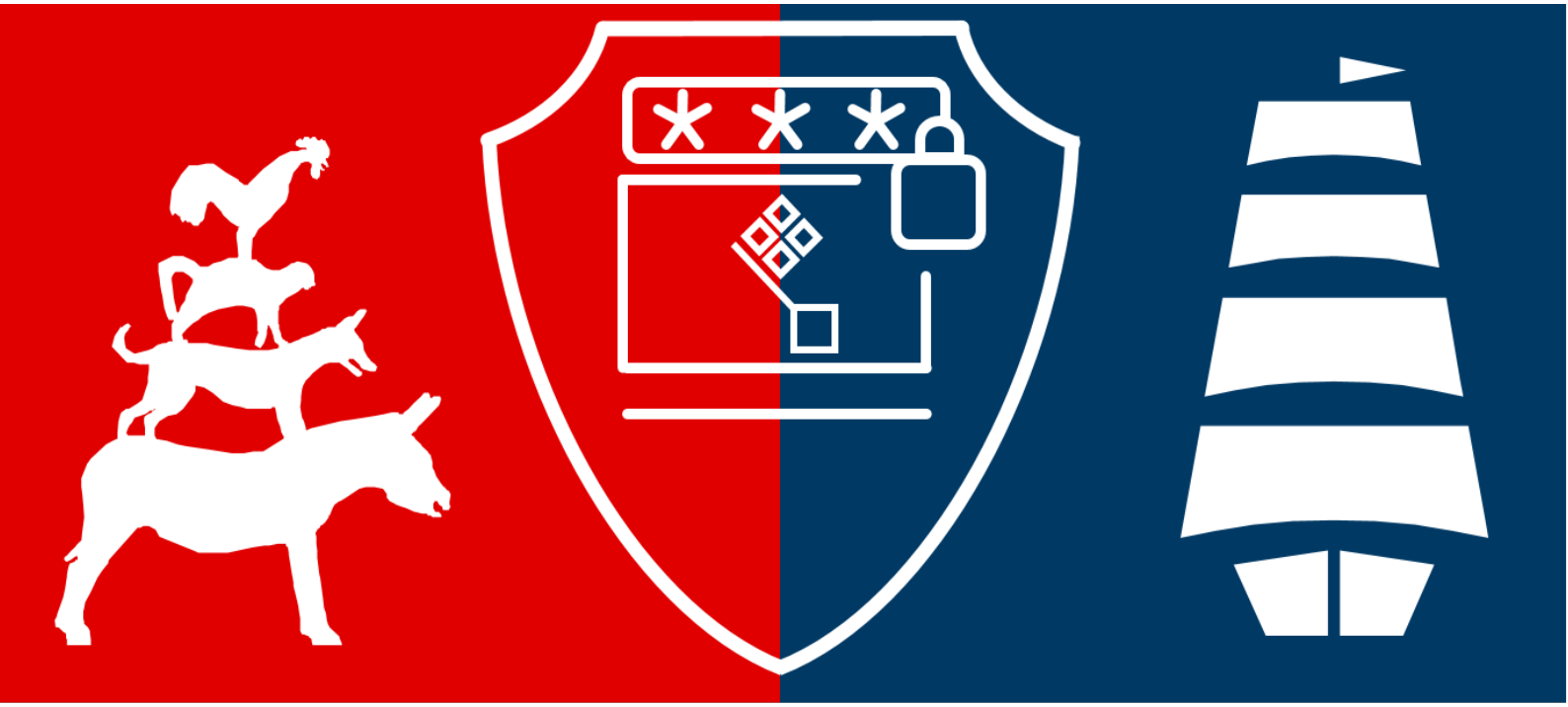


EVALUATIONSBERICHT

Bremische Cybersicherheitsstrategie 2023

Die Senatorin für Inneres und Sport

02.02.2026

Inhaltsverzeichnis

1. Einleitung

Mit der Verabschiedung der Bremischen Cybersicherheitsstrategie 2023 wurde ein Evaluationsintervall konkretisiert, welches eine erstmalige Bewertung nach zwei Jahren vorsieht. Dieses Intervall wurde bewusst sehr kurz gewählt, um eine zügige Errichtung erster struktureller Maßnahmen voranzubringen und gleichzeitig der hohen Dynamik des Phänomenbereichs gerecht zu werden: Maßnahmen von heute passen möglicherweise schon nicht mehr zu den Bedrohungen von morgen.

Gleichzeitig war es wichtig, eine verbindliche Architektur für die Steigerung der Cybersicherheit im Land Bremen zu schaffen und diese anschlussfähig zu machen: Da Cyberkriminelle nicht an Landesgrenzen Halt machen, fällt der Interoperabilität sowie Harmonisierung von Maßnahmen eine wichtige Rolle zu, sowohl in Bezug auf Abstimmungen unterschiedlicher Akteur:innen auf Landesebene als auch auf Bundesebene. Eine abgestimmte strategische Ausrichtung stellt hierbei sicher, dass alle Beteiligten im digitalen Tauziehen um mehr Cybersicherheit auf der gleichen Seite stehen und darüber hinaus am selben Seil ziehen.

Da der vorliegende Evaluationsbericht die Grundlage für die Fortschreibung der Bremischen Cybersicherheitsstrategie im Jahr 2026 darstellt, wurde die Entscheidung getroffen, sowohl die Erstellung der Strategie als auch die Umsetzung der Maßnahmen in eigenständigen Kapiteln zu bewerten. Die Stärkung der Cyberresilienz stellt eine überaus herausfordernde Aufgabe dar, der gewissenhaft und mit größtmöglicher Expertise begegnet werden sollte. Der Erstellung dieses Berichts liegt deshalb das umfangreiche Rahmenwerk zur Erstellung nationaler Cybersicherheitsstrategien[1] zugrunde, welches für die vorliegende Evaluation systematisch angewandt wurde.

Der Bericht gliedert sich hierbei in sieben Kapitel. Nach dieser Einleitung folgt in Kapitel zwei eine Betrachtung der aktuellen Bedrohungslandschaft sowie des zurzeit gültigen Rechtsrahmens. Hiermit wird der notwendige Kontext geschaffen, innerhalb dessen aktuelle Maßnahmen bewertet und das Erfordernis zukünftiger Bemühungen geprüft werden müssen. Im dritten Kapitel wird ein kurzer Überblick über die Entstehung der ersten Bremischen Cybersicherheitsstrategie sowie ihre Inhalte gegeben, welche die Grundlage für die vorliegende Evaluation darstellen. Im vierten Kapitel werden die methodischen Grundlagen für die Evaluation einer Cybersicherheitsstrategie erläutert und auf den vorliegenden Evaluationsbericht angewendet, bevor dann in den Kernkapiteln des Berichts eine Evaluation der Konzeption der Strategie in Kapitel fünf und eine Evaluation ihrer Umsetzung in Kapitel sechs erfolgt. Der Bericht schließt mit einer Zusammenfassung und einem Ausblick zur Roadmap für die Strategieerstellung 2026.

[1] www.ncsguide.org

2. Aktuelle Rahmenbedingungen

Maßnahmen zur Stärkung der Cybersicherheit wirken stets im Kontext der hochdynamischen und komplexen Bedrohungslandschaft und müssen regelmäßig auf ihre Wirksamkeit hin überprüft werden. Das folgende Kapitel bietet deshalb eine Grundlage mit einer Betrachtung der aktuellen Bedrohungslandschaft mit typischen Angriffsmustern sowie, entsprechend dem Aufbau in der Cybersicherheitsstrategie selbst, einer Betrachtung der (inter)nationalen sowie landesspezifischen Bedrohungslage im Cyberraum.

2.1 Typische Bedrohungen in der aktuellen Cybersicherheitslandschaft

Die Cybersicherheitslandschaft ist auch im Jahr 2025 hochdynamisch und komplex. Mit der fortschreitenden Digitalisierung, der Verbreitung von Künstlicher Intelligenz (KI), dem Internet der Dinge („Internet of Things“, IoT) und der weiter zunehmenden Vernetzung wächst auch die Angriffsfläche für Cyberkriminelle. Unternehmen, öffentliche Einrichtungen und Privatpersonen stehen vor einer Vielzahl neuer und sich stetig weiterentwickelnder Bedrohungen. Die aktuelle Bedrohungslandschaft umfasst hierbei nicht nur unmittelbar akute Phänomene, sondern auch zukünftige Herausforderungen. Bei diesen ist bereits heute abzusehen, dass sie sich perspektivisch auf die Cybersicherheitslage auswirken werden. Hierzu zählen neben KI-gestützten Cyberangriffen der stark zunehmende Einsatz von Ransomware, Angriffe auf Lieferketten („supply chain attacks“), Bedrohungen durch IoT sowie 5G aufgrund vergrößerter Angriffsflächen, Social Engineering und Deepfakes sowie Quantum Computing als Zukunftsrisiko:

Abbildung 1 - Aktuelle und zukünftige Bedrohungen in der Cybersicherheit

KI-gestützte Cyberangriffe

Der Einsatz von Künstlicher Intelligenz kann einerseits die Verteidigung, zum Beispiel durch intelligente Erkennung und Automatisierung, unterstützen; andererseits wird aber auch bei Angriffen Künstliche Intelligenz genutzt, um diese zu automatisieren, zu verschleiern und gezielt Schwachstellen auszunutzen. Besonders gefährlich sind KI-generierte

Phishing-Kampagnen, Deepfakes zur Identitätsmanipulation und adaptive Malware, die sich in automatisiert an bestehende Sicherheitsmaßnahmen anpassen kann.

Ransomware

Ransomware bleibt eine der größten Bedrohungen im Cyberraum. Die Angreifer:innen verschlüsseln nicht nur Daten, sondern kopieren diese zusätzlich, um mit der Veröffentlichung sensibler Informationen zu drohen („Double Extortion“). Hierbei lässt sich feststellen, dass die Qualität der Angriffe weiter steigt. Neben der Gefahr für alle Unternehmen und Institutionen werden auch zunehmend kritische Infrastrukturen angegriffen.

Angriffe auf Lieferketten (Supply Chain Attacken)

Cyberkriminelle nutzen Schwachstellen bei zuliefernden oder dienstleistenden Unternehmen, um Zugang zu den Netzwerken ihrer eigentlichen Ziele zu erhalten. Ein einziges kompromittiertes dienstleistendes Unternehmen kann Hunderte anderer Unternehmen gefährden. Besonders betroffen sind Unternehmen, welche IT-Dienstleistungen anbieten, Software herstellen oder Cloud-Lösungen anbieten.

Bedrohungen durch das IoT und 5G

Durch die zunehmende Vernetzung vieler IoT-Geräte und die weite Verbreitung von 5G-Netzen vergrößern sich sowohl die Angriffsfläche als auch die Angriffsmöglichkeiten. Viele IoT-Geräte sind nicht ausreichend gegen Angriffe geschützt bzw. werden nicht oder nur unzureichend mit sicherheitskritischen Updates versorgt. Durch die Vielzahl an verbundenen Geräten und die Geschwindigkeit der Kommunikationsnetze können die Angreifer:innen immer neue Taktiken und Methoden entwickeln und einsetzen.

DDoS- und Netzwerkangriffe

Distributed-Denial-of-Service (DDoS)-Angriffe nehmen an Häufigkeit, Komplexität und Intensität zu. Multi-Vektor-Angriffe und die Ausnutzung von Netzwerkprotokollen wie DNS oder NTP führen dazu, dass mit dem Internet verbundene Dienste in kürzester Zeit kompromittiert werden können.

Social Engineering und Deepfakes

Social Engineering ist eine besonders effektive Methode, um an sensible Informationen zu gelangen. Durch sogenannte Deepfakes – täuschend echte, KI-generierte Audio- und Videoinhalte – werden klassische betrügerische Vorgehensweisen, wie CEO-Fraud oder Phishing, glaubwürdiger und gefährlicher.

Quantum Computing als Zukunftsrisiko

Obwohl die Entwicklung und der Einsatz von Quantencomputern sich noch in den Anfängen befinden, besteht die Gefahr, dass Verschlüsselungsverfahren, die heutzutage als sicher bewertet werden, in der Zukunft entschlüsselt werden können. Dies führt auch dazu, dass Angreifer:innen schon heute verschlüsselte Daten abfangen und für eine spätere Entschlüsselung speichern („Harvest now, decrypt later“).

2.1.1 (Inter-)Nationale Cybersicherheitslage

Seit dem Jahr 2005 veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinen Lagebericht zur IT-Sicherheit in Deutschland. Erschien der Bericht in den Jahren 2005 bis 2013 nur alle zwei Jahre, wird dieser seit 2014 jährlich publiziert. Bereits 2015 schätzte das BSI die Gefährdungslage in vielen Bereichen als hoch ein – diese Einschätzung hat sich in den vergangenen zehn Jahren nicht geändert. Seit dem russischen Angriffskrieg auf die Ukraine hat sich diese bereits angespannte Lage weiter zugespitzt. Hierdurch werden Staat, Wirtschaft und Gesellschaft vor große Herausforderungen gestellt, denn angesichts der zunehmenden Digitalisierung aller Lebensbereiche und der wachsenden Bedrohung durch Cyberkriminalität fällt dem Schutz digitaler Infrastrukturen eine immer größere Bedeutung zu.

Im Bericht zur Lage der IT-Sicherheit in Deutschland 2024 des BSI wird darauf hingewiesen, dass die Professionalisierung und Spezialisierung der Cyberkriminellen weiterwachsende Herausforderungen darstellen. Kriminelle Gruppen agieren arbeitsteilig, nutzen Zero-Day-Schwachstellen und setzen zunehmend auf Erpressung durch die Androhung der Veröffentlichung sensibler Daten, welche häufig im Rahmen von Ransomware-Angriffen exfiltriert wurden.

Neben häufig finanziell motivierten Angriffen ist auch festzustellen, dass zunehmend staatlich assoziierte und staatlich gesteuerte Akteur:innen versuchen, Zugriff auf kritische Systeme zu erhalten. Dort versuchen diese dann, gespeicherte sensible Daten zu kopieren oder sich in diesen Systemen festzusetzen, um sie im Bedarfsfall stören zu können (hybride Kriegsführung sowie Spionage und Sabotage).

Ebenso ist festzustellen, dass zielgerichtete Maßnahmen der Desinformation, insbesondere in zeitlichem Bezug zu Wahlereignissen und geopolitischen Konflikten, zunehmen und eine nicht zu unterschätzende Bedrohung für die Stabilität von Staat und Gesellschaft darstellen. Obwohl das Bewusstsein für die Bedeutung der Cybersicherheit weiter steigt und insbesondere viele große Unternehmen stetig in den Schutz der eigenen IT-Systeme investieren, muss auch festgestellt werden, dass vor allem kleine und mittlere Betriebe oft unzureichend vorbereitet sind. Studien zeigen, dass das Problembewusstsein zwar wächst, effektive Schutzmaßnahmen jedoch oft nicht in der gleichen Geschwindigkeit umgesetzt werden. Viele Firmen überschätzen zudem ihre eigene Resilienz und unterschätzen die Bedrohungslage.

Es ist davon auszugehen, dass zukünftig Fragestellungen der „Digitalen Souveränität“ weiter zunehmen werden. Aktuell wird der Markt digitaler Dienstleistungen, wie Text- und Mailsoftware, Cloudspeicherlösungen oder Betriebssysteme, durch eine geringe Anzahl von produzierenden Unternehmen bedient. Diese haben aufgrund ihrer Marktdurchdringung de facto eine Monopolstellung in bestimmten Bereichen inne. Insbesondere in Hinblick auf die Abhängigkeit moderner Gesellschaften von digitalen Daten besteht die Gefahr, dass diese Marktdurchdringung und die hiermit verbundenen Abhängigkeiten als politisches Druckmittel genutzt werden könnten.

Zur Sicherstellung der Integrität und der Verfügbarkeit über diese digitalen Daten der Bevölkerung, der Wissenschaft, der Wirtschaft und der Verwaltung wird es als zielführend erachtet, nationale oder europäische Alternativen in diesen Bereichen zu entwickeln.

Ein weiteres Augenmerk muss auf die Gesellschaft an sich geworfen werden, denn trotz der stetig steigenden Bedrohungen sinkt das Risikobewusstsein in der Bevölkerung. Besonders junge Menschen gehen immer sorgloser mit digitalen Gefahren um, während ältere Menschen Gefahr laufen, sich bei den rasanten Entwicklungen von moderner Technik abgehängt zu fühlen.

Zur Stärkung der Cyberresilienz ist es daher notwendig, im Rahmen einer ganzheitlichen Strategie zu agieren: Der Ausbau der Zusammenarbeit zwischen Staat, Wirtschaft und Gesellschaft, die Stärkung der Detektionsmechanismen und die Förderung der Resilienz sind wichtige Bausteine, die systematisch ineinandergreifen müssen. Nur durch gemeinsames, proaktives Handeln kann die digitale Zukunft Deutschlands sicher gestaltet werden.

Dem Staat kommt dabei die Aufgabe zu, durch sinnstiftende und zielführende Regulierung Rahmenbedingungen zu schaffen, unter denen Cybersicherheit gestärkt werden kann. Cybersicherheit ist nicht nur eine technische, sondern auch eine politische und gesellschaftliche Aufgabe. Der Staat muss durch geeignete Gesetze, Sicherheitsstandards und Aufsicht sicherstellen, dass digitale Systeme geschützt und die Bevölkerung vor Cyberangriffen, Datenmissbrauch und Manipulation bewahrt wird. Zugleich sind Unternehmen gefordert, in sichere IT-Strukturen zu investieren und Verantwortung für den Schutz sensibler Informationen zu übernehmen.

2.1.2 Cybersicherheitslage im Land Bremen

Generell unterscheidet sich die Cybersicherheitslage im Land Bremen nicht von der im Bund, denn finanziell motivierte Angreifer:innen wählen die entsprechenden Ziele aufgrund der bestehenden Angriffsmöglichkeiten, wie veralteter Software oder bestehender Sicherheitslücken, aus und nicht aufgrund einer örtlichen Gegebenheit. Gleichwohl existieren im Land Bremen sogenannte „Hochwertziele“, die insbesondere im Interesse fremder Staaten stehen.

Der Abwehr und Aufklärung von Cyberangriffen fremder Nachrichtendienste auf Unternehmen oder exponierte Einzelpersonen fällt seit Jahren eine wachsende Bedeutung zu. Im Zuge der fortschreitenden Digitalisierung ergeben sich stetig neue Herausforderungen. Damit einher geht ein qualitativer und quantitativer Anstieg von Cyberangriffen. Hiervon bleibt auch Bremen nicht verschont. Im vergangenen Jahr wurden regelmäßig Cyberangriffe zum Zwecke der Spionage bzw. der Ausforschung auf sogenannte Hochwertziele festgestellt. Da diese Hochwertziele zumeist über mehrere Standorte und Niederlassungen verfügen, die über ganz Deutschland verteilt sind, kann auch hier nicht auf ein besonders erhöhtes Risiko im Land Bremen geschlossen werden.

Im Jahr 2024 wurden durch die Polizei Bremen insgesamt 213 Fälle registriert, die der Cybercrime im engeren Sinne zugeordnet wurden (ohne Computerbetrug gem. § 263a StGB). Im Vergleich zum Vorjahr entspricht dies einem Anstieg um 13 Fälle. Hierbei handelte es sich in drei Fällen um solche, die dem Phänomen Ransomware zugeordnet werden können. Alle weiteren Angriffe auf Unternehmen, die der Zentralen Ansprechstelle

Cybercrime (ZAC) des Landeskriminalamtes bekannt wurden, konnten vor einer Verschlüsselung bzw. Feststellung eines entsprechenden nachgeladenen Schadcodes unterbunden werden.

Bei Cybercrime-Delikten ist jedoch stets zu beachten, dass die rein quantitative Betrachtung der manchmal niedrig erscheinenden Fallzahlen nicht in Relation zu den hohen Arbeitsaufwänden und den hiermit verbundenen Herausforderungen sowie dem hohen Risikopotenzial der Schadwirkung bei den betroffenen Unternehmen und Privatpersonen steht und darüber hinaus in diesem Deliktbereich ein hohes Dunkelfeld existiert.

Auch die mit dem Internet verbundene IT-Infrastruktur der öffentlichen Verwaltung Bremens ist, wie jedes an das Internet angeschlossene System, Angriffen ausgesetzt. Neben Spam- und Phishing-Mails, die zumeist automatisiert gefiltert werden, wurden die Websites der Freien Hansestadt Bremen in den letzten Jahren wiederholt mit Distributed Denial of Service-Attacken angegriffen. In der weitaus überwiegenden Mehrzahl der Fälle konnten die Angriffe durch die zugrundeliegenden Schutzmaßnahmen abgewehrt werden, ohne, dass es zu Einschränkungen bei der Erreichbarkeit der Websites gekommen ist.

Eine weitere Herausforderung, derer sich die Verwaltung der Freien Hansestadt Bremen in den kommenden Jahren stellen muss, ist der Einsatz einer Vielzahl von Fachverfahren, welche in Teilen nicht mehr dem aktuellen Stand der Technik entsprechen (sogenannte Legacy-IT). Hierbei ist zu prüfen, welche Fachverfahren ggf. abgeschaltet bzw. durch neuere Software abgelöst werden können, um aktuellen Sicherheitsanforderungen zu entsprechen. Sollten Fachverfahren nicht migriert werden können, sei es aufgrund geänderter Systemstrukturen oder sonstiger Gründe, so ist eine konsequente Isolierung dieser in einem Legacy-Segment (Domäne) ohne Internet und Rechte anzustreben, um das bestehende Sicherheitsniveau aufrechtzuerhalten.

2.2 Aktueller Rechtsrahmen

Da digitale Bedrohungen grenzüberschreitend wirken, sollten gesetzliche Regelungen auf internationaler, nationaler und regionaler Ebene stets im Gesamtgefüge betrachtet werden. Im folgenden Unterkapitel wird daher ein nicht abschließender Einblick in aktuelle Entwicklungen des Cybersicherheits-Rechtsrahmens gegeben, um aufzuzeigen, welche Vorgaben bereits existieren und wo perspektivisch für eine rechtlich abgesicherte Cybersicherheitsarbeit im Land Bremen noch Lücken zu schließen sind.

2.2.1 (Inter-)Nationaler Rechtsrahmen

Moderne Staaten sind gekennzeichnet durch ein hohes Maß an Digitalisierung, welche Prozesse in der Privatwirtschaft sowie der öffentlichen Verwaltung stetig weiterentwickelt. Durch die fortschreitende Digitalisierung sind Prozesse und Dienstleistungen jedoch zunehmend auf informationstechnische Systeme und ihre Vernetzung angewiesen, was sie verwundbar gegenüber Angriffen aus dem Cyberraum macht. Geopolitische Konflikte und stetig fortschreitende technische Möglichkeiten führen in der Folge zu einer angespannten Bedrohungslage im Cyberraum, welche sich auf öffentliche Verwaltungen, Unternehmen, kritische Infrastrukturen und Lieferketten gleichermaßen auswirkt. Um diese bestmöglich schützen zu können, ist ein umfassender Rechtsrahmen erforderlich, der Staaten in die Lage versetzt, diesen Bedrohungen mit angemessenen Mitteln begegnen zu können.

Die zunehmende Komplexität der Informations- und Cybersicherheit, die historische Entwicklung sowie die zahlreichen Schnittmengen zu anderen Rechtsgebieten haben jedoch dazu geführt, dass sehr umfangreiche, teilweise korrespondierende und mitunter sich überschneidende, gesetzliche Regelungen auf europäischer, nationaler und subnationaler Ebene bestehen.

Weltweit haben die Vereinten Nationen einen neuen permanenten Cybersicherheitsdialog eingeführt. Mit dem Abschlussbericht der zweiten „Open-Ended Working Group“ (OEWG) einigten sich die vertretenen Staaten unter anderem darauf, das Völkerrecht und politisch bindende Cybernormen zu bestätigen und weiterzuentwickeln.

Auf europäischer Ebene sind maßgebliche Regelungen unter anderem im EU Cyber Resilience Act (EU CRA) oder der CER-Richtlinie (Critical Entities Resilience Directive) zu finden. Darüber hinaus wurde die Richtlinie zur Netz- und Informationssicherheit (NIS-1-Richtlinie) erlassen und, als Reaktion auf die stetig steigende Bedrohungslage im Cyberraum, durch die am 16.01.2023 in Kraft getretene NIS-2-Richtlinie ergänzt, welche am 27.12.2022 im Amtsblatt der Europäischen Union veröffentlicht wurde.

Die EU NIS-2-Richtlinie verfolgt das übergreifende Ziel, den europäischen Binnenmarkt resilienter gegenüber Bedrohungen aus dem Cyberraum zu machen. Zwischen den Mitgliedstaaten bestehende Unterschiede sollen beseitigt werden, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Durchsetzungsmaßnahmen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden.

Ein bedeutsames Ziel der Europäischen Union und ihrer Mitgliedstaaten ist die Erhöhung der Wirtschaftssicherheit und die Verbesserung der Resilienz als Reaktion auf neue geopolitische Rahmenbedingungen. Mit der am 20.06.2023 veröffentlichten Europäischen Strategie für wirtschaftliche Sicherheit identifiziert die Europäische Kommission das Risiko für die Sicherheit kritischer Infrastrukturen vor physischen und Cyberangriffen als eines von vier Hauptrisiken für die europäische Volkswirtschaft.

Auf nationaler Ebene existieren beispielhaft das IT-Sicherheitsgesetz und der korrespondierende Gesetzesentwurf zum NIS2-Umsetzungsgesetz des Bundes. Darüber hinaus ist der Bund bemüht, der Gefahr durch hybride Bedrohungen im Bereich digitaler Infrastrukturen mit der Erarbeitung eines KRITIS-Dachgesetzes 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. Der Einbindung der Länder in diesen Prozess fällt hierbei eine wichtige Rolle zu, da nur so sichergestellt werden kann, dass Regelungen auf Bundes- sowie Länderebene später konfliktfrei ineinandergreifen. Die Umsetzung der EU-Mindeststandards der NIS-2-Richtlinie in nationales Recht ist durch

das am 05.12.2025 im Bundesgesetzblatt veröffentlichte NIS2UmsuCG erfolgt. Die Umsetzung der CER-Richtlinie (EU) in nationales Recht mittels KRITIS-Dachgesetz-E befindet sich mit Ende des Jahres 2025 noch im Gesetzgebungsverfahren.

Neben dem Bestreben, den Wirtschaftsraum sowie Binnenmarkt cybersicher zu machen, ergeben sich aus den Digitalisierungserfordernissen auch für die Öffentliche Verwaltung Herausforderungen. Indem beispielsweise Verwaltungsleistungen zunehmend digital angeboten werden, bedarf es auch hier der Schaffung passender gesetzlicher Grundlagen.

2.2.2 Rechtsrahmen im Land Bremen

Ein umfassender Rechtsrahmen für die Informationssicherheit und hier insbesondere die Cybersicherheit in der Freien Hansestadt Bremen ist eine wesentliche Voraussetzung für eine erfolgreiche Digitalisierung der Öffentlichen Verwaltung. Es muss sichergestellt werden, dass die in der öffentlichen Verwaltung des Landes und der Stadtgemeinden Bremen und Bremerhaven genutzten technischen oder nichttechnischen Systeme zur Informationsverarbeitung und Speicherung von Informationen sicher sind und dieser Schutz rechtlich abgesichert ist. Ein wesentlicher Bestandteil notwendiger Regelungen ist der Schutz von Informationen und Informationssystemen in Bezug auf die drei Werte der Integrität, Vertraulichkeit und Verfügbarkeit.

Mit der zunehmenden Verwaltungsdigitalisierung steigt die Wahrscheinlichkeit, dass die Bremische öffentliche Verwaltung auch zunehmend personenbezogene Daten speichert und verarbeitet. Hierbei sind im Rahmen der Informationssicherheit sowohl die Belange des personenbezogenen Datenschutzes als auch die Belange der Informationsverarbeitungs- und Speicherungssysteme zu beachten.

Mit Blick auf den Schutz personenbezogener Daten gibt die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (Verordnung (EU) 2016/679) den rechtlichen Rahmen vor. Mit der DSGVO werden klare Pflichten für alle Organisationen, die personenbezogene Daten verarbeiten, vorgegeben. Für die Informationssicherheit bedeutet dies, dass technische und organisatorische Maßnahmen zum Schutz von Daten verpflichtend sind. Dazu gehören unter anderem Zugriffskontrollen, Verschlüsselung, regelmäßige Sicherheitsüberprüfungen, Backup-Systeme und die Schulung von Mitarbeiter:innen. Die DSGVO fordert außerdem eine Dokumentation aller Datenverarbeitungsvorgänge und die Meldung von Datenschutzvorfällen innerhalb von 72 Stunden, wodurch die Verwaltung gezwungen wird, Sicherheitsvorfälle frühzeitig zu erkennen und schnell zu reagieren.

Das bremische Ausführungsgesetz zur DSGVO (BremDSGVOAG) konkretisiert die Anforderungen der DSGVO auf Landesebene und gibt zusätzliche Vorgaben für die Umsetzung in Behörden und öffentlichen Einrichtungen. Es regelt insbesondere die Verantwortlichkeiten von Datenschutzbeauftragten, interne Kontrollmechanismen, Informationspflichten gegenüber Betroffenen sowie besondere Sicherheitsanforderungen für kritische Datenverarbeitungen. Durch diese zusätzlichen Regelungen können Behörden in Bremen die Informationssicherheit gezielt stärken, indem sie Prozesse, Zuständigkeiten und Sicherheitsstandards verbindlich festlegen.

