Cybersicherheitsstrategie für den Sektor Öffentliche Verwaltung im Land Berlin (Landesverwaltung Berlin)

Version 1.0 F

Stand: 12.08.2025

Der Regierende Bürgermeister von Berlin

Senatskanzlei

Dokumenteninformationen

BEZEICHNUNG	INHALT	BEARBEITUNGSHINWEIS
Autor	Klaus-Peter Waniek, Senatskanzlei, Landesbevollmächtigter für Informationssicherheit des Landes Berlin	[Stellenzeichen: Verantwortliche Person Fachbereich für die Erstellung und Pflege des Dokuments]
Status	Final	[Entwurf, Vorlage zur Freigabe, Final]
Klassifizierung	Nur für Dienstgebrauch	[Einstufung nach Sicherheitsanforderungen]
Dokumenten-Kennung	Cybersicherheitsstrategie_Sektor_ÖV_Berlin_V1.0F	[Die Dokumenten-Kennung wird vom Landes-InfSiBe vergeben]
Dokumententyp	Landesweite Strategie	[Typ des Dokumentes Richtlinie, Arbeitsanweisung, etc.]
Titel des Dokuments	Cybersicherheitsstrategie für den Sektor Öffentliche Verwaltung Land Berlin (Landesverwaltung Berlin)	[Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.]
Version	V 1.0 F	[E=Entwurf, V=Vorlage zur Freigabe, F=Finales Dokument freigegeben]
Dateiname	20250725_Cybersicherheitsstrategie_Sektor_ÖV_Berlin-V1.0 F	[Name der Datei, Hinweis: keine Leerzeichen, sondern Unterstriche nutzen]
Speicherort		[Ablageort]
Freigabedatum	12.08.2025	[Datum der Freigabe]
Freigabe durch	CDO	[Stellenzeichen: Verantwortliche Person für die Freigabe- CDO]
Revisionsdatum	Klicken oder tippen Sie, um ein Datum einzugeben.	[Datum der nächsten Überprüfung; mindestens alle 2 Jahre]
Verteiler		[Mitarbeitendenportal oder spezifischer Verteiler]

Tabelle 1: Informationen zur Dokumentenlenkung

Inhaltsverzeichnis

Vorwort

Berlin ist nicht nur Stadt, Hauptstadt und Bundesland zugleich - Berlin erhebt auch den Anspruch, das Innovationszentrum der Bundesrepublik Deutschlands zu sein. Gleichzeitig steht Berlin vor der Aufgabe, die digitale Transformation voranzutreiben und sie zugleich auch sicher und nachhaltig zu gestalten. Digitalisierung und Cybersicherheit sind dabei untrennbar miteinander verbunden – insbesondere auch aufgrund der vielfältigen Landesbehörden, kommunalen Einrichtungen und öffentlichen Dienstleistungen. Vor diesem Hintergrund treibt diese Cybersicherheitsstrategie das Ziel voran, ein zukunftsfähiges, resilient aufgestelltes Verwaltungsnetzwerk zu schaffen – digital souverän, sicher, effizient und handlungsfähig.

Die vorliegende Cybersicherheitsstrategie schafft einen Rahmen, um die digitale Infrastruktur der Berliner Landesverwaltung zu schützen, die Resilienz gegenüber Cyberbedrohungen zu stärken und das Vertrauen der Bürgerinnen und Bürger in digitale Angebote der Verwaltung zu fördern. Die Bedrohungslage im Cyberraum nimmt stetig zu. Angriffe auf öffentliche Einrichtungen, Unternehmen und kritische Infrastrukturen werden zunehmen mehr, wie der aktuelle Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) zeigt.

Staat, Wirtschaft und Gesellschaft müssen vor diesen Gefahren geschützt werden. Gleichzeitig bietet die Digitalisierung dem Land Berlin enorme Chancen – von einer modernen, bürgernahen Verwaltung bis hin zu einer dynamischen Wirtschaft, die von Innovation und digitaler Souveränität profitiert. Diese Cybersicherheitsstrategie verfolgt daher einen ganzheitlichen Ansatz, der auf den Prinzipien der Zusammenarbeit, Prävention und Resilienz basiert. Sie ist eng mit der Cybersicherheitsstrategie des Bundes verzahnt und berücksichtigt die föderalen Besonderheiten Berlins. Gemeinsam mit den anderen Bundesländern arbeiten wir in der Digitalministerkonferenz daran, ein harmonisiertes Cybersicherheitsniveau für die gesamte Bundesrepublik Deutschland zu schaffen, das den Herausforderungen der digitalen Welt gerecht wird. Dabei setzt Berlin auf eine enge Kooperation mit Wirtschaft, Wissenschaft und Zivilgesellschaft, um innovative Lösungen zu entwickeln.

