] Im Land Bremen fehlten im Jahr 2021 rund 3.350 qualifizierte Arbeitskräfte. Dies entsprach einer Fachkräftelücke von durchschnittlich 32 Prozent.[77]

Im 4. Quartal 2022 behinderte der Fachkräftemangel bereits die Geschäftstätigkeit von 45,7 Prozent der Unternehmen. Offene Stellen in Unternehmen sind inzwischen, mit steigender Tendenz, im Durchschnitt fünf Monate vakant.[78]

Hierbei betrifft der Fachkräftemangel auch den Bereich der Cybersicherheit. So ist bereits heutzutage die Bereitstellung von qualifiziertem Personal die größte Herausforderung bei der Sicherstellung der Cybersicherheit.[79] Diese Situation wird sich durch die allgemeine Entwicklung des demografischen Wandels noch verstärken, da perspektivisch weniger Berufsanfänger:innen für den Arbeitsmarkt zur Verfügung stehen werden.[80]

Neben spezialisierten Fachkräften zur Sicherstellung der Cybersicherheit werden zudem Fachkräfte mit IT-Sicherheitsexpertise benötigt, um sichere Software zu entwickeln, die die neuen Technologien von digitalisierten Fahrzeugen bis hin zu Smart Home-Geräten nutzbar macht.[81]

Da der Staat zunehmend Aufgaben wie die Unterstützung des Schutzes kritischer Infrastrukturen übernimmt und bei der polizeilichen Aufklärung und der Verteidigung vermehrt technische Mittel einsetzt, werden auch hier IT-Fachkräfte benötigt. Allerdings steht der öffentliche Dienst bei der Rekrutierung geeigneten Personals in direkter Konkurrenz mit der Wirtschaft. Nach Angaben der Bundesagentur für Arbeit arbeiten allerdings nur drei Prozent der Informatikstudierenden, die ihr Studium abschließen, in der öffentlichen Verwaltung.[82]

Durch eine attraktivere Gestaltung bestehender Gehaltsstrukturen im öffentlichen Dienst könnten Beschäftigungsverhältnisse für IT-Fachkräfte attraktiver gestaltet werden. Neben einer konkurrenzfähigen Vergütung, welche die Qualifikation der Fachkräfte sowie ihren Bedarf angemessen reflektiert, nehmen auch die Gestaltung des Arbeitsplatzes sowie angebotene Arbeitszeitmodelle selbst eine wichtige Rolle ein. Diese können sich an den bereits in der Wirtschaft typischen Modellen orientieren, um hier konkurrenzfähig zu bleiben.

3.7.1.2 Ausschöpfung des Fachkräftepotenzials

Trotz der großen Anzahl an unbesetzten Stellen im Bereich Informatik und Cybersicherheit und der im Vergleich zu anderen Berufsfeldern überdurchschnittlichen Vergütung entschließen sich nur knapp 10 Prozent aller Studierenden für ein Informatik-Studium.[83] Insbesondere Frauen sind, wie die folgende Grafik zeigt, in MINT-Studiengängen stark unterrepräsentiert.

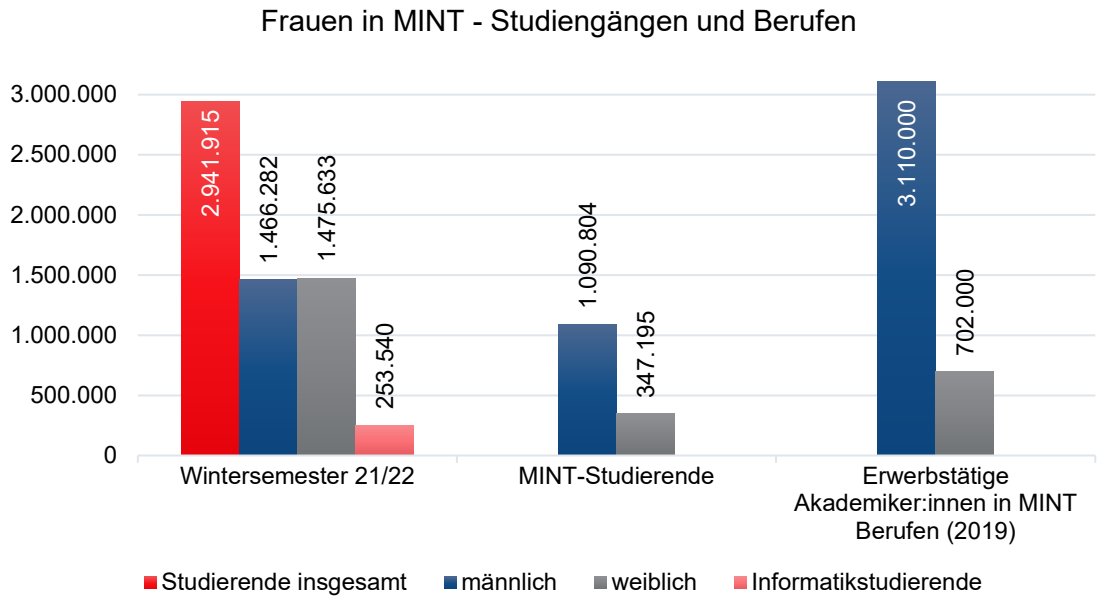


Abbildung 13 - Frauen in MINT-Studiengängen und Berufen

Da auch bei jungen Frauen ein Interesse an den MINT-Bereichen besteht, ist hier ein großes Potential an zukünftigen Fachkräften vorhanden. Mädchen und junge Frauen interessieren sich, ebenso wie ihre Mitschüler, für naturwissenschaftliche Fächer. Das Interesse nimmt jedoch tendenziell im Laufe des Alters ab, sodass Mädchen bereits frühzeitig während der Schulzeit für MINT-Fächer begeistert werden müssen, wenn die Erhöhung ihres Anteils an den MINT-Studiengängen (und -Berufen) angestrebt wird.[84]

Ein weiterer Schlüssel gegen den Fachkräftemangel ist die Inklusion. So galten zum Stichtag 31.12.2021 fast 7.800.000 Menschen im erwerbsfähigen Alter in Deutschland als schwerbehindert. Hiervon waren fast 173.000 arbeitslos. Hierbei sind neurodiverse Personen nicht erfasst, so dass die Anzahl an beeinträchtigen Personen im erwerbsfähigen Alter wesentlich höher sein dürfte.[85]

Diese Personengruppen besonders mit Blick auf den Erwerb von Kompetenzen im Bereich von IT-Sicherheitsthemen zu begeistern und in inklusiven Arbeitsverhältnissen auf dem allgemeinen Arbeitsmarkt gezielt zu fördern bietet eine große Chance, Fachkräfte für den Bereich Cybersicherheit zu gewinnen und vorhandene Potenziale zielgruppenorientierter auszuschöpfen.

3.7.2 Nationale Maßnahmen gegen den Fachkräftemangel

Die Bundesregierung hat im November 2018 eine Strategie zur Sicherung von Fachkräften vorgelegt und setzt an verschiedenen Punkten an, um dem Fachkräftemangel entgegenzuwirken.[86]

Hier werden Unternehmen unterstützt, die Vorteile einer vielfältigen Arbeitnehmer:innenschaft, die aus Menschen unterschiedlichen Geschlechts und Alters sowie verschiedener Herkunft besteht und auch Menschen mit Behinderung einschließt, zu nutzen und von diesen zu profitieren.