Die Informationssicherheitsleitlinie von Bund und Ländern definiert einheitliche Mindeststandards für den Schutz von Informationen in der öffentlichen Verwaltung und legt die

Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit fest. Sie fordert die Einführung von Informationssicherheitsmanagement-Systemen, welche die Planung, Durchführung, Kontrolle und kontinuierliche Verbesserung von Sicherheitsmaßnahmen ermöglichen.
Die Leitlinie sorgt dafür, dass auch bei übergreifenden IT-Verfahren zwischen Bund, Ländern und kommunalen Verwaltungen ein einheitliches Sicherheitsniveau besteht und Verantwortlichkeiten klar geregelt sind. Sie umfasst organisatorische, technische und personelle Maßnahmen, fördert die Sensibilisierung von Mitarbeiter:innen und gibt vor, dass Ressourcen für Informationssicherheit bereitgestellt werden. Durch Standardisierung, Messbarkeit und regelmäßige Anpassung an die Bedrohungslage unterstützt sie Bund und Länder dabei, Sicherheitsvorfälle frühzeitig zu erkennen, abzuwehren und die digitale Resilienz der Verwaltung zu erhöhen.

Die Informationssicherheitsleitlinie der Freien Hansestadt Bremen vom 16.01.2018 legt die Grundsätze und verbindlichen Anforderungen für den Schutz von Informationen in der bremischen Verwaltung fest. Sie definiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit und stellt sicher, dass alle Dienststellen, Eigenbetriebe und Einrichtungen diese einheitlich umsetzen. Die Leitlinie fordert den Aufbau von Informationssicherheitsmanagement-Systemen, die technische, organisatorische und personelle Maßnahmen zur Abwehr von Cyberrisiken umfassen. Dazu gehören unter anderem Zugriffsregelungen, Verschlüsselung, Virenschutz, Protokollierung von Aktivitäten und Schulungen für Mitarbeiter:innen. Die Informationssicherheitsleitlinie sorgt außerdem dafür, dass Verantwortlichkeiten klar geregelt sind und Ressourcen für Sicherheitsmaßnahmen bereitgestellt werden. Durch diese Maßnahmen stärkt die Leitlinie die digitale Resilienz der Verwaltung, ermöglicht eine frühzeitige Erkennung von Sicherheitsvorfällen und trägt zu einem hohen Informationssicherheitsniveau im Land Bremen bei.

Mit der Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet Zugängen vom 01.02.2004 (Internet-Richtlinie FHB) wurde bereits vor vielen Jahren die sichere Bereitstellung und Nutzung von Internet- und Intranet-Zugängen innerhalb des Bremischen Verwaltungsnetzes geregelt. Sie legt technische und organisatorische Vorgaben fest, die den Schutz der IT-Infrastruktur und sensibler Daten gewährleisten sollen. Dazu gehören Maßnahmen wie der Einsatz von Virenschutz, Proxy- und Terminalservern, sowie die Protokollierung von Internetzugriffen. Mit dem Addendum zur Internet-Richtlinie wurde diese Regelung an die gestiegene Bedrohungslage im Cyberraum angepasst. Die zentrale Protokollierung von Internetzugriffen wurde erweitert, um Sicherheitsvorfälle besser nachvollziehen und analysieren zu können.

Die Umsetzung der NIS-2-Richtlinie soll für den Mitgliedsstaat Deutschland im Wesentlichen durch das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG) erfolgen. Gemäß der grundgesetzlichen Kompetenzordnung besitzt der Bund dabei die Regelungsbefugnis für den Bereich der Wirtschaft und für die Bundesverwaltung. Den Ländern obliegt hingegen die Umsetzung hinsichtlich der ihrer Hoheit unterliegenden Landesverwaltung. Hierbei verpflichtet die Richtlinie zur Identifizierung von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene, die nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätig-

keiten haben könnten. Der regionalen Ebene sind insoweit die in den Ressorts zu verortende Teile der unmittelbaren Landesverwaltung zuzuordnen. Zur Ermittlung der hierbei betroffenen Einrichtungen hat der IT-Planungsrat in seiner 42. Sitzung am 03.11.2023 ein Identifizierungskonzept beschlossen (Beschluss 2023/39), das von den Ländern anzuwenden ist.

Die von der EU gesetzte Umsetzungsfrist zum 17.10.2024 ist neben dem Bund auch von den Ländern zu beachten gewesen. Wegen der noch nicht erfolgten bzw. nicht vollständigen Umsetzung auf Bundesebene, hat die EU-Kommission am 28.11.2024 ein Vertragsverletzungsverfahren (Art. 258 ff. des Vertrages über die Arbeitsweise der Europäischen Union – AEUV) gegen Deutschland eingeleitet. Nach dem Gesetz zur Lastentragung im Bund-Länder-Verhältnis bei Verletzung von supranationalen oder völkerrechtlichen Verpflichtungen (Lastentragungsgesetz – LastG) sind die Länder dabei gemäß ihrem Verursachungsbeitrag anteilig an daraus folgenden etwaigen Kosten (vor allem Strafzahlungen) zu beteiligen. Das nationale Gesetzgebungsverfahren zur Umsetzung der Richtlinie (EU) 2022/2555 wurde nunmehr zum 05.12.2025 abgeschlossen.

Zur Regelung der Anteile, für welche eine Gesetzgebungskompetenz des Landes besteht, hat der Senat des Landes Bremen bereits am 14.01.2025 die Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) beschlossen. Das Ziel der Verwaltungsvorschrift besteht darin, die Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen. Die Schaffung einer ersten rechtlichen Grundlage zur Umsetzung der Maßnahmen auf Landesebene stellt sicher, dass das Land Bremen den EU-Anforderungen gerecht wird.

Durch die Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) werden die identifizierten Einrichtungen dazu verpflichtet, sowohl bestimmte Risikomanagementmaßnahmen zu ergreifen als auch erhebliche Sicherheitsvorfälle zu melden. Ebenso müssen Leitungsverantwortliche die Umsetzung der erforderlichen Maßnahmen überwachen und sich regelmäßig zu Fragen der Cybersicherheit schulen lassen, sowie den Beschäftigten entsprechende Schulungen ermöglichen. Darüber hinaus wurde die Rolle der Zentralstelle Cybersicherheit beim Senator für Inneres und Sport gestärkt.

Die Zentralstelle Cybersicherheit übernimmt gemäß der VV NIS2 Ums FHB hierbei einerseits die Rolle der „zuständigen Behörde“, koordiniert die Umsetzung der Richtlinie im Land Bremen und überwacht die Einhaltung der hieraus resultierenden Verpflichtungen; andererseits fungiert sie als Computer Security Incident Response Team (CSIRT) und stellt perspektivisch die Gewährleistung der hiermit verbundenen Aufgaben sicher, welche sich aus der NIS-2-Richtlinie ergeben.

Beide Funktionen wurden bis zum Senatsbeschluss vom 14.01.2025 noch nicht in dieser Form in der Freien Hansestadt Bremen ausgeübt und wurden damit als grundsätzlich neue Aufgabenkreise eingeführt. Lediglich bestimmte Tätigkeiten des CSIRT, insbesondere der Betrieb eines Warn- und Informationsdienstes sowie die Funktion als Meldestelle bei Sicherheitsvorfällen, werden derzeit für die gesamte öffentliche Verwaltung der Freien Hansestadt Bremen vom CERT Nord wahrgenommen. Bei diesem handelt es sich um ein

Computer Emergency Response Team (CERT), das die Freie Hansestadt Bremen mit den anderen Dataport-Trägerländern unterhält.

Die Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen stellte einen ersten wichtigen Schritt zur Verbesserung der Widerstandsfähigkeit der Landesverwaltung gegen Cyberangriffe dar. Dieser Schritt allein reicht jedoch nicht aus, um europäischen Anforderungen zu entsprechen.

Zur rechtssicheren Umsetzung aller Verpflichtungen auf Landesebene ist es zwingend erforderlich, dass neben der grundsätzlichen Aufgabenverteilung im Bereich der IT- und Cybersicherheit weitere spezifische Rechtsgrundlagen für im Rahmen der Gewährleistung ihrer IT-Sicherheit erforderliche Datenverarbeitungen durch öffentliche Stellen geschaffen werden.

Mit dem geplanten Bremischen Cybersicherheitsbasisgesetz (BremCSBG) sollen spezifische Rechtsgrundlagen geschaffen werden, welche die für im Rahmen der Gewährleistung ihrer IT-Sicherheit erforderliche Datenverarbeitungen durch öffentliche Stellen regelt. Diese zusätzlich zu schaffenden Rechtsgrundlagen sind auch für die praktische Umsetzung der Anforderungen und Pflichten aus der NIS-2-Richtlinie erforderlich, da die einschlägigen allgemeinen Rechtsgrundlagen aus der DSGVO und der BremDSGVOAG (vor allem Artikel 6 DSGVO ggf. i. V. m. § 3 BremDSGVOAG) mit Blick auf die besonderen Verarbeitungsvorgänge zurzeit keine klare und rechtssichere Handhabung ermöglichen.

Mittel- und langfristig wird der Erlass eines ganzheitlichen Bremischen Cybersicherheitsgesetzes (BremCSG) angestrebt, das nicht nur die Regelungen des BremCSBG und der VV NIS2Ums FHB zusammenführt, sondern auch weitere für die IT- und Cybersicherheit relevante Bereiche gesetzlich regeln soll. Aufgrund der grundsätzlichen Verantwortung des Senators für Finanzen für die Landes-IT und die IT-Sicherheit der öffentlichen Verwaltung, ist dessen enge fachliche Einbindung bei Erarbeitung der gesetzlichen Grundlagen erforderlich.

3. Genese und Aufbau der Bremischen Cybersicherheitsstrategie

Die im Jahr 2023 erstmals durchgeführte Erarbeitung der Cybersicherheitsstrategie ging mit einer Anpassung der Geschäftsverteilung des Senats einher und setzte den Fokus auf eine gemeinschaftliche und transparente Herangehensweise bei der Erstellung eines Grundlagenpapiers, auf welchem die Cybersicherheitsarbeit der kommenden Jahre kontinuierlich aufbauen könnte. Im Folgenden werden daher kurz die Genese, die Architektur und die Grundinhalte der Strategie skizziert.

3.1 Hintergrund und Genese der Bremischen Cybersicherheitsstrategie

Die Entscheidung zur systematischen Stärkung der Cybersicherheit im Land Bremen begann mit einem Senatsbeschluss zur Änderung der Geschäftsverteilung des Senats am 04.10.2022, um die organisatorische Verantwortlichkeit zu klären sowie eine Zuständigkeitsabgrenzung im Phänomenbereich zu gewährleisten.

Im Geschäftsbereich des Senators für Finanzen wurde im Feld „Zentrales IT-Management, Digitalisierung öffentlicher Dienste“ der Geschäftsbereich „Informationssicherheit im Bereich der IT der öffentlichen Verwaltung“ hinzugefügt. Im Geschäftsbereich 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)“ ergänzt.

Nach dieser institutionellen Verankerung der künftigen Neuaufteilung folgte in einem zweiten Schritt die strategische Ausgestaltung eines ganzheitlichen Ansatzes zur Steigerung der Cyberresilienz im Land Bremen mithilfe der Bremischen Cybersicherheitsstrategie 2023. Bei ihrer Erstellung waren zwei zentrale Anliegen von besonderer Bedeutung: die Gewährleistung einer hohen Akzeptanz, um einen tragfähigen Rahmen zu schaffen, sowie die Schaffung größtmöglicher Interoperabilität, um einer zunehmenden Fragmentierung der nationalen Cybersicherheitslandschaft und -bemühungen entgegenzuwirken.

Um diese Ziele zu erreichen, wurde einerseits eine umfassende und frühzeitige Beteiligung unterschiedlicher Akteur:innen im Land Bremen bei der Erstellung der Cybersicherheitsstrategie sichergestellt, sodass viele Perspektiven und Bedürfnisse in ihre Gestaltung einfließen konnten; andererseits orientierte sich die inhaltliche Strukturierung der Strategie mithilfe einzelner Handlungsfelder sowie die Verwendung zentraler Begriffe eng an der Leitlinie der Länderarbeitsgruppe (LAG) Cybersicherheit zur Erstellung föderaler Cybersicherheitsstrategien.

Dieses Vorgehen gewährleistete eine größtmögliche Vereinheitlichung und Harmonisierung, wodurch auch der Zielvorstellung des Bundes Rechnung getragen wurde, dass sich Bund und Länder in den individuellen Bemühungen um mehr Cyberresilienz gegenseitig ergänzen und somit die föderale Zusammenarbeit auf dem Gebiet der Cybersicherheit stärken.

3.2 Architektur der Bremischen Cybersicherheitsstrategie

Die Erstellung der Bremischen Cybersicherheitsstrategie 2023 wurde von drei Leitgedanken getragen (s. Abbildung 2):

Zukunftsfähige Cybersicherheitsarbeit besitzt ein tragfähiges Fundament: Cybersicherheit ist herausfordernd: Ein umfassender Beteiligungsprozesses sowie ein transparentes methodisches Vorgehen sollen sicherstellen, dass alle Beteiligtenan einem Strang ziehen und eine gemeinschaftliche dynamische Cybersicherheitsarbeit vor dem Hintergrund stetiger Veränderungen ermöglichen.

Umfassende Cybersicherheit wird von vielen Schultern (Säulen) getragen: Cybersicherheit ist vielfältig: Sowohl die vorhandenen Bedürfnisse und Anforderungen an Cybersicherheit als auch die eingebrachten Kompetenzen und Fachkenntnisse unterscheiden sich in den Bereichen Staat, Wirtschaft, Wissenschaft und Gesellschaft deutlich. Nur wenn alle Perspektiven angemessen berücksichtigt und Fähigkeiten genutzt werden, können vorhandene Potenziale voll ausgeschöpft und blinde Flecken vermieden werden.

Innovative Cybersicherheitsarbeit braucht Handlungsspielräume: Cybersicherheit ist dynamisch: Um auf künftige Herausforderungen mit Kreativität und Innovation reagieren zu können, müssen Handlungsspielräume geschaffen werden. Diese entstehen regelmäßig erst dann, wenn grundlegende Bedürfnisse an die Informations- und Cybersicherheit erfüllt werden und proaktives Vorgehen stetiges Reagieren ersetzt.

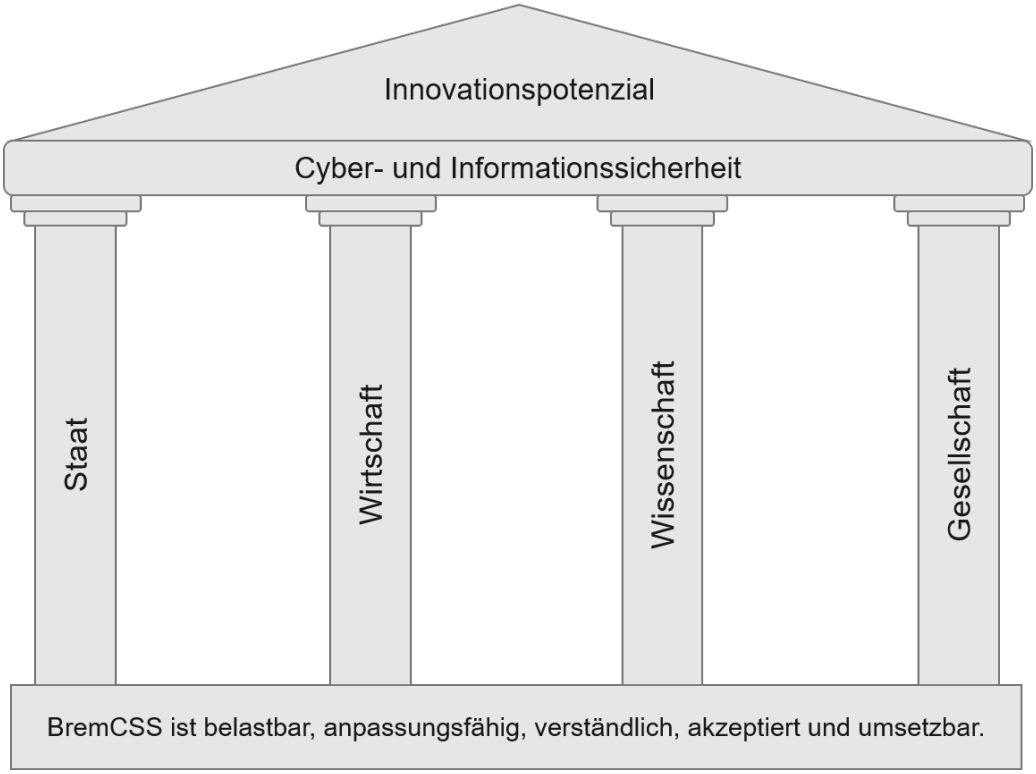
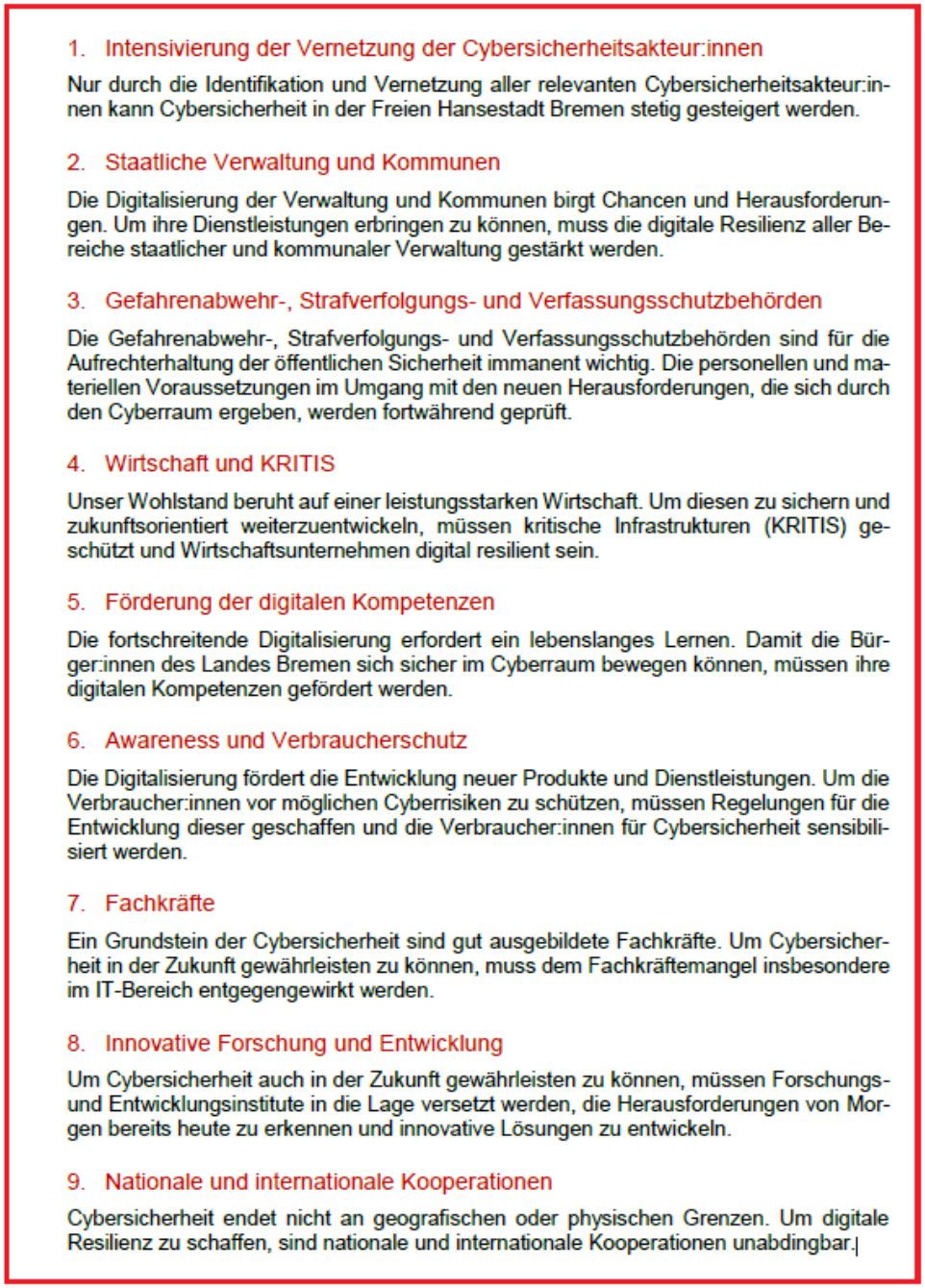


Abbildung 2 – Architektur der Bremischen Cybersicherheitsstrategie

3.3 Kerninhalte der Bremischen Cybersicherheitsstrategie

Um die Architektur mit Leben zu füllen, wurden neun Handlungsfelder identifiziert und mit Kurzbeschreibungen versehen (s. Abbildung 3). Im Rahmen der Handlungsfeldbetrachtungen wurden diese dann um eine leitende Perspektive ergänzt, welche sowohl die Zielsetzung als auch den Fokus einzelner Handlungsfelder lenkte.



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.

Abbildung 3 - Identifizierte Handlungsfelder der Cybersicherheitsstrategie mit Kurzbeschreibung

In einem letzten Schritt erfolgte sodann eine erste Zuordnung der Handlungsfelder zu den vier benannten Zielgruppen. Dieses Vorgehen verfolgte einerseits das Ziel, die erste Analyse und Handlungsfeldbeschreibung zu erleichtern und andererseits einen dringend notwendigen Fokus bei der erstmaligen Strategieerstellung zu setzen.

4. Grundlagen der Evaluation einer Cybersicherheitsstrategie

Bereits mit der Verabschiedung der Bremischen Cybersicherheitsstrategie 2023 wurde eine erste Evaluation nach zwei Jahren festgeschrieben, welche nun erstmals umgesetzt wurde. Diese wurde geleitet von dem Gedanken, dass eine Evaluation nicht nur den Selbstzweck eines Werturteils besitzen sollte. Vielmehr muss sie über das Potenzial verfügen, ein wichtiger Bestandteil des iterativen Entwicklungs- und Fortschreibungsprozesses der Maßnahmen und Ziele zu sein, welche sie überprüfen soll. Sie muss somit als Teil eines größeren Gesamtbildes verstanden werden (s. Abbildung 4).

Im Jahr 2018 wurde durch ein internationales Konsortium aus staatlichen, wissenschaftlichen sowie privatwirtschaftlichen Akteur:innen[2] das „Handbuch zur Entwicklung einer Nationalen Cybersicherheitsstrategie“ veröffentlicht und im Jahr 2021 in der zweiten Edition fortgeschrieben. Im „Guide to Developing a National Cybersecurity Strategy (NCS, im Folgenden als „NCS-Handbuch“ bezeichnet)“ wird aufgezeigt, welchem Lebenszyklus eine Cybersicherheitsstrategie idealtypischer Weise folgt und welche Rolle eine Evaluation (Phase 5) innerhalb dieses Ablaufs einnimmt:

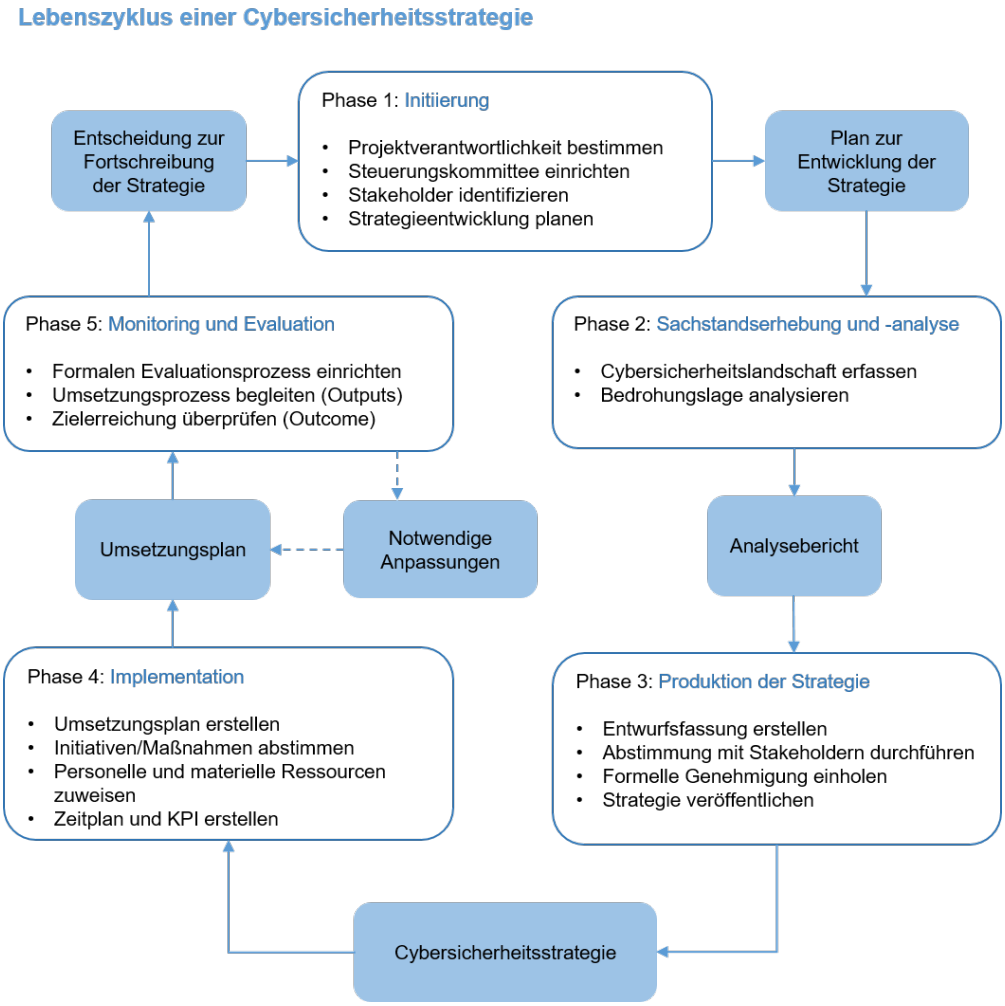


Abbildung 4 - Lebenszyklus einer Cybersicherheitsstrategie (angelehnt an: NCS-Guide 2021, Abb. 1, S. 17).

[2] Weiterführende Informationen zum Konsortium und der Publikation: www.ncsguide.org

4.1 Festlegen der Zielrichtung der Evaluation

Im Lebenszyklusmodell des NCS-Handbuchs verfolgt die Monitoring- und Evaluationsphase vor allem zwei Ziele: die Intervention während der Umsetzungsphase und die abschließende Bewertung. Während der Umsetzungsphase kann ein begleitendes Monitoring der Zielerreichung dazu beitragen, Hindernisse zu identifizieren, den laufenden Fortschritt zu überprüfen und erforderliche Anpassungen am Umsetzungsplan vorzunehmen. Hierdurch wird eine Kurskorrektur möglich, die trotz oder gerade im Falle erkannter Probleme sicherstellen soll, dass die übergeordneten Ziele innerhalb der angestrebten Umsetzungsperiode erreicht werden. Nach Erreichen des zuvor festgelegten Zeitintervalls dient eine abschließende Evaluation der Bewertung des Strategieerfolgs insgesamt. Hierbei fließen die generierten Erkenntnisse in die Entscheidung ein, ob und wie die Cybersicherheitsstrategie fortgeschrieben wird.

Damit die vorliegende Evaluation als belastbare Grundlage für die Weiterentwicklung der Bremischen Cybersicherheitsstrategie genutzt werden kann, reicht es insofern nicht aus, lediglich die Umsetzung geplanter Maßnahmen zu bewerten. Vielmehr soll eine kritische Bewertung der zugrundeliegenden Methodik selbst vorgenommen werden.

4.2 Übertragung der theoretischen Ansätze auf die vorliegende Evaluation

Die Erstellung der Bremischen Cybersicherheitsstrategie 2023 basierte auf der Leitlinie zur Erstellung föderaler Cybersicherheitsstrategien der LAG Cybersicherheit. Diese verfolgt das Ziel, eine Empfehlung zum Aufbau und der Weiterentwicklung der Cybersicherheitsarchitektur in den Ländern zu geben, um durch Harmonisierung, größere Interoperabilität und fachlichen Austausch den nötigen Raum für Innovation und Weiterentwicklung zu eröffnen. Da das Land Bremen zu diesem Zeitpunkt gerade erst eine Neuverteilung der Phänomenverantwortung vorgenommen hatte und der Aufbau einer korrespondierenden Cybersicherheitsarchitektur noch ganz am Anfang stand, war diese Wahl naheliegend und ermöglichte einen niedrigschwelligen Einstieg.

Die Leitlinie zur Erstellung föderaler Cybersicherheitsstrategien sieht jedoch, abgesehen von einem Hinweis auf regelmäßig durchzuführende Evaluationen gemäß des Plan Do Check Act (PDCA)-Zyklus‘, keine konkreten Hinweise zur Herangehensweise an ihre Bewertung vor, sodass für die vorliegende Evaluation die umfassende und erprobte Methodik des NCS-Handbuchs ausgewählt wurde. Die im NCS-Handbuch zugrundeliegenden Schritte zur Erstellung einer Cybersicherheitsstrategie haben bei der Konzeption der ersten Bremischen Cybersicherheitsstrategie keine Anwendung gefunden, sodass erwartbar ist, dass viele Empfehlungen nicht berücksichtigt wurden; teilweise sind NCS-Standards auch nicht unverändert anwendbar, da sie die Konzeption einer Strategie auf nationalstaatlicher Ebene adressieren. Dennoch werden die einzelnen Phasen im Folgenden als Grundlage verwendet, um die Evaluation auf Basis erprobter und empfohlener Standards durchzuführen.

Dieses ambitionierte Vorgehen führt an vielen Stellen zwangsläufig zur Identifikation von Schwachstellen sowie Verbesserungsvorschlägen, die jedoch mit Blick auf den Wunsch nach einer stetigen Professionalisierung und Verbesserung des eigenen Vorgehens unerlässlich sind, um die Cybersicherheitsarbeit langfristig auf hohem Niveau zu entwickeln.