Unsere Vision für Berlin lautet: Eine öffentliche Verwaltung, die moderne digitale Dienstleistungen sicher bereitstellen kann, Daten integritätsgesichert verwaltet, Vertrauen schafft sowie Cyberangriffe früh erkennt und wirksam abwehrt. Mit dieser Strategie wollen wir den Weg dorthin aktiv gestalten.

Die Umsetzung dieser Strategie ist eine gesamtgesellschaftliche Aufgabe, die nur gemeinsam gemeistert werden kann. Mit klaren Leitlinien, definierten Handlungsfeldern und einem transparenten Berichtswesen schaffen wir die Grundlage für eine sichere digitale Zukunft unserer. Berlins. Gemeinsam mit unseren Partnern im Bund, in den Ländern und in der Wirtschaft stellen wir die Weichen dafür, dass Berlin eine sichere und widerstandsfähige Weltmetropole bleibt.

Martina Klement
Staatssekretärin für Digitalisierung und Verwaltungsmodernisierung
Chief Digital Officer des Landes Berlin

Einleitung

In einer Zeit, in der die Digitalisierung in allen Lebensbereichen zunehmend an Bedeutung gewinnt, steht Berlin vor der Herausforderung, die Chancen und Möglichkeiten, die sich daraus ergeben, bestmöglich zu nutzen. Als pulsierende Hauptstadt Deutschlands und eine der führenden digitalen Metropolen Europas ist Berlin besonders von den Chancen und Herausforderungen der Digitalisierung betroffen. Digitale Innovationen durchdringen den Alltag der Berlinerinnen und Berliner, transformieren die Art und Weise, wie in unserer Stadt gearbeitet, gelernt und kommuniziert wird.

Die fortschreitende Digitalisierung in der Berliner Verwaltung bringt allerdings nicht nur Chancen, sondern auch Risiken mit sich. Die Bedrohung durch Cyberangriffe, die persönliche Daten, die Infrastrukturen der Stadt und die Grundlagen der Demokratie gefährden, wächst stetig an. Das Vertrauen in die digitale Transformation gilt es deshalb zu bewahren und zu stärken.

Besonders die Bundeshauptstadt Berlin benötigt aufgrund ihrer politischen und wirtschaftlichen Bedeutung einen erhöhten Sicherheitsstandard. Die Jahresberichte des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie die Berichterstattung über sich häufende Sicherheitsvorfälle verdeutlichen die Bedeutung der Informationssicherheit für eine sichere Digitalisierung. Immer häufiger werden Einrichtungen der öffentlichen Verwaltung durch Cyberangriffe beeinträchtigt.

Die Gewährleistung von Cyber- und Informationssicherheit ist ein unmittelbarer Erfolgsfaktor für das Wohlergehen und den Schutz der Berliner Verwaltung. Die stetig zu beobachtende Professionalisierung der Cyber-Angriffsmethoden und die gravierenden Folgen von Ransomware-Angriffen, die steigende Vielfalt von Schadprogramm-Varianten und kritische Schwachstellen in verbreiteten Softwareprodukten belegen, dass die Cyber- und Informationssicherheit kontinuierlich gestärkt werden muss. Zur Unterstützung dieses Ziels müssen nachhaltige finanzielle Rahmenbedingungen geschaffen werden, um das notwendige Informationssicherheitsniveau der öffentlichen Verwaltung zu ermöglichen. Aufgrund des ständig wachsenden Ausmaßes an Cyberangriffen muss der Schutz davor gestärkt werden und die Informationssicherheit in der Berliner Verwaltung höchste Priorität haben.