Neben der Qualifizierung und Weiterbildung der Arbeitnehmer:innen soll zudem die Attraktivität, Qualität und Leistungsfähigkeit der dualen Ausbildungen gestärkt werden.

Ergänzend zu den allgemeinen Maßnahmen der Bundesministerien zur Sicherung von Fachkräften existieren auch privatwirtschaftliche Maßnahmen, durch die der Fachkräftemangel im Bereich Cybersicherheit gemindert werden soll.

So entwickelt zum Beispiel der Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) in Zusammenarbeit mit dem Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI) und privaten Trägern ein IT-Ausbildungsprogramm zur Cybersicherheit und zum Schutz kritischer Infrastrukturen, welches sich auch an Quereinsteiger:innen richtet.[87]

3.7.3 Fachkräfteförderung in der Freien Hansestadt Bremen

In der Freien Hansestadt Bremen werden diverse Studiengänge im Bereich Informatik angeboten.

Die Universität Bremen bietet einen Bachelor- und Masterstudiengang „Computer Science“, einen Bachelor „Wirtschaftsinformatik“ sowie einen Masterstudiengang „Management Information Systems“ an.

Die Hochschule Bremen bietet sowohl den dualen Studiengang „Informatik“ (Bachelor und Master) als auch den Studiengang „Software- und Systemtechnik“ (Bachelor) an.

Eine Besonderheit an der Hochschule Bremen ist, dass zudem der „Internationale Frauenstudiengang Informatik (IFI)“ (Bachelor) angeboten wird. Somit besteht bereits jetzt eine besondere Förderung, um der Unterrepräsentanz von Frauen in diesem Fachbereich entgegenzuwirken.

Die Hochschule Bremerhaven bietet im Bachelorbereich die Studiengänge "Informatik" sowie "Wirtschaftsinformatik" an. Weiterführend steht der Masterstudiengang "Digitalisierung, Innovation und Informationsmanagement" zur Verfügung. Als berufliches Weiterbildungsformat führt die Hochschule den Kurs "Geprüfte/r Meister/in - Vernetzte Industrie" durch.

Weiterhin bietet die Technikerschule Bremen ab dem Sommersemester 2023 eine Aufstiegsfortbildung zur/zum Staatlich Geprüften Informationstechniker:in mit der Spezialisierung IT-Cyber-Security an. Diese Aufstiegsfortbildung umfasst die aktuellen Grundlagen der technischen Informatik, Rechnerarchitekturen und Betriebssystemen über Netzprotokolle, Netzsicherheit und Kryptographie bis hin zur IT-Forensik, Risikobewertung und Angriffsanalyse. Neben der Theorie liegt hier der Fokus auf praktischen Erarbeitungen.

Zusätzlich zu diesen Aus- und Fortbildungsmöglichkeiten betreibt die Senatorin für Wirtschaft, Arbeit und Europa die Website www.fachkraefte-fuer-bremen.de. Neben mehreren Stellenportalen, auf denen vakante Stellen im Land Bremen ausgeschrieben werden, wird hier eine Toolbox mit wichtigen Informationen und Materialen für die Personalakquise gestellt. Zudem werden sogenannte Stammtische veranstaltet, bei denen Arbeitgeber:innen regelmäßiger Austausch ermöglich werden soll.

3.7.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Um die beschriebenen Herausforderungen zu bewältigen, wurden folgende Maßnahmen bei der Erstellung der Bremischen Cybersicherheitsstrategie 2023 identifiziert:

- Sichtung bestehender (inter)nationaler Konzepte zur Fachkräftegewinnung und Prüfung, inwieweit diese im Land Bremen bereits genutzt werden oder Anwendung finden können
- Prüfung des Potenzials der Fachkräftegewinnung durch Inklusion
- Überprüfung und ggf. Anpassung der bestehenden Anforderungen und Vergütung an Bewerber:innen im Bereich Cybersicherheit für den öffentlichen Dienst
- Überprüfung und ggf. Anpassung der Fortbildungsmöglichkeiten für Bedienstete im öffentlichen Dienst mit Blick auf cybersicherheitsrelevante Themen
- Steigerung der Attraktivität von MINT-Berufen und Studiengängen für Frauen
- Stärkere Vernetzung von Hochschulen, Wirtschaft und Behörden, um auf das Thema Cybersicherheit aufmerksam zu machen
- Prüfung des Ausbaus der Kapazitäten für die Schaffung und Durchführung von Ausbildungen und Studiengängen im Bereich Cybersicherheit

3.8 Innovative Forschung und Entwicklung

Cybersicherheit kann vor allem durch technische Vorkehrungen erhöht werden. Die hierfür erforderlichen prozess- und plattformunterstützten Lösungen werden meist im Zusammenspiel von Wissenschaft, außeruniversitärer Forschung sowie Anwendungsentwicklung durch Wirtschaftsunternehmen geschaffen. Gerade junge Unternehmen im Bereich der IT-Sicherheitsforschung und -entwicklung verfügen jedoch teilweise über wenige Ressourcen, um Produkte und Lösungen schnell zur Marktreife zu bringen. Sie werden durch das Schaffen von Austausch- und Kooperationsplattformen zwischen Wirtschaft und Wissenschaft unterstützt. Auch die diskriminierungsfreie sowie vielfaltssensible Entwicklung von Anwendungen und Geräten ist hierbei wichtig.

3.8.1 Herausforderungen des Handlungsfelds

Die Digitalisierung hat dazu geführt, dass die Märkte globaler geworden sind und die Konkurrenz zwischen Unternehmen und einzelnen Staaten größer geworden ist. Nichtmehr nur Rohstoffe und geografische Gegebenheiten entscheiden über den wirtschaftlichen und politischen Erfolg, sondern auch Innovationen.

Grundlage für Innovationen sind Ideen, Wissen und Know-how in den Köpfen der Menschen. Forschung und deren wirkungsvoller Transfer in die Praxis bauen die Kompetenzen auf, die in einer digitalen und globalisierten Welt zwingend erforderlich sind.

Durch diesen Transfer in die Praxis werden permanent neue IT-Systeme und Dienstleistungen geschaffen und stehen für eine Vielzahl von Bereichen, wie die Medizin, die Industrie, die öffentliche Verwaltung sowie die Endverbraucher:innen, zur Verfügung.

Werden Entwicklungen in diesen Bereichen nicht konsequent und nachhaltig gefördert, besteht die Gefahr, dass Deutschland von den internationalen Entwicklungen abgehängt wird und somit das Profil eines wichtigen Wirtschaftsstandorts für digitale Innovationen verliert. Um digitale Schlüsseltechnologien sowie Innovations- und Wertschöpfungspotentiale nutzen zu können, müssen die Forschung und Entwicklung, auch im Bereich der Cybersicherheit, daher konsequent weiter gefördert werden.