5. Evaluation der Strategie anhand des Lebenszyklusmodells

Die Evaluation der Strategie wird in den folgenden zwei Kapiteln dieses Berichts vorgenommen. Sie ist entsprechend umfangreich und orientiert sich an einem einheitlichen Schema, um eine bessere Übersichtlichkeit zu gewährleisten. Zunächst werden in Kapitel fünf die jeweils zentralen Anforderungen des NCS-Handbuchs an die jeweiligen Lebenszyklusphasen einer Cybersicherheitsstrategie mit den ihnen zugeordneten wichtigen Schritten beschrieben[3] und mit der praktischen Umsetzung bei der Konzeption der Bremischen Cybersicherheitsstrategie 2023 abgeglichen. Eine Bewertung der Umsetzung der benannten Maßnahmen erfolgt in Kapitel sechs. In den Fällen, in denen sich Empfehlungen des NCS-Handbuchs explizit auf die nationalstaatliche Ebene beziehen, wird eine Übertragung auf das funktionale Äquivalent der Länderebene angestrebt.

Die Analyse der Einzelschritte folgt hierbei einem identischen Muster: Zunächst wird ein Überblick gegeben, welche Schritte erfolgreich umgesetzt wurden und wie dies geschehen ist; in der Folge werden Herausforderungen bei der Umsetzung adressiert. Diese bilden die Grundlage für den Ausblick und Anregungen zu Veränderungen und erkannten Verbesserungspotenzialen, welche dann bei der Fortschreibung der Bremischen Cybersicherheitsstrategie im Jahr 2026 systematisch Einfluss finden sollen.

5.1 Phase 1: Initiierung

Die Initiierungsphase (s. Abbildung 5) schafft das Fundament für eine erfolgreiche Strategieerstellung. Der Fokus liegt auf der Identifikation relevanter Prozesse und Stakeholder, welche an der Strategieerstellung beteiligt werden sollen, sowie der Erstellung eines Zeitplans. Hierbei sind etwaige Genehmigungsverfahren (etwa durch die Regierung oder verantwortliche staatliche Stellen) zu berücksichtigen.

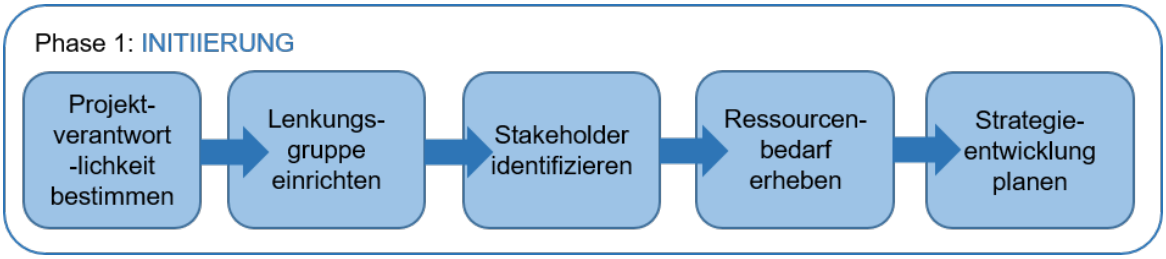


Abbildung 5 - Wichtige Schritte während der Initiierungsphase

5.1.1 Projektverantwortlichkeit bestimmen

Um eine klare Rollenverteilung und -verantwortlichkeit zu gewährleisten, sollte die zentrale Verantwortlichkeit für die Erstellung der Cybersicherheitsstrategie festgelegt werden (etwa durch ein Ministerium, eine Agentur oder eine hierfür zu schaffende Stelle). Die sogenannte „Lead Project Authority“ (im Folgenden als „Projektleitung“ bezeichnet) sollte wiederum eine Person (oder ein Team) benennen, welche(s) hauptverantwortlich für die Begleitung der Strategieentwicklung ist.

[3] Hierbei wird auf eine detaillierte Zitation der einzelnen Textstellen verzichtet. Sämtliche formal beschriebenen Anforderungen entstammen dem NCS-Guide und wurden lediglich ins Deutsche übersetzt. Das Dokument kann auf der Website https://ncsguide.org in verschiedenen Sprachen heruntergeladen werden.

Die Projektleitung sollte hierbei eine organisatorische Unabhängigkeit aufweisen und nicht zur Zielgruppe derjenigen gehören, welche die Maßnahmen der Strategie umzusetzen haben. Sollte dies nicht möglich sein, sollten Mechanismen installiert werden, mithilfe derer ein Wettbewerb um verfügbare Ressourcen vermieden wird.

Umgesetzte Empfehlungen

Ein formeller Auftrag zur Erarbeitung einer Cybersicherheitsstrategie für das Land Bremen bis zum ersten Quartal 2023 erfolgte per Senatsbeschluss am 04.10.2022: Hierbei bat der Senat den Senator für Inneres und den Senator für Finanzen unter Beteiligung aller übrigen Ressorts sowie des Magistrats der Stadt Bremerhaven um die Erarbeitung einer Cybersicherheitsstrategie bis spätestens im ersten Quartal 2023 unter Berücksichtigung der für die Region tätigen systemrelevanten Unternehmen und Interdependenzen. Im Zuge der Neuverteilung und Ergänzung der Geschäftsbereiche des Senats wurde dem Senator für Inneres das Aufgabenfeld „Grundsatzangelegenheiten und ressortübergreifende Koordinierung des Handlungsfeldes Cybersicherheit (ohne Informationssicherheit im Bereich der IT der öffentlichen Verwaltung) zugewiesen. Die organisatorische Gesamtverantwortung wurde bei der neu eingerichteten „Projektgruppe Cybersicherheit“ (PG Cybersicherheit) beim Senator für Inneres angegliedert. Es erfolgte eine personelle Besetzung mit einer hauptverantwortlichen Projektleitung sowie einer Sachbearbeitung.

Herausforderungen bei der Umsetzung

Die Zuweisung von Grundsatzangelegenheiten sowie der ressortübergreifenden Koordinierung des Handlungsfeldes der Cybersicherheit zum Innenressort führt bereits organisatorisch bedingt zwangsläufig zu der Herausforderung, dass dieses Ressort Aspekte des zugewiesenen Verantwortungsbereichs für das gesamte Land erarbeiten und gegebenenfalls regeln muss, von welchen es auch selbst betroffen sein wird. Eine wie im NCS-Guide geforderte vollständige organisatorische Unabhängigkeit ist somit nicht umsetzbar. In der Konsequenz muss insofern stets klar getrennt werden zwischen der Koordinierung der Belange der Cybersicherheit, welche der Senator für Inneres und Sport im Rahmen seiner Aufgabenzuweisung für das Land übernimmt, und jenen Aufgaben, welche aufgrund im Land Bremen geltender Verpflichtungen durch alle Ressorts, und somit auch die Innenbehörde als Adressatin etwaiger Maßnahmen, umgesetzt werden müssen und welche in dezentraler Aufgabenwahrnehmung durch jeweils verantwortliche Cybersicherheitsbeauftragte des Ressorts erfolgt.

Ausblick und Anregungen

Da die Fortschreibung der Bremischen Cybersicherheitsstrategie der mittlerweile beim Senator für Inneres und Sport eingerichteten Zentralstelle Cybersicherheit per Aufgabenzuweisung übertragen wurde, ist auch für die im Jahr 2026 geplante Fortschreibung der Bremischen Cybersicherheitsstrategie keine vollständige organisatorische Unabhängigkeit zu erreichen. Eine alternative Übertragung dieser Aufgabe an eine externe Stelle (etwa eine Agentur) wäre darüber hinaus mit hohen Kosten verbunden. Es ist daher besonders wichtig, die Mechanismen zur klaren Rollenkommunikation und -trennung für den Bereich der Cybersicherheit mit Blick auf zentrale und dezentrale Aufgabenwahrnehmungen sowohl in den Ressorts als auch zwischen den Ressorts weiter zu stärken und aktiv zu kommunizieren, um eine größtmögliche Transparenz und Akzeptanz bei allen Beteiligten zu erzeugen und aufrechtzuerhalten.

5.1.2 Lenkungsgruppe einrichten

Zusätzlich zur Projektleitung soll eine Lenkungsgruppe etabliert werden, die gemeinsam mit der Projektleitung den Prozess der Strategieerstellung begleitet. Hierdurch sollen sowohl die Transparenz als auch die Inklusivität des Prozesses gewährleistet werden. Damit die Lenkungsgruppe ihren Auftrag erfüllen kann, muss der Zugang zu möglicherweise als sensibel eingestuften Informationen und Dokumenten gewährleistet werden bzw. dieser darf kein Problem darstellen. Auch müssen die hier vertretenen Personen die notwendigen Kompetenzen mitbringen, um die mit ihrem Auftrag verbundenen Rollen im Rahmen der Begleitung der Strategieerstellung auszuüben.

Umgesetzte Empfehlungen

Zur Koordinierung der Strategieerstellung wurde die „ressortübergreifende Arbeitsgruppe Cybersicherheit“ (AG Cybersicherheit) eingerichtet, in welcher Vertreter:innen alle Ressorts sowie des Magistrats der Stadt Bremerhaven vertreten waren. Diese wurden während der Erarbeitungsphase der Strategie im Rahmen von sechs Arbeitsgruppentreffen sowie im Rahmen bilateraler Gespräche und Abstimmungen im Umlaufverfahren aktiv in den Prozess der Strategieerstellung eingebunden. Die Arbeitsgruppe wurde nicht formal als Lenkungsgruppe identifiziert; durch die etablierten Arbeitsstrukturen und Beteiligungsprozesse wurde jedoch eine intensive Vorbereitung unterschiedlicher Arbeitsschritte (etwa die inhaltliche Abstimmung der Strategie, die Abstimmung auf Leitungsebene sowie die formale Verabschiedung durch den Senat) überhaupt erst möglich, sodass der Zweck dieses Organs erfüllt wurde.

Herausforderungen bei der Umsetzung

Während der Strategieerstellung wurde nicht auf als Verschlusssache eingestufte Dokumente zurückgegriffen. Insofern existierten keine besonderen Anforderungen (etwa Sicherheitsfreigaben) an die Mitglieder der Arbeitsgruppe. Es wurde jedoch deutlich, dass das Gremium sehr heterogen besetzt wurde; zum Teil wurde eine Besetzung nach Führungs- und Entscheidungskompetenz vorgenommen, zum Teil nach Fachexpertise (etwa mit Fokus auf den Bereich der Informationssicherheit). Diese Heterogenität bereichert die Arbeit der Arbeitsgruppe um vielfältige Perspektiven, führte aber auch zu aufwändigeren Abstimmungsprozessen.

Ausblick und Anregungen

Nach Abschluss der Strategieerstellung wurde die „ressortübergreifende Arbeitsgruppe Cybersicherheit“ aufgelöst und in nahezu identischer Besetzung in den nunmehr etablierten „Arbeitskreis Cybersicherheit“ (AK Cybersicherheit) überführt. Für die Fortschreibung der Strategie sollte geprüft werden, ob das Erfordernis einer separaten Lenkungsgruppe auf übergeordneter Führungsebene gesehen wird, um insbesondere Führungsentscheidungen schneller herbeizuführen, die sensibler Abwägung bedürfen (etwa mit Blick auf benötigte personelle und materielle Ressourcen) und regelmäßig auf Arbeitsebene nicht getroffen werden können. Hierdurch könnte der zur Entgegenwirkung möglicher Zielkonflikte geforderte Mechanismus zusätzlich gestärkt werden.

5.1.3 Stakeholder identifizieren

Durch die Projektleitung müssen erste Stakeholder identifiziert werden, welche bei der Erstellung der Strategie mitwirken sollen. Hierbei müssen die Anforderungen und Erwartungen an die Rolle und den Beitrag unterschiedlicher Stakeholder klar kommuniziert werden. Es ist wichtig, hier unterschiedliche Fachkompetenzen zu berücksichtigen, was dem besonderen Inklusivitätsgedanken Rechnung trägt. Falls der Umfang der zu berücksichtigenden Stakeholder zu groß wird, ist die Einrichtung eines „Advisory Committees“ (etwa eines Beirats) sinnvoll.

Umgesetzte Empfehlungen

Neben der Beteiligung der Ressorts sowie dem Magistrat der Stadt Bremerhaven wurden auch weitere Akteur:innen in die AG Cybersicherheit eingeladen. Hierzu zählten etwa die Landesbeauftragte für Datenschutz und Informationssicherheit (LfDI), der Landesbehindertenbeauftragte (LBB) sowie die Zentralstelle zur Verwirklichung der Gleichberechtigung der Frau (ZGF). Durch ihre Einbeziehung sollte sichergestellt werden, dass während der Auswahl relevanter Handlungsfelder, dem Entwurf einzelner Zielvisionen sowie auch der Niederschrift der Strategie selbst ein sensibles Augenmerk auf spezielle Verantwortungsbereiche (etwa geschlechtsspezifische oder inklusionsbedingte Bedürfnisse und Anforderungen) gelegt wurde. Als Ergebnis dieser Bemühungen wurde etwa die Strategie selbst zusätzlich in einem barrierefreien Format erstellt und veröffentlicht. Darüber hinaus sollte die Einbindung der Landesbeauftragten für Datenschutz und Informationssicherheit die frühzeitige Identifikation möglicherweise datenschutzrechtlich relevanter Regelungserfordernisse gewährleisten, um diese im Rahmen des sehr knappen Bearbeitungszeitraums erforderlichenfalls vorbereiten und angemessen adressieren zu können.

Herausforderungen bei der Umsetzung

Für die Strategieerstellung war ein Zeitrahmen von maximal fünf Monaten vorgesehen. Der Fokus bei der Auswahl relevanter Stakeholder lag deshalb für die erstmalige Erstellung der Strategie zunächst auf der kohärenten Gesamtgestaltung der Cybersicherheitsarchitektur, die darauf ausgelegt sein sollte, vielfältige Zielgruppen zu berücksichtigen. Eine intensive Befassung einzelner (etwa mit den Handlungsfeldern korrespondierender) Zielgruppen wäre aufgrund des hohen Zeitaufwandes im Rahmen des Erarbeitungs- und Abstimmungsprozesses nicht möglich gewesen. In einem umfangreichen Informationsverfahren wurden daher zunächst zahlreiche Stellen über die Erstellung der Bremischen Cybersicherheitsstrategie informiert. Ein intensiver inhaltlicher Austausch war jedoch im ersten Anlauf nicht möglich.

Ausblick und Anregungen

Um bei der Fortschreibung der Strategie vielfältige Interessen und Bedürfnisse adäquat und in angemessener fachlicher Tiefe abzubilden, sollte ein Austauschprozess mit relevanten Stakeholdern frühzeitig geplant und durchgeführt werden. Die Auswahl relevanter Akteur:innen könnte sich an einzelnen Sektoren oder zuvor definierten Handlungsfeldern orientieren und dazu beitragen, dass sektor- oder themenfeldspezifische Bedürfnisse beleuchtet und in der Strategiefortschreibung angemessen berücksichtigt werden. Bei umfangreichen Beteiligungen muss jedoch stets berücksichtigt werden, dass auch innerhalb definierter Bereiche Interessenschwerpunkte und Bedürfnisse sehr heterogen sein können

und mit steigender Anzahl der Beteiligten ein intensives Stakeholder-Management erforderlich wird, um Missverständnisse und Konflikte bei den Zielerwartungen zu reduzieren. Der Umfang sowie das Format des angestrebten Beteiligungsprozesses stehen hierbei in direkter Abhängigkeit vom Zeitplan sowie den benötigten personellen Ressourcen und müssen vor dem Hintergrund der politischen Zielvorstellung an die Fortschreibung der Cybersicherheitsstrategie abgewogen werden.

5.1.4 Ressourcenbedarf erheben

Die Projektleitung muss an dieser Stelle benötigte personelle und materielle Ressourcen identifizieren, die für die Erstellung der Strategie erforderlich sind, und klären, wie diese zu beschaffen sind. Ressourcen können entweder über eine Neuverteilung vorhandener Mittel oder das zusätzliche Einwerben externer Mittel generiert werden. Besonders bedeutsam ist hierbei das Einwerben von Mitteln, welche über den gesamten Lebenszyklus der Cybersicherheitsstrategie gewährt werden und somit eine verlässliche Planung der Strategieerstellung und -fortschreibung ermöglichen.

Umgesetzte Empfehlungen

Für die Erstellung der Bremischen Cybersicherheitsstrategie wurde eine Projektgruppe mit zwei Mitarbeiter:innen eingerichtet und per Abordnung besetzt, sodass für die gesamte Koordinierung, Erarbeitung und Niederschrift der Strategie zwei Vollzeiteinheiten (VZE) beim Senator für Inneres zur Verfügung standen. Die Besetzung der ressortübergreifenden AG Cybersicherheit durch alle Ressorts sowie den Magistrat der Stadt Bremerhaven war nur durch die Bereitstellung eigener Mitarbeiter:innen möglich, welche diese Aufgabe zusätzlich zu ihren originären Funktionen übernahmen.

Herausforderungen bei der Umsetzung

Da innerhalb der Ressorts sowie beim Magistrat der Stadt Bremerhaven keine personellen Ressourcen für die Mitwirkung an der Erstellung der Cybersicherheitsstrategie vorgesehen waren, führte diese Beteiligung zu einer Mehrfachbelastung der entsandten Mitarbeiter:innen sowie der betroffenen Organisationseinheiten, was zu einer Reduktion der Akzeptanz des Vorhabens führen kann. Für die künftige Strategiefortschreibung besteht darüber hinaus die Herausforderung, dass die zu diesem Zweck errichtete Projektgruppe Cybersicherheit beim Senator für Inneres und Sport mittlerweile aufgelöst wurde und die mit der Fortschreibung der Strategie betrauten Mitarbeiter:innen diese Aufgabe nun zusätzlich zu den mittlerweile in der Zentralstelle Cybersicherheit geschaffenen Aufgaben übernehmen.

Ausblick und Anregungen

Der mögliche Detailgrad einer Strategie ist von den für die Erstellung verfügbaren Ressourcen abhängig. Gleichzeitig verfügt die nunmehr für die Strategiefortschreibung verantwortliche Zentralstelle Cybersicherheit beim Senator für Inneres und Sport nicht über die Kompetenz, Entscheidungen über die Neuverteilung von materiellen oder personellen Ressourcen zu diesem Zweck vorzunehmen, was zu einem Zielkonflikt führen kann. Um die Zielvorstellung an die Fortschreibung der Cybersicherheitsstrategie in eine realistische Erwartungshaltung zu überführen, ist daher im Vorfeld eine übergeordnete und gemeinsam getragene Entscheidung (etwa auf politischer Ebene) erforderlich, welche konkrete Zielrichtung für die Strategiefortschreibung gewünscht ist, nach welcher sich in der Folge

auch der Umfang einer etwaigen Stakeholder-Beteiligung orientiert. Dieser Zielrichtung sollte dann mit einem angemessenen Zeit- und Ressourcenansatz begegnet werden, damit Erwartungen realistisch erfüllt werden können.

Grundsätzlich wird empfohlen, etwa 10 Prozent des IT-Budgets für Maßnahmen der Informations- und Cybersicherheit einzuplanen. Dieser Richtwert dient als Orientierung und stellt sicher, dass genügend Ressourcen für technische und organisatorische Maßnahmen bereitgestellt werden. Die konkrete Höhe der Ressourcen sollte jedoch auf einer fundierten Risikoanalyse basieren und vorhandene IT-Strukturen berücksichtigen. Regelmäßige Überprüfungen und Anpassungen des Budgets sind notwendig, um auf die sich ständig ändernde Bedrohungslage reagieren zu können und die digitale Resilienz der Organisation nachhaltig zu stärken.

5.1.5 Strategieentwicklung planen

Die Projektleitung soll die Lenkungsgruppe auf geeignete Art und Weise über die Entwicklung der Strategie sowie den Zeitplan informieren. Hierbei soll entschieden werden, ob die Strategie verbindlichen Charakter (etwa als Teil der Gesetzgebung) erhält oder eher einen politischen bzw. strategischen Empfehlungscharakter besitzt; darüber hinaus wirkt sich die (Rechts-)Form der geplanten Strategie auf mögliche Beteiligungs- und Abstimmungsprozesse aus, die im Land formal vorgeschrieben sein könnten.

Umgesetzte Empfehlungen

Die AG Cybersicherheit wurde durch die Projektleitung im Rahmen von sechs Arbeitsgruppentreffen über den Zeitraum von fünf Monaten engmaschig in den Prozess der Strategieerstellung im Rahmen eines umfassenden Informationsaustauschs eingebunden. Zur Strukturierung des Projekts sowie zur Herstellung größtmöglicher Transparenz und Verbindlichkeit wurde durch die Projektleitung ein Projektphasenplan erstellt, der neben einer angestrebten Zeitplanung auch einen Überblick über Meilensteine sowie Abstimmungserfordernisse beinhaltete. Mithilfe dieses Projektphasenplans wurde bei jedem Arbeitsgruppentreffen eine Fortschrittsbewertung vorgenommen sowie ein Überblick über anstehende Aufgaben oder aktuelle Herausforderungen gegeben.

Die Bremische Cybersicherheitsstrategie besitzt einen strategischen Empfehlungscharakter und unterbreitet gemeinsam erarbeitete Vorschläge zur Errichtung einer an den Bedürfnissen des Landes Bremen ausgerichteten Cybersicherheitsarchitektur, in welcher Aufgaben der Cybersicherheit koordiniert und bewältigt werden können. Als Abstimmungserfordernis wurde insofern zunächst während des Beteiligungsprozesses die umfangreiche Einbindung der Ressorts sowie des Magistrats der Stadt Bremerhaven identifiziert; für den Schritt der Verabschiedung der Strategie wurde eine Senatsbefassung vorgesehen. Diese wurde am 11.04.2023 durchgeführt und mündete in der formalen Verabschiedung und Veröffentlichung der Bremischen Cybersicherheitsstrategie 2023.

Herausforderungen bei der Umsetzung

Die Bremische Cybersicherheitsstrategie sollte vor allem grundlegende Zielvorstellungen und eine auch zukünftig skalierbare und mit länderübergreifenden Strukturen interoperable Cybersicherheitsarchitektur schaffen, was im Rahmen der Arbeitsgruppe sehr gut gelang.

Eine Benennung konkret erforderlicher Haushaltsmittel war aufgrund des Abstraktionsniveaus bei der erstmaligen Strategieerstellung jedoch nicht möglich. Sollten bei der künftigen Strategieerstellung im Rahmen eines Umsetzungsplans konkrete Maßnahmen beschrieben werden, sind die landesspezifischen Verfahren sowie haushaltsrechtliche Vorgaben bei der Einwerbung von Mitteln zu beachten.

Ausblick und Anregungen

Um die unterschiedlichen Anforderungen an die Verfahren einer abstrakten Strategieerstellung einerseits und einer konkreten Ressourcenaufstellung andererseits angemessen erfüllen zu können, sollten beide Prozesse, wie durch das NCS-Handbuch beschrieben, voneinander getrennt werden. In einem Strategiedokument können die übergeordneten Ziele erarbeitet werden, welche etwaige Bedürfnisse aller beteiligten Akteur:innen im Kontext der aktuellen politischen, rechtlichen und bedrohungsspezifischen Lage konkretisieren; in einem separat zu erarbeitenden Umsetzungsplan können Maßnahmen zur Verwirklichung der einzeln benannten Ziele erarbeitet, priorisiert und mit einem Mittelansatz versehen werden. Eine Priorisierung und Durchführungsplanung einzelner Maßnahmen kann in der Folge nur im Rahmen zur Verfügung gestellter Haushaltsmittel erfolgen, die nach den landesspezifischen haushaltsrechtlichen Vorgaben einzuwerben sind.

5.2 Phase 2: Sachstandserhebung und -analyse

Das Ziel dieser Phase besteht darin, Informationen über die aktuelle Bedrohungslandschaft sowie mögliche Entwicklungen zu erheben, damit diese dann in die Strategieerstellung und -ausrichtung einfließen können. Hierbei sollen Expert:innen (das sogenannte „advisory committee“) hinzugezogen werden; der Output dieser Phase sollte in einem abschließenden Bericht an die Lenkungsgruppe bestehen. Bevor mit der Niederschrift der Strategie begonnen wird, sollte die Projektleitung die gewonnenen Informationen analysieren und bewerten, um Schwachstellen oder Lücken zu identifizieren und Handlungsvorschläge zu unterbreiten, welche diese adressieren könnten. Die Analyse sollte mit einer Bewertung schließen, inwieweit die aktuellen rechtlichen, strategischen und operativen Rahmenbedingungen im Land die identifizierten Anforderungen erfüllen können und wo es noch Lücken gibt. Die Analyse kann auch auf detaillierterer Ebene durchgeführt werden, um spezielle Lücken (etwa in der Aus- und Fortbildung) zu identifizieren.

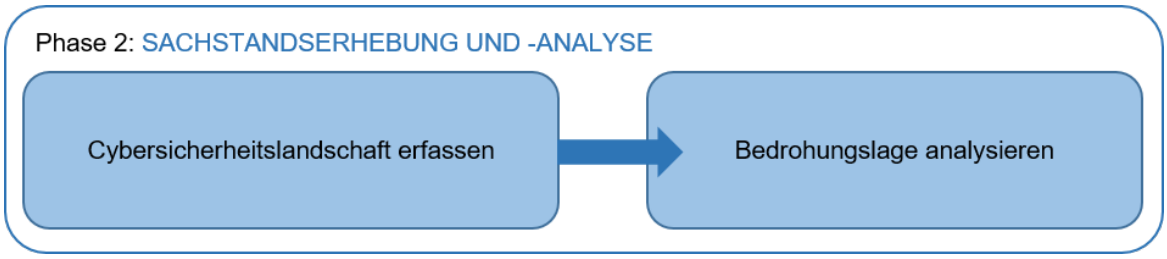


Abbildung 6 - Wichtige Schritte während der Sachstandserhebungs- und -analysephase

5.2.1 Cybersicherheitslandschaft erfassen

Hier sollen die Stärken und Schwächen der aktuellen Cybersicherheitslandschaft auf Basis relevanter Dokumente und mithilfe verschiedener Akteur:innen aus Staat, Wirtschaft und Zivilgesellschaft betrachtet werden. Hierbei sollen auch die verschiedenen Rollen der Stakeholder und ihr möglicher Beitrag zur Stärkung der Cybersicherheit identifiziert werden.

Als Teil dieser Analyse können sowohl bereits vorhandene Kompetenzen benannt als auch besonders kritische Bereiche identifiziert werden, die für das Funktionieren von Gesellschaft und Wirtschaft besonders bedeutsam sind. Darüber hinaus können hier auch Informationen über Projekte, Initiativen, Abkommen und Vereinbarungen einfließen. Es wird empfohlen, ähnliche Empfehlungen auf regionaler Ebene einzuholen und darüber hinaus sektorspezifische Strategien und Initiativen zu betrachten.

Umgesetzte Empfehlungen

Im Rahmen der Strategieerstellung wurde mithilfe der vordefinierten Handlungsfelder des Leitfadens zur Erstellung föderaler Cybersicherheitsstrategien die bestehende staatliche Cybersicherheitsarchitektur in der Freien Hansestadt Bremen beschrieben. Darüber hinaus wurden teilweise für einzelne Handlungsfelder relevante Initiativen oder Projekte bei der jeweiligen Sachstandsdarstellung für die Freie Hansestadt Bremen (jeweils im dritten Unterkapitel der Handlungsfeldanalyse) benannt.

Herausforderungen bei der Umsetzung

Für die erstmalige Strategieerstellung fand zunächst eine Fokussierung auf staatliche Kompetenzen und Bemühungen statt. Eine umfassende systematische Erfassung vorhandener Kompetenzen in den Bereichen Staat, Wirtschaft, Gesellschaft und Wissenschaft (etwa im Rahmen einer umfassenden Landkarte) war jedoch im ersten Anlauf nicht möglich und gestaltete sich aufgrund der Heterogenität sowie Vielzahl vorhandener Akteur:innen im Land als herausfordernd.

Ausblick und Anregungen

In der geplanten Strategiefortschreibung sollte eine differenziertere Erfassung vorhandener Kompetenzen und Initiativen erfolgen. Eine Bewertung etwaiger Lücken ist jedoch regelmäßig nur möglich, wenn Bedarfe erkannten Herausforderungen gegenübergestellt werden. Eine denkbare Lösung könnte deshalb darin bestehen, zunächst Herausforderungen und hieraus abgeleitete Handlungsbedarfe zu identifizieren und in einem zweiten Schritt das Delta zwischen benötigten (Soll) und vorhandenen (Ist) Kompetenzen zu ermitteln. Je konkreter hierbei die Anforderungen an die benötigten Kompetenzen formuliert werden können, desto zielgerichteter kann die Erhebung erfolgen.

Diese Herangehensweise steht im Gegensatz zu dem umfassenden Bemühen, eine vollständige Landkarte beteiligter Akteur:innen zu erstellen, die eher darauf ausgerichtet wäre, einen vollständigen Überblick über die Cybersicherheitslandschaft im Land an sich zu geben. Der informatorische Mehrwert einer solchen Übersicht muss daher stets mit dem Erstellungs- und Pflegeaufwand abgeglichen und ins gewünschte Verhältnis gesetzt werden.

5.2.2 Bedrohungslage analysieren

Auf Basis der erhobenen Informationen sollen die Risiken identifiziert werden, welchen das Land aufgrund seiner digitalen Abhängigkeit ausgesetzt ist. Dies kann regelmäßig durch eine Risikoanalyse und -bewertung erfolgen. Eine allgemeine Risikoanalyse kann hierbei die Grundlage für spezifischere Risikoanalysen in der Zukunft darstellen. Eine besondere Bedeutung fällt dem Ansatz des Risikomanagements zu.