Die Cybersicherheitsstrategie für den Sektor Öffentliche Verwaltung im Land Berlin umfasst sechs spezifische Handlungsfelder, die von der Cybersicherheit der Landesverwaltung Berlin über die Vernetzung der Cybersicherheitsakteure über Förderung von Innovationen bis hin zu Kooperationen reichen. Jedes dieser Felder ist essentiell, um ein hohes Niveau an Cybersicherheit in Berlin zu gewährleisten und die digitale Resilienz der Stadt zu fördern.

Diese Cybersicherheitsstrategie ist ein klares Bekenntnis zu einer sicheren, vertrauenswürdigen und inklusiven digitalen Zukunft für alle Berlinerinnen und Berliner. Die Vorteile der Verwaltungsdigitalisierung sollen genutzt werden, ohne dabei die Sicherheit und die Grundrechte der Bürgerinnen und Bürger zu gefährden. Alle Beteiligten sind eingeladen, sich an diesem wichtigen Prozess zu beteiligen und zusammenzuarbeiten, um Berlin zu einer noch sichereren und widerstandsfähigeren digitalen Stadt zu machen.

Mit dieser Cybersicherheitsstrategie für den Sektor Öffentliche Verwaltung des Landes Berlin wird ein ganzheitlicher Ansatz verfolgt, der alle relevanten Akteure einbindet und die Resilienz der digitalen Infrastrukturen stärkt. Auf Prävention, Sensibilisierung und die Förderung digitaler Kompetenzen wird gesetzt, um die öffentliche Verwaltung gegenüber Cyberbedrohungen zu stärken.

1. Grundsatz

1.1. Zielstellung und Vision

Diese Cybersicherheitsstrategie dient dem Ziel, die Landesverwaltung Berlin, die Berliner Infrastruktur, die Bürgerinnen und Bürger sowie die Wirtschaft vor Cyberkriminalität und digitaler Bedrohungen in zunehmend digital geprägten Lebenslagen zu schützen.

Die Umsetzung der Cybersicherheitsstrategie ist ein dynamischer Prozess, der Flexibilität und Anpassungsfähigkeit erfordert. Da sich die digitale Landschaft kontinuierlich verändert und neue Bedrohungen entstehen, wird die Strategie regelmäßig überprüft und weiterentwickelt, um sicherzustellen, dass sie stets den aktuellen und zukünftigen Herausforderungen gerecht wird.

Die Vision für Berlin ist eine digitale Stadt, die durch eine robuste und dynamische Cybersicherheitsstrategie gesichert wird.

Durch fortlaufende Zusammenarbeit aller Beteiligten, kontinuierliche Anpassung an neue Bedrohungen und eine starke Fokussierung auf Prävention und Bildung soll Berlin zu einem Ort werden, an dem digitale Sicherheit und technologische Exzellenz Hand in Hand gehen. Diese Cybersicherheitsstrategie baut deshalb auf den Erfahrungen und Erkenntnissen aus nationalen und internationalen Strategien auf und passt diese an die spezifischen Bedürfnisse und Gegebenheiten der Stadt an. Ein ganzheitlicher Ansatz wird verfolgt, der alle relevanten Akteure einbindet und die Resilienz der digitalen Infrastrukturen stärkt. Auf Prävention, Sensibilisierung und die Förderung digitaler Kompetenzen wird gesetzt, um die Bürgerinnen und Bürger Berlins, die Wirtschaft, die Wissenschaft und die öffentliche Verwaltung gegenüber Cyberbedrohungen zu stärken.

1.2. Rechtliche Rahmenbedingungen

Die gegenwärtigen rechtlichen Rahmenbedingungen schaffen für die Cybersicherheit des Sektors Öffentliche Verwaltung eine Handlungsgrundlage für Maßnahmen, um für die sich ändernden Anforderungen des digitalen Zeitalters resilient und zukunftsfähig zu bleiben.