3.8.1.1 Entwicklung sicherer IKT-Systeme

Digitale Technologien können nur erfolgreich sein, wenn diese breitflächig eingesetzt werden und es somit allen Menschen erlauben, die Chancen der Digitalisierung auch barrierefrei zu nutzen. Breiter Einsatz ist regelmäßig das Resultat von ausreichender Verfügbarkeit sowie Vertrauen der Verbraucher:innen in Technologien. Dieses Vertrauen wird regelmäßig beeinträchtigt, wenn Angriffe auf von ihnen genutzte IKT-Systeme erfolgreich verlaufen.

Cybersicherheit ist daher eine der grundlegenden Voraussetzungen für den Einsatz digitaler Systeme. Die besondere Herausforderung hierbei liegt darin, fortwährend ein umfangreiches Gefahrenspektrum in angemessener Tiefe abzudecken. Um dies zu gewährleisten und allen Nutzer:innen zielgerichtet entwickelte Sicherheitslösungen anbieten zu können, ist eine freie und unabhängige Forschungsinfrastruktur erforderlich, in der nachweisbar sichere und über den gesamten Lebenszyklus verlässliche IKT-Produkte und Dienstleistungen entwickelt werden können.

3.8.1.2 Transfer aus der Forschung in die Praxis

Damit der Informationstransfer zwischen Forschung und Praxis optimal funktioniert, müssen Anwendungsbereiche sowie praktische Probleme bereits bei der Entwicklung neuer Technologien mitgedacht werden. Die hierfür erforderliche Denkweise wird in besonderem Maße durch interdisziplinäre Studiengänge vermittelt, da hier zu einem Denken über den Tellerrand ermutigt wird und Studierende bereits frühzeitig üben, Probleme aus unterschiedlichen Fachgebieten mit praktischen Herausforderungen zu verknüpfen.

Ein weiterer Baustein im erfolgreichen Wissenstransfer liegt in der engen Zusammenarbeit zwischen Forschungseinrichtungen und den Nutzer:innen entwickelter Lösungen. Hierdurch wird sichergestellt, dass Unternehmen bei der Entwicklung cybersicherer Hard- und Softwarelösungen die Ergebnisse der Forschung zielführend nutzen und gegebenenfalls einen wertvollen Input leisten können, wie die Anwendbarkeit und der Nutzen neuer Technologien weiter gesteigert werden könnte.

Ein Treiber des Wissenstransfers in die Wirtschaft sind deshalb Start-ups. Start-ups sind neu gegründete Unternehmen, die sich durch einen hohen Innovationsgrad kennzeichnen. Das Ziel eines Start-ups ist die Entwicklung einer neuen Lösung in Form eines Produkts oder einer Dienstleistung, weshalb Start-ups häufig in der Technologiebranche beheimatet sind. Sie haben für einen Wirtschaftsstandort eine herausgehobene Bedeutung: Neben der Schaffung von Arbeitsplätzen fördern sie auch die Wettbewerbs- und Innovationsfähigkeit.

3.8.2 Innovationsförderung auf Ebene des Bundes und der Länder

Durch die Europäische Union sowie durch die Bundesregierung werden Forschungsvorhaben im Bereich der Cybersicherheit unterstützt. So wurde durch den Bund das Forschungsprogramm „Digital – Sicher – Souverän“ (2021-2026) ins Leben gerufen. Mit diesem Rahmenprogramm soll die exzellente Forschung für IT-Sicherheit und Privatheit gefördert werden.[88]

Weiterhin werden durch den Bund und die Länder diverse Einrichtungen und Forschungsprojekte zur Cybersicherheit, wie zum Beispiel das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE, gefördert.

Mit der Initiative „IT-Sicherheit in der Wirtschaft“ unterstützt das Bundesministerium für Wirtschaft und Energie Unternehmen darin, ihre IT-Sicherheit zu verbessern. Insbesondere kleine und mittelständische Unternehmen werden für das Thema Cybersicherheit sensibilisiert. KMU werden hierbei durch konkrete Hilfsangebote bei der Erhöhung ihres IT-Sicherheitsniveaus unterstützt (zum Beispiel durch Webseitenchecks, Handlungsleitfäden, Schulungs- und Lehrmaterialien).

Im Rahmen der Initiative wurden in den vergangenen Jahren mehrere Projekte gefördert, die konkrete Unterstützungs-, Sensibilisierungs- und Qualifikationsangebote für KMU erarbeitet haben.

3.8.3 Forschung und Innovationsförderung in der Freien Hansestadt Bremen

An den im Land Bremen beheimateten Hochschulen wird ebenfalls zum Themenfeld Cybersicherheit geforscht.

So besteht eine Kooperation zwischen der bremischen Verwaltung mit dem Technologiezentrum Informatik (TZI) zur Verbesserung der Informationssicherheit in der Verwaltung.

Das TZI beteiligt sich unter anderem an der Entwicklung und Weiterentwicklung von Standards für Cybersicherheit, der Erkennung und Validierung von Security Patterns und der Entwicklung sicherer mobiler Anwendungen zur Steuerung von Smart Home-Systemen.

An der Hochschule Bremen forscht das Zentrum für Informatik und Medientechnologien (ZIMT) zu Themen der Cybersicherheit und durch das Deutsche Institut für Luft- und Raumfahrt (DLR) mit seinem Institut für die Sicherung maritimer Infrastrukturen wird am Standort Bremerhaven zu relevanten Fragen der Cybersicherheit in Bezug auf BOS und maritime Sicherheit geforscht.

Forschung zum Thema Cybersicherheit erfolgt zudem am Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI Standort Bremen), am Institut für Seeverkehrswirtschaft und Logistik (ISL) sowie der Universität Bremen (primär am TZI), zum Teil unter Hinzuziehung weiterer bremischer Forschungspartner:innen.

Cybersicherheit spiegelt sich auch in den Inhalten von Lehrveranstaltungen der Hochschulen wider. Beispielhaft ist die Veranstaltung „Informationssicherheit“ an der Universität Bremen zu benennen, in der pro Jahr ca. 100 Studierende der Informatik und benachbarter Studiengänge die Grundlagen der Informationssicherheit erlernen.

Zudem gibt es im Land Bremen mehrere größere Forschungsverbundprojekte im Bereich IT-Sicherheit, unter anderem in Kooperation mit lokalen (Bremer) Firmen, bei denen Fragen der Cybersicherheit im Mittelpunkt stehen.

3.8.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Der Erfolg neuer Technologien basiert unter anderem auf ihrem breitflächigen Einsatz. Dies hat zur Folge, dass Aspekte der Benutzer:innenfreundlichkeit sowie der Betriebswirtschaftlichkeit bei der Entwicklung neuer Technologien eine bestimmende Rolle einnehmen. Um zu gewährleisten, dass die Aspekte der Cybersicherheit bereits bei der Ideenfindung und im weiteren Verlauf der Entwicklung berücksichtigt werden, ist es erforderlich, die Grundkompetenzen und das spezifische Fachwissen zum Thema Cybersicherheit in allen Forschungs- und Entwicklungsdisziplinen zu stärken. Hierzu könnten bereits bestehende Forschungsverbünde gestärkt und weitere Forschungskapazitäten zur Grundlagen- und Methodenforschung aufgebaut werden.