Umgesetzte Empfehlungen

Jedem Handlungsfeld in der Cybersicherheitsstrategie wurde eine Zielvorstellung vorangestellt (diese werden noch einmal in Kapitel 6 abgebildet), welche durch die Lenkungsgruppe erarbeitet wurde. Hierdurch wurden der strategische Fokus und Umfang eines jeden Handlungsfeldes festgelegt, innerhalb dessen sich zu verwirklichende Ziele einordnen müssen. Ebenfalls wurden die mit jedem Handlungsfeld korrespondierenden Herausforderungen und Handlungserfordernisse beschrieben, um geeignete Maßnahmen zur Zielerreichung ableiten zu können.

Herausforderungen bei der Umsetzung

Eine umfassende Risiko- und Schwachstellenanalyse innerhalb einzeln definierter Handlungsfelder hätte eine umfassende Stakeholder-Identifizierung und Beteiligung in den jeweils benannten Bereichen erforderlich gemacht, welche im Rahmen der Strategieerstellung nicht möglich war. Aufgrund des Abstraktionsgrads der Erhebung wurde ebenfalls keine systematische Risikobewertung im Rahmen eines Risikomanagements durchgeführt.

Ausblick und Anregungen

Ein systematisches Risikomanagement würde dabei helfen, Schwachstellen zu erkennen und darüber hinaus Handlungserfordernisse zu priorisieren, was vor dem Hintergrund knapper Ressourcen ein erstrebenswertes Ziel ist. Gleichzeitig muss jedoch berücksichtigt werden, dass ein Risikomanagement ebenfalls mit einem erhöhten Ressourcenaufwand verbunden ist, welcher sich jedoch regelmäßig langfristig bewährt.

Für die Fortschreibung der Strategie wäre es daher wünschenswert, erste Instrumente des Risikomanagements bei der Analyse und Bewertung (gegebenenfalls zunächst mit dem Fokus auf einzelne Handlungsfelder bezogener) möglicher Bedrohungen zu implementieren, um eine solide Grundlage für notwendige Priorisierungsentscheidungen zu schaffen. Hierbei können verschiedene Stakeholder betroffener Bereiche eingeladen werden, sich an der Beschreibung und Analyse der Bedrohungslandschaft zu beteiligen, um durch ihre Expertise ein umfassenderes Bild zu erhalten.

5.3 Phase 3: Produktion der Strategie

In dieser Phase soll der Text der Strategie entworfen werden. Hierzu sollen identifizierte Stakeholder aus allen Zielgruppen im Rahmen eines Konsultationsprozesses (etwa über Arbeits- oder Diskussionsgruppen) eingebunden werden. Diese größere Gruppe an Stakeholdern, koordiniert durch die Projektgruppe, kann die übergeordnete Vision sowie den Umfang innerhalb der Strategie festlegen und eine Priorisierung möglicher Ziele mit Blick auf den Einfluss im jeweils für sie relevanten Bereich vornehmen. Ebenfalls müssen hier die erforderlichen Ressourcen festgelegt und gesichert werden, um die vorgesehenen Ziele zu erreichen.

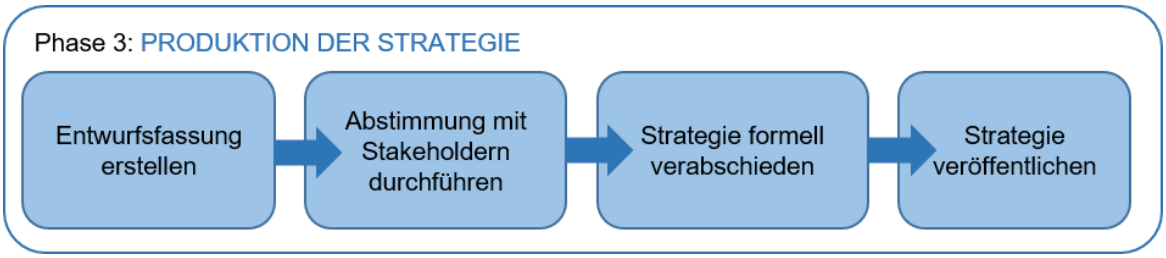


Abbildung 7 - Wichtige Schritte während der Produktionsphase

5.3.1 Entwurfsfassung der Cybersicherheitsstrategie erstellen

Zur Erstellung der Strategie sollten Arbeitsgruppen gebildet werden, welche sich mit spezifischen Themen oder einzelnen Kapiteln der Strategie beschäftigen. Die Strategie sollte eine Richtung aufzeigen, in welche sich das Land im Phänomenbereich der Cybersicherheit bewegen möchte, eine klare umrissene Vision sowie Ziele benennen, die im Rahmen der ersten Strategieumsetzung bewältigt werden sollen. Hierbei sollen Maßnahmen mit Blick auf ihren möglichen Wirkungsgrad priorisiert werden. Die Strategie kann hierbei verschiedene Verläufe skizzieren, Handlungsmotivationen schaffen und die Voraussetzungen für die Zuweisung der für die Umsetzung benötigten Ressourcen schaffen. Hierbei können Ergebnisse der Sachstandserhebung und Analysephase berücksichtigt werden.

Das Strategiedokument sollte im Rahmen guter Governance Schlüsselrollen sowie die jeweilige Verantwortung der Stakeholder benennen. Dies beinhaltet die Identifikation einer verantwortlichen Stelle für das Management der Strategieevaluation und -fortschreibung sowie einer verantwortlichen Stelle für das Management der Umsetzung der Strategie (auf nationaler Ebene wird hierfür beispielsweise ein Nationaler Cybersicherheitsrat benannt). Die Strategie muss für mehr Klarheit und Transparenz darüber hinaus das Mandat verschiedener Institutionen bestätigen oder definieren, die in der Cybersicherheitsarchitektur vertreten sind. Dazu zählen Verantwortlichkeiten für die Initiierung und Weiterentwicklung von Policies im Bereich der Cybersicherheit, die Sammlung und Auswertung von Gefährdungsbewertungen, die Bewältigung von Cybervorfällen (etwa durch ein CERT oder CSIRT) sowie die Planung und Vorbereitung eines Krisenmanagements.

Umgesetzte Empfehlungen

Entwurfsfassungen des Strategiedokuments wurden durch die Projektleitung erstellt und sodann der AG Cybersicherheit vorgelegt, in welcher diese diskutiert und abgestimmt sowie Änderungsbedarfe formuliert wurden. Die Einarbeitung von Vorschlägen und Änderungswünschen erfolgte hierbei zentral durch die PG Cybersicherheit, sodass die Koordinierung des Abstimmungsprozesses in einer Hand blieb. Es wurden keine separaten Arbeitsgruppen zur Erstellung des Strategiedokuments eingerichtet.

Die Strategie zeigt auf, wie die Cybersicherheitsarchitektur für das Land Bremen aufgebaut werden soll und benennt für einzeln identifizierte Handlungsfelder konkrete Zielvorstellungen. Ebenfalls werden erste hiermit korrespondierende Maßnahmen im jeweils letzten Unterkapitel benannt. Konkrete Verantwortlichkeiten wurden in den Bereichen benannt, die bereits im Rahmen der Geschäftsverteilung des Senats dem Senator für Inneres und Sport sowie dem Senator für Finanzen zugewiesen wurden, etwa die Einrichtung der Zentralstelle Cybersicherheit als koordinierende Stelle für Belange der Cybersicherheit im Land

Bremen sowie die Weiterentwicklung des Cybersicherheitsrechtsrahmens. Hierdurch wurde der Senatsbeschluss zur geänderten Geschäftsverteilung weiter konkretisiert und mit einer arbeitsfähigen Struktur hinterlegt.

Herausforderungen bei der Umsetzung

Eine separate Erstellung einzelner Kapitel durch unterschiedliche Beteiligte erfolgte nicht, da dies zu einer unverhältnismäßigen Arbeitsbelastung geführt und zusätzliche Koordinierungsaufwände verursacht hätte, die mit Blick auf den Umfang der Arbeitsgruppe nicht gerechtfertigt gewesen wären. Es erfolgte keine Priorisierung von Zielen; vielmehr wurden diese zunächst für jedes Handlungsfeld gleichwertig ausgearbeitet, um hier keine Bewertung vorwegzunehmen. Darüber hinaus wurden keine individuellen Verantwortlichkeiten für Bereiche oder einzelne Maßnahmen festgelegt, die über die per Senatsbeschluss zugewiesene Geschäftsverteilung in den Ressortbereichen des Senators für Inneres und Sport und des Senators für Finanzen hinausgehen.

Ausblick und Anregungen

Um die Verbindlichkeit in der Umsetzung von Maßnahmen zu erhöhen sowie eine notwendige Verantwortungs- und Rollenklarheit zu schaffen, sollte in der Strategiefortschreibung geprüft werden, ob eine themen- oder ressortspezifische Aufteilung der Verantwortung für bestimmte Maßnahmen, welche im Kern den Hauptverantwortungsbereich einzelner Akteur:innen treffen, im Rahmen der Umsetzung möglich und sinnvoll ist.

Die bereits per Geschäftsverteilung des Senats festgelegten Verantwortlichkeiten sowie insbesondere die Notwendigkeit der übergreifenden Koordinierung bleiben hiervon unberührt. Dies würde dem Umstand Rechnung tragen, dass ganzheitliche Cybersicherheit von vielen verschiedenen Akteur:innen getragen werden muss und nicht nur durch einzelne Stellen bewältigt werden kann. Gleichzeitig können vielfältige Synergien genutzt werden, wenn diese bei Kernaufgaben der eigenen Arbeit stets mitgedacht wird.

5.3.2 Abstimmung mit identifizierten Stakeholdern durchführen

Damit die spätere Strategie auf einer gemeinsamen breit angelegten Vision fußt, sollte das Dokument nach Fertigstellung des Entwurfs umfangreich an mögliche Stakeholder verteilt werden. Darüber hinaus sollte Feedback eingefordert werden, welches dann in der Finalisierung der Strategie Einfluss findet.

Umgesetzte Empfehlungen

Das fertiggestellte Dokument wurde mit dem Kreis identifizierter Stakeholder abgestimmt, die bereits engmaschig bei der Erstellung der Strategie involviert wurden (s. Kapitel 5.1.3). Darüber hinaus wurde eine Vielzahl relevanter Akteur:innen über den Erstellungsprozess informiert (s. hierzu das Kapitel „Informationsprozess“ in der Bremischen Cybersicherheitsstrategie 2023).

Herausforderungen bei der Umsetzung

Ein umfangreiches Beteiligungsverfahren vielfältiger Stakeholder, über den Kreis der an der Mitwirkung beteiligten Akteur:innen hinaus, hat nicht stattgefunden. Voraussetzung für ein solches Vorgehen ist einerseits ein angemessener zeitlicher Rahmen, um Rückmeldungen zu erlauben und sinnvoll in die Strategie einarbeiten zu können; andererseits erfordert ein Beteiligungsverfahren eine vorherige Konkretisierung einzelner Handlungsschwerpunkte bis zu dem Maß, dass eine Bestimmung der hiervon betroffenen Akteur:innen möglich wird und ihr Beitrag konkret definiert werden kann.

Ausblick und Anregungen

Die Empfehlungen hier unterscheiden sich im Wesentlichen nicht von denen in Kapitel 5.1.3 (Stakeholder identifizieren). Es könnte jedoch zielführend sein zu prüfen, ob sich der Personenkreis identifizierter Stakeholder, welche aktiv in die Erarbeitung einzelner Inhalte eingebunden werden können, von jenem unterscheidet, welcher das fertig gestellte Dokument prüfen soll und Feedback einfließen lassen kann. Hierzu könnten insbesondere bereits vorhandene Organisationsstrukturen in spezifischen Bereichen (etwa Industrie- sowie Handwerks- und Handelskammern) eine Hilfestellung bieten, um Zugang zu einzelnen Zielgruppen zu erhalten und ihre Beteiligung zu koordinieren.

5.3.3 Strategie formell verabschieden

Im finalen Schritt der Strategieerstellung muss die Projektleitung dafür sorgen, dass die Strategie von der Exekutive förmlich verabschiedet wird, beispielsweise durch einen parlamentarischen Prozess. Maßgeblich für den Erfolg der Strategie ist, dass nicht nur die Erstellung der Strategie (bzw. ihre Verabschiedung) vom Parlament gebilligt wird, sondern diese Unterstützung auch während der Umsetzungsphase anhält.

Umgesetzte Empfehlungen

Die förmliche Verabschiedung der Bremischen Cybersicherheitsstrategie 2023 durch den Senat erfolgte am 11.04.2023. Der hierfür erforderliche Senatsbeschluss wurde durch die Projektleitung in Abstimmung mit der AG Cybersicherheit vorbereitet.

Herausforderungen bei der Umsetzung

Eine über die Verabschiedung der Strategie hinausgehende Senatsbefassung war nicht vorgesehen. Ebenfalls erfolgte keine separate Anmeldung von Haushaltsmitteln, weil diese noch nicht konkret beziffert werden konnten.

Ausblick und Anregungen

Neben der Verabschiedung des konkreten Strategiepapiers könnte zukünftig eine zusätzliche Senatsbefassung mit einem separat zu erstellenden Umsetzungsplan für die Strategie erfolgen (s. hierzu Kapitel 5.1.5). Dies würde die Grundlage für erforderliche Ressourcenzuweisungen schaffen, ohne die eine systematische Umsetzung der Maßnahmen zur Steigerung der Cybersicherheit im Land Bremen nicht möglich ist. Eine verlässliche Planung über den Strategiezeitraum hinweg würde hierbei Handlungs- und Planungssicherheit für alle an der Umsetzung beteiligten Stellen schaffen.

5.3.4 Strategie veröffentlichen

Bei der Strategie sollte es sich um ein öffentliches Dokument handeln, welches leicht verfügbar gemacht wird. Die Strategie sollte mit begleitender interner und externer Öffentlichkeitsarbeit bekannt gemacht werden. Diese breite Verfügbarkeit ist wichtig, damit die Öffentlichkeit von der Strategie und den Bemühungen der Regierung Kenntnis erhält. Gleichzeitig kann so dem Bemühen Rechnung getragen werden, mehr Aufmerksamkeit auf das Thema Cybersicherheit zu lenken. Sollte die Strategie gemeinsam mit einem Umsetzungsplan verfasst worden sein, sollte dieser auf zusätzliche Möglichkeiten hinweisen, wie sich Akteur:innen aus Wirtschaft und Gesellschaft bei der Umsetzung einbringen können.

Umgesetzte Empfehlungen

Die Verabschiedung der Strategie durch den Senat wurden durch eine Pressekonferenz am 11.04.2023 sowie begleitende Presse- und Öffentlichkeitsarbeit flankiert. Ihre Veröffentlichung im Internet erfolgte in zwei Versionen (regulär und barrierefrei), um eine größtmögliche Verfügbarkeit und Nutzbarkeit für Interessierte zu gewährleisten. Darüber hinaus erfolgte eine breite Rezeption des Strategiedokuments durch Dritte (etwa durch die Presse); diese unterlag nicht den Steuerungsmöglichkeiten der Projektleitung, trug jedoch zusätzlich zu einer breiteren Kenntnisnahme bei.

Herausforderungen bei der Umsetzung

Bei der Veröffentlichung der Strategie selbst wurden keine Herausforderungen sichtbar. Bei der erstmaligen Anfertigung der Strategie wurde kein separater Umsetzungsplan verfasst, sodass die Empfehlung nicht umgesetzt werden konnte, Beteiligungsmöglichkeiten zur systematischen Nutzung der Ressourcen Dritter auszuweisen.

Ausblick und Anregungen

Bei der Strategiefortschreibung könnten (ggf. im Rahmen eines Umsetzungsplans) Hinweise gegeben werden, wie sich Akteur:innen in den jeweils betroffenen Themenbereichen in die Verwirklichung der Zielvorstellungen einzelner Handlungsfelder einbringen können. Hierdurch können möglicherweise Potenziale genutzt werden, die im Rahmen einer ersten Stakeholder-Identifikation übersehen wurden. Gleichzeitig ist hierbei jedoch auch zu beachten, dass es unbeabsichtigt zu einer wahrgenommenen Einschränkung kommen kann, wenn etwaige Beteiligungsmöglichkeiten Dritter vorab zu stark konkretisiert werden. Eine denkbare Herangehensweise könnte deshalb in einem aktiven Kommunikationsprozess während der Stakeholder-Analyse liegen, in welcher am Cybersicherheitsnetzwerk Beteiligte selbst über Art und Umfang einzubringender Bedarfe und Ressourcen entscheiden.

5.4 Phase 4: Implementation

Die Implementations- oder auch Umsetzungsphase ist die wichtigste im Lebenszyklus einer jeden Cybersicherheitsstrategie. Eine strukturierte Herangehensweise an die Umsetzung, unterstützt mit ausreichenden personellen und materiellen Ressourcen, ist kritisch für den Erfolg der Strategie und muss daher bereits während der Strategieentwicklung berücksichtigt werden. Die Implementationsphase fußt auf einem Umsetzungsplan, der einen Überblick über den Ablauf der angestrebten Maßnahmen verschafft.

Da bei der Erarbeitung der Bremischen Cybersicherheitsstrategie 2023 kein separater Umsetzungsplan erstellt wurde, werden in diesem Kapitel lediglich Empfehlungen abgeleitet, welche sich aus dem NCS-Handbuch ergeben und welche sich möglicherweise auf den kommenden Strategiezyklus übertragen lassen. Das bedeutet jedoch nicht, dass keine Maßnahmen umgesetzt wurden, sondern nur, dass dies nicht in Form eines Umsetzungsplans erfolgte. Eine konkrete Betrachtung der während des Umsetzungszeitraums umgesetzten Maßnahmen findet in Kapitel 6 statt.

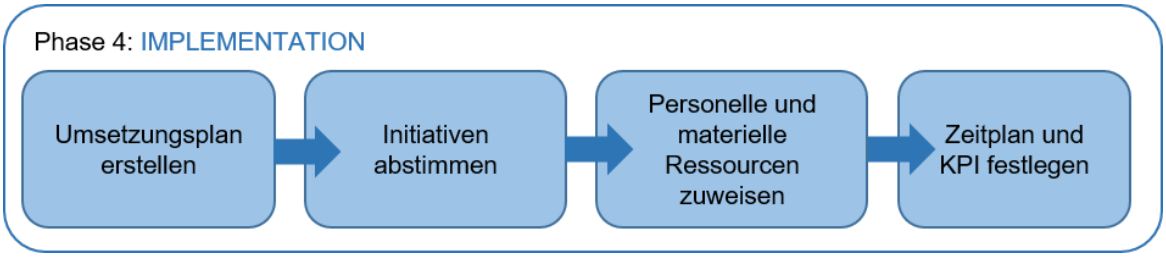


Abbildung 8 - Wichtige Schritte während der Implementationsphase

5.4.1 Umsetzungsplan erstellen

Wie bereits die Entwicklung der Strategie kann auch ihre Umsetzung nicht in der Verantwortlichkeit einer einzelnen Stelle liegen. Vielmehr sind das Engagement und die Einbeziehung unterschiedlicher Stakeholder aus den Bereichen Staat, Wirtschaft und Gesellschaft erforderlich. Ein Umsetzungsplan, in welchem Rollen klar verteilt und benötigte Ressourcen benannt wurden und zugewiesen sind, kann die effektive Umsetzung der Strategie zielgerichtet unterstützen. Hierbei fällt der Erstellung des Umsetzungsplans eine fast ebenso große Bedeutung wie seiner Ausführung zu. Der Prozess sollte durch die Projektleitung begleitet und koordiniert werden. Bedeutsam ist auch hier die Benennung klarer Verantwortlichkeiten, Rollen und Ressourcenzuweisungen.

Ausblick und Anregungen

Die gewissenhafte Erstellung eines Umsetzungsplans erfordert eine systematische Befassung mit den hierfür erforderlichen Anforderungen. Entsprechend des Lebenszyklus-Modells des NCS-Handbuchs sollte die Erstellung eines Umsetzungsplans konsequenterweise im Anschluss an die Strategieerstellung stattfinden und den gleichen Arbeitsprinzipien folgen wie bereits die Erstellung der Cybersicherheitsstrategie selbst. Sie stellt somit einen separaten Prozess dar, welcher in zeitlichem Anschluss an die Verabschiedung der Strategie erfolgen sollte.

Da für die zweite Evaluation ein Zeitraum von vier Jahren nach Verabschiedung der Strategie vorgesehen ist, wäre es wünschenswert, einen Umsetzungsplan zu entwickeln, welcher Ziele (s. hierzu das Kapitel 5.5) und Indikatoren benennt, anhand derer die Zielerreichung messbar wird. Durch eine Befassung des Senats mit einem die Strategie begleitenden Umsetzungsplan kann ein Verständnis über erforderliche Maßnahmen auf höchster politischer Ebene gestärkt werden, die Einwerbung erforderlicher Mittel gemeinsam vorbereitet und darüber hinaus koordiniert werden, um dem Zielkonflikt eines intergouvernementalen Wettbewerbs um erforderliche Ressourcen (s. hierzu Kapitel 5.1.1) mit einem geeigneten Mechanismus entgegenzuwirken.

5.4.2 Initiativen abstimmen

Die Cybersicherheitsstrategie gibt einen Überblick über die strategischen Ziele, auf die sich die Stakeholder mit Blick auf identifizierte Handlungsfelder verständigt haben und besitzt daher naturgemäß einen eher abstrakteren Charakter. Im Umsetzungsplan hingegen sollten in der Folge die spezifischen Initiativen identifiziert werden, welche zu den Zielen bzw. Zielvorstellungen der einzelnen Handlungsfelder beitragen sollen. Beispiele hierfür können etwa das Planen und Durchführen von Cybersicherheitsübungen, das Festlegen von Mindestsicherheitsstandards für kritische Infrastrukturen oder das Abstimmen von Meldewegen nach Cybersicherheitsvorfällen sein. Hierbei sollten Aufgaben mit Blick auf ihre mögliche (Aus-)Wirkung priorisiert werden (auch nach Kritikalität), um knappe Ressourcen sinnvoll zu verteilen. Hierbei kann insbesondere auf die Ergebnisse der Bedrohungsanalyse (s. hierzu Kapitel 5.2.2) sowie einer gegebenenfalls durchgeführten Risikoanalyse eingegangen werden.

Ausblick und Anregungen

Das Erfordernis, Maßnahmen auf Basis einer ausreichenden Datengrundlage zu planen, unterstreicht die Notwendigkeit einer systematischen Bedrohungsanalyse und -bewertung. Obwohl es sich bei der Erstellung der Cybersicherheitsstrategie und des Umsetzungsplans um zwei verschiedene Aufgaben handelt, wird insbesondere in diesem Punkt die wechselseitige Abhängigkeit sehr deutlich. Erfordernisse an einen Umsetzungsplan müssen daher bereits während der Strategiefortschreibung mitgedacht werden, um ein späteres Ineinandergreifen zu ermöglichen.

5.4.3 Personelle und materielle Ressourcen zuweisen

Sobald priorisierte Initiativen identifiziert wurden, sollten Verantwortliche für diese bestimmt werden. Hierdurch entsteht eine spezifische Verantwortlichkeit für die Umsetzung der Maßnahmen sowie die hierzu erforderliche Koordinierung relevanter bzw. am Prozess beteiligter Akteur:innen. Damit die benannten Verantwortlichen ihrer Aufgabe auch nachkommen können, müssen sie sowohl über das notwendige rechtliche Mandat verfügen als auch die hierfür erforderlichen Ressourcen, die gemeinsam mit der Projektleitung ermittelt werden können. Hierunter fallen sowohl personelle als auch materielle Ressourcen sowie die für die Umsetzung der Initiativen notwendige Expertise. Gemeinsam mit der Projektgruppe müssen Verantwortliche in Übereinstimmung mit den Anforderungen an haushaltsrechtliche Prozesse im Land die Ressourcenbedarfe benennen und einfordern bzw. anmelden.

Ausblick und Anregungen

Im Land Bremen besteht Ressorthoheit. Viele Maßnahmen, die zur Verwirklichung der Stärkung der Cybersicherheit geeignet sind, fallen daher nicht explizit in die per Geschäftsverteilung des Senats zugewiesenen Verantwortungsbereiche für die IT- und Cybersicherheit, sondern finden sich in den Zuständigkeitsbereichen einzelner Ressorts wieder. Eine gemeinsam vereinbarte Zuweisung klarer Verantwortungsbereiche zur Übernahme bestimmter Maßnahmen(-bereiche), welche die Zuständigkeiten der Ressorts widerspiegeln, könnte daher für die Umsetzung von Maßnahmen erfolgskritisch sein und bestehende zugewiesene Kompetenzen im Rahmen der Ressorthoheit achten.

Gleichermaßen kann dies jedoch auch den Wettbewerb um begrenzte finanzielle und materielle Ressourcen fördern, der gerade im Zuge einer gemeinschaftlichen Stärkung der Cybersicherheit vermieden werden soll. Es sollte daher geprüft werden, ob die Einrichtung eines separaten Haushaltstitels für den Bereich der Cybersicherheit einen ersten Schritt darstellen könnten, um die Einwerbung notwendiger Ressourcen zur Umsetzung in der Strategie benannter Maßnahmen zu harmonisieren und gleichzeitig die materiellen Aufwände zur Steigerung der Cybersicherheit im Land einfacher messbar und kontrollierbar zu machen.

5.4.4 Zeitplan und Key Performance Indicators festlegen

Das letzte erfolgskritische Element eines Umsetzungsplans ist die Entwicklung spezifischer Messgrößen und Kennzahlen, anhand derer eine Überprüfung der erreichten Ziele möglich wird (sogenannte key performance indicators, KPI). Hierbei ist es wichtig, auch einen korrespondierenden Zeitplan zu erstellen. Die Messgrößen und Kennzahlen sollten von der Projektleitung gemeinsam mit den für die jeweiligen Aufgaben verantwortlichen Stellen entwickelt werden. Hierbei können die für einzelne Initiativen Verantwortlichen detailliertere Kennzahlen entwickeln, welche sie bei der Bewertung der Effektivität und Effizienz der getroffenen Maßnahmen unterstützen.

Ausblick und Anregungen

Durch die Entwicklung spezifischer Kennzahlen zur Messung des Umsetzungserfolgs (s. hierzu Kapitel 5.5) wird eine belastbare Grundlage für eine Evaluation der Maßnahmen (Bewertung der Umsetzung einzelner Maßnahmen) sowie letztlich auch der Zielerreichung selbst (Bewertung des Strategieerfolgs) geschaffen. Die gemeinsame Entwicklung geeigneter KPI stellt daher einen dringend erforderlichen Schritt bei der Fortschreibung der Strategie (und der Erstellung eines etwaigen Umsetzungsplans) dar und sollte darüber hinaus nach vorab definierten Standards erfolgen, um eine hohe Datenqualität sowie – insbesondere mit Blick auf in allen Bereichen anzuwendende Maßnahmen – Vergleichbarkeit zu gewährleisten.

So wird es nicht nur möglich, Umsetzungserfolge zu bewerten und bei erkannten Diskrepanzen erforderlichenfalls gegenzusteuern; auch kann auf Grundlage so erhobener belastbarer Kennzahlen dem bereits geäußerten regelmäßigen parlamentarischen Informations- und Kontrollbedürfnis zur Lage der Cybersicherheit im Land Bremen entsprochen werden. Hierzu ist eine regelmäßige Berichterstattung in der staatlichen Deputation für Inneres sowie dem Ausschuss für Wissenschaft, Medien, Datenschutz, Informationssicherheit und Digitalisierung (WMDID) denkbar.

5.5 Phase 5: Monitoring und Evaluation

Eine Strategie zu entwickeln und umzusetzen ist ein fortlaufender Prozess. Um diesen zu begleiten, sollte eine kompetente und verantwortliche Stelle einen formalen Monitoring- und Evaluationsprozess einrichten. In der Monitoringphase wird überprüft, ob der Umsetzungsplan eingehalten wurde; in der Evaluationsphase wird bewertet, ob die Strategie – gemessen an der Bewertung der Risikolandschaft – noch relevant und aktuell ist und ob sie politische Zielsetzungen noch angemessen reflektiert oder einer Anpassung bedarf.

Obwohl vor der erstmaligen Strategieüberprüfung kein formelles Monitoring während der Umsetzung durchgeführt wurde, ist eine Evaluation nach zwei Jahren vorgesehen, welche nunmehr durchgeführt wird. Die folgende Bewertung beinhaltet daher wieder eine Bewertung der umgesetzten Empfehlungen und Herausforderungen (wo anwendbar), bevor Anregungen für das nächste Umsetzungsintervall gegeben werden.

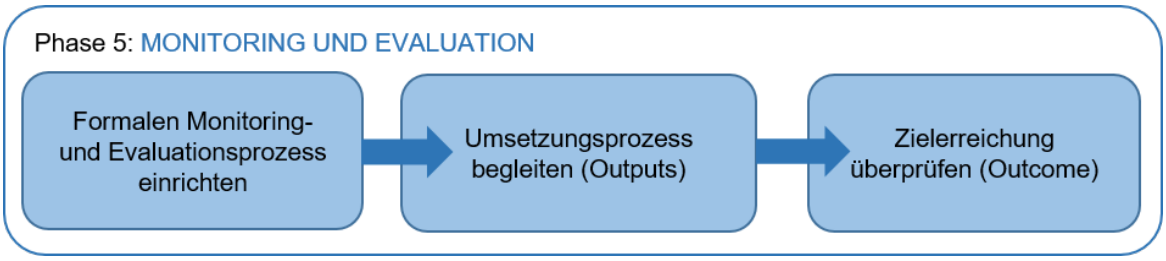


Abbildung 9 - Wichtige Schritte während der Monitoring- und Evaluationsphase

5.5.1 Formalen Monitoring- und Evaluationsprozess einrichten

Um ein effektives Monitoring sowie eine zuverlässige Evaluation der Umsetzung der Strategie zu ermöglichen, sollte eine unabhängige Stelle mit dieser Aufgabe betraut werden. Diese sollte idealerweise auch in die Festlegung relevanter KPI involviert sein, die während der Initiierungs- und Produktionsphase entwickelt werden. Eine kontinuierliche Überprüfung des Umsetzungsplans sollte Teil guter Governance-Mechanismen des Landes sein und Verantwortlichkeiten (sowohl im Sinne einer Zuständigkeit als auch Rechenschaftspflicht) klar benennen.