1.2.1. E-Government Gesetz Berlin

Das seit Mai 2016 geltende E-Government Gesetz Berlin (EGovG Bln) hat zum Ziel, Verwaltungsverfahren und -strukturen aller Verwaltungsebenen und -bereiche der Berliner Verwaltung unter Nutzung der Möglichkeiten der IKT umzustellen. Demnach ist nach § 21 „der IKT-Staatssekretär oder die IKT-Staatssekretärin ... zuständig für die alle Verwaltungsebenen und -bereiche umfassende Förderung, Weiterentwicklung und flächendeckende Einführung von E-Government und Informations- und Kommunikationstechnologie in der Berliner Verwaltung und für Verwaltungsmodernisierung im Sinne des § 2.“ Im folgenden Absatz 3 des § 21 umfasst die Zuständigkeit auch die „Festsetzung und Überwachung der Einführung der Standards für einen sicheren, wirtschaftlichen, benutzerfreundlichen und medienbruchfreien IKT-Einsatz.“ Daraus ist die Gewährleistung der Cybersicherheit für die IKT-Architektur der Landesverwaltung Berlin abzuleiten.

1.2.2. NIS-2-Richtlinie

Die Richtlinie (EU) 2022/2055 des Europäischen Parlaments ist seit dem 16. Januar 2023 in Kraft und gibt Maßnahmen für ein gemeinsame Cybersicherheit auf hohem Niveau in der Union vor. Gemäß Artikel 7 der Richtlinie obliegt es jedem Mitgliedsstaat, eine nationale Cybersicherheitsstrategie zu erlassen. Darin sollen „die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessen politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus“ enthalten sein. Aufgrund der föderalen Struktur der Bundesrepublik Deutschland besteht für die Bundesländer die Anforderung, jeweils eine eigene Cybersicherheitsstrategie zu verfassen und umzusetzen.

1.2.3. Leitlinie zur Entwicklung föderaler Cybersichersicherheitsstrategien

Für die nachhaltige Stärkung der föderal gekennzeichneten Cybersicherheitsarchitektur hat die Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz (IMK) die Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien im Jahr 2021 erarbeitet. Darin sind die wichtigsten Handlungsfelder sowie Zielgruppen benannt, die bei der Konzeption einer Cybersicherheitsstrategie von den Ländern zur Orientierung zu nutzen sind, um eine Standardisierung der Cybersicherheitsarchitektur zu erreichen. Die vorliegende Cybersicherheitsstrategie der Landesverwaltung Berlin hat die Handlungsfelder der Leitlinie bei der Konzeption berücksichtigt.

1.3. Fokussierung auf den Sektor Öffentliche Verwaltung Land Berlin

Die thematischen Schwerpunkte und Aufgaben im Sektor Öffentliche Verwaltung des Landes Berlin (Berliner Landesverwaltung) leiten sich aus den Vorgaben des E-Government-Gesetzes Berlin zur IKT-Sicherheitsstrategie und der Umsetzung des Informationssicherheitsmanagementsystems (ISMS) nach den Standards des BSI ab. Zur Gewährleistung eines vergleichbaren Informationssicherheitsniveaus zwischen den Bundesländern und mit dem Bund wurde u.a. zur Etablierung ebenenübergreifender Verfahren vom IT-Planungsrat (IT-PlR) die Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018 (Beschluss 2019/04) beschlossen. Zur Leitlinie des IT-Planungsrates wurde im Jahr 2020 ein Umsetzungsplan mit Maßnahmen und Ziele beschlossen (Beschluss 2020/05). Im Umsetzungsplan zur Leitlinie für Informationssicherheit für die öffentliche Verwaltung 2018 werden die Handlungsfelder zur systematischen Verbesserung des Informationssicherheitsniveaus mit konkreten Maßnahmen und messbaren Zielen unterlegt, die spezifisch, konkret und auch messbar sind. Sowohl zum Informationssicherheitsmanagement in der Landesverwaltung Berlin als auch zur Umsetzung der Leitlinie des IT-Planungsrates erfolgt eine jährliche Berichterstattung, um den Fortschritt und die Wirksamkeit der umgesetzten Maßnahmen zu dokumentieren und zu bewerten.

2. Handlungsfelder der Cybersicherheits-Strategie der Landesverwaltung Berlin

2.1. Informationssicherheitsmanagement

Die nach dem E-Government-Gesetz Berlin bestehende gesetzliche Verpflichtung zum Aufbau und zur Weiterentwicklung eines Informationssicherheitsmanagementsystems (ISMS) nach den Standards des BSI in der Landesverwaltung Berlin ist ein zentrales Element der IKT-Sicherheitsarchitektur Berlins und ein wichtiger Baustein zur Verbesserung der Cybersicherheit. Das ISMS ist aufgrund des umzusetzenden kontinuierlichen Verbesserungsprozesses ein wichtiges Werkzeug für die Steuerung und Lenkung der Informationssicherheit für die jeweilige Leitungsebene. Es gilt, Aufgaben, Aktivitäten und Maßnahmen zu planen, umzusetzen, regelmäßig zu überprüfen und zu verbessern.