Auch kann durch die Etablierung interdisziplinärer Studiengänge erreicht werden, dass ein Wissenstransfer zwischen den einzelnen Fachrichtungen stattfindet, was wiederum die Entwicklung innovativer Lösungen fördert. Um darüber hinaus möglichst praxisnahe und barrierefreie Technologien zu entwickeln, ist es zudem erforderlich, dass ein Wissens- und Technologietransfer zwischen der Wirtschaft sowie den Forschungsinstituten stattfindet.

Durch die Zusammenarbeit zwischen Forschung und Entwicklung sowie den Endanwender:innen können innovative Lösungen erdacht werden bzw. Probleme beim Einsatz der Technologien bei den Endanwender:innen frühzeitig identifiziert und beseitigt werden.

Maßnahmen zur Erreichung dieser Ziele im Rahmen der Strategie sind:

- Stärkung der Grundkompetenzen und des spezifischen Fachwissens zum Themenbereich „Cybersicherheit“ durch
  - Auf- und Ausbau sowie Vermittlung und Weiterentwicklung durch die bereits vorhandenen Bildungs- und Forschungseinrichtungen
  - Prüfung der Etablierung interdisziplinärer Studiengänge zur Cybersicherheit

- Stärkung des Wissens- und Technologietransfers zwischen Wissenschaft und Wirtschaft

- Stärkung von Start-Ups und Forschungsverbünden bei der Entwicklung von Produkten und Dienstleistungen im Bereich der Cybersicherheit

3.9 Nationale und internationale Kooperationen

Der Cyberraum macht vor Länder- und Staatengrenzen nicht halt. Eine tiefergehende Vernetzung beteiligter Akteur:innen auf unterschiedlichen Ebenen ist notwendig, um einen effektiven und effizienten Austausch zur Prävention und Bewältigung von Herausforderungen im Cyberraum zu gewährleisten. Durch gezielte Kooperationsvereinbarungen sowie die Teilnahme an multilateralen Foren können Synergieeffekte erzeugt und das gemeinsame Erreichen von Cybersicherheit ganzheitlich und verbindlich gestaltet werden. Kooperationspartner:innen profitieren in konkreter Form von den gemeinsamen Kenntnissen, Fähigkeiten und Ressourcen und tragen somit dazu bei, das Cybersicherheitsniveau zu steigern.

3.9.1 Herausforderungen des Handlungsfelds

Der Cyberraum ist ein globales Medium ohne geografische Grenzen. Hierdurch können Ziele im Land Bremen von überall aus der Welt digital angegriffen werden. In Soft- oder Hardware vorhandene Schwachstellen betreffen nicht mehr nur einige wenige Anwender:innen. Vielmehr sind sie als globale Risiken zu sehen. Behörden, Unternehmen und Privatpersonen stehen hierbei vor sehr ähnlichen Herausforderungen, die sie bewältigen müssen.

Daher sind nationale und internationale Kooperationen im Bereich Cybersicherheit essenziell. So können zum Beispiel Schwachstellen in einzelnen Anwendungen, die angegriffen werden und ggf. durch den Einzelnen als nicht kritisch bewertet werden, kaskadenartige Folgen nach sich ziehen. Durch Kooperationsnetzwerke, in denen Informationen und Wissen geteilt werden, können Abhängigkeiten besser erkannt, bewertet und Risiken gemindert werden. Nicht nur wissenschaftlichen Kooperationen, auch der internationalen Vernetzung staatlicher Akteur:innen, fällt hierbei eine hohe Bedeutung zu.

Weiterhin können durch nationale und internationale Kooperationen Synergien geschaffen werden, denn aufgrund der weiten Verbreitung von gleichen oder ähnlichen Hard- und Softwaresystemen ist davon auszugehen, dass diverse Akteur:innen Kenntnisse über Schwachstellen haben und ggf. bereits an der Beseitigung dieser arbeiten. Ebenso können so Ressourcen gebündelt werden, um bestehende Probleme zu identifizieren und zu bewältigen. Somit ist der effektive und effiziente Austausch zur Prävention und Bewältigung der Risiken des Cyberraums ein weiterer essenzieller Baustein, um die Cybersicherheit des Landes Bremen zu steigern.

Neben der Etablierung von Netzwerken, die sich auf Informationen zum aktuellen Stand der Cybersicherheit beziehungsweise die Informationssteuerung von Schwachstellen konzentrieren, ist es gleichermaßen wichtig, dass Netzwerke im Bereich der Forschung und Wissenschaft auf- und ausgebaut werden. So können die Ansprüche der Cybersicherheit bei der Entwicklung aktueller und zukünftige Technologien bereits heute mitgedacht werden.

Durch den interdisziplinären Austausch vieler Akteur:innen unterschiedlicher Fachrichtungen wird darüber hinaus ein ganzheitliches Problemverständnis gestärkt, welches bei der Entwicklung zielgerichteter Lösungsansätze hilfreich ist. Die digitale Barrierefreiheit ist als Querschnittsthema und Qualitätsmerkmal mit zu berücksichtigen. Nur über die aktive Mitarbeit in Gremien und über den Abschluss bilateraler Kooperationsvereinbarungen, etwa durch Wirtschaftsverbände, Wissenschaftskooperationen oder staatliche Kooperationsverträge, kann Cybersicherheit für bestimmte Zielgruppen ganzheitlich und verbindlich gestaltet werden.

3.9.2 Nationale und internationale Kooperationen auf Bundesebene

Es existieren diverse Institutionen und Interessenvertretungen, auf internationaler, nationaler und Länderebene, die sich mit dem Thema Cybersicherheit beschäftigen.

Ein Überblick über die umfangreichen nationalen Strukturen und Vernetzungen im Bereich Cybersicherheit bieten das „Online Kompendium Nationaler Cybersicherheitspakt“ des BMI sowie die Publikation „Deutschlands staatliche Cybersicherheitsstruktur“ der Stiftung Neue Verantwortung (vgl. Handlungsfeld 1).

3.9.3 Nationale und internationale Kooperationen in der Freien Hansestadt Bremen

Die Freie Hansestadt Bremen wird durch mehrere Behörden in nationalen Cybersicherheitsnetzwerken, wie der Allianz für Cybersicherheit, vertreten. Weiterhin ist das Land Bremen aktiv an der Arbeitsgruppe Cybersicherheit der Innenministerkonferenz beteiligt.

Perspektivisch wird eine noch engere, auch vertraglich abgesicherte, Kooperation mit dem BSI, insbesondere in den Bereichen Informationsaustausch, Sensibilisierung und Fortbildung sowie der gegenseitigen Unterstützung bei der Umsetzung von Cybersicherheitsmaßnahmen, angestrebt.