Maßnahmen lassen sich immer dann besonders gut messen, wenn einerseits Verantwortlichkeiten für die Ausführung klar voneinander abgegrenzt wurden (wer tut was) und andererseits geeignete KPI entwickelt wurden. Dies trifft insbesondere dann zu, wenn nicht bloß ein binäres Ergebnis bewertet werden muss (etwa ob eine Maßnahme „durchgeführt“ oder „nicht durchgeführt“ wurde), sondern Fortschritte systematisch bewertet und Verbesserungspotenziale identifiziert werden sollen. In diesem Fall ist es nicht nur erforderlich, geeignete KPI zu entwickeln, sondern darüber hinaus auch Basiswerte („baseline metrics“) zu erheben, die einen langfristigen Vergleich ermöglichen. Zur Strukturierung geeigneter KPI verweist das NCS-Handbuch hier auf das SMARRT-Modell:

Strukturierung von Key Performance Indicators mithilfe des SMARRT-Modells

Specific: Einen konkreten Handlungsbereich sowie eine spezifische Veränderung bestimmen.
Measurable: Die Zielerreichung quantifizieren oder mit geeigneten Indikatoren messbar machen.
Achievable: Ziele mit Blick auf vorhandene Ressourcen realistisch und erreichbar formulieren.
Relevant: Für den angestrebten Prozess besonders relevante Fortschrittsindikatoren bestimmen.
Responsible: Für eine Maßnahme oder Handlung verantwortliche Stellen bestimmen.
Time-related: Einen realistischen Zeithorizont für das Erzielen der Ergebnisse festlegen.

Abbildung 10 - SMARRTE Kriterien zur Strukturierung von KPI

Erst wenn geeignete KPI entwickelt und erstmals erhoben wurden, kann mithilfe der so festgelegten Basislinie eine regelmäßige Erhebung durchgeführt werden, die aufgrund vergleichbarer Werte in der Folge belastbare Aussagen über die Entwicklungen zulässt. Sollen KPI nicht nur zur Bewertung eines Endergebnisses im Rahmen der abschließenden Evaluation herangezogen werden, sondern auch eine Steuerungsrelevanz während der Implementationsphase besitzen, ist die Erhebung auf Basis eines abgestimmten Zeitplans zu Beginn und während der Implementations- und Umsetzungsphase erforderlich. Hierdurch können Abweichungen von der Zielerreichung frühzeitig bemerkt und die Gründe hierfür (etwa eine Verschiebung von Prioritäten oder unzureichend zugewiesene Ressourcen) identifiziert werden, damit ein frühzeitiges Gegensteuern möglich wird.

Umgesetzte Empfehlungen

Eine regelhafte Evaluation wurde bereits bei der Strategieerstellung verbindlich festgelegt. Die erste Evaluation erfolgt in einem kurzen Abstand zur Strategieverabschiedung nach bereits zwei Jahren, um insbesondere den Erfolg erster struktureller Maßnahmen zügig zu bewerten; für folgende Evaluationen ist ein Intervall von vier Jahren vorgesehen, sodass die Strategie dann, analog zur Nationalen Cybersicherheitsstrategie, alle fünf Jahre fortgeschrieben wird. Die Zuständigkeit hierfür liegt bei der Zentralstelle Cybersicherheit, welche den AK Cybersicherheit als Lenkungsgruppe in die Erstellung des Evaluationsberichtes einbindet und hierdurch eine Einbindung der Ressorts sowie des Magistrats der Stadt Bremerhaven sicherstellt. Sowohl die Veröffentlichung des Evaluationsberichts als auch die angestrebte Senatsbefassung stellen Rechenschaftsmechanismen (gegenüber der Öffentlichkeit sowie dem Parlament) dar, mit denen ein transparentes Vorgehen gewährleistet wird.

Herausforderungen bei der Umsetzung

Eine Evaluation durch eine unabhängige (externe) Stelle wurde nicht vorgesehen und wäre mit einem zusätzlichen Kosten- bzw. Ressourcenaufwand verbunden. Den beschriebenen Mechanismen zum inklusiven und transparenten Vorgehen fällt somit weiterhin eine besondere Bedeutung zu. Umzusetzende Maßnahmen wurden nicht in einem Umsetzungsplan, sondern in der Strategie selbst, beschrieben. Hierbei ist zwischen einmaligen Errichtungsmaßnahmen sowie Maßnahmen zu unterscheiden, die fortwährend implementiert und somit zu einem Strategieerfolg beitragen können (etwa Schulungsmaßnahmen). Im Rahmen der ersten Strategieerstellung wurden keine konkreten KPI im Sinne des SMARRT-Modells festgelegt.

Ausblick und Anregungen

Idealerweise sollten mit der Fortschreibung der Bremischen Cybersicherheitsstrategie auch konkretisierende Maßnahmen im Rahmen eines Umsetzungsplans beschrieben werden, die anhand der SMARRT-Kriterien gemessen werden können. Bei der erstmaligen Entwicklung geeigneter KPI würde die Erhebung eines Basiswertes darüber hinaus dazu führen, dass Veränderungen über die Jahre nachverfolgt werden können. Ebenfalls würden sie das Monitoring während der Umsetzungsphase erleichtern und die Belastbarkeit von erhobenen Zahlen stärken.

5.5.2 Umsetzungsprozess begleiten

Die für die Evaluation verantwortliche Stelle sollte in Übereinstimmung mit dem hierfür festgelegten Zeitplan den gesamten Lebenszyklus der Cybersicherheitsstrategie bewerten. Das Ergebnis (etwa in Form eines Evaluationsberichts) sollte Abweichungen vom Zeitplan und mögliche Gründe hierfür identifizieren. Dies sollte zusätzlich zu den Bewertungen einzelner Stakeholder, die für individuelle Prozesse und ihre Umsetzung verantwortlich sind, geschehen. Hierbei sollte sichergestellt werden, dass alle relevanten Stakeholder aktiv in das Monitoring sowie die Evaluation der Umsetzung der Strategie einbezogen werden.

Durch diesen Ansatz soll eine Verbindlichkeit mit Blick auf die Zielerreichung für alle beteiligten Stakeholder geschaffen werden. Darüber hinaus stellt dieses Vorgehen sicher, dass Umsetzungshindernisse frühzeitig erkannt und notwendige Anpassungen in den Rahmenbedingungen (etwa Ressourcen) oder der Ausrichtung (etwa definierten Zielen) vorgenommen werden können.

Umgesetzte Empfehlungen

Der vorliegende ausführliche Evaluationsbericht setzt zwei Untersuchungsschwerpunkte: Einerseits wird die methodische Herangehensweise an die Strategieerstellung und -umsetzung anhand des hierfür als geeignet identifizierten Lebenszyklusmodells kritisch bewertet. Obwohl die umfassenden theoretischen Grundlagen des NCS-Handbuchs bei der initialen Strategieerstellung keine Anwendung fanden und diese darüber hinaus Staaten auf nationaler Ebene adressieren, zeigt die vorliegende Evaluation, dass viele der formulierten Hinweise bereits bei der erstmaligen Strategieerstellung berücksichtigt wurden. Durch das Identifizieren von Abweichungen wurde es darüber hinaus möglich, kontextspezifische Empfehlungen für den Prozess der Strategiefortschreibung zu entwickeln, sodass im Ergebnis das methodische Vorgehen nicht nur transparent und kritisch bewertet wird, sondern auch stetig und unter Berücksichtigung der in der Freien Hansestadt Bremen existierenden Rahmenbedingungen professionalisiert wird. Andererseits wird in der vorliegenden Evaluation der Umsetzungserfolg einzelner Maßnahmen im Kontext vorab definierter Handlungsfelder geprüft (s. Kapitel 6).

Herausforderungen bei der Umsetzung

Für die Durchführung einzelner Maßnahmen wurde kein konkreter Zeitplan erstellt; ebenfalls wurden keine Verantwortlichkeiten benannt, die über die in der Geschäftsverteilung des Senats beschriebenen Zuständigkeiten beim Senator für Finanzen und Senator für Inneres und Sport hinausgehen. Die fehlende Möglichkeit, Mittel für die Umsetzung vieler Maßnahmen einzuwerben, erschwerte die Bewältigung zusätzlich und zeigt, wie kritisch ein mit personellen und finanziellen Ressourcen hinterlegter Umsetzungsplan für den Erfolg einer Cybersicherheitsstrategie ist.

Ausblick und Anregungen

Die Anregungen zur Implementationsphase sind auch hier anwendbar; insbesondere wird auf die Kapitel 5.4.1 und 5.4.4 verwiesen.

5.5.3 Zielerreichung überprüfen

Neben der Messung von bloßen Outputs in Form erbrachter Arbeitsleistungen ist es erforderlich, regelmäßig auch die Wirkung einer Maßnahme, den sogenannten Outcome, zu bewerten. Hierbei wird überprüft, ob Maßnahmen ihrem Zweck und ihrer Ausrichtung nach (noch) geeignet sind, zur Verwirklichung übergeordneter strategischer Ziele beizutragen. Dies wird insbesondere durch eine Re-Evaluation der spezifischen Risikolandschaft sowie einen Abgleich mit politischen Zielsetzungen und Prioritäten möglich.

Umgesetzte Empfehlungen

Die in Kapitel 6 durchgeführte Handlungsfeldbewertung betrachtet den Umsetzungserfolg einzelner Maßnahmen. Ebenfalls wurde bewertet, inwieweit diese geeignet sind, zu den in den Handlungsfeldern vorangestellten Zielvorstellungen beizutragen. Eine wissenschaftlich fundierte und umfängliche Bewertung des Wirkungszusammenhangs (Outcome) war im Rahmen der für die vorliegende Evaluation zur Verfügung stehenden Ressourcen jedoch nicht möglich.

Ein Abgleich mit politischen Zielsetzungen und Prioritäten wird im Rahmen der Fortschreibung der Bremischen Cybersicherheitsstrategie vorgenommen werden und einerseits durch die frühzeitige Einbindung aller Ressorts sowie des Magistrats der Stadt Bremerhaven über den bewährten Rahmen des AK Cybersicherheit gewährleistet und andererseits durch die Befassung des Senats zur Verabschiedung etwaiger erstellter Dokumente (der Fortschreibung der Cybersicherheitsstrategie sowie gegebenenfalls eines Umsetzungsplans) sichergestellt.

Herausforderungen bei der Umsetzung

Eine vollumfängliche Re-Evaluation der Risikolandschaft konnte im Rahmen des hier erstellten Evaluationsberichts nicht vorgenommen werden. Der mögliche Umfang und Detailgrad einer solchen Analyse steht in unmittelbarem Zusammenhang mit zeitlichen und personellen Ressourcen sowie der Entscheidung über die Art und den Umfang des Beteiligungsprozesses relevanter Stakeholder, der für die Fortschreibung der Strategie Anwendung finden soll.

Ausblick und Anregungen

Da insbesondere die (Neu-)Bewertung der Risikolandschaft eine Bewertung der Geeignetheit angestrebter Maßnahmen ermöglicht, sollte dieser bei der Fortschreibung der Strategie besondere Aufmerksamkeit zufallen. Es gelten insofern weiter die Hinweise und Empfehlungen zum Prozess der Sachstandserhebung und -analyse in Kapitel 5.2.

6. Betrachtung der einzelnen Handlungsfelder der Strategie

Im folgenden Kapitel werden die neun Handlungsfelder der Bremischen Cybersicherheitsstrategie differenziert betrachtet und bewertet. Zur besseren Übersicht folgt das Kapitel erneut einem einheitlichen Aufbau.

Zur Einführung in jedes Handlungsfeld wird in einem ersten Schritt zunächst die jeweilige Vision vorangestellt, welche im Rahmen der Strategieerstellung durch die ressortübergreifende Arbeitsgruppe Cybersicherheit gemeinsam formuliert wurde, um den Umfang und die Intention des jeweiligen Handlungsfeldes näher zu bestimmen.

Hieran anschließend werden im zweiten Schritt die Zielvorstellungen und Handlungserfordernisse beschrieben, welche sich aus der Vision und den in den jeweiligen Handlungsfeldern geschilderten Sachstandsbeschreibungen ergeben und im Rahmen einzelner Maßnahmen jeweils am Kapitelende der Strategie aufgelistet wurden.

In einem dritten Schritt erfolgt ein tabellarischer Abgleich für jede einzelne Maßnahme mit Blick auf den Umsetzungsstand und ihren Zielbeitrag:

Handlungserfordernis:
Beschreibung der Maßnahme lt. Bremischer Cybersicherheitsstrategie 2023
Überblick über die aktuelle Umsetzung:
Beschreibung des aktuellen Umsetzungsstands, ggf. Abschluss der Maßnahme
Perspektivische Umsetzung:
Beschreibung der perspektivischen Umsetzung, wenn noch nicht abgeschlossen
Ziel:
Beschreibung des Beitrags der individuellen Maßnahme
Übergeordneter Zielbeitrag:
Zuordnung des Zielbeitrags zu übergeordneten Zielvorstellungen

Zur Erhebung des Umsetzungsstandes wurde ein tabellarischer Erfassungsbogen, welcher jede Maßnahme im oben gezeigten Format beschreibt, an alle Ressorts sowie den Magistrat der Stadt Bremerhaven versandt. Die Rückmeldungen wurden gesammelt und zusammengefasst, um einen Gesamtüberblick über den aktuellen Umsetzungsstand der Strategie zu ermöglichen.

6.1 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.

6.1.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurden folgende konkretisierte Ziele abgeleitet:

- Z.1-1 Strategische Vernetzung
- Z.1-2 Enge Kooperation
- Z.1-3 Eindeutige Ansprechbarkeiten
- Z.1-4 Schneller und sicherer Informationsfluss
- Z.1-5 Regelmäßiger Austausch

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

1.1	Einrichtung einer Zentralstelle Cybersicherheit beim Senator für Inneres und Sport
1.2	Einrichtung der Position des Chief Cyber Security Officers (CCSO) zur Leitung der Zentralstelle Cybersicherheit
1.3	Steuerung cybersicherheitsrelevanter Informationen an ein definiertes Netzwerk staatlicher Akteur:innen
1.4	Einrichtung der Zentralstelle Cybersicherheit als SPoC beim BSI
1.5	Informationssteuerung zwischen Bund/anderen Ländern/eigener Länderebene
1.6	Aktive Einbindung in die Gremienarbeit
1.7	Zentrale Auswertung rechtlicher Rahmenbedingungen
1.8	Zentralstelle als Kompetenzknotenpunkt für Staat, Wirtschaft, Wissenschaft und gesellschaftliche Akteur:innen etablieren

6.1.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 1.1

Handlungserfordernis:
Einrichtung einer Zentralstelle Cybersicherheit beim Senator für Inneres und Sport
Überblick über die aktuelle Umsetzung:
Einrichtung zum 01.05.2023 ist erfolgt.

Perspektivische Umsetzung:
entfällt
Ziel:
Zentrale Verantwortlichkeit für die Cybersicherheit im Land Bremen an einer Stelle
Übergeordneter Zielbeitrag:
Z.1-3

Maßnahme Nummer 1.2

Handlungserfordernis:
Einrichtung der Position des Chief Cyber Security Officers (CCSO) zur Leitung der Zentralstelle Cybersicherheit
Überblick über die aktuelle Umsetzung:
Position ist eingerichtet und seit dem 01.01.2025 fest besetzt.
Perspektivische Umsetzung:
entfällt
Ziel:
Verantwortung für die Zentralstelle Cybersicherheit im Land Bremen
Übergeordneter Zielbeitrag:
Z.1-3

Maßnahme Nummer 1.3

Handlungserfordernis:
Steuerung cybersicherheitsrelevanter Informationen an ein definiertes Netzwerk staatlicher Akteur:innen innerhalb des Landes Bremen
Überblick über die aktuelle Umsetzung:
Relevante Informationen werden durch die Zentralstelle Cybersicherheit entweder über den AK Cybersicherheit insgesamt oder nach Einzelfallbewertung an ausgewählte staatliche Akteur:innen im Land Bremen gesteuert. Die Steuerung erfolgt bei Bedarf durch den Einsatz kryptographischer Verfahren.
Perspektivische Umsetzung:
Der Kreis grundsätzlich beteiligter staatlicher Akteur:innen wird fortwährend geprüft und im Bedarfsfall aktualisiert.
Ziel:
Schaffung eines einheitlichen Kenntnisstands und Vorgehens bzgl. der Cybersicherheit in allen Ressorts sowie beim Magistrat der Stadt Bremerhaven
Übergeordneter Zielbeitrag:
Z.1-1, Z.1-2, Z.1-4, Z.1-5

Maßnahme Nummer 1.4

Handlungserfordernis:
Einrichtung der Zentralstelle Cybersicherheit als SPoC beim BSI
Überblick über die aktuelle Umsetzung:

Die Zentralstelle Cybersicherheit ist als zentrale Kontaktstelle Land (ZKL) beim BSI gemeldet. Sie ist darüber hinaus die im Rahmen der Kooperationsvereinbarung zwischen dem BSI und dem Land Bremen benannte Ansprechstelle. Im Rahmen der Tätigkeiten als Zentrale Kontaktstelle Land nimmt die Zentralstelle Cybersicherheit die jährliche Übersichtsmeldung für einen durch das Gesetz anteilig bestimmten Kreis von im Land Bremen ansässigen kritischen Infrastrukturen (KRITIS) an. Hierfür wurden entsprechende Verschlüsselungsverfahren implementiert, um einen sicheren Empfang und eine sichere Verarbeitung zu ermöglichen.
Perspektivische Umsetzung:
entfällt
Ziel:
Zentralisierung des Informationsflusses vom / zum BSI sowie Absicherung des Informationsflusses durch authentifizierten und bei Bedarf verschlüsselten Austausch
Übergeordneter Zielbeitrag:
Z.1-1, Z.1-2, Z.1-3, Z.1-4

Maßnahme Nummer 1.5

Handlungserfordernis:
Informationssteuerung zwischen Bund/anderen Ländern/FHB
Überblick über die aktuelle Umsetzung:
Die Zentralstelle Cybersicherheit steuert relevante Informationen anderer staatlicher Akteur:innen (etwa aus der Gremienarbeit) entweder an das Netzwerk staatlicher Akteur:innen im Land Bremen (etwa über den AK Cybersicherheit) oder nach Einzelfallbewertung an einzelne staatliche Stellen. Darüber hinaus werden durch die Zentralstelle Cybersicherheit relevante und geeignete Informationen mit betroffenen staatlichen Stellen (etwa im Rahmen der Bund-Länder-Zusammenarbeit) geteilt.
Perspektivische Umsetzung:
Bei der Informationssteuerung handelt es sich um eine fortwährende Aufgabe. In diesem Rahmen werden Netzwerke kontinuierlich überprüft und ggf. angepasst.
Ziel:
Gewährleistung einer effizienten Informationssteuerung bei Belangen der Cybersicherheit in der Bund-Länder-Arbeit
Übergeordneter Zielbeitrag:
Z.1-1, Z.1-2, Z.1-4, Z.1-5

Maßnahme Nummer 1.6

Handlungserfordernis:
Aktive Einbindung in die Gremienarbeit
Überblick über die aktuelle Umsetzung:
Auf Landesebene hat die Zentralstelle Cybersicherheit die Geschäftsführung des AK Cybersicherheit inne. Es erfolgt darüber hinaus ein enger Austausch mit dem ITA und der AG ISM. Im Bund-Länder-Austausch vertritt die Zentralstelle Cybersicherheit das Land Bremen in der LAG Cybersicherheit und ist Mitglied des UP KRITIS. Es erfolgt darüber hinaus

ein Austausch mit den Sicherheitsverantwortlichen der Dataport Trägerländer und eine informatorische Beteiligung an der AG InfoSic.
Perspektivische Umsetzung:
Es erfolgt eine fortwährende Prüfung vorhandener Formate und Beteiligungsmöglichkeiten durch die Zentralstelle Cybersicherheit.
Ziel:
Durch die starke Vernetzung mit aktiven Akteur:innen der Cybersicherheitsarchitektur findet ein effizienter Austausch statt. Schnittstellen können erkannt und bearbeitet werden. Synergien können genutzt werden.
Übergeordneter Zielbeitrag:
Z.1-1, Z.1-2, Z.1-3, Z.1-5

Maßnahme Nummer 1.7

Handlungserfordernis:
Zentrale Auswertung rechtlicher Rahmenbedingungen
Überblick über die aktuelle Umsetzung:
Es wurde eine Referent:innenstelle für Cybersicherheitsrecht in der Zentralstelle Cybersicherheit eingerichtet und besetzt. Durch diese Stelle wurde die Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen erarbeitet. Ebenfalls erfolgt hier eine querschnittliche Befassung mit Rechtsfragen der Aufgabenfelder Katastrophenschutz, Kritische Infrastruktur und Zivile Verteidigung.
Perspektivische Umsetzung:
Bei der Auswertung und notwendigen Fortschreibung rechtlicher Rahmenbedingungen handelt es sich um eine fortwährende Aufgabe.
Ziel:
Fortwährende Auswertung der (inter)nationalen Entwicklung des Rechtsrahmens mit Bezug zur Cybersicherheit. Frühzeitiges Erkennen und Bewerten etwaiger Handlungserfordernisse. Kontinuierliche Weiterentwicklung des Cybersicherheits-Rechtsrahmens in der Freien Hansestadt Bremen.
Übergeordneter Zielbeitrag:
Z.1-1, Z.1-2, Z.1-5

Maßnahme Nummer 1.8

Handlungserfordernis:
Zentralstelle als Kompetenzknotenpunkt für Staat, Wirtschaft, Wissenschaft und gesellschaftliche Akteur:innen etablieren
Überblick über die aktuelle Umsetzung:
Die Zentralstelle Cybersicherheit baut kontinuierlich das bestehende Netzwerk durch bilaterale Kontakte sowie die Teilnahme an Fachforen und Fachkonferenzen mit Bezug zur IT- oder Cybersicherheit aus.
Perspektivische Umsetzung:
Perspektivisch soll die Teilnahme an Fortbildungen und Fachveranstaltungen sowie die Zusammenarbeit mit weiteren Akteur:innen in Cybersicherheitsarbeit intensiviert werden, um Kompetenzen der Zentralstelle Cybersicherheit stetig zu erweitern.
Ziel:

Die Zentralstelle Cybersicherheit ist in der Freien Hansestadt Bremen als Kompetenzknotenpunkt bekannt.
Übergeordneter Zielbeitrag:
Z.1-1, Z.1-2, Z.1-5

6.2 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.

6.2.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurden folgende konkretisierte Ziele abgeleitet:

- Z.2-1 Absicherung der Handlungsfähigkeit staatlicher Verwaltung durch eine resiliente technische Infrastruktur
- Z.2-2 Stärkung der Fähigkeit zur Krisenbewältigung der staatlichen Verwaltung
- Z.2-3 Kompetenzaufbau im staatlichen Notfall- und Krisenmanagement

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

2.1	Aufbau grundschutzkonformer ISMS
2.2	Beratungsleistungen zu bestehenden Strukturen zur vor-Ort-Unterstützung
2.3	Ausbau der bestehenden Strukturen und Kompetenzen im Bereich der IT-Sicherheit
2.4	Steuerung von IoC-Listen
2.5	Anbindung an oder Aufbau einer MISP („Malware Information Sharing Platform“)
2.6	Aufbau eines Kompetenznetzwerks zur Abwehr von IT-Angriffen
2.7	Zentralisierung und Ausbau bestehender Arbeitsstrukturen für das IT-Notfallmanagement
2.8	Beratung zu IT-Notfallübungen
2.9	Beratung zur Notfall- und Krisenkommunikation
2.10	Aufbau Fachkräftepool zur IT-Notfallbewältigung (vgl. auch Maßnahme 2.6)
2.11	Ausbau der Kooperation zwischen Polizei, Staatsanwaltschaft und Zentralstelle für Cybersicherheit

6.2.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 2.1

Handlungserfordernis:
Aufbau grundschutzkonformer ISMS
Überblick über die aktuelle Umsetzung:

Der Aufbau und Reifegrad entsprechender ISMS innerhalb der Ressorts ist unterschiedlich stark vorangeschritten. In einigen Ressorts wurden bereits erste organisatorische Vorkehrungen für die Einrichtung eines ISMS vorgenommen. Ebenfalls wurden zum Teil bereits die für ein ISMS erforderlichen Dokumente erstellt (etwa eine interne Informationssicherheitsleitlinie, Dienstanweisung zum Umgang mit Informationssicherheitsvorfällen, IT-Notfallkonzept, Kommunikationsplan). Hierbei erfolgt überwiegend eine Orientierung am IT-Grundschutz-Standard zum Aufbau eines ISMS. In einem Fall ist der Aufbau eines grundschutzkonformen ISMS bereits abgeschlossen. Die zentral durch Dataport verwalteten Anwendungen werden in einem IT-grundschutzkonformen Rechenzentrum betrieben. Dort, wo Organisationen der FHB selbst als Betreiber verantwortlich sind, ist ein grundschutzkonformer Betrieb überwiegend noch nicht gegeben. In Bremerhaven wurde durch den BIT im Jahr 2023 ein zentrales grundschutzkonformes ISMS nach CISIS12-Standard kommunal etabliert.
Perspektivische Umsetzung:
Die Implementation und sukzessive Ausweitung grundschutzkonformer ISMS sowie die Erhöhung des Reifegrades vorhandener ISMS wird stetig weiterverfolgt. Hierzu zählen auch organisatorische Vorbereitungen zur Verortung der Verantwortlichkeiten für ISB / IT-SiBe in den Ressorts. In Bereichen, die zur kritischen Infrastruktur zählen, wird zuerst eine Einführung von ISMS vorgenommen, bevor dann sukzessive die übrigen Geschäftsbereiche und -prozesse in den Umfang des ISMS mit einbezogen werden. In Bereichen, die bereits ein ISMS implementiert haben, sind Wirksamkeitsprüfungen (etwa interne Audits) vorgesehen, auch werden Zertifizierungen erwogen. Perspektivisch kann ebenfalls geprüft werden, ob eine stärkere zentrale Bereitstellung von Anwendungen für alle Organisationen in der FHB zur Erhöhung der Grundschutzkonformität in allen Bereichen beitragen kann. In Bremerhaven wird eine Re-Zertifizierung und Weiterentwicklung des ISMS nach ISO 27001 angestrebt. Ebenfalls ist eine Ausweitung auf die Stadtverwaltung vorgesehen.
Ziel:
Steigerung der IT-Sicherheit der Verwaltung durch Etablierung ganzheitlicher, systematischer und standardisierter Informationssicherheitsprozesse zur dauerhaften Gewährleistung der IT Grundschutz-Schutzziele.
Übergeordneter Zielbeitrag:
Z.2-1, Z.2-2

Maßnahme Nummer 2.2

Handlungserfordernis:
Beratungsleistungen zu bestehenden Strukturen zur vor-Ort-Unterstützung
Überblick über die aktuelle Umsetzung:
Die Zentralstelle Cybersicherheit steht den Ressorts sowie dem Magistrat der Stadt Bremerhaven bei allen organisatorischen und koordinierenden Fragen der Cybersicherheit zur Verfügung. Ebenfalls besteht ein enger Kontakt zum Bundesamt für Sicherheit in der Informationstechnik. Teilweise erfolgt eine proaktive Sondierung des Marktes für IT-Forensik-Dienstleistungen.