Zur Unterstützung der Dokumentation der Maßnahmen im ISMS wird ein ISMS-Tool bereitgestellt, mit dem die Entwicklung transparent und messbar abgebildet und gesteuert werden kann. So wird ermöglicht, dass erforderliche Maßnahmen zur Sicherung und Erhaltung der Informationssicherheit gemäß der aktuellen Sicherheitslage angepasst werden können. Daher ist die Implementierung und Pflege eines Informationssicherheitsmanagementsystems (ISMS) von entscheidender Bedeutung für die Erhöhung der Cybersicherheit. Die Aktualisierung des ISMS-Tools und die mandantenfähige Nutzung sind zu entwickeln. Dadurch wird erreicht, dass neben der Bereitstellung von Mustervorlagen und Handreichungen standardisiert vorbereitete Bausteine zur Verfügung gestellt werden; z.B. für vom IT-Dienstleister erbrachte IKT-Infrastrukturleistungen, wie der Zugang zum Berliner Landesnetz.

Für die Weiterentwicklung des ISMS zur Stärkung der Cybersicherheit liegen die Schwerpunkte auf zielgruppenbezogenen Maßnahmen zur Schulung und Sensibilisierung, auf der Verbesserung der verfügbaren Ressourcen für das Informationssicherheitsmanagement und auf allen Projekten mit dem Schwerpunkt der Modernisierung von Infrastrukturen, wie beispielsweise die Weiterentwicklung der Mandantenzugänge zum Berliner Landesnetz und die Migration von IKT-Infrastruktur am Verwaltungsarbeitsplatz in die virtuellen Betriebsumgebungen des ITDZ.

2.2. Analyse- und Reaktionsfähigkeit vor Ort stärken

Für die Bewältigung der Herausforderungen der sich dynamisch ändernden und wachsenden Bedrohungslage werden die Einrichtungen der Berliner Landesverwaltung auf der Grundlage der Vorgaben des E-Government-Gesetzes Berlin wirksam durch das beim zentralen IT-Dienstleister, dem ITDZ Berlin, betriebenen Berliner Computer Emergency Response Team (Berlin-CERT) in der Rolle eines zentralen operativen Cybersicherheitsakteurs unterstützt. Für den Schutz des Berliner Landesnetzes, dessen Nutzung für alle Einrichtungen der Berliner Landesverwaltung gemäß der IKT-Architektur verbindlich vorgegeben ist, ist das Berlin-CERT ein essentieller Teil der IKT-Sicherheitsarchitektur. Dessen Wirksamkeit wird insbesondere durch die im E-Government-Gesetz Berlin verankerten Meldeverpflichtungen gewährleistet. Das Berlin-CERT wird als Computer Security Incident Response Team (CSIRT) der Berliner Landesverwaltung Verwaltung gemäß der NIS2-Richtlinie etabliert.

Weitere zentrale Akteure sind neben dem Berlin-CERT das Cyber Defence Center der Landesverwaltung (CDC-LV) mit dem dort betrieben Security Operations Center (SOC) als Cybersicherheitsleitstand sowie die Fachbereiche der zuständigen Abteilung des ITDZ Berlin. Mit dem SOC wird eine kontinuierliche Überwachung zum Schutz der IKT-Infrastrukturen des Landes gewährleistet. Berlin-CERT und CDC-LV mit dem SOC bilden ein Lagezentrum, das nicht nur bei festgestellten Ereignissen

aktiv wird, sondern sofort auf Sicherheitsvorfälle reagieren kann und auch präventiv agiert. Die Leistungen der genannten Akteure stehen den Einrichtungen der Landesverwaltung Berlin durch ein Portfolio von Betriebsverträgen zu Cybersicherheitsdienstleistungen zur Abwehr von Cyberangriffen landesweit zur Verfügung. Zu den Leistungen gehören regelmäßige und anlassbezogene Sicherheitsüberprüfungen von Informationsverbünden mittels Discovery-Scans, Schwachstellen-Scans und Penetrationstests sowie Informationssicherheitsberatungsleistungen.