3.9.4 Handlungserfordernisse und Ziele im Rahmen der Strategieumsetzung

Aufgrund der globalen Bedeutung des Themenbereichs „Cybersicherheit“ besteht eine Vielzahl am nationalen und internationalen Kooperationen, an denen auch das Land Bremen partizipieren kann. Um von dem Informationsfluss aus diesen Netzwerken zu profitieren und gleichzeitig das Errichten von Parallel- oder Doppelstrukturen zu vermeiden, wird die noch auszugestaltenden Zentralstelle für Cybersicherheit als SPoC der öffentlichen Verwaltung für alle die Cybersicherheit betreffenden Netzwerke bestimmt. So kann sichergestellt werden, dass die in den Netzwerken gewonnen Informationen an die entsprechenden Stellen in der öffentlichen Verwaltung der Freien Hansestadt Bremen gesteuert werden und Inhalte gleichermaßen auch in die jeweiligen Netzwerke hineintransportiert werden können.

Zudem können durch den Aufbau von Kooperationsbeziehungen mit anderen Cybersicherheitsbehörden Synergieeffekte bei der Erkennung von Cybersicherheitsrisiken sowie der Bewältigung von Sicherheitsvorfällen geschaffen werden.

Neben einem Erfahrungsaustausch durch Netzwerkarbeit ist zudem angestrebt, dass durch wechselseitige Hospitationen auf Landesebene die Fähigkeiten der noch auszugestaltenden Zentralstelle Cybersicherheit optimiert werden können.

Um die beschriebenen Herausforderungen zu bewältigen, wurden folgende Maßnahmen bei der Erstellung der Bremischen Cybersicherheitsstrategie 2023 identifiziert:

- Einrichtung der noch auszugestaltenden Zentralstelle für Cybersicherheit als Single Point of Contact der öffentlichen Verwaltung für alle die Cybersicherheit betreffenden Netzwerke

- Aufbau von Kooperationsbeziehungen mit anderen Cybersicherheitsbehörden auf Länder- und Bundesebene durch die noch auszugestaltende Zentralstelle für Cybersicherheit

4. Zusammenfassung und Ausblick

Cybersicherheit ist im Land Bremen kein neues Handlungsfeld. Es bestehen bereits viele Bestrebungen und Initiativen, IKT-Strukturen resilienter zu machen, Mitarbeiter:innen besser auf Cybergefahren vorzubereiten und Verbraucher:innen besser zu schützen. Die Komplexität der Thematik spiegelt sich jedoch auch in der Vielzahl der Akteur:innen sowie der Maßnahmen wieder, welche zu einer Stärkung der Cybersicherheit im Land beitragen.

Ein wichtiger Schritt bestand deshalb darin, einen Überblick über die bisherigen Aktivitäten und Akteur:innen zu erhalten und die erlangten Informationen zu strukturieren. Dies ist mit der Bremischen Cybersicherheitsstrategie 2023 geschehen.

So wurde aufgezeigt, dass staatliche Strukturen zur Cybersicherheit auf europäischer sowie nationaler Ebene bestehen, allerdings in den wenigsten Bundesländern bereits dezidierte Stellen existieren, die für diesen Themenkomplex verantwortlich sind. Es herrscht hingegen ein komplexes Geflecht an Akteur:innen unterschiedlichster Art, die sich mit Teilbereichen der Cybersicherheit befassen. Hierbei existieren teilweise Doppelstrukturen, während Zuständigkeiten noch nicht abschließend geregelt sind. Gleichermaßen existiert eine Vielzahl rechtlicher Rahmenbedingungen auf subnationaler, nationaler und supranationaler Ebene, die von den Akteur:innen beachtet werden müssen. Dies alles geschieht vor dem Hintergrund zunehmend aktiver europäischer Regulierung, der zusätzliche Anforderungen an die Übernahme sowie Schaffung rechtlicher Regelungen auf nationaler Ebene stellt.

Um die bereits bestehenden Bemühungen zur Steigerung der Cybersicherheit in der Freien Hansestadt Bremen zu intensivieren und noch stärker zu harmonisieren, sind weiterreichende Veränderungen und Ausrichtungen erforderlich, die nur im Verbund der beteiligten Akteur:innen erreicht werden können.

Die Bremische Cybersicherheitsstrategie 2023 ist als erster Schritt in einem fortlaufenden Prozess zu verstehen. In ihr wurden Handlungserfordernisse identifiziert und dargestellt, um das weitere Vorgehen planbarer zu gestalten.

Zur Steigerung der Cybersicherheit werden klare Zuständigkeiten festgelegt und eine gesamtverantwortliche Stelle in der Freien Hansestadt Bremen bestimmt. Hierfür werden die bestehenden rechtlichen Grundlagen kritisch geprüft und gegebenenfalls angepasst bzw. geschaffen. Ebenfalls wird geprüft werden, wie die Zusammenarbeit zwischen Bund, Land, Kommunen, der Wirtschaft und den Bürger:innen rechtssicher und nachhaltig gestaltet werden kann, damit alle an den Vorzügen der Digitalisierung partizipieren können.

Im Rahmen der Erstellung der Cybersicherheitsstrategie wurden bereits einzelne Akteur:innen identifiziert, denen eine tragende Rolle bei der Stärkung der digitalen Resilienz in der Freien Hansestadt Bremen zuteilwird und die in den weiteren Prozess eingebunden werden müssen. Allerdings ist den verantwortlichen Stellen ebenfalls bewusst, dass es sich hierbei nicht um eine abschließende Liste handelt und weitere, bisher nicht identifizierte Akteur:innen, existieren, die ebenfalls einen wichtigen Beitrag zur Steigerung der digitalen Resilienz in der Freien Hansestadt Bremen leisten können. Diese gilt es in einem nächsten Schritt ebenfalls zu identifizieren und am Prozess zu beteiligen.

Die Bremische Cybersicherheitsstrategie 2023 stellt einen konzeptuellen Rahmen für die Ausrichtung der Cybersicherheitspolitik der Freien Hansestadt Bremen dar, die auf Basis dieser umfangreichen Ausarbeitung zielgerichtet, planvoll und informiert gestaltet werden kann.

Für viele Handlungsfelder konnten bereits vielversprechende Ansätze für Maßnahmen entwickelt werden, um die Ziele in den jeweiligen Handlungsfeldern zu verwirklichen.

Es ist daher erforderlich, weitere Umsetzungspläne zu entwickeln, in denen die strategische Ausrichtung mit messbaren Maßnahmen und Zielen verknüpft und Zuständigkeiten und Verantwortlichkeiten definiert werden.

Hierbei müssen bereits bestehende Expertisen identifiziert und genutzt werden, um unnötige Doppelungen zu vermeiden und ressourcenschonend zu agieren.

Weiterhin ist es erforderlich, den Prozess und das weitere Vorgehen transparent zu gestalten und mit proaktiver Kommunikation zu begleiten. Nur so kann eine breite Akzeptanz bei allen Akteur:innen geschaffen und eine konstruktive Zusammenarbeit zur Stärkung der Cybersicherheit stattfinden.

Oberstes Ziel dieses Prozesses muss es sein, die digitale Resilienz aller Akteur:innen in der Freien Hansestadt Bremen zu steigern und Cybersicherheitsgefahren zu minimieren.