In einigen Bereichen werden bereits Audits durchgeführt.
Perspektivische Umsetzung:
Zur strukturellen Stärkung der Vor-Ort-Unterstützung ist ein weiterer Kompetenzaufbau in den jeweiligen Dienststellen erforderlich. Gleichzeitig sollen Melde- und Eskalationswege sowie Prozesse zur Vorfallsbewältigung festgelegt werden, um die Reaktionsfähigkeit bei Vorfällen zu erhöhen. Ein koordinierter regelmäßiger Erfahrungsaustausch kann zusätzliche Synergien schaffen und die Kenntnis über bestehende Angebote und Strukturen weiter steigern. Darüber hinaus wären Audits in allen Organisationen des Landesnetzes erstrebenswert, ggf. auch in Bremerhaven. Informationen zu vorhandenen Angeboten/Serviceleistungen sind zentral abrufbar.
Ziel:
Strukturen zur Vorfallsbewältigung sind bekannt und die organisationsinternen Prozesse auf diese abgestimmt, um im Bedarfsfall Beratungs- und Unterstützungsleistung zeitnah abrufen zu können und so im Rahmen eines umfangreichen IT-Sicherheitsvorfalls schneller Hilfe zu erhalten.
Übergeordneter Zielbeitrag:
Z.2-1, Z.2-2, Z.2-3

Maßnahme Nummer 2.3

Handlungserfordernis:
Ausbau der bestehenden Strukturen und Kompetenzen im Bereich der IT-Sicherheit
Überblick über die aktuelle Umsetzung:
Es existieren Angebote zur Aus- und Fortbildung von IT-Sicherheitsbeauftragten sowie Sensibilisierungskampagnen. Die Ressorts verfügen über Informationssicherheitsbeauftragte (ISB), welche die IT-Sicherheitsaufgaben koordinieren. Ein Austausch findet teilweise in den Ressorts, darüber hinaus ressortübergreifend im Rahmen der AG ISM statt. Des Weiteren erfolgt eine Anbindung an das CERT Nord zum Informationsaustausch, beispielsweise im Rahmen des Warn- und Informationsdienstes (WID) sowie der Meldung von Sicherheitsvorfällen. Eine wichtige Aufgabe besteht darin, die Funktion und Rolle der ISB im Ressort klar zu kommunizieren, damit diese ihren koordinierenden Tätigkeiten nachkommen können. Der Umfang der Aufgabenbewältigung ist hierbei von den verfügbaren personellen Ressourcen abhängig. Teilweise werden Schulungen zum bzw. zur IT-Grundschutzpraktiker:in durchgeführt, darüber hinaus findet eine fortwährende Sensibilisierung von Mitarbeiter:inne statt. Neben personellen und strukturellen Verbesserungen werden teilweise technische Maßnahmen durchgeführt, etwa die Beschaffung zusätzlicher Sicherheitswerkzeuge (z. B. Netzwerk-Monitoring). Die Stadt Bremerhaven hat für den Ausbau des bestehenden ISMS zwei zusätzliche Stellen für Informationssicherheitsbeauftragte geschaffen. Zusätzlich wurde ein Team für IT-Sicherheit geformt, das unter anderen auch internes Schwachstellenmanagement durchführt. Alle IT-Richtlinien wurden Anfang 2025 überarbeitet und neu veröffentlicht.
Perspektivische Umsetzung:

Eine Steuerung der Aus- und Fortbildung durch das zentrale Personalbüro für alle Beschäftigten könnte Synergien nutzbar machen und Standards etablieren. Perspektivisch müssen die personellen und organisatorischen Ressourcen in allen Ressorts sowie beim Magistrat der Stadt Bremerhaven ausgebaut werden, um Kompetenzen im Bereich der IT-Sicherheit fortwährend zu stärken. Darüber hinaus soll die Infrastruktur zur Detektion und Abwehr von Cyberbedrohungen und etwaigen Angriffen in allen Bereichen ausgebaut werden, um Angriffe schneller erkennen und abwehren zu können. Dies geht mit einer fortwährenden Steigerung des Geltungsbereichs sowie Reifegrads existierender ISMS einher. Die Integration von Sicherheitsprozessen in den Arbeitsalltag kann darüber hinaus dafür sorgen, Kommunikationswege und Bewältigungsprozesse einzuüben, damit diese bei Bedarf gut funktionieren. Durch einen engen Austausch mit der Zentralstelle Cybersicherheit sowie anderen Behörden sollen der Kompetenzzuwachs beschleunigt und Doppelarbeit vermieden werden.
Ziel:
Erweiterung des bestehenden Angebots bzgl. der IT-Sicherheit sowie der Cybersicherheit sowie Monitoring des Stands der Ausbildung inkl. Prüfung der Verbindlichkeit von Schulungsmaßnahmen, mehrfache Anbindung vorhandener Fachkompetenzen und Bündelung von Fachwissen zur besseren Nutzbarmachung vorhandenen Potenzials, um klare Verantwortlichkeiten und effektive Sicherheitsprozesse zu ermöglichen. Langfristig soll der Reifegrad vorhandener ISMS stetig erhöht werden, sodass die Resilienz der IT-Sicherheitsorganisation in allen betroffenen Bereichen gesteigert wird.
Übergeordneter Zielbeitrag:
Z.2-1, Z.2-2, Z.2-3

Maßnahme Nummer 2.4

Handlungserfordernis:
Steuerung von IoC-Listen
Überblick über die aktuelle Umsetzung:
Indicators of Compromise (IoC) werden zurzeit z. B. über den Verwaltungs-CERT-Verbund (VCV) an einen vorab definierten Empfängerkreis versendet. Zudem können IoC-Listen aus weiteren, öffentlichen Quellen bezogen werden. Diese werden für durch die durch Dataport zentral verwaltete IT durch das Security Operations Center (SOC) bei Dataport eingespielt. So können z. B. Schadsoftware und maliziöse Anfragen automatisiert gesperrt werden. Ebenso werden, sofern erforderlich, bei Bereichen, die eigene IT betreiben, die entsprechenden IoC selbst eingespielt.
Perspektivische Umsetzung:
Im Rahmen der stetigen Weiterentwicklung der Angriffserkennungs- und Abwehrsysteme sollen, neben bestehenden Informationsquellen, auch neue Informationsquellen identifiziert und in die Systeme implementiert werden.
Ziel:
Stärkung der Threat Intelligence zur schnelleren Erkennung und verbesserten Abwehr nicht berechtigter Zugriffe und in der Folge Stärkung der Resilienz der IT-Systeme. Verbesserung der Reaktionszeiten durch automatisierte Verarbeitung in den entsprechenden Hard- und Softwaresystemen.
Übergeordneter Zielbeitrag:

Z. 2-1, Z.2-2

Maßnahme Nummer 2.5

Handlungserfordernis:
Anbindung an oder Aufbau einer MISP („Malware Information Sharing Platform“)
Überblick über die aktuelle Umsetzung:
Dataport als zentraler IT-Dienstleister betreibt eine eigene MISP. Die dort generierten Informationen finden Einfluss in die Angriffserkennungs- und Abwehrsysteme der zentral verwalteten IT.
Perspektivische Umsetzung:
Im Rahmen der Umsetzung der NIS-2-Richtlinie in Bundesrecht wird die Möglichkeit der Anbindung der IT-Dienstleister der Länder an eine zentral durch das BSI betriebene MISP geprüft.
Ziel:
Ausbau der Informationsgewinnung im Zusammenhang mit Malware sowie verlässliche und automatisierte Steuerung von Erkenntnissen über Schadsoftware an die an der MISP teilnehmenden Akteur:innen. Verbesserung der Geschwindigkeit bei der Detektion und Abwehr von Schadsoftware für die Landesnetze der Freien Hansestadt Bremen.
Übergeordneter Zielbeitrag:
Z.2-1, Z.2-2, Z.2-3

Maßnahme Nummer 2.6

Handlungserfordernis:
Aufbau eines Kompetenznetzwerks zur Abwehr von IT-Angriffen
Überblick über die aktuelle Umsetzung:
Der Aufbau des Kompetenznetzwerks zur Abwehr von IT-Angriffen findet sowohl auf Ebene einzelner Organisationen als auch organisationsübergreifend sowie in Zusammenarbeit mit Dritten statt. Kontakte zwischen der Zentralstelle Cybersicherheit, der Arbeitsgruppe ISM sowie den Sicherheitsbeauftragten der Ressorts werden kontinuierlich gepflegt und gestärkt, um einen grundsätzlichen sowie situativen niedrigschwelligen Austausch zu ermöglichen. In Bremerhaven findet ein halbjährlicher Austausch zur IT-Sicherheit mit den Fachadministrator: innen der jeweiligen Organisationseinheiten des Magistrats statt.
Perspektivische Umsetzung:
Die bestehenden operativen Kompetenzen zur Abwehr von IT-Angriffen sollen weiter ausgebaut werden, ggf. durch Einbindung spezialisierter Unternehmen. Verantwortlichkeiten und Ansprechbarkeiten sollen, sofern noch nicht erfolgt, festgelegt und bekannt gemacht werden; Kommunikationsprozesse, die bei der Abwehr von IT-Angriffen zum Tragen kommen, müssen definiert werden, um von allen Beteiligten im Ernstfall routiniert genutzt werden zu können. Austauschmöglichkeiten aller betroffenen Akteur:innen untereinander sollen sowohl in der intra- als auch inter-organisationalen Zusammenarbeit systematisch gestärkt werden.
Ziel:

Befähigung zu einer fachkundigen und schnellen Reaktion auf IT-Angriffe auf die Verwaltung in der Freien Hansestadt Bremen durch ein bremisches Kompetenznetzwerk.
Übergeordneter Zielbeitrag:
Z.2-1, Z.2-2, Z.2-3

Maßnahme Nummer 2.7

Handlungserfordernis:
Zentralisierung und Ausbau bestehender Arbeitsstrukturen für das IT-Notfallmanagement
Überblick über die aktuelle Umsetzung:
Der Umsetzungsstand im IT-Notfallmanagement ist heterogen und in weiten Teilen der FHB noch nicht umgesetzt. Einige Ressorts bzw. zugeordnete Dienststellen haben bereits ein IT-Notfallmanagement mit unterschiedlichem Umsetzungsstand realisiert, etwa durch die Erstellung von Notfallhandbüchern oder Notfallplänen im Rahmen der Notfallvorsorge. Teilweise wurden interne Ablaufpläne erstellt und Kommunikationsprozesse festgelegt. In Bremerhaven wurde für das Verwaltungsnetz im Rahmen des Aufbaus eines ISMS ein Notfallmanagement eingerichtet sowie ein Notfallhandbuch erstellt.
Perspektivische Umsetzung:
Ausbau und kontinuierliche Verbesserung des IT-Notfallmanagements unter Berücksichtigung der Schnittstellen zu Geheimschutzmaßnahmen sowie perspektivisch die Überprüfung und Stärkung der Notfallmanagement-Strukturen, beispielsweise durch zentral koordinierte Notfallmanagement-Runden oder landesweite Krisenstab-Übungen für Cybersicherheitsvorfälle.
Ziel:
Erzeugung von Synergieeffekten lokaler und zentraler Kompetenzen des Notfallmanagements sowie Bündelung von Ressourcen, um einen einheitlichen Notfallmanagement-Standard in allen Bereichen der Verwaltung der Freien Hansestadt Bremen zu schaffen. Ein besonderes Augenmerk sollte hierbei auf der Wiederherstellung / Sicherung der Handlungsfähigkeit, der Schadensminimierung sowie dem Schutz der Mitarbeiter:innen liegen.
Übergeordneter Zielbeitrag:
Z.2-2, Z.2-3

Maßnahme Nummer 2.8

Handlungserfordernis:
Beratung zu IT-Notfallübungen
Überblick über die aktuelle Umsetzung:
Beratungen zu IT-Notfallübungen haben in der Stadt Bremen bisher nicht flächendeckend stattgefunden. Vereinzelt wurden in begrenztem Umfang Übungen durchgeführt, etwa Wiederherstellungsübungen für Backups oder simulierte Teilausfälle einzelner Fachverfahren.

In Bremerhaven finden jährlich Beratungen zu IT-Notfällen sowie zur Notfall- und Krisenkommunikation im Rahmen des jährlichen internen Audits statt, die von externer Stelle bereitgestellt werden.
Perspektivische Umsetzung:
Durchführung von Planbesprechungen, Stabsübungen, technischen Tests, Simulationen oder Vollübungen in der FHB sowie im Verbund der Dataport Trägerländer. Beratung ggf. durch das BSI im Rahmen des geschlossenen Kooperationsvertrags. In einzelnen Bereichen gibt es bereits Planungen zu Notfallübungen.
Ziel:
Stärkung der digitalen Resilienz der Verwaltung der Freien Hansestadt Bremen durch Übungserfahrung, die Kenntnis von Abläufen und Zusammenarbeit zwischen den einzelnen Akteur:innen, sowie die Ableitung von Verbesserungspotenzial durch bei den Übungen festgestellten Schwachstellen; Prüfung und Steigerung der Wirksamkeit von Notfall- und Reaktionsplänen zur Identifikation und Behebung von Schwachstellen und Stärkung der im Ernstfall erforderlichen Routinen bei allen Beteiligten.
Übergeordneter Zielbeitrag:
Z.2-1, Z.2-2, Z.2-3

Maßnahme Nummer 2.9

Handlungserfordernis:
Beratung zur Notfall- und Krisenkommunikation
Überblick über die aktuelle Umsetzung:
Zur Notfall- und Krisenkommunikation wird in den Ressorts auf die bestehenden Kommunikationsstrukturen zurückgegriffen. Teilweise gibt es erste Regelungen zu einer Notfall- und Krisenkommunikation. Darüber hinaus wurden erste Vorbereitungen zur VS-Kommunikation getroffen, um bei Bedarf eine sichere Kommunikation zu ermöglichen. In Bremerhaven finden extern bereitgestellte Beratungen zu IT-Notfällen sowie zur Notfall- und Krisenkommunikation im Rahmen des jährlichen internen Audits statt.
Perspektivische Umsetzung:
Die Notfall- und Krisenkommunikation sollte in allen Bereichen durch Konzepte zur Krisenkommunikation geregelt sein. Eine ressort- und behördenübergreifende Abstimmung und Vereinheitlichung der Kommunikationsstrukturen im Not- und Krisenfall trägt zur Harmonisierung und Funktionalität dieser Strukturen bei. Die technischen Voraussetzungen für eine sichere Kommunikation, erforderlichenfalls auch eine Geheimschutzkommunikation, müssen weiterentwickelt und für alle an der Notfall- und Krisenkommunikation beteiligten Akteur:innen verfügbar sein. In Bremerhaven werden perspektivisch Übungen zu IT-Notfällen sowie im weiteren auch Krisenübungen stattfinden. In diesem Zusammenhang soll auch die bestehende Notfall- und Krisenkommunikation überprüft werden.
Ziel:
Überprüfung und bei Bedarf Verbesserung der Notfall- und Krisenkommunikation sowie Ermöglichung einer Geheimschutzkommunikation. Steigerung des Vertrauens und der Kompetenz aller am Prozess Beteiligten durch das Beüben relevanter Abläufe.

Übergeordneter Zielbeitrag:
Z.2-2, Z.2-3

Maßnahme Nummer 2.10

Handlungserfordernis:
Aufbau Fachkräftepool zur IT-Notfallbewältigung
Überblick über die aktuelle Umsetzung:
In den Ressorts wird für die IT-Notfallbewältigung zurzeit auf die bereits eingerichteten Stellen (ISB, IT-Stellen) zurückgegriffen. Eine Erweiterung hat hier nicht stattgefunden. In Bremerhaven wird im Rahmen der IT-Notfallbewältigung auf den bestehenden Fachkräftepool zurückgegriffen werden, welcher durch den BIT sichergestellt wird.
Perspektivische Umsetzung:
Erstellung und Pflege eines „Fähigkeitenkatasters“ der in der Verwaltung der Freien Hansestadt tätigen Fachkräfte, um Synergien nutzbar zu machen. Eine Ausweitung des vorhandenen Fachkräftepools zur IT-Notfallbewältigung ist anzustreben.
Ziel:
Vernetzung bereits vorhandener Fachkräfte, Ausbildung neuer Fachkräfte und Schaffung eines Überblicks über vorhandene Expertisen, um die eigene Resilienz zu steigern und im Notfall zeitnah auf die Expertise der Fachkräfte zurückgreifen zu können.
Übergeordneter Zielbeitrag:
Z.2-1, Z.2-3

Maßnahme Nummer 2.11

Handlungserfordernis:
Ausbau der Kooperation zwischen Polizei, Staatsanwaltschaft und Zentralstelle für Cybersicherheit
Überblick über die aktuelle Umsetzung:
Kommunikationsebenen zur Polizei und zum Landesamt für Verfassungsschutz bestehen seit Längerem. Ebenfalls besteht eine Kooperation zwischen Polizei, Staatsanwaltschaft und ZAC, die kontinuierlich gepflegt wird.
Perspektivische Umsetzung:
Etablierung eines Formats für eine institutionalisierte Zusammenarbeit.
Ziel:
Intensivierung des Austauschs gewonnener Erkenntnisse, um ein ganzheitliches Lagebild bzgl. der Cybersicherheit in der Freien Hansestadt Bremen erstellen zu können sowie etwaig aufkommende Trends und Vorgehensweisen im Rahmen rechtskonformer und intensivierter Zusammenarbeit frühzeitig zu erkennen.
Übergeordneter Zielbeitrag:
Z. 2-2, Z.2-3

6.3 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.

6.3.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurden folgende konkretisierte Ziele abgeleitet:

- Z.3-1 Absicherung der Handlungsfähigkeit von Gefahrenabwehr-, Strafverfolgungs- und Verfassungsschutzbehörden im Phänomenbereich Cybersicherheit
- Z.3-2 Stärkung digitaler Fachkompetenzen im Bereich der Bekämpfung von Cybercrime und Sicherstellung einer effektiven Cyberabwehr

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

3.1	Einführung grundschutzkonformer ISMS in Leitstellen von Polizeien und Feuerwehren
3.2	Auf- und Ausbau von IT-Notfallvorsorgekonzepten
3.3	Flächendeckende Umsetzung größtmöglicher IT-Sicherheitsstandards in o. g. Behörden
3.4	Etablierung von IT-Notfallmanagementkonzepten (auch BCM)
3.5	Betreuung und Beratung der betroffenen Behörden
3.6	Identifikation und Vernetzung in der Prävention von Cyberkriminalität tätiger Akteur:innen
3.7	Identifikation und Bewertung der bestehenden Schulungsangebote für Mitarbeiter:innen in den staatlichen Einrichtungen in Bezug auf die Prävention von Cyberkriminalität
3.8	Vereinheitlichung und Ausbau der Schulungsangebote
3.9	Bewertung der personellen und technischen Kapazitäten LfV zur Cyberabwehr.
3.10	Bewertung der personellen und technischen Kapazitäten der Strafverfolgungsbehörden zur effektiven Kriminalitätsbekämpfung im Bereich der Cybersicherheit

6.3.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 3.1

Handlungserfordernis:
Einführung grundschutzkonformer ISMS in Leitstellen von Polizeien und Feuerwehren

Überblick über die aktuelle Umsetzung:

Bei der Polizei Bremen wird ein neues modernes Sprachvermittlungssystem für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) ab August 2025 parallel zum bestehenden Sprachvermittlungssystem aufgebaut und eine Testumgebung zum bestehenden Einsatzleitrechner (ELR) über eine neue IFC-Schnittstelle hergestellt. Im September wurde das neue Sprachvermittlungssystem in einer Testumgebung einem ersten Leistungs- und Funktionstest mit 29 angebundenen Client-PC in der Leitstelle, dem Zentralruf und KDD unterzogen. Dazu erfolgen auch entsprechende Schulungen/Einweisungen zum System.

Bei der Ortspolizeibehörde Bremerhaven ist die Leitstelle Bestandteil der IT-Sicherheits-, Datenschutz- und Geheimschutzbetrachtung. BSI-Bausteine im Umfeld der Leitstelle werden sukzessive umgesetzt.

Bei der Feuerwehr Bremen sind bewährte Sicherheitsmechanismen vorhanden.

In Bremerhaven hat sich die Integrierte Regionalleitstelle Unterweser-Elbe (IRLS) aufgrund ihrer Zuständigkeit nicht nur für Bremerhaven, sondern auch für die beiden niedersächsischen Landkreise Cuxhaven und Osterholz, von der zentralen IT-Sicherheitsrichtlinie des Magistrats abgekoppelt. Daher muss die IRLS ein eigenes ISMS auf Basis des BSI-Grundschutzes erstellen und implementieren. Diese Maßnahme ist bisher noch nicht abschließend erfolgt.

Perspektivische Umsetzung:

Grundsätzlich wird der Ausbau von ISMS in den betroffenen Bereichen im Rahmen des PDCA-Zyklus regelmäßig überprüft und fortgeführt.

In der Polizei Bremen soll im November 2025 das neue modulare Sprachvermittlungssystem aus dem Testbetrieb in den vollständigen Echtbetrieb im Zusammenspiel mit dem ELR überführt werden. Das alte Sprachvermittlungssystem wird danach abgeschaltet und zurückgebaut. Aus diesem Grund ist es aktuell nicht zielführend, das „Grundschutzprofil Leitstelle“ an den genannten zentralen Komponenten FNA und ELR zu prüfen bzw. durchzuführen. Die weitere und eingehende Überprüfung des „Grundschutzprofils Leitstelle“ mit dem ELR kann nach der Überleitung in den Echtbetrieb und den technischen Administrator-Schulungen perspektivisch ab 2026 begonnen werden.

Bei der Feuerwehr Bremen werden mit der Einführung neuer Technik mögliche Schwachstellen analysiert und im laufenden Projekt des neuen Kommunikationsmanagementsystems (KMS) mit allen Projektbeteiligten bewertet und umgesetzt.

In Bremerhaven ist die Erstellung eines ISMS für die IRLS in Vorbereitung. Eine externe Unterstützung wird hierbei angestrebt. Erste Gespräche mit einem externen Unternehmen sind initiiert worden. Eine Umsetzung soll kurzfristig erfolgen.

Die Ortspolizeibehörde Bremerhaven strebt, in Abhängigkeit der personellen und finanziellen Rahmenbedingungen, eine kontinuierliche Erweiterung der Maßnahmen an.

Ziel:

Steigerung der IT-Sicherheit in den Leitstellen der benannten Behörden durch die Schaffung eigenständiger, grundschutzkonformer ISMS sowie durch die kontinuierliche Erhöhung des Reifegrads.
Übergeordneter Zielbeitrag:
Z.3-1

Maßnahme Nummer 3.2

Handlungserfordernis:
Auf- und Ausbau von IT-Notfallvorsorgekonzepten
Überblick über die aktuelle Umsetzung:
Bei der Senatorin für Justiz und Verfassung liegt ein grundlegendes IT-Notfallvorsorgekonzept vor. Bei der Polizei Bremen liegt ein vollständiges IT-Notfallvorsorgekonzept noch nicht vor. Bisher wurden vor allem die Kernpunkte „Präventive Maßnahmen“ (etwa Notstromversorgung, AntiVirus und Malware-Scanner sowie die Einhaltung der BSI-Vorgaben zur IT-Sicherheit, beispielsweise P-A-P-Strukturen zum Schutz von VS-NfD Netzwerken im Bereich der Sicherheitsgateways), sowie weitere Notfallpläne umgesetzt. Bei der Feuerwehr Bremen bestehen Notfallkonzepte zur Rücksicherung von ggf. betroffenen Datenbeständen und es können ad-hoc Netzwerke, wie z. B. beim Einrichten mobiler Führungsstellen, genutzt werden Für die IRLS liegt noch kein IT-Notfallvorsorgekonzept vor. Es wurde damit begonnen, relevante Maßnahmen zu dokumentieren. Bei der OPB Bremerhaven wurde die Notwendigkeit für den Auf- und Ausbau von IT-Notfallvorsorgekonzepten erkannt und akzeptiert.
Perspektivische Umsetzung:
Grundsätzlich sollen IT-Notfallvorsorgekonzepte in den o. g. Behörden implementiert bzw. überprüft und bei Bedarf weiterentwickelt werden. Bei der Feuerwehr Bremen können mobile Führungsstellen für diese Zwecke entsprechend mit zusätzlichem Material ausgerüstet werden. In Bremerhaven ist im Rahmen des Aufbaus eines ISMS für die IRLS auch geplant, ein Notfallkonzept (inkl. Ausfall- und Wiederanlaufplänen) in Anlehnung an den BSI Standard 200-4 zu erstellen.
Ziel:
Steigerung der Resilienz der Behörden in Bezug auf die Auswirkungen von IT-Ausfällen durch die fortlaufende Einführung und Anpassung von ISMS sowie der damit verbundenen Steigerung des Reifegrads der ISMS.
Übergeordneter Zielbeitrag:
Z.3-1, Z.3-2

Maßnahme Nummer 3.3

Handlungserfordernis:
Flächendeckende Umsetzung größtmöglicher IT-Sicherheitsstandards in o. g. Behörden
Überblick über die aktuelle Umsetzung:
Bei der Senatorin für Justiz und Verfassung wurden die meisten Standards, vorwiegend über Dataport, umgesetzt. Bei der Polizei Bremen wurde im Jahr 2020 das Regelwerk Informationssicherheit, welches aus mehreren Richtlinien besteht, in Kraft gesetzt. Daraus resultiert die Einrichtung eines operativen Informationssicherheitsmanagements, welches aktuell mit drei Stellen ausgestattet ist. Basis für die Arbeit des ISM der Polizei ist der BSI Grundschutz mit der Ergänzung durch das IT-Grundschutzprofil „Polizei“. Bei der Feuerwehr Bremen sind entsprechende Sicherheitsrichtlinien vorhanden. In Bremerhaven sind für die IRLS bereits erste IT-Sicherheitsstandards umgesetzt. Die Ortspolizeibehörde Bremerhaven hat mit dem Stabsbereich 2 einen technischen Bereich, der sich im gesamten Systemzyklus mit den Herausforderungen größtmöglicher IT-Sicherheit beschäftigt und unter den gegebenen personellen und finanziellen Rahmenbedingungen berücksichtigt. Zurzeit gibt es einen IT-Sicherheitsbeauftragten, der sich mit einem Volumen von 0,3 VZE dem Themenkomplex der IT-Sicherheit widmet. Das Landesamt für Verfassungsschutz Bremen betreibt zum eigenen Schutz besonders gesicherte Netze, die den entsprechenden Schutzanforderungen der Verschlusssachenanweisung des Bundes und des BSI entsprechen. Der Schutz dieser Netze umfasst hierbei diverse technische, organisatorische und personelle Maßnahmen.
Perspektivische Umsetzung:
Grundsätzlich sollen die nach dem jeweils aktuellen Stand der Technik gültigen IT-Sicherheitsstandards auf allen Ebenen umgesetzt und Regelungen zur Cyberhygiene eingeführt und eingehalten werden. Die Umsetzung besonderer Aufgaben, etwa des Risikomanagements oder Business Continuity Managements (BCM), steht in unmittelbarem Zusammenhang mit den hierfür vorgesehenen oder verfügbaren Personalressourcen. In der Polizei Bremen ist eine Überprüfung der Richtlinie Informationssicherheitsmanagement im Hinblick auf aktuelle Anforderungen vorgesehen, um ggf. neuen Anforderungen Rechnung tragen zu können. In der Feuerwehr Bremen erfolgt ein fortwährendes Monitoring von Anforderungen, die bei Bedarf laufend in bereits vorhandene Richtlinien integriert werden. In Bremerhaven werden für die IRLS im Rahmen der ISMS-Erstellung geltende Standards berücksichtigt. Es ist geplant, die bisherigen bestehenden Sicherheitsstandards

im nächsten Schritt auszubauen, um einen systematisch und übergreifend Ansatz umzusetzen. Die Priorität liegt hierbei auf der Systemhärtung und Zugangskontrolle. In der Ortspolizeibehörde Bremerhaven ist eine Erweiterung der Maßnahmen in Abhängigkeit von den personellen und finanziellen Ressourcen vorgesehen.
Ziel:
Absicherung der IT und der hierauf verarbeiteten Daten gegen Verlust und unbefugten Zugriff sowie die Steigerung der Resilienz gegen IT-Angriffe.
Übergeordneter Zielbeitrag:
Z.3-1

Maßnahme Nummer 3.4

Handlungserfordernis:
Etablierung von IT-Notfallmanagementkonzepten (auch BCM)
Überblick über die aktuelle Umsetzung:
Bei der Senatorin für Justiz und Verfassung ist ein übergreifendes IT-Notfallkonzept vorhanden. Bei der Polizei Bremen bezieht sich das Notfallmanagement aktuell auf die Wiederherstellung des IT-Betriebs im Rahmen des vorhandenen Wiederanlaufplans. Bei der Feuerwehr Bremen befinden sich entsprechende Konzepte in der Entwicklung. In Bremerhaven ist für die IRLS oder die Ortspolizeibehörde derzeit noch kein adäquates IT-Notfallmanagement oder BCM implementiert.
Perspektivische Umsetzung:
Einführung eines BCM in Verbindung mit einem ISMS in den o. g. Behörden. Bei der Senatorin für Justiz und Verfassung ist die Erstellung von Einzelkonzepten für Verfahren geplant. In der Polizei Bremen werden aufgrund der bereits bestehenden Verpflichtungen und Aufgaben Einzelmaßnahmen umgesetzt. Die Planung zur Etablierung eines übergreifenden BCM befindet sich aktuell in der weiteren Abstimmung. In Bremerhaven ist für die IRLS die Einführung eines abgestuften BCM-Konzepts als mittelfristige Maßnahme im Rahmen des ISMS geplant. Auch die Ortspolizeibehörde Bremerhaven plant kurz- bis mittelfristig initiale Maßnahmen im Rahmen von Ausbildung und Qualifikationsaufbau.
Ziel:
Steigerung der Resilienz für den Fall des Ausfalls kritischer Geschäftsprozesse durch die Etablierung eines BCMS.
Übergeordneter Zielbeitrag:
Z.3-1

Maßnahme Nummer 3.5

Handlungserfordernis:
Betreuung und Beratung der betroffenen Behörden
Überblick über die aktuelle Umsetzung:
Eine explizite Beratung der betroffenen Behörden durch die Zentralstelle Cybersicherheit hat aufgrund der noch eingeschränkten Ressourcen nicht stattgefunden. In Einzelfällen wurde ein erster Austausch initiiert. Über den Präventionsbereich des Landesamtes für Verfassungsschutz werden regelmäßig Informationen über staatlich gesteuerte Cyberaktivitäten fremder Akteure an betroffene Entitäten ausgesteuert. Zu den regelmäßig betroffenen Entitäten zählen auch Politik und Verwaltung.
Perspektivische Umsetzung:
Die Zentralstelle Cybersicherheit soll perspektivisch befähigt werden, die betroffenen Behörden zu Themen der Cybersicherheit (z. B. BCM, Prozessintegration) zu beraten und somit dort vorhandenes Fachwissen weiter stärken zu können.
Ziel:
Schaffung zentraler Kompetenzen, um die Einführung und Umsetzung entsprechender Managementsysteme möglichst landeseinheitlich und ressourcenschonend, bei gleichzeitigem Wissenstransfer zwischen den entsprechenden Stellen, zu ermöglichen. Durch den übergreifenden Ansatz sollen ebenfalls eine externe Qualitätssicherung der Entwicklungsprozesse ermöglicht und Optimierungspotentiale identifiziert werden.
Übergeordneter Zielbeitrag:
Z.3-1, Z.3-2

Maßnahme Nummer 3.6

Handlungserfordernis:
Identifikation und Vernetzung in der Prävention von Cyberkriminalität tätiger Akteur:innen
Überblick über die aktuelle Umsetzung:
Die Prävention von Cyberkriminalität ist eine interorganisationale Aufgabe, bei der eine enge Zusammenarbeit zwischen Polizei und Staatsanwaltschaft erforderlich ist. Zu diesem Zwecke besteht eine Vernetzung der zwischen den. Cybercrime-Dezernenten der Staatsanwaltschaft sowie der Polizei. In der Polizei Bremen ist im Ermittlungsabschnitt K 134 Cybercrime die „Zentrale Ansprechstelle Cybercrime für die Wirtschaft“ (ZAC) angegliedert. Die ZAC steht Unternehmen in Präventionsfragen als auch bei IT-Schadensfällen als Ansprechpartner zur Verfügung. Die Tätigkeit wird neben der Cybercrime-Sachbearbeitung durchgeführt. Sollte sich zukünftig ein Bremerhavener Unternehmen an die ZAC der Polizei Bremen wenden, dann wird ein Incident-Report gefertigt und eine Erstberatung zwecks Durchführung von Sofortmaßnahmen zur Schadensminimierung durchgeführt. Anschließend wird zwecks Strafanzeigenaufnahme sowie der Übernahme der weiteren Ermittlungen

an die OPB Bremerhaven verwiesen. Als 24/7-Ansprechstelle der OPB wurde der KDD benannt, welcher in Bremerhaven eine Annahme- und Steuerungsfunktion übernimmt.