Bei IT-Sicherheitsvorfällen wird durch das CDC-LV und das Berlin-CERT neben der zentralen Koordination von Maßnahmen eine direkte Vor-Ort-Unterstützung sichergestellt. Damit wird erreicht, dass Vorfälle durch qualifiziertes Handeln sofort vor Ort analysiert, Beweise gesichert und entsprechende Gegenmaßnahmen eingeleitet werden können. Zu den bestehenden Analyse- und Reaktionskompetenzen des IT-Dienstleisters und der dort aktiven Akteure sollen weitere hinzukommen, um die Schwerpunkte Weiterentwicklung der Detektions- und Response-Fähigkeiten, Spam-Analyse-Plattform sowie die Weiterentwicklung des Schwachstellenmanagements abzudecken.

Begleitet werden diese Vorhaben durch Maßnahmen der Konsolidierung der Infrastruktur in den Einrichtungen der Landesverwaltung Berlin, wo im Rahmen des Programmes OneIT@Berlin der dezentrale Infrastrukturbetrieb der Verwaltungsarbeitsplätze in die vom IT-Dienstleister bereitgestellte virtuelle Betriebsumgebung überführt wird. Im Ergebnis werden dadurch ressourcenbedingt Verbesserungen für das Informationssicherheitsmanagement der Einrichtungen der Landesverwaltung erwartet.

2.3. Gemeinsame Abwehr von IT-Angriffen

Die gemeinsame Abwehr von IT-Angriffen auf die Infrastruktur der Berliner Landesverwaltung erfolgt im Wege der koordinierten Zusammenarbeit der Cybersicherheitsakteure auf Landesebene und länderübergreifend, wobei die etablierten Informations- und Kommunikationskanäle wirksam zum Tragen kommen. Auf Landesebene sind primär das IKT- und Informationssicherheitsmanagement der Einrichtungen der Landesverwaltung, das im ITDZ etablierte Berlin-CERT und das Cyber-Defence-Center der Landesverwaltung (CDC-LV) sowie ereignisbezogen weitere Akteure der Gefahrenabwehr des Landes (z.B. Wirtschafts- und Sabotageschutz) einbezogen.

Auf Grund der zunehmenden Vernetzung der Infrastrukturen zwischen den Ländern und dem Bund werden Ereignisse im Verwaltungs-CERT-Verbund (VCV) kommuniziert und gemeinsame Maßnahmen koordiniert. Dieser Verbund spielt eine zentrale Rolle beim Informationsaustausch und der Unterstützung bei der Abwehr von IT-Angriffen. Die Zusammenarbeit zwischen dem BSI und den Cybersicherheitsakteuren des Landes Berlin optimiert die Reaktionsfähigkeit und stärkt die Verteidigung gegen Cyberbedrohungen.

Im Rahmen dieser Zusammenarbeit werden von den jeweiligen die Erkenntnisse erlangenden Stellen - unter Wahrung der Anforderungen an Vertraulichkeit - in geeigneter Weise Informationen zu Sicherheitslücken sowie Hinweise auf mögliche Cyberangriffe bzw. deren Erkennung geteilt und unterstützende technische Informationen wie beispielsweise als Indicators of Compromise (IoC) adressatengerecht übermittelt. Die Übermittlung von IoCs erfolgt zumeist anlassbezogen - also erst, wenn Sicherheitsvorfälle im Erkenntnisbereich der die Information teilenden Behörde eingetreten sind bzw. eine potentielle Bedrohung identifiziert wurde. Diese anlassbezogene Bereitstellung ermöglicht es den beteiligten Akteuren, unmittelbar nach Bekanntwerden eines Sachverhaltes gezielte Schutzmaßnahmen in ihren Infrastrukturumgebungen und Netzwerken umzusetzen.

Eine besonders effektive Methode zur Verwaltung und Verbreitung dieser IoC-Informationen ist die Nutzung mittels Malware Information Sharing Plattform (MISP). Solche Plattformen ermöglichen eine strukturierte und koordinierte Verbreitung der IoC-Listen und verbessern somit die Reaktionsfähigkeit

aller Beteiligten. Durch die zentrale Steuerung und zeitnahe Bereitstellung der IoCs können Sicherheitslücken schneller geschlossen und potenzielle Schäden minimiert werden. Die Einrichtung und Vernetzung von MISP ist ein strategisch wichtiges Instrument zum Schutz der Infrastrukturen der Öffentlichen Verwaltung.