Die vorliegende Cybersicherheitsstrategie stellt einen wichtigen Schritt in einem sich ständig weiterentwickelnden Zyklus zur Stärkung der digitalen Resilienz der Freien Hansestadt Bremen dar. Im Rahmen dieses Prozesses wird sie regelmäßig evaluiert, an neue Gegebenheiten angepasst und stetig weiterentwickelt werden.

Informationsprozess

Folgende Stellen wurden über die Erstellung der Bremischen Cybersicherheitsstrategie im Vorfeld informiert. Ihnen wurde Gelegenheit gegeben, Punkte zu benennen, die aus ihrer Sicht für die Stärkung der Resilienz gegenüber Cyberbedrohungen eine besondere Bedeutung einnehmen. Es ist beabsichtigt, diese Stellen im Rahmen der Evaluation der Bremischen Cybersicherheitsstrategie zu einer Stellungnahme einzuladen.

- AG AP Arbeitsgemeinschaft Ambulante Pflege
- Alevitische Gemeinde Bremen
- Alevitisches Kulturzentrum in Bremen und Umgebung e. V.
- Ameos Klinikum Bremen
- Arbeitnehmerkammer
- AOK Bremen / Bremerhaven
- Apothekerkammer Bremen
- Arbeitsgemeinschaft der Krankenkassenverbände in Bremen
- Ärztekammer Bremen
- Behandlungszentrum Nord
- BKK Landesverband Mitte, Landesvertretung Bremen
- Bremenports GmbH & Co. KG
- Bremer Aufbau-Bank GmbH
- Bremer Krebsgesellschaft – Landesverband der Deutschen Krebsgesellschaft e. V.
- Bremer Pflegerat
- Bremer Psychoanalytische Vereinigung e. V.
- Bremerhavener Gesellschaft für Investitionsförderung und Stadtentwicklung mbH (BIS)
- Bremische Evangelische Kirche
- Bremische Schwesternschaft vom Roten Kreuz e. V.
- Die Unternehmensverbände im Lande Bremen e. V. (UVHB)
- DITIB Islamische Religionsgemeinschaften Niedersachsen und Bremen
- Flughafen Bremen GmbH
- Freies Institut für IT-Sicherheit e. V.
- Glocke Verwaltungs-GmbH
- Handelskammer Bremen für Bremen und Bremerhaven
- Handwerkskammer
- Hebammenlandesverband Bremen e. V.
- HEIM-MITWIRKUNG – Unabhängige Selbsthilfe-Initiative für Pflegebetroffene
- Hochschule Bremen
- Hochschule Bremerhaven
- Hochschule für Künste
- IKK gesund plus
- IPP Bremen GmbH
- Islamische Föderation Bremen e. V.
- Jüdische Gemeinde im Lande Bremen
- Kassenärztliche Vereinigung Bremen
- Kassenärztliche Vereinigung im Lande Bremen
- Kassenzahnärztliche Vereinigung im Lande Bremen
- Katholischer Gemeindeverband Bremen
- Klinikum Bremen-Ost (Psychiatrie)
- Klinikum Reinkenheide (Psychiatrie)
- Krankenhausgesellschaft der Freien Hansestadt Bremen e. V.
- Kreishandwerkerschaft Bremen
- LandesArbeitsGemeinschaft (LAG) der Freien Wohlfahrtspflege Bremen e. V.
- Landesfrauenrat Bremen – Bremer Frauenausschuss e.V. (bfa)
- Landesverband der Islamischen Kulturzentren Norddeutschland e. V. – VIKZ
- M3B GmbH
- Medizinischer Dienst Bremen

- Menorah – Jüdische Gemeinde zu Bremerhaven/Bremen e. V.
- NOKI Bremen
- Norddeutsches Institut für Verhaltenstherapie e. V.
- Paritätisches Bildungswerk Landesverband Bremen e. V.
- Psychoanalytisches Institut Bremen e. V.
- Psychotherapeutenkammer Bremen
- SCHURA – Islamische Religionsgemeinschaften Bremen e. V.
- Techniker Krankenkasse, Landesvertretung Bremen
- Tierärztekammer Bremen
- Unfallkasse Freie Hansestadt Bremen
- Universität Bremen
- Universum Managementgesellschaft mbH
- Verband der Ersatzkassen (vdek), Landesvertretung Bremen
- Verband Deutscher Alten- und Behindertenhilfe e. V. (VDAB) – Landesvertr. Bremen
- Verbraucherzentrale Bremen e. V.
- Verein 21 Hoch 3 e. V.
- WFB Wirtschaftsförderung Bremen GmbH
- Zahnärztekammer Bremen

Die Auflistung erfolgte alphabetisch.

Bildnachweis

Deckblattgestaltung: Samuel Streppel, SI.

Abbildungsverzeichnis

Tabellenverzeichnis

Quellennachweise

1 Destatis (2022): Pressemitteilung Nr. 035 vom 26. Januar 2022. Wiesbaden. Online: Pressemitteilung Nr. 35 vom 26. Januar 2022 (letzter Abruf: 20.03.2023).
2 bitkom (2021): Ein Jahr Corona: Wie digital arbeiten deutsche Unternehmen? Berlin. Online: Ein Jahr Corona: Wie digital arbeiten deutsche Unternehmen? (letzter Abruf: 20.03.2023).
3 Destatis (2022): Zahl der Woche Nr. 23 vom 14. Juni 2022. Wiesbaden. Online: Die Zahl der Woche Nr. 23 vom 14. Juni 2022 (letzter Abruf: 20.03.2023).
4 bitkom (2022): Das intelligente Zuhause: Smart Home 2022. Berlin. Online: Das intelligente Zuhause: Smart Home 2022 (letzter Abruf: 20.03.2023).
5 Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz (2021): Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien. Verfügbar auf Anfrage.
6 Die Senatorin für Wirtschaft, Arbeit und Europa (2021): Schlüssel zu Innovationen 2030 – Strategie für Innovation, Dienstleistungen und Industrie im Land Bremen. Bremen. Online: Schlüssel zu Innovationen 2030 - Strategie für Innovation, Dienstleistungen und Industrie im Land Bremen (letzter Abruf: 20.03.2023).
7 Bundesministerium der Verteidigung (2022): FAQ: Cyber-Abwehr. Berlin. Online: FAQ: Cyber-Abwehr (letzter Abruf: 20.03.2023).
8 Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (2021): Strategie Cyber VBS. Bern. Online: Strategie Cyber VBS (letzter Abruf: 20.03.2023).
9 Schubert, C. (2021): Flammen wüten bei größtem Cloud-Anbieter Europas. Frankfurt faz.net. Online: Flammen wüten bei größtem Cloud-Anbieter Europas (letzter Abruf: 20.03.2023).
10 Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit in Deutschland 2022. Bonn. Online: Die Lage der IT-Sicherheit in Deutschland 2022 (letzter Abruf: 20.03.2023).
11 bitkom (2022): Wirtschaftsschutz 2022. Berlin. Online: Wirtschaftsschutz 2022 (letzter Abruf: 20.03.2023).
12 Kipker, D.-K. (Hrsg.) (2020): Cybersecurity: Rechtshandbuch. München: C.H. Beck.
13 Kipker, D.-K. (2023): Cybersecurity Navigator. Online: Cybersecurity Navigator (letzter Abruf: 20.03.2023).
14 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.
15 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 (ABl. L 333 vom 27.12.2022, S. 80).
16 Europäische Kommission (2022): Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020.
17 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015.
18 Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23. Juni 2017.
19 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021.
20 Bundesministerium des Innern und für Heimat (2022): Eckpunkte für das KRITIS-Dachgesetz. Berlin. Online: Eckpunkte für das KRITIS-Dachgesetz (letzter Abruf: 20.03.2023).
21 Europäische Kommission (2020): Die Cybersicherheitsstrategie der EU für die digitale Dekade, Brüssel. Online: Die Cybersicherheitsstrategie der EU für die digitale Dekade (letzter Abruf: 20.03.2023).
22 Bundesministerium des Innern und für Heimat (2011): Cyber-Sicherheitsstrategie für Deutschland, Berlin.
23 Bundesministerium des Innern und für Heimat (2016): Cyber-Sicherheitsstrategie für Deutschland, Berlin.
24 Bundesministerium des Innern und für Heimat (2021): Cyber-Sicherheitsstrategie für Deutschland, Berlin.
25 S. EN 24.
26 S. EN 5.
27 BSI-Errichtungsgesetz vom 17. Dezember 1990 (BGBl. I S. 2834), zuletzt geändert durch Artikel 11 der Verordnung vom 25. November 2003 (BGBl. I S. 2304). Online: Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (letzter Abruf: 20.03.2023).
28 Bundesamt für Sicherheit in der Informationstechnik (2022): Auftrag. Bonn. Online: Auftrag des BSI (letzter Abruf: 20.03.2023).
29 Bundesministerium des Innern und für Heimat (2020): Online-Kompendium Cybersicherheit in Deutschland, Berlin. Online: Online-Kompendium Nationaler Pakt Cybersicherheit (letzter Abruf: 20.03.2023).
30 S. EN 29.
31 Herpig, S./ Rupp, C. (2022): Deutschlands staatliche Cybersicherheitsarchitektur. 9. Auflage. Berlin: Stiftung Neue Verantwortung. Online: Deutschlands staatliche Cybersicherheitsarchitektur (letzter Abruf: 20.03.2023).