Der Präventionsbereich des Landesamtes für Verfassungsschutz ist im regelmäßigen und vertrauensvollen Austausch mit den wesentlichen Akteuren und Sicherheitsbehörden von Bund und Ländern.

Perspektivische Umsetzung:

Die bestehenden Strukturen der Zusammenarbeit werden fortwährend überprüft und im Bedarfsfall angepasst, um den Aufbau eines landesweiten Kompetenznetzwerks mit den in der Freien Hansestadt Bremen in der Prävention von Cyberkriminalität tätigen Akteur:innen stetig zu verbessern. Perspektivisch soll die Kooperation zwischen der ZAC und der Ortspolizeibehörde Bremerhaven weiter gestärkt werden.

Aufgrund der aktuellen Sicherheitslage ist davon auszugehen, dass die entsprechenden Vernetzungsaktivitäten des Landesamtes für Verfassungsschutz in Abhängigkeit der vorhandenen Ressourcen ausgeweitet werden.

Ziel:

Schaffung eines Kompetenznetzwerks, um Synergieeffekte für die Entwicklung und Durchführung von Präventionsmaßnahmen zu nutzen sowie eine möglichst große Wirkung bei der Durchführung von Präventionsmaßnahmen zu entfalten. Hierzu zählt auch die verlässliche polizeiliche Begleitung von Unternehmen bei IT-Schadensfällen oder -fragen.

Übergeordneter Zielbeitrag:

Z.3-1, Z.3-2

Maßnahme Nummer 3.7

Handlungserfordernis:

Identifikation und Bewertung der bestehenden Schulungsangebote für Mitarbeiter:innen in den staatlichen Einrichtungen in Bezug auf die Prävention von Cyberkriminalität

Überblick über die aktuelle Umsetzung:

Bei der Senatorin für Justiz und Verfassung wird neben den internen Schulungsangeboten sowie denen des AFZ zusätzlich für alle Mitarbeiter:innen ein Schulungsportal zum sicherheitsgerechten Verhalten angeboten. Desweiterem finden Awareness-Kampagnen statt.

In Bremerhaven werden für die IRLS über den externen Dienstleister für Datenschutz (Datenschutzbeauftragten) der Feuerwehr online Schulungen mit den Themenschwerpunkten Datenschutzgrundverordnung (DSGVO) und relevante IT-Sicherheitsstandards angeboten. Diese werden als praxisnahe und verständliche Lernmodule in Form von Kurzvideos über die Schulungsplattform des Dienstleisters angeboten. Darüber hinaus muss eine Unterweisung mit anschließenden Prüfungen zu den Themen IT-Sicherheit und Datenschutz abgelegt werden. Alle Beschäftigten sind verpflichtet, diese zu absolvieren. Zusätzlich bietet der externe Dienstleister regelmäßig themenspezifische Aufklärungsvideos an (Sensibilisierungen zu IT-sicherheitsrelevanten Aspekten wie Phishing-Mails, Betrugsversuche via E-Mail und Telefon etc.). Auch hier sind alle Beschäftigten dazu verpflichtet, sich diese im Selbststudium anzuschauen.

In der Ortspolizeibehörde Bremerhaven gibt es zurzeit keine expliziten Schulungsangebote für den Bereich der Cyberkriminalität. Es wurde ein Leitfaden für die professionalisierte Aufnahme von Cybercrime-Vorgängen für erstaufnehmende Organisationseinheiten entwickelt und eingeführt.
Perspektivische Umsetzung:
Grundsätzlich sollte eine weitere Bestandsaufnahme vorhandener Schulungsangebote stattfinden. Bei der Feuerwehr Bremen ist mit dem Vorliegen ressortinterner Vorgaben eine Umsetzung kurzfristig bei einer Datenschutzunterweisung möglich. Bei der Ortspolizeibehörde Bremerhaven ist die Aus- und Fortbildung mindestens einer Ermittlungsperson für den o. g. Bereich sowie langfristig ein Aufwuchs dieser Kapazität durch eine weitere IT-Fachkraft vorgesehen. Die so ausgebildeten Personen sollen dann als Wissens-Multiplikatoren für alle Fachbereiche der Ortspolizeibehörde Bremerhaven dienen.
Ziel:
Identifikation von „Best Practices“ und wirksamen Schulungsangeboten zur Etablierung eines einheitlichen „Cybersicherheitsbewusstseins, mit dem Ziel einer Standardisierung der in der Freien Hansestadt Bremen genutzten Schulungskonzepte sowie die verbindliche Einführung entsprechender Schulungen.
Übergeordneter Zielbeitrag:
Z.3-2

Maßnahme Nummer 3.8

Handlungserfordernis:
Vereinheitlichung und Ausbau der Schulungsangebote
Überblick über die aktuelle Umsetzung:
Zurzeit bestehen vor allem in den einzelnen Bereichen individuelle Schulungsangebote. Die Senatorin für Justiz und Verfassung arbeitet an einer fortwährenden Aktualisierung und Erweiterung der vorhandenen Schulungsangebote. Aktuell bietet das Informationssicherheitsmanagement der Polizei Bremen ein Informationsangebot über Themen der Informationssicherheit an. Darüber hinaus sind Schulungen im Intranet der Stadt Bremen vorhanden.
Perspektivische Umsetzung:
Die Vereinheitlichung sowie der Ausbau vorhandener Schulungsangebote sollen kontinuierlich vorangetrieben werden. Hierbei können Schulungsplattformen eine Möglichkeit darstellen, um Inhalte möglichst ökonomisch und standardisiert für die entsprechenden Zielgruppen verfügbar zu machen. Darüber hinaus kann geprüft werden, inwieweit relevante Schulungen als Teil der verschiedenen Ausbildungen sowie Lehrgänge integriert werden können.

In Bremerhaven wird für die IRLS die Erstellung einer internen Schulungsplattform angestrebt.
Ziel:
Kontinuierliche Erweiterung und wo sinnvoll Standardisierung von sowie Verpflichtung zu Schulungsangeboten, um den Wissensstand der Mitarbeiter:innen in der Freien Hansestadt Bremen in Belangen der Cybersicherheit zu erhöhen.
Übergeordneter Zielbeitrag:
Z.3-1, Z.3-2

Maßnahme Nummer 3.9

Handlungserfordernis:
Bewertung der personellen und technischen Kapazitäten LfV zur Cyberabwehr
Überblick über die aktuelle Umsetzung:
Die personelle Ausstattung der Fachbereiche des Landesamtes für Verfassungsschutz ist als Verschlusssache eingestuft und somit nicht für die Veröffentlichung geeignet. Unabhängig davon arbeitet das Landesamt für Verfassungsschutz im Bereich der Cyberabwehr eng mit den anderen Nachrichtendiensten von Bund und Ländern zusammen.
Perspektivische Umsetzung:
Die Bewertung der personellen und technischen Kapazitäten wird wiederkehrend überprüft.
Ziel:
Steigerung der Kapazitäten bzw. Optimierung der bestehenden Fähigkeiten zur Detektion und ggf. Abwehr von Cyberangriffen im Rahmen des gesetzlichen Auftrags des Landesamtes für Verfassungsschutz.
Übergeordneter Zielbeitrag:
Z.3-1

Maßnahme Nummer 3.10

Handlungserfordernis:
Bewertung der personellen und technischen Kapazitäten der Strafverfolgungsbehörden zur effektiven Kriminalitätsbekämpfung im Bereich der Cybersicherheit
Überblick über die aktuelle Umsetzung:
Die dem Geschäftsbereich der Senatorin für Justiz und Verfassung zugeordnete Staatsanwaltschaft verfügt über zwei Sonderdezernate zur Bekämpfung der Cybercrime. In der Polizei Bremen bearbeitet der Abschnitt K 134 Cybercrimestraftaten, bietet Unterstützungsleistungen von Recherche und Kryptowährungsanalyse und stellt die Zentrale Ansprechstelle Cybercrime für die Wirtschaft dar. In der Ortspolizeibehörde Bremerhaven sind die Fähigkeiten im Ermittlungsbereich derzeit stark begrenzt und werden im Rahmen der vorliegenden Ressourcen durchgeführt. Der SPoC bei Anzeigenaufnahme für Cybercrimestraftaten ist der Kriminaldauerdienst.

Perspektivische Umsetzung:
Zur Gewährleistung des Mindeststandards ist unter Berücksichtigung der Entwicklungen in Zusammenhang mit der IT-Nutzung in allen Deliktsbereichen sowie der eigentlichen Cybercrime im engeren Sinne sowie der zunehmenden Verbreitung von Kryptowährungen zu prüfen, inwiefern mittelfristig eine Anpassung des Personalkörpers im Fachreferat erforderlich ist.
Ziel:
Sicherstellung ausreichender und an zukünftige Entwicklungen des Phänomenbereichs angepasste personelle und technische Kapazitäten zur Ermöglichung einer effektiven Strafverfolgung im Bereich der Cybercrime. Hierzu zählen unter anderem die tiefgehende Betreuung von Ermittlungsreferaten im Zusammenhang mit IT-bezogenen Ermittlungen, tiefgehende Rechercheunterstützungen in Ermittlungsverfahren sowie vollwertige Analysen und Unterstützungsleistungen im Zusammenhang mit Kryptowerten.
Übergeordneter Zielbeitrag:
Z.3-1, Z.3-2

6.4 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.

6.4.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurden folgende konkretisierte Ziele abgeleitet:

- Z.4-1 Compliance mit geltendem Cybersicherheitsrecht
- Z.4-2 Steigerung der Cyberresilienz von Unternehmen und Einrichtungen im Land Bremen
- Z.4-3 Ausbau des Austauschs zwischen staatlichen Stellen und Wirtschaftsunternehmen im Land Bremen

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

4.1	Übernahme der Zentralstellenfunktion für das Land Bremen durch die Zentralstelle Cybersicherheit
4.2	Enger Austausch zwischen Arbeitskreisen, Netzwerken und Betreiber:innen kritischer Infrastrukturen sowie der Zentralstelle Cybersicherheit
4.3	Prozessentwicklung NIS-2-Richtline
4.4	Erarbeitung eines Bremischen Cybersicherheitsgesetzes zur Regelung der behördlichen Zuständigkeiten, welche sich aus der NIS-2-Richtlinie ergeben
4.5	Ausbau von Ansprechstellen und Beratungsangeboten für KMU im Rahmen eines IT-Kompetenznetzwerks für Bremen und Bremerhaven
4.6	Förderung der Vernetzung von Akteur:innen aus Staat und Wirtschaft

6.4.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 4.1

Handlungserfordernis:
Übernahme der Zentralstellenfunktion für das Land Bremen durch die Zentralstelle Cybersicherheit

Überblick über die aktuelle Umsetzung:
Diese Maßnahme kann erst im Nachgang zur Bundesgesetzgebung und den hieraus resultierenden Ergebnissen geprüft und näher ausgestaltet werden.
Perspektivische Umsetzung:
Ziel:
Compliance mit der NIS-2-Richtlinie
Übergeordneter Zielbeitrag:
Z.4-1

Die Gesetzgebungs- und Regelungskompetenz für die Wirtschaft liegt beim Bund. Nach aktuellem Stand der Umsetzung der NIS-2-Richtlinie in Bundesrecht ist davon auszugehen, dass keine die Wirtschaft betreffenden Maßnahmen auf Landesebene umzusetzen sind. Die Zuständigkeit für den Bereich der öffentlichen Verwaltung wird in HF1 geregelt.

Maßnahme Nummer 4.2

Handlungserfordernis:
Enger Austausch zwischen Arbeitskreisen, Netzwerken und Betreiber:innen kritischer Infrastrukturen sowie der Zentralstelle Cybersicherheit
Überblick über die aktuelle Umsetzung:
Perspektivische Umsetzung:
Bei der Senatorin für Gesundheit, Frauen und Verbraucherschutz ist ein Runder Tisch zum Thema Krankenhausalarm- und -einsatzpläne für Ende 2025 geplant, bei welchem auch das Thema Cybersicherheit besprochen werden soll. Zu dem Austausch soll neben den Krankenhäusern auch die Zentralstelle Cybersicherheit eingeladen werden.
Ziel:
Identifikation von aktuellen und zukünftigen Trends im Bereich der Cybersicherheit sowie von Best Practices und bestehender Herausforderungen sowie Steigerung des gegenseitigen Vertrauens.
Übergeordneter Zielbeitrag:
Z.4-3

Maßnahme Nummer 4.3

Handlungserfordernis:
Prozessentwicklung NIS-2-Richtlinie
Überblick über die aktuelle Umsetzung:
Perspektivische Umsetzung:
Ziel:
Definition von eindeutigen Zuständigkeiten, Kompetenzen und Befugnissen.
Übergeordneter Zielbeitrag:
Z.4-1

Die Gesetzgebungs- und Regelungskompetenz für die Wirtschaft liegt beim Bund. Nach aktuellem Stand der Umsetzung der NIS-2-Richtlinie in Bundesrecht ist davon auszugehen, dass keine die Wirtschaft betreffenden Maßnahmen auf Landesebene umzusetzen sind. Die Zuständigkeit für den Bereich der öffentlichen Verwaltung wird in HF1 geregelt.

Maßnahme Nummer 4.4

Handlungserfordernis:
Erarbeitung eines Bremischen Cybersicherheitsgesetzes zur Regelung der behördlichen Zuständigkeiten, welche sich aus der NIS-2-Richtlinie ergeben
Überblick über die aktuelle Umsetzung:
In einem ersten Schritt wurde die Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) durch den Senat verabschiedet. Diese ist am 15.01.2025 in Kraft getreten.
Perspektivische Umsetzung:
Zur ganzheitlichen Regelung der Belange der Cybersicherheit im Land Bremen ist ein Bremisches Cybersicherheitsgesetz erforderlich, welches jedoch einer umfassenden Vorbereitung bedarf. Interimsweise wird daher die Verabschiedung eines Bremischen Cybersicherheitsbasisgesetzes angestrebt.
Ziel:
Compliance mit der NIS-2-Richtlinie
Übergeordneter Zielbeitrag:
Z.4-1

Maßnahme Nummer 4.5

Handlungserfordernis:
Ausbau von Ansprechstellen und Beratungsangeboten für KMU im Rahmen eines IT-Kompetenznetzwerks für Bremen und Bremerhaven
Überblick über die aktuelle Umsetzung:
Es wurden erste Angebote bekannt gemacht, etwa die Nutzung des „Cybersicherheitschecks“ für KMU. Hierfür werden in einem ersten Schritt Multiplikator:innen der Industrie- und Handelskammern geschult, um dann gemeinsam mit Unternehmen etwaige Bedarfe zur Steigerung der Cybersicherheit zu erheben.
Perspektivische Umsetzung:
Unterstützung bestehender Ansprechstellen und Beratungsangebote, durch z. B. Fachvorträge, die Vermittlung an „zertifizierte“ Dienstleistende und Stellen sowie die Breitstellung bestimmter Dienstleistungen (siehe digitale Ersthelfer / Versand von Lagebildern etc.).
Ziel:
Steigerung der digitalen Resilienz von in der Freien Hansestadt Bremen ansässigen KMU.
Übergeordneter Zielbeitrag:
Z.4-2, Z.4-3

Maßnahme Nummer 4.6

Handlungserfordernis:
Förderung der Vernetzung von Akteur:innen aus Staat und Wirtschaft
Überblick über die aktuelle Umsetzung:
Die Senatorin für Wirtschaft, Häfen und Transformation hat im Umsetzungszeitraum unterschiedliche Maßnahmen zur Förderung der Vernetzung von Akteur:innen aus Staat und Wirtschaft durchgeführt. Hierzu gehörten vor allem Vernetzungstreffen sowie die Teilnahme an Informationsveranstaltungen mit Akteur:innen der Zentralstelle Cybersicherheit, dem Digital Hub Industrie (DHI), dem Mittelstand-Digitalzentrum (MDZ) Bremen / Oldenburg sowie der Transferstelle Cybersicherheit, die im Rahmen der Mittelstandsförderung vom Bundeswirtschaftsministerium gefördert wird.
Perspektivische Umsetzung:
Bei der Förderung der Vernetzung von Akteur:innen aus Staat und Wirtschaft handelt es sich um eine fortlaufende Aufgabe.
Ziel:
Durch die Vernetzung zwischen Akteur:innen aus Staat und Wirtschaft kann das Vertrauensverhältnis weiter gestärkt werden. Durch eine möglichst transparente Kommunikation untereinander können etwaige Kooperationsmöglichkeiten identifiziert werden.
Übergeordneter Zielbeitrag:
Z.4-2, Z.4-3

6.5 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.

6.5.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurde folgendes konkretisiertes Ziel abgeleitet:

- Z.5-1 Die Stärkung alters-, geschlechter- und vielfaltssensible Förderung digitaler Kompetenzen

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

5.1	Stärkung des formalen sowie des informellen Lernens
5.2	Befähigung der Mitarbeiter:innen in Kitas und Schulen, um die digitalen Kompetenzen sowie die Cyberresilienz so früh wie möglich zu stärken

6.5.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 5.1

Handlungserfordernis:
Stärkung des formalen sowie des informellen Lernens
Überblick über die aktuelle Umsetzung:
Medienbildung spielt in allen Bremer Schulen eine große Rolle, ist curricular verankert und als Querschnittsthema in vielen Fächern existent. Es werden dabei Themen wie Sicherheit im Netz, Schutz vor (Online-)Betrug und sicherer Umgang mit persönlichen Daten im Netz behandelt. In einzelnen Ressorts gibt es interne Fortbildungsmaßnahmen zur Steigerung der digitalen Kompetenzen, die Mitarbeiter:innen zur Verfügung stehen. In Bremerhaven werden im Geschäftsbereich des Amtes für Jugend, Familie und Frauen die pädagogischen Fachkräfte in den Bremerhavener Kindertageseinrichtungen im Zusammenhang mit der dienstlichen Nutzung digitaler Endgeräte (überwiegend Tablets) für das Thema Cybersicherheit sensibilisiert. Die Schulung erfolgt durch die

Abteilung ADV des Amtes 51 (51/01). Das Sachgebiet Qualifizierung bietet darüber hinaus Fortbildungen für pädagogische Fachkräfte zum Thema Datenschutz an.
Perspektivische Umsetzung:
Alters-, geschlechter- sowie vielfaltssensible Angebote zur Stärkung digitaler Kompetenzen sollen kontinuierlich ausgebaut werden. In Bremerhaven finden im Geschäftsbereich des Amtes für Jugend, Familie und Frauen im Rahmen des Fachtags zum Thema Medienbildung am 06.11.2025 Workshops zu den Themen Datenschutz und Elternarbeit statt. Die Fachkräfte werden hier für das Thema Cybersicherheit sensibilisiert und in ihrer Rolle als Multiplikator:innen für Eltern gestärkt. Weitere Fortbildungsangebote sind geplant.
Ziel:
Verminderung des Risikos der Opferwerdung der Einwohner:innen der Freien Hansestadt Bremen im Cyberraum durch eine Erhöhung des Risiko- und Gefahrenbewusstsein, z. B. durch die Steigerung an digitalen Lernangeboten bzgl. der o. g. Risiken.
Übergeordneter Zielbeitrag:
Z.5-1

Maßnahme Nummer 5.2

Handlungserfordernis:
Befähigung der Mitarbeiter:innen in Kitas und Schulen, um die digitalen Kompetenzen sowie die Cyberresilienz so früh wie möglich zu stärken
Überblick über die aktuelle Umsetzung:
Für die Stadt Bremen wurden der Zentralstelle Cybersicherheit für den Umsetzungszeitraum keine Maßnahmen zur Umsetzung dieses Handlungsfeldes gemeldet. In Bremerhaven wird im Geschäftsbereich des Amtes für Jugend, Familie und Frauen das Thema Cybersicherheit im Rahmen medienpädagogischer Arbeit mit den Kindern thematisiert. Zum Thema Medienpädagogik und Medienbildung finden im Sachgebiet Qualifizierung Fortbildungen für die pädagogischen Fachkräfte aus den Bremerhavener Kindertageseinrichtungen statt.
Perspektivische Umsetzung:
Die Befähigung der Mitarbeiter:innen in Kitas und Schulen zur frühestmöglichen Förderung und Stärkung digitaler Kompetenzen sowie der individuellen Cyberresilienz stellt weiterhin einen zentralen Ansatz dar, der fortwährend gestärkt werden sollte. In Bremerhaven findet im Geschäftsbereich des Amtes für Jugend, Familie und Frauen zum Thema Medienpädagogik am 06.11.2025 ein Fachtag statt. Unter anderem werden die Fachkräfte hier für das Thema Cybersicherheit sensibilisiert. Weitere Fortbildungsangebote für pädagogische Fachkräfte zu diesem Themenbereich sind geplant.
Ziel:
Kinder und Jugendliche in der Freien Hansestadt Bremen sollen über die entsprechenden Gefahren, die die Nutzung von neuen Medien mit sich bringen frühzeitig aufgeklärt werden, um die hiermit verbundenen Risiken einschätzen und minimieren zu können. So kann das Risiko der späteren Opferwerdung in Bezug auf Gefahren im Cyberraum verringert werden.

Übergeordneter Zielbeitrag:
Z.5-1

6.6 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.

6.6.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurden folgende konkretisierte Ziele abgeleitet:

- Z.6-1 Stärkung der Eigenverantwortung und der digitalen Resilienz von Verbraucher:innen im Umgang mit digitalen Endgeräten und Anwendungen
- Z.6-2 Vernetzung der Akteur:innen im Verbraucherschutz zur besseren Koordinierung der Sensibilisierungsmaßnahmen

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

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

6.6.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 6.1

Handlungserfordernis:
Stärkung der Verbraucher:innen in ihrer Eigenverantwortung und Entscheidungsfindung
Überblick über die aktuelle Umsetzung:

In der FHB stellt eine zentrale Ansprechstelle bei der Stärkung der Verbraucher:innen in ihrer Eigenverantwortung und Entscheidungsfindung die Verbraucherzentrale Bremen dar. Auf Bundesebene stellt das BSI kostenlose Informationen bereit. Es wurden durch die Senatorin für Gesundheit, Frauen und Verbraucherschutz in Kooperation mit dem Präventionszentrum der Polizei Bremen, der Verbraucherzentrale sowie der Bremischen Landesmedienanstalt bereits mehrmals Online-Informationsveranstaltungen zu betrügerischen Methoden in der digitalen Welt durchgeführt.
Perspektivische Umsetzung:
Durch die o. g. Stellen werden die entsprechenden Angebote wiederkehrend geprüft und bei Bedarf aktualisiert.
Ziel:
Befähigung der Verbraucher:innen, auf Grundlage von frei verfügbaren Informationen, z. B. durch die Bereitstellung entsprechender Informationen auf bremischen Internetseiten, bewusste Entscheidungen im Umgang mit Endgeräten bzw. dem Cyberraum im Allgemeinen treffen zu können.
Übergeordneter Zielbeitrag:
Z.6-1

Maßnahme Nummer 6.2

Handlungserfordernis:
Befähigung der Verbraucher:innen, Gefahren im Zusammenhang mit dem Einsatz von Hard- und Software eigenständig zu erkennen und resilienter diesen gegenüber zu werden
Überblick über die aktuelle Umsetzung:
Bei der Befähigung von Verbraucher:innen im Zusammenhang mit dem Einsatz von sicherer Hard- und Software sind unterschiedliche Akteur:innen aktiv. Auf Landesebene sind beispielsweise das Präventionszentrum der Polizei Bremen oder Weiterbildungsinstitutionen wie die Volkshochschule zu nennen. Auf Bundesebene werden wichtige Informationen durch das BSI zur Verfügung gestellt.
Perspektivische Umsetzung:
Durch die o. g. Stellen werden die entsprechenden Angebote wiederkehrend geprüft und bei Bedarf aktualisiert.
Ziel:
Befähigung der Verbraucher:innen, auf Grundlage von frei verfügbaren Informationen, z. B. durch die Bereitstellung entsprechender Informationen auf bremischen Internetseiten, bewusste Entscheidungen im Umgang mit Endgeräten bzw. dem Cyberraum im Allgemeinen treffen zu können.
Übergeordneter Zielbeitrag:
Z.6-1

Maßnahme Nummer 6.3

Handlungserfordernis:

Zusammenführung der vielfältigen Akteur:innen des Verbraucherschutzes im Bereich Cybersicherheit auf Landesebene durch die auszugestaltende Zentralstelle Cybersicherheit, um Synergien sowie eine größtmögliche Reichweite zu schaffen und einen Beitrag zur Präventionsarbeit im Land Bremen zu leisten
Überblick über die aktuelle Umsetzung:
In diesem Bereich konnten aufgrund der noch eingeschränkten Ressourcen der Zentralstelle Cybersicherheit im Umsetzungszeitraum keine Maßnahmen durchgeführt werden.
Perspektivische Umsetzung:
Die Ausgestaltung und Erweiterung der Kooperationsformate, etwa durch die Einrichtung eines Runden Tisches oder anderer Formen der institutionalisierten Zusammenarbeit, wird fortwährend geprüft.
Ziel:
Erzeugung von Synergien durch die Zusammenarbeit der vielfältigen Akteur:innen, um eine möglichst große Reichweite in Bezug auf Cybersicherheitsthemen unter den Verbraucher:innen in der Freien Hansestadt Bremen unter optimaler Nutzung der begrenzt zur Verfügung stehenden Ressourcen zu generieren.
Übergeordneter Zielbeitrag:
Z.6-2

Maßnahme Nummer 6.4

Handlungserfordernis:
Förderung des Designansatzes "Security by Design" durch Hinweise auf sicherheitskonforme IT-Produkte und Dienste in enger Zusammenarbeit mit den anderen Akteur:innen des Verbraucherschutzes
Überblick über die aktuelle Umsetzung:
Im Oktober 2024 wurde durch die EU die Verordnung 2024/2847 (Cyber Resilience Act) verabschiedet. In dieser werden Regeln zur Cybersicherheit von Produkten mit digitalen Elementen EU-weit vereinheitlicht. Dadurch sollen ein hohes Cybersicherheitsniveau in der Union sichergestellt und der freie Verkehr von Produkten mit digitalen Elementen im europäischen Binnenmarkt gewährleistet werden. Die Verordnung trat am 10.12.2024 in Kraft und gilt ab dem 11.12.2027.
Perspektivische Umsetzung:
Im Rahmen der Umsetzung der Verordnung 2024/2847 soll geprüft werden, wie die entsprechenden Produkte, die die Anforderungen der Verordnung erfüllen, gekennzeichnet werden und ob auf diese Kennzeichnungen separat hingewiesen werden kann.
Ziel:
Nutzer:innen sollen auf das Vorhandensein entsprechender Produkte und Dienste hingewiesen werden, so dass Aspekte der Sicherheit bei zukünftigen Kaufentscheidungen mit in den Entscheidungsprozess einbezogen werden.
Übergeordneter Zielbeitrag:
Z.6-1, Z.6-2

Maßnahme Nummer 6.5

Handlungserfordernis:
Einrichtung der auszugestaltenden Zentralstelle Cybersicherheit als zentrale Ansprechstelle für Sensibilisierungsmaßnahmen aller Verwaltungs- und Behördenmitarbeiter:innen im Land Bremen
Überblick über die aktuelle Umsetzung:
Die Zentralstelle Cybersicherheit wurde zum 01.05.2023 beim Senator für Inneres und Sport eingerichtet und hat sich seitdem als zentrale Ansprechstelle für alle Ressorts sowie den Magistrat der Stadt Bremerhaven in allen Belangen der Cybersicherheit etabliert. Beim Senator für Inneres und Sport wurde für alle Mitarbeiter:innen ein Sensibilisierungsportal zur Cyber- und Informationssicherheit eingerichtet.
Perspektivische Umsetzung:
Die Nutzung vorhandener Angebote steigern sowie den Ausbau bestehender Sensibilisierungsmaßnahmen in Zusammenarbeit mit allen betroffenen Akteur:innen weiter auszubauen.
Ziel:
Bestmögliche Nutzung vorhandener Kompetenzen, Schaffung von Synergieeffekten und Entwicklung von „best practices“, um die vorhandenen Ressourcen effizient zu nutzen.
Übergeordneter Zielbeitrag:
Z.6-1, Z.6-2

6.7 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.