Eine weitere Form zur Übung der gemeinsamen Abwehr von IT-Angriffen ist die unter Federführung von BBK, BMI und BSI regelmäßig durchgeführte länder- und ressortübergreifenden Krisenmanagement-Übung (LÜKEX). Berlin beteiligt sich aktiv an diesen Übungen und führt dazu auf die Übungsinhalte abgestimmte Schulungen durch.

2.4. IKT-Business Continuity Management (IKT-BCM)

IT-Systeme können niemals vollständig gegen alle potenziellen Bedrohungen abgesichert werden, da nach Eintrittshäufigkeit und Schadwert als tragbar bewertete Risiken stets bestehen bleiben. So werden immer neue Schwachstellen gefunden, die häufig zuerst von Angreifern entdeckt und ausgenutzt werden. Auf die daraus möglichen IKT-Notfälle gilt es u.a. mittels einer strukturierten Vorsorge zur IKT-Geschäftsfortführung (IKT-BCM) auf der Basis der Standards des BSI entwickelter Konzepte angemessen vorbereitet zu sein. Diese Konzepte sollten auf der Grundlage der regulären Landeskonzepte situationsbezogen die besonderen Rollen und Aufgaben und deren personelle Zuordnung wiedergeben. Damit wird für das IKT-BCM gewährleistet, dass es integraler Bestandteil des umfassenden Geschäftsfortführungsmanagement (Business Continuity Management - BCM) jeder Organisation ist. Derzeit erfolgt die IKT-Notfallbewältigung in den meisten Einrichtungen reaktiv. Bisher vorliegende Konzepte und Strukturen bilden die Voraussetzung für die Entwicklung eines Geschäftsfortführungsmanagementsystems (BCMS) mit einem höheren Reifegrad.

Die umgesetzten und kontinuierlich weiterentwickelten Maßnahmen der Landesverwaltung Berlin tragen wirksam zum BCM bei. Dazu gehören Maßnahmen zur regelmäßigen Sensibilisierung der Beschäftigten, Notfallschulungen für Verantwortliche sowie angekündigte und unangekündigte Notfallübungen. Dabei wird in Erfüllung der nach dem E-Government-Gesetz Berlin bestehenden Verpflichtung durch die IKT-Steuerung mindestens eine behördenübergreifende Notfallübung unter Einbeziehung des ITDZ Berlin als IT-Dienstleister der Berliner Verwaltung mit Begleitung und Auswertung durch eine zertifizierten externen Dienstleister durchgeführt. Die Durchführung der Übung erfolgt seit 2020 regelmäßig mit wechselnden Szenarien und bis zu 5 teilnehmenden Behörden. Dies sensibilisiert die Führungskräfte der Behörden für die Bedeutung eines funktionierenden IKT-BCM (IKT-Notfallmanagements). Für die wirksame Vorbereitung und Zusammenarbeit bei Vorfällen wurde festgestellt, dass sich das einheitliche Werkzeug, das für die Verwaltung digitaler Daten im Katastrophenschutz genutzt wird dahingehend erweitern lässt, dass die für das IKT-BCM erforderlichen Daten (IKT-Notfalldaten) ebenfalls aufgenommen werden. Mit der Integration der IKT-BCM Prozesse in das etablierte Werkzeug des Katastrophenschutzes wird gewährleistet, dass bei einem IKT-BCM-Vorfall bereits alle verfügbaren Informationen eingegeben werden. Diese können weiter genutzt werden, wenn sich ein IKT-BCM Notfall zu einer Krise oder Katastrophe entwickelt.

2.5. Revision rechtlicher Rahmenbedingungen

Berlin beteiligt sich aktiv am nationalen und internationalen Diskurs zur Cybersicherheit, wobei der Schwerpunkt derzeit auf der nationalen Ebene liegt. Das Land Berlin setzt sich kontinuierlich mit den erforderlichen Anpassungen der rechtlichen und institutionellen Rahmenbedingungen auseinander

und arbeitet daran, diese fortlaufend zu verbessern, um eine umfassende Cybersicherheit zu gewährleisten.