[32] Bundesministerium der Justiz (2019): IT-Staatsvertrag in der Fassung der Bekanntmachung vom 13. Dezember 2019 (BGBl. I S. 2852). Online: IT-Staatsvertrag (letzter Abruf: 20.03.2023).
[33] Arbeitsgruppe Informationssicherheit des IT-Planungsrats (2018): Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung. Online: Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (letzter Abruf: 20.03.2023).
[34] Ministerium des Inneren, für Digitalisierung und Kommunen des Landes Baden-Württemberg (2021): Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026. Stuttgart. Online: Cybersicherheitsstrategie Baden-Württemberg Perspektive 2026 (letzter Abruf: 20.03.2023).
[35] Ministerium des Inneren des Landes Nordrhein-Westfalen (2021): Cybersicherheitsstrategie des Landes Nordrhein-Westfalen, Düsseldorf. Online: Cybersicherheitsstrategie des Landes Nordrhein-Westfalen (letzter Abruf: 20.03.2023).
[36] LT-Drs. des Landes Baden-Württemberg (2021): Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften vom 04.02.2021 – LT-Drs.16/9723.
[37] Der Senat der Freien Hansestadt Bremen (2022): 205. Sitzung des bremischen Senats am 04.10.2022 (2022): TOP 1 – Cybersicherheit im Land Bremen. Online: Cybersicherheit im Land Bremen (letzter Abruf: 20.03.2023).
[38] Initiative D21 e.V. (2022): eGovernment Monitor 2022: Fortschritte bei der Verwaltungsdigitalisierung bleiben aus Sicht der Bevölkerung weiter aus. München. Online: eGovernment-Monitor 2022 (letzter Abruf: 20.03.2023).
[39] Kommune 21 (2023): Bremen: Gut aufgestellt. Online: Bremen: Gut aufgestellt (letzter Abruf: 20.03.2023).
[40] Bundesministerium des Innern und für Heimat (2022): Cyberkriminalität. Berlin.
[41] Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 30. März 2021.
[42] Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 3 des Gesetzes vom 21. Juli 2022 (BGBl. I S. 1182) geändert worden ist.
[43] Bundeskriminalamt (2022): Zentrale Ansprechstellen Cybercrime der Polizeien, Wiesbaden. Online: Zentrale Ansprechstellen Cybercrime (letzter Abruf: 20.03.2023).
[44] Bundesamt für Verfassungsschutz (2022): Verfassungsschutzverbund, Köln. Online: Verfassungsschutzverbund (letzter Abruf: 20.03.2023).
[45] Bundeskriminalamt (2022): Cybercrime Bundeslagebild 2021. Wiesbaden. Online: Bundeslagebild Cybercrime 2021 (letzter Abruf: 20.03.2023).
[46] Bundesamt für Verfassungsschutz (2022): Publikationen. Köln. Online: Publikationssuche (letzter Abruf: 20.03.2023).
[47] S. EN 10.
[48] § 8a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik. Online: BSIG (letzter Abruf: 20.03.2023).
[49] Der Mittelstand, Bundesverband mittelständische Wirtschaft e.V. (o.J.): Der Mittelstand ist Garant für Stabilität und Fortschritt. Online: BVMW Zahlen und Fakten (letzter Abruf: 20.03.2023).
[50] Bundesamt für Sicherheit in der Informationstechnik (o.J.): UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland. Online: UP KRITIS (letzter Abruf: 20.03.2023).
[51] Statista (2022): Größte Häfen in der Europäischen Union nach Containerumschlag 2021. Online: Größte Häfen in der EU nach Containerumschlag 2021 (letzter Abruf: 20.03.2023).
[52] Der Senator für Wirtschaft, Arbeit und Häfen (2018): „Bremen Digital 2019-2021“ – Die Digitalisierungsinitiative zur Stärkung der Innovationskraft der Wirtschaft im Land Bremen. Bremen.
[53] Destatis (2022): Internetnutzer/-innen und Online-Einkäufer/-innen. Online: IT-Nutzung: Internetnutzer/-innen und Online-Einkäufer/-innen 2022 (letzter Abruf: 20.03.2023).
[54] Beisch, N. / Koch, W. (2022): Aktuelle Aspekte der Internetnutzung in Deutschland. ARD/ZDF-Onlinestudie: Vier von fünf Personen in Deutschland nutzen täglich das Internet. In: Media Perspektiven 10/2022: S. 460-470. Online: ARD/ZDF-Online-Studie (letzter Abruf: 20.03.2023).
[55] Initiative klicksafe im Digital Europe Program (DIGITAL) vertreten durch die Medienanstalt Rheinland-Pfalz (o.J.): Cybergrooming - Hilfe bei sexueller Belästigung von Kindern (klicksafe.de). Online: Klicksafe: Cybergrooming (letzter Abruf: 20.03.2023).
[56] Vuorikari, R. / Kluzer, S. / Punie, Y. (2022): DigComp 2.2 The digital Competence Framework for Citizens. Brüssel: Publications Bureau of the European Union. Online: DigComp2.2 (letzter Zugriff: 20.03.2023).
[57] initiative D21 e.V. (2021): Digital Skills Gap. So (unterschiedlich) digital kompetent ist die deutsche Bevölkerung. Online: Digital Skills Gap (letzter Abruf: 20.03.2023).
[58] S. EN 57.
[59] initiative D21 e.V. (2020): Digital Gender Gap. Lagebild zu Gender(un)gleichheiten in der digitalisierten Welt. Online: Gender Digital Gap (letzter Abruf: 20.03.2023).
[60] initiative D21 e.V. (2023): D21-Digital-Index 2022/23. Jährliches Lagebild zur Digitalen Gesellschaft. Online: D21-Digital-Index 2022/2023 (letzter Abruf: 20.03.2023).
[61] Deloitte (2021): Cyber Security Report 2021. Wahljahr 2021 – digitale Meinungsbildung ein Risiko. Online: Cyber Security Report 2021 (letzter Abruf: 20.03.2023).
[62] Deutschland sicher im Netz e.V. (o.J.): Digitaler Engel. Online: Digitaler Engel (letzter Abruf: 20.03.2023).