6.7.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurden folgende konkretisierte Ziele abgeleitet:

- Z.7-1 Gewinnung und Bindung von IT-Fachkräften
- Z.7-2 Steigerung des Frauenanteils unter den Beschäftigten der IT-Branche
- Z.7-3 Ermöglichung eines niedrigschwelligen Einstiegs in die IT- und Cybersicherheit
- Z.7-4 Weiterentwicklung der Freien Hansestadt Bremen zum attraktiven Standort für IT-Fachkräfte

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

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

6.7.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 7.1

Handlungserfordernis:
Sichtung bestehender (inter)nationaler Konzepte zur Fachkräftegewinnung und Prüfung, inwieweit diese im Land Bremen bereits genutzt werden oder Anwendung finden können
Überblick über die aktuelle Umsetzung:
Die Gewinnung von IT-Fachkräften erfolgt in der FHB aktuell bedarfsorientiert und nicht auf Basis eines übergreifenden Konzepts. Eine systematische Sichtung und Nutzung bestehender (inter)nationaler Strategien zur Fachkräftegewinnung ist bislang nicht erfolgt. Bei der Senatorin für Justiz und Verfassung liegt der Schwerpunkt beispielsweise auf der gezielten Nachwuchsgewinnung in den justizspezifischen Ausbildungsberufen.
Perspektivische Umsetzung:
Ziel:
Entwicklung von „best-practices“ zur Fachkräftegewinnung, die auf die Freie Hansestadt Bremen abgestimmt sind.
Übergeordneter Zielbeitrag:
Z.7-1, Z.7-2, Z.7-3

Maßnahme Nummer 7.2

Handlungserfordernis:
Prüfung des Potenzials der Fachkräftegewinnung durch Inklusion
Überblick über die aktuelle Umsetzung:
In der öffentlichen Verwaltung des Landes Bremen werden Stellenausschreibungen stets mit dem „Hinweis auf die bevorzugte Berücksichtigung von schwerbehinderten Menschen bei gleicher Eignung“ zur Sicherstellung der Chancengleichheit und dem Schutz vor Benachteiligung versehen.
Perspektivische Umsetzung:
Die Fortsetzung des Abbaus struktureller Benachteiligung von Menschen mit Schwerbehinderung ist eine fortlaufende Aufgabe.
Ziel:
Integration neurodiverser Menschen in den ersten Arbeitsmarkt sowie Identifikation und Einsatz der besonderen Fähigkeiten dieser Personen
Übergeordneter Zielbeitrag:
Z.7-1

Maßnahme Nummer 7.3

Handlungserfordernis:
Überprüfung und ggf. Anpassung der bestehenden Anforderungen an Bewerber:innen im Bereich Cybersicherheit für den öffentlichen Dienst
Überblick über die aktuelle Umsetzung:

Stellen im öffentlichen Dienst im Bereich der Cybersicherheit betreffen unter anderem die Funktion der Informationssicherheitsbeauftragten sowie der ITSK. Stellenprofile werden durch die ausschreibenden Behörden bedarfsorientiert überprüft und erforderlichenfalls an aktuelle Entwicklungen angepasst.
Perspektivische Umsetzung:
Ziel:
Steigerung der Attraktivität des öffentlichen Dienstes für (IT-) Fachkräfte sowie eine verbesserte Ausschöpfung des vorhandenen Bewerber:innenpotentials
Übergeordneter Zielbeitrag:
Z.7-1, Z.7-2

Maßnahme Nummer 7.4

Handlungserfordernis:
Überprüfung und ggf. Anpassung der Fortbildungsmöglichkeiten für Bedienstete im öffentlichen Dienst mit Blick auf cybersicherheitsrelevante Themen
Überblick über die aktuelle Umsetzung:
In diesem Bereich konnten aufgrund der noch eingeschränkten Ressourcen der Zentralstelle Cybersicherheit im Umsetzungszeitraum keine Maßnahmen durchgeführt werden.
Perspektivische Umsetzung:
Bei der Überprüfung und Anpassung vorhandener Fortbildungsmöglichkeiten im öffentlichen Dienst mit Blick auf cybersicherheitsrelevante Themen handelt es sich um eine fortwährende Aufgabe.
Ziel:
Optimierung der bereits vorhandenen personellen Ressourcen durch die Fortbildung am Themenfeld „Cybersicherheit“ interessierterer Bediensteter sowie Steigerung der Attraktivität des öffentlichen Dienstes für externe Bewerber aufgrund interner Fortbildungs- und Aufstiegsmöglichkeiten
Übergeordneter Zielbeitrag:
Z.7-1, Z.7-3, Z.7-4

Maßnahme Nummer 7.5

Handlungserfordernis:
Steigerung der Attraktivität von MINT-Berufen und Studiengängen für Frauen.
Überblick über die aktuelle Umsetzung:
Die staatlichen Hochschulen arbeiten kontinuierlich daran, den Anteil an Studentinnen in den MINT-Studiengängen weiter zu steigern. Entsprechende Maßnahmen sind sowohl in den Umsetzungsvereinbarungen zum Zukunftsvertrag Studium und Lehre stärken als auch in den Zielvereinbarungen zwischen Land und Hochschulen enthalten. Insgesamt stieg der Anteil an Studentinnen in MINT-Studiengängen an den landesbremischen Hochschulen von rund 30 Prozent 2018 auf 33,3 Prozent 2024 (deutschlandweit: 32,9 Prozent).
Perspektivische Umsetzung:

Die staatlichen Hochschulen setzen ihre Anstrengungen zur Akquirierung und Förderung von Studentinnen in MINT-Fächern weiter fort und erweitern sie. In diesem Zusammenhang kommen der Kooperation und Vernetzung mit Schulen und außerschulischen Lernorten und relevanten Partner:innen eine besondere Bedeutung zu.
Ziel:
Mehr Frauen sollen in MINT-Berufen und Studiengängen Fuß fassen und die hiermit verbundenen beruflichen Chancen nutzen können. An den staatlichen Hochschulen soll der Frauenanteil an den Professuren in den MINT-Fächern bis zum Jahr 2030 auf 28 Prozent gesteigert werden (siehe Wissenschaftsplan 2030).
Übergeordneter Zielbeitrag:
Z.7-2, Z.7-4

Maßnahme Nummer 7.6

Handlungserfordernis:
Stärkere Vernetzung von Hochschulen, Wirtschaft und Behörden, um auf das Thema Cybersicherheit aufmerksam zu machen
Überblick über die aktuelle Umsetzung:
Zwischen den Hochschulen und der Wissenschaftsbehörde besteht bereits ein regelmäßiger und anlassbezogener Austausch.
Perspektivische Umsetzung:
Eine stärkere Institutionalisierung des Austauschs zwischen Ressort und Hochschulen ist vorgesehen sowie die (Weiter-)Entwicklung und Implementierung von IT-Sicherheitsstrategien, die für alle Hochschulen verbindlich sind.
Ziel:
Steigerung der „Sichtbarkeit“ des Themas Cybersicherheit in allen Bereichen des öffentlichen Lebens, um hierdurch die digitale Resilienz zu stärken und um eine möglichst große Anzahl an Menschen auf die (beruflichen) Chancen, die sich in diesem Bereich entwickeln, hinzuweisen
Übergeordneter Zielbeitrag:
Z.7-1, Z.7-3, Z.7-4

Maßnahme Nummer 7.7

Handlungserfordernis:
Prüfung des Ausbaus der Kapazitäten für die Schaffung und Durchführung von Ausbildungen und Studiengängen im Bereich Cybersicherheit
Überblick über die aktuelle Umsetzung:
Im Bereich der öffentlichen Verwaltung sind zurzeit keine Ausbildungs- oder Studiengänge im Bereich der Cybersicherheit geplant. An der Hochschule Bremerhaven existieren zwei Studiengänge, die neue Fachkräfte ausbilden, um mit den genannten Risikolagen – darunter auch Cybersicherheit – umzugehen: der MA Integrated Safety and Security Management sowie der MA Informatik Vertrauenswürdige Softwaresysteme. Die HS Bremerhaven kann zudem auf das Insti-

tute for Safety and Security Studies (ISaSS) verweisen. Dieses befasst sich mit aktuellen Forschungs- und Entwicklungsaufgaben zur Aufrechterhaltung und Verbesserung der Sicherheit im öffentlichen Bereich und in der Wirtschaft. Das ISaSS kooperiert in Form von gemeinsamen Projektaktivitäten unter anderem mit dem European Forum for Urban Security (Efus) und dem DLR Institut für den Schutz maritimer Infrastrukturen.

An der Hochschule Bremen kann der Master Informatik mit einem Schwerpunkt Informationssicherheit studiert werden. Des Weiteren gibt es das „Cyber Security Lab“, eine Lernplattform, die die aktuellen Themen im Bereich Informationssicherheit und sichere Softwareentwicklung aufgreift und verständlich vermittelt. Zudem existiert an der HSB ein Laboratory for IT-Security Architectures (lisa). Hierbei handelt es sich um ein virtuelles Labor, das eine modulare Entwicklungs- und Evaluierungsplattform für IT-Sicherheitsarchitekturen bietet und welches die Informatikstudierenden für Projekte nutzen dürfen.

Perspektivische Umsetzung:

entfällt

Ziel:

Steigerung des (akademisch) ausgebildeten Fachkräftepotentials im Bereich Cybersicherheit in der Freien Hansestadt Bremen

Übergeordneter Zielbeitrag:

6.8 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.

6.8.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurden folgende konkretisierte Ziele abgeleitet:

- Z.8-1 Diskriminierungsfreie sowie vielfaltssensible Entwicklung von Anwendungen und Geräten durch Stärkung relevanter Fachkenntnisse im Entwicklungsbereich
- Z.8-2 Schaffung geeigneter Rahmenbedingungen für den Wissens- und Technologietransfer zwischen Wissenschaft und Wirtschaft

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

8.1	Stärkung der Grundkompetenzen und des spezifischen Fachwissens zum Themenbereich "Cybersicherheit"
8.2	Auf- und Ausbau sowie Vermittlung und Weiterentwicklung durch die bereits vorhandenen Bildungs- und Forschungseinrichtungen
8.3	Etablierung interdisziplinärer Studiengänge zur Cybersicherheit
8.4	Stärkung des Wissens- und Technologietransfers zwischen Wissenschaft und Wirtschaft

6.8.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 8.1

Handlungserfordernis:
Stärkung der Grundkompetenzen und des spezifischen Fachwissens zum Themenbereich "Cybersicherheit".
Überblick über die aktuelle Umsetzung:
Der Zentralstelle Cybersicherheit wurden für den Umsetzungszeitraum keine Maßnahmen zur Verwirklichung dieses Zieles gemeldet.
Perspektivische Umsetzung:
Ziel:
Steigerung der digitalen Resilienz in der Freien Hansestadt Bremen.

Übergeordneter Zielbeitrag:

Maßnahme Nummer 8.2

Handlungserfordernis:
Auf- und Ausbau sowie Vermittlung und Weiterentwicklung durch die bereits vorhandenen Bildungs- und Forschungseinrichtungen.
Überblick über die aktuelle Umsetzung:
Für den Umsetzungszeitraum wurden keine spezifischen Maßnahmen mit Bezug zu diesem Handlungsfeld an die Zentralstelle Cybersicherheit gemeldet.
Perspektivische Umsetzung:
Ziel:
Nutzung bestehender Ressourcen und der dort vorhandenen Expertise, um auf bestehende Lösungen vorhandener Probleme hinzuweisen sowie neue Lösungsmöglichkeiten zu entwickeln.
Übergeordneter Zielbeitrag:

Maßnahme Nummer 8.3

Handlungserfordernis:
Etablierung interdisziplinärer Studiengänge zur Cybersicherheit.
Überblick über die aktuelle Umsetzung:
Für den Umsetzungszeitraum wurden keine spezifischen Maßnahmen mit Bezug zu diesem Handlungsfeld an die Zentralstelle Cybersicherheit gemeldet.
Perspektivische Umsetzung:
Ziel:
Erhöhung des Fachkräftepotentials sowie Erzeugung von Synergieeffekten, durch die neue Lösungen für Herausforderungen im Bereich Cybersicherheit entwickelt werden können.
Übergeordneter Zielbeitrag:

Maßnahme Nummer 8.4

Handlungserfordernis:
Stärkung des Wissens- und Technologietransfers zwischen Wissenschaft und Wirtschaft.
Überblick über die aktuelle Umsetzung:
Für den Umsetzungszeitraum wurden keine spezifischen Maßnahmen mit Bezug zu diesem Handlungsfeld an die Zentralstelle Cybersicherheit gemeldet.
Perspektivische Umsetzung:

Ziel:
Verbesserte Nutzung des vorhandenen akademischen Wissens bei der Entwicklung neuer Lösungen im Bereich der Cybersicherheit
Übergeordneter Zielbeitrag:

6.9 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.

6.9.1 Zielvorstellungen und Handlungserfordernisse des Handlungsfeldes

Aus der Handlungsfeldbeschreibung wurde folgendes konkretisiertes Ziel abgeleitet:

- Z.9-1 Ganzheitliche Verwirklichung von Cybersicherheit und Nutzung möglicher Synergieeffekte durch strategische Kooperationen auf nationaler und internationaler Ebene.

Zur Erreichung der Ziele wurden folgende Maßnahmen benannt:

9.1	Einrichtung der noch auszugestaltenden Zentralstelle Cybersicherheit als Single Point of Contact der öffentlichen Verwaltung für alle die Cybersicherheit betreffenden Netzwerke
9.2	Aufbau von Kooperationsbeziehungen mit anderen Cybersicherheitsbehörden auf Länder- und Bundesebene durch die noch auszugestaltende Zentralstelle Cybersicherheit

6.9.2 Umsetzungsstand und Zielbeitrag einzelner Maßnahmen

Maßnahme Nummer 9.1

Handlungserfordernis:
Einrichtung der noch auszugestaltenden Zentralstelle Cybersicherheit als Single Point of Contact der öffentlichen Verwaltung für alle die Cybersicherheit betreffenden Netzwerke
Überblick über die aktuelle Umsetzung:
Die Zentralstelle Cybersicherheit wurde zum 01.05.2023 beim Senator für Inneres und Sport eingerichtet und fungiert gemäß der Geschäftsverteilung des Senats als zentrale koordinierende Ansprechstelle in allen Belangen der Cybersicherheit. Darüber hinaus ist sie seit dem 15.01.2025 gem. VV NIS2Ums FHB die zuständige Behörde im Sinne des Art. 8 Abs. 1 NIS-2-Richtlinie und nimmt darüber hinaus die Aufgaben eines CSIRT im Sinne der Art. 10 und 11 der NIS-2-Richtlinie wahr. Hiermit einhergegangen ist die Übernahme der Auftraggeberrolle über das CERT Nord.
Perspektivische Umsetzung:
Bei der Etablierung neuer und Pflege bestehender Netzwerke handelt es sich um eine fortwährende Aufgabe, welche durch die Zentralstelle Cybersicherheit wahrgenommen wird.
Ziel:

Zentrale Zuständigkeit und Verantwortung für den Themenbereich Cybersicherheit, um Anfragen aus den entsprechenden Netzwerken gezielt bearbeiten bzw. Anfragen in die Netzwerke gezielt steuern zu können
Übergeordneter Zielbeitrag:
Z.9-1

Maßnahme Nummer 9.2

Handlungserfordernis:
Aufbau von Kooperationsbeziehungen mit anderen Cybersicherheitsbehörden auf Länder- und Bundesebene durch die noch auszugestaltende Zentralstelle Cybersicherheit
Überblick über die aktuelle Umsetzung:
Die Zentralstelle Cybersicherheit hat sowohl zu weiteren Landesbehörden als auch mit Bundesbehörden und Einrichtungen Kontakte geknüpft. Im Rahmen der Aufgabenerfüllung findet hierbei bei Bedarf ein lageangepasster Austausch statt.
Perspektivische Umsetzung:
Die Vernetzung mit Cybersicherheitsbehörden auf Länder- und Bundesebene ist eine fortwährende Aufgabe, welche durch die Zentralstelle Cybersicherheit wahrgenommen wird.
Ziel:
Schaffung von Synergieeffekten sowie Etablierung eines effektiven bilateralen Austauschs, um neue Erkenntnisse schnell und unkompliziert austauschen zu können bzw. bereits vorhandene Kenntnisse und Fähigkeiten nutzen zu können.
Übergeordneter Zielbeitrag:
Z.9-1

7. Zusammenfassung und Ausblick

Die Bremische Cybersicherheitsstrategie 2023 wurde vor dem Hintergrund einer sich rasant wandelnden Bedrohungslage entwickelt. Cyberangriffe auf kritische Infrastrukturen, öffentliche Verwaltungen, Unternehmen und auch Privatpersonen nehmen stetig zu, sowohl in ihrer Häufigkeit als auch in ihrer Professionalität. Ransomware-Angriffe, gezielte Datenlecks, Desinformationskampagnen und hybride Bedrohungen stellen heute eine reale Gefahr für Funktionsfähigkeit, Vertrauen und Stabilität staatlicher Strukturen dar. Für den Zwei-Städte-Staat Bremen mit seiner vielfältigen Cybersicherheitslandschaft ist eine robuste Cybersicherheitsarchitektur damit zum zentralen Bestandteil staatlicher Daseinsvorsorge geworden.

Die Bremische Cybersicherheitsstrategie 2023 verfolgt das Ziel, Cybersicherheit als gemeinsame Aufgabe des gesamten Landes zu verankern: ressortübergreifend, koordiniert und in enger Verzahnung mit Bund, Wirtschaft, Wissenschaft und Zivilgesellschaft. Sie legt den organisatorischen, rechtlichen und kulturellen Rahmen fest, um die digitale Souveränität Bremens zu stärken und die Cyberresilienz langfristig zu sichern und definiert hierzu verschiedene Maßnahmen in neun Handlungsfeldern, die als Grundlage für die Ausarbeitung erster Maßnahmen herangezogen wurden:

- Die Intensivierung der Vernetzung der Cybersicherheitsakteur:innen,
- 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.

Nach der Verabschiedung der Bremischen Cybersicherheitsstrategie durch den Senat am 11.04.2023 wurde in einem ersten Umsetzungsschritt zum 01.05.2023 die Zentralstelle Cybersicherheit beim Senator für Inneres und Sport eingerichtet und somit die bisherige Projektarbeit an der Cybersicherheit in eine dauerhafte und organisatorisch klar verankerte Struktur überführt.

Im Rahmen einer gemeinsamen Kraftanstrengung wurde in den folgenden zwei Jahren in enger Zusammenarbeit mit dem Senator für Finanzen, den übrigen Ressorts sowie dem Magistrat der Stadt Bremerhaven an der Umsetzung der Ziele der Bremischen Cybersicherheitsstrategie gearbeitet. Innerhalb dieses kurzen Zeitraums konnten nicht alle gesteckten Ziele umgesetzt werden; es wurden jedoch einige wichtige Meilensteine erreicht. Diese sollen im Folgenden kurz dargestellt werden, bevor auf zentrale Empfehlungen eingegangen wird sowie ein Ausblick auf die Strategiefortschreibung 2026 gegeben wird.

7.1 Erreichte Meilensteine der Grundlagenphase

Die Evaluation nach rund zwei Jahren zeigt: Die Bremische Cybersicherheitsstrategie hat ihre Grundlagenphase erfolgreich abgeschlossen. Strukturen, Rollen und Prozesse sind geschaffen, die ressortübergreifende Zusammenarbeit hat sich deutlich verbessert und die Cybersicherheit ist als politisches und administratives Handlungsfeld etabliert worden. Hierbei sind einige erreichte Meilensteine besonders hervorzuheben.

Institutionelle Verankerung: Während der Senator für Finanzen die Verantwortung für die Sicherheit der IT der öffentlichen Veraltung trägt, wurde mit der Einrichtung der Zentralstelle Cybersicherheit beim Senator für Inneres und Sport eine dauerhafte und koordinierende Stelle geschaffen, die ressortübergreifend alle übrigen Belange der Cybersicherheit betreut und als zentrale Anlaufstelle für das Land und darüber als etablierte Schnittstelle zum Bund fungiert. Diese institutionelle Verankerung bildet das Rückgrat der bremischen Cybersicherheitsarchitektur und schafft hierdurch klare Ansprechbarkeiten und Verantwortungsbereiche, um die gemeinschaftliche Cybersicherheitsarbeit durch Handlungssicherheit und Rollenklarheit strukturiert zu stärken.

Koordination und Vernetzung: Durch die stetige Vernetzungsarbeit zwischen den an der Cybersicherheitsarbeit im Land Bremen beteiligten Akteur:innen ist eine tragfähige Kooperationsstruktur zwischen den Ressorts, Behörden und weiteren Partner:innen entstanden. Hierdurch wurden Informationsflüsse verbessert und das Vertrauen in die gemeinsame Zusammenarbeit gestärkt, was einen niedrigschwelligen Kontakt und die Ausnutzung vielfältiger Synergien ermöglicht, während Entscheidungen regelmäßig schnell abgestimmt und gefällt werden können.

Rechtliche Grundlagen: Mit der Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2 Ums FHB) wurde ein erster Schritt hin zu einem verbindlichen Rechtsrahmen geschaffen, der die europäischen Cybersicherheits-Anforderungen in die bremische Verwaltungslandschaft integriert und so für Rechtssicherheit und Vergleichbarkeit sorgt. Die perspektivische Weiterentwicklung des Rechtsrahmens mithilfe eines Bremischen Cybersicherheitsbasisgesetzes sowie langfristig eines Bremischen Cybersicherheitsgesetzes ist ein zwingender Schritt, um größtmögliche Handlungssicherheit zu gewährleisten und notwendige Grundlagen zur Stärkung der Cybersicherheit im Land Bremen zu schaffen.

Stärkung technischer Resilienz: In den vergangenen zwei Jahren wurden in den Ressorts sowie dem Magistrat der Stadt Bremerhaven eine Reihe technischer Maßnahmen umgesetzt sowie vorhandene Strukturen in ihrem Reifegrad gestärkt, um die Widerstandsfähigkeit der IT-Strukturen zu verbessern. Hierbei wurde deutlich, dass die fortschreitende Zentralisierung sicherheitsrelevanter Dienste, die Einführung standardisierter Verfahren zum Notfallmanagement sowie die Harmonisierung bestehender Strukturen eine zentrale Rolle einnehmen.

7.2 Zentrale Erkenntnisse der methodischen Evaluation

Die Bewertung entlang des internationalen *National Cybersecurity Strategy Lifecycle* zeigt: Bremen hat den Übergang von der Planungs- zur Umsetzungsphase erfolgreich vollzogen. Die Strategie besitzt eine klare Ausrichtung, hat ein funktionierendes Governance-System etabliert und erste sichtbare Fortschritte produziert. Gleichzeitig zeigt die Analyse jedoch auch, dass die nächste Entwicklungsphase stärker auf Aspekte der Verstetigung, Operationalisierung und Wirkungsmessung ausgerichtet sein sollte. Hierbei sind besonders wichtige Querschnittsempfehlungen hervorzuheben:

Stärkung der Cybersicherheit als integraler Bestandteil der Sicherheitsarchitektur: Das gemeinsame Verständnis der Cybersicherheit als integraler Bestandteil einer ganzheitlichen und kohärenten staatlichen Sicherheitsarchitektur ist von höchster Bedeutung. Dieses generiert politischen Rückhalt und ermöglicht es, richtungsweisende Entscheidungen zu treffen, die sowohl für die Ausrichtung als auch insbesondere die Umsetzung der Cybersicherheitsarbeit im Land erforderlich sind.

Verstetigung von Ressourcen und Strukturen: Um das bisherige Engagement sowie die erfolgreiche Umsetzung von Maßnahmen abzusichern, bedarf es einer ausreichenden Bereitstellung personeller sowie materieller Ressourcen. Eine dauerhafte Verankerung dieser in den Verwaltungsstrukturen schafft Handlungssicherheit und eine verlässliche Umsetzbarkeit für alle an der Produktion der Cybersicherheit beteiligten Akteur:innen.

Systematische Bedrohungsanalyse: Eine differenzierte und systematische Analyse der Bedrohungslage im Land, welche auf regionale Besonderheiten und Strukturen eingeht, stellt die zwingende Voraussetzung für die Erarbeitung spezifischer Maßnahmen dar, welche SMARRTE Kriterien erfüllen und nicht lediglich auf ihre Umsetzung, sondern auch auf ihre Wirksamkeit hin, überprüft werden können.

Messbare Wirksamkeit: Die Einführung eines systematischen Monitoring- und Evaluationsprozesses anhand geeigneter Kennzahlen (KPI) ermöglicht es, Fortschritte systematisch sichtbar und Entwicklungen nachvollziehbar messbar zu machen. Sie stellt die Grundlage für belastbare Priorisierungsentscheidungen dar und ermöglicht es, Informationsbedürfnissen transparent zu begegnen.

Ausbau von Awareness und Qualifizierung: Das zielgruppenorientierte Verständnis spezifischer Cybersicherheitsbedrohungen sowie die Kompetenz, mit diesen umzugehen, stellen maßgebliche Schritte zur Stärkung der gesamtgesellschaftlichen digitalen Resilienz dar. Sie müssen durch einen fortwährenden Ausbau vorhandener Schulungsangebote gestärkt werden.

7.3 Ausblick und Roadmap zur Fortschreibung der Strategie 2026

Die Fortschreibung der Bremischen Cybersicherheitsstrategie im Jahr 2026 markiert den Übergang von einer erfolgreichen Aufbauphase hin zu einer Phase der Konsolidierung und strategischen Vertiefung. Die vergangenen zwei Jahre haben gezeigt, dass das Land Bremen über tragfähige Strukturen, klare Zuständigkeiten und ein stetig wachsendes Netzwerk von Akteur:innen verfügt, welche Cybersicherheit als gemeinsame Aufgabe verstehen. Nun gilt es, diese Grundlagen zu verstetigen und systematisch auf ihnen aufzubauen.

In der nächsten Strategieperiode sollte Cybersicherheit nicht nur organisatorisch, sondern auch operativ stärker in das Verwaltungshandeln integriert werden. Bisher geschaffene Strukturen bilden dafür ein solides Fundament: Koordinationsmechanismen greifen, der Informationsaustausch funktioniert und Zuständigkeiten sind etabliert. Um die Wirksamkeit weiter zu erhöhen, muss Cybersicherheit noch stärker als ganzheitlicher Prozess verstanden werden, der alle Phasen der Planung, Entwicklung, Umsetzung und Evaluierung durchdringt. Dazu gehört es, Erfolge und Fortschritte künftig messbarer zu gestalten, um die Wirkung einzelner Maßnahmen besser nachvollziehen und gezielt steuern zu können.

Ein weiterer Schwerpunkt sollte darin bestehen, bestehende Governance-Strukturen auf politisch-strategischer Ebene zu stärken. Die ressortübergreifende Zusammenarbeit hat sich bewährt, würde jedoch durch klarere Steuerungsimpulse aus der Leitungsebene an Verbindlichkeit gewinnen. Damit ließen sich Prioritäten transparenter festlegen, Entscheidungsprozesse beschleunigen und Ressourcen effizienter einsetzen. Ebenso wichtig ist die dauerhafte Sicherung personeller und finanzieller Kapazitäten, um die bislang projektorientierte Umsetzung in eine stabile, verlässliche Cybersicherheitsarbeit zu überführen.

Zukünftig müssen Maßnahmen stärker an einem systematischen Verständnis von Risiko und Resilienz ausgerichtet werden. Die fortwährende Dynamik der Bedrohungslage erfordert ein vorausschauendes, datenbasiertes Risikomanagement, das sowohl technische als auch organisatorische Aspekte berücksichtigt. Durch die engere Verzahnung mit den Sicherheitsbehörden des Bundes kann Bremen seine Position im föderalen Sicherheitsverbund darüber hinaus weiter festigen und seine Handlungssicherheit erhöhen.

Auch der gesellschaftliche Aspekt von Cybersicherheit sollte in der nächsten Strategiephase stärker in den Fokus rücken, um auf dem Weg der Sensibilisierung zur aktiven Befähigung voranzuschreiten. Es gilt, Cybersicherheit als Bestandteil einer modernen Sicherheitskultur gesamtgesellschaftlich zu etablieren. Die Förderung von Kompetenzen und Verantwortungsbewusstsein bildet damit nicht nur eine Ergänzung technischer Maßnahmen, sondern ist eine zentrale Voraussetzung für langfristige Resilienz der Bevölkerung.

Das Land Bremen steht an einem Punkt, an dem die Grundlagen gelegt und funktionsfähige Strukturen aufgebaut wurden. Die Fortschreibung der Strategie 2026 bietet die Gelegenheit, den erfolgreichen Aufbau zu einer konsolidierten, lernenden und wirkungsorientierten Cybersicherheitsarchitektur weiterzuentwickeln. Entscheidend ist nun, die erreichten Fortschritte zu verstetigen, bestehende Maßnahmen zu vertiefen und neue Impulse auf Basis der bisherigen Erfahrungen zu setzen. Damit kann das Land Bremen den eingeschlagenen Weg konsequent fortsetzen und seine Rolle als verlässlicher, innovativer und vorausschauender Akteur im Bereich der Cybersicherheit weiter ausbauen.

Impressum

Freie Hansestadt Bremen

Herausgeberin

Die Senatorin für Inneres und Sport
im Auftrag des Senats der Freien Hansestadt Bremen

Stand: Dezember 2025

Copyright

Die Senatorin für Inneres und Sport, Freie Hansestadt Bremen, 2025

Die Vervielfältigung und Verbreitung dieses Dokuments werden, auch auszugsweise, mit Quellenangabe gestattet.

Bildnachweis

Sämtliche Bilder und Tabellen wurden, wo nicht separat ausgewiesen, durch die Zentralstelle Cybersicherheit erstellt.

Deckblattgestaltung: Zentralstelle Cybersicherheit