Hinsichtlich der übergreifenden Anforderungen im Verwaltungshandeln zwischen den Ländern und dem Bund wirkt Berlin im Rahmen des IT-Planungsrates und seiner Gremien und bei der Umsetzung der Beschlüsse aktiv mit.

Der erforderliche Prozess wurde unter Einbeziehung aller Stakeholder begonnen, um die Bedingungen für eine effektive Verbesserung der Cybersicherheit auf Landesebene zu schaffen. Damit werden auch die zur Gewährleistung der Cybersicherheit geltenden Regelungen u.a. in den §§ 20-23 des E-Government-Gesetzes Berlin gemäß der aktuellen Rechtslage evaluiert und fortgeschrieben. Die aktuellen Anforderungen an die Landesverwaltung werden bereits jetzt bei der Fortschreibung der IKT-Architektur und IKT-Sicherheitsarchitektur berücksichtigt und aufgenommen.

3. Vernetzung mit Cybersicherheitsakteuren intensivieren

Cybersicherheit betrifft Verwaltung, Wissenschaft, Wirtschaft und weitere gesellschaftliche Bereiche gleichermaßen. Es wird immer wichtiger, gegen klassische, aber auch gegen hybride Bedrohungen durch staatliche oder nichtstaatliche Akteure Schutzstrategien zu entwickeln. Damit ist Cybersicherheit auch ein zentrales Element einer ressortübergreifenden Sicherheitspolitik, Über die Jahre hinweg hat sich ein komplexes Netzwerk verschiedener Akteure im Bereich der Cybersicherheit gebildet. Diese Komplexität kann die Suche nach Ansprechstellen erschweren und die Effizienz im Zusammenwirken der Akteure beeinträchtigen.

Die Einrichtungen der Berliner Landesverwaltung stellen sektorspezifische Cybersicherheitsakteure dar. Durch die übergreifende Vernetzung bringen sie ihre jeweiligen sektorspezifische Kompetenzen in die Cybersicherheitsstrategie ein.

Innerhalb des Landes Berlin koordiniert der Geschäftsbereich der bzw. des Chief Digital Officer (CDO) die Digitalisierung der Landesverwaltung, die mit dem ITDZ Berlin als IT-Dienstleister der Berliner Verwaltung sowie anderen städtischen und regionalen Akteuren umgesetzt wird. Die Kommunikation zwischen den verschiedenen Cybersicherheitsakteuren erfolgt durch Koordinationsmeetings und Strategiegespräche, um die Abstimmung der verschiedenen digitalen Initiativen sicherzustellen.

Das ITDZ Berlin ist nicht nur der zentrale IT-Dienstleister des Landes Berlin, sondern auch mit den Dienstleistungen u.a. zum Berliner Computer Emergency Response Team (Berlin-CERT) und dem Cyber Defense Center der Landesverwaltung (CDC-LV) beauftragt. Diese Bereiche sind unterstützen die Einrichtungen der Landesverwaltung und arbeiten gemeinsam daran, die Informations- und Cybersicherheit für den Sektor Öffentliche Verwaltung in Berlin zu gewährleisten. Die Kommunikation zwischen den verschiedenen Cybersicherheitsakteuren erfolgt über interne Plattformen und Netzwerke, die den Austausch von Informationen und die Koordination von Sicherheitsmaßnahmen ermöglichen.

Das Berlin-CERT im ITDZ bearbeitet IT-Sicherheitsvorfälle und arbeitet eng mit dem CDC-LV zusammen, um Cyberbedrohungen zu analysieren und abzuwehren. Durch Incident Reports und technische Meetings wird der Informationsaustausch über Sicherheitsvorfälle und -lösungen sichergestellt. Das CDC-LV überwacht IT-Systeme in Echtzeit, kooperiert mit dem Berlin-CERT im ITDZ und betreibt unterstützend ein Security Operations Center (SOC). Die Kommunikation erfolgt durch Echtzeit-Monitoring-Systeme und Alarmierungsprotokolle, die eine schnelle Reaktion auf Bedrohungen ermöglichen.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) kontrolliert und berät zur Einhaltung der Regelungen zum Datenschutz und