[63] Initiativbüro "Gutes Aufwachsen mit Medien" (o.J.): Gutes Aufwachsen mit Medien – Schützen. Handeln. Stärken. Online: Gutes Aufwachsen mit Medien (letzter Abruf: 20.03.2023).
[64] Deutschland sicher im Netz e.V. (o.J.): Deutschland sicher im Netz. Online: Deutschland sicher im Netz (letzter Abruf: 20.03.2023).
[65] Initiative klicksafe im Digital Europe Program (DIGITAL) vertreten durch die Medienanstalt Rheinland-Pfalz (o.J.): Klicksafe. Online: https://www.klicksafe.de/ (letzter Abruf: 20.03.2023).
[66] Projektbüro SCHAU HIN! (o.J.): www.schau-hin.info. Online: Schau hin! (letzter Abruf: 20.03.2023).
[67] Der Senat der Freien Hansestadt Bremen (2022): Medienkompetenzförderung in Bremen und Bremerhaven - Gesamtstrategie und Bestandsaufnahme. Bremen.
[68] Bremische Landesmedienanstalt (o. J.): Medienkompetenz: Fit für die digitale Welt. Online: Medienkompetenz: Bremische Landesmedienanstalt (bremische-landesmedienanstalt.de) (letzter Abruf: 20.03.2023).
[69] Der Senator für Finanzen (2021): Qualifica Digitalis: Forschungs-, Entwicklungs- und Umsetzungsprojekt für die Qualifizierung des digitalisierten öffentlichen Sektors. Online: QUALIFICA digitalis (letzter Abruf: 24.03.2023).
[70] S. EN 10.
[71] S. EN 10.
[72] Bundesamt für Sicherheit in der Informationstechnik (2022): Social Engineering – der Mensch als Schwachstelle. Online: Social Engineering (letzter Abruf: 20.03.2023).
[73] Europäische Kommission (2022): EU Cyber Resilience Act – New EU cybersecurity rules ensure safer hardware and software. Online: EU Cyber Resilience Act (letzter Zugriff: 20.03.2023).
[74] Bundesamt für Sicherheit in der Informationstechnik (2021): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). Online: IT-Sicherheitsgesetz 2.0 (letzter Abruf: 20.03.2023).
[75] Die Senatorin für Gesundheit, Frauen und Verbraucherschutz (2022): Internet-Abzocke und Cybercrime: Wie schütze ich mich? Online: Internet-Abzocke und Cybercrime: Wie schütze ich mich? (letzter Abruf: 20.03.2023).
[76] Projekt Kompetenzzentrum Fachkräftesicherung (2022): Ländersteckbrief Deutschland. Online: Ländersteckbrief Deutschland (letzter Abruf: 20.03.2023).
[77] Projekt Kompetenzzentrum Fachkräftesicherung (2022): Ländersteckbrief Bremen, Online: Ländersteckbrief Bremen (letzter Abruf: 20.03.2023).
[78] Marjenko, A. / Müller, M. / Sauer, S. (2021): Das KfW-ifo-Fachkräftebarometer: Jedes fünfte deutsche Unternehmen wird derzeit durch Fachkräftemangel beeinträchtigt. In: ifo Schnelldienst 74(4), S. 57-59.
[79] Schindler, J. (2022): Unternehmenschefs zu IT-Sicherheit: Die größte Herausforderung ist das Personal. Online: Unternehmenschefs zu IT-Sicherheit (letzter Abruf: 20.03.2023).
[80] Institut für Arbeitsmarkt- und Berufsforschung (2022): Zentrale Befunde zu aktuellen Arbeitsmarktthemen 2021/2022. Online: Zentrale Befunde zu aktuellen Arbeitsmarktthemen (letzter Abruf: 20.03.2023).
[81] Schuetze, J. (2018): Warum dem Staat IT-Sicherheitsexpert:innen fehlen. Eine Analyse des IT-Sicherheitsfachkräftemangels im Öffentlichen Dienst. Berlin: Stiftung Neue Verantwortung. Online: IT-Sicherheitsfachkräftemangel (letzter Abruf: 20.03.2023).
[82] Schüür-Langkau, A. (2021): Verwaltung braucht fast 50.000 IT-Fachkräfte. Online: Verwaltung braucht fast 50.000 IT-Fachkräfte (letzter Abruf: 20.03.2023).
[83] Destatis (2022): Durchschnittliche Bruttojahresverdienste von Vollzeitbeschäftigten im Jahr 2021. Online: Bruttojahresverdienste nach Branchen (letzter Abruf: 20.03.2023).
[84] Suessenbach, F. / Schröder, E. / Winde, M. (2022): Informatik für alle! Informatikunterricht zur gesellschaftlichen Teilhabe und Chancengleichheit, Essen: Stifterverband für die Deutsche Wirtschaft e.V. Online: Informatik für alle! (letzter Abruf: 20.03.2023).
[85] Aktion Mensch e.V. (2022): Inklusionsbarometer Arbeit 2022. 10. Jahrgang (2022). Online: Inklusionsbarometer Arbeit 2022 (letzter Abruf: 20.03.2023).
[86] Bundesministerium für Wirtschaft und Klimaschutz (2022): Fachkräfte für Deutschland. Online: Dossier: Fachkräfte für Deutschland (letzter Abruf: 20.03.2023).
[87] VDE (2022): Cybersecurity und Fachkräftemangel größte Herausforderung bei Energiewende. Online: Cybersecurity und Fachkräftemangel größte Herausforderung bei Energiewende (letzter Abruf: 20.03.2023).
[88] Bundesministerium für Bildung und Forschung – Referat Vernetzung und Sicherheit digitaler Systeme (2021): Digital. Sicher. Souverän Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit. Online: Digital. Sicher. Souverän. Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit (letzter Abruf: 20.03.2023).

Impressum

Freie
Hansestadt
Bremen

Herausgeber

Der Senator für Inneres
im Auftrag des Senats der Freien Hansestadt Bremen

Stand

April 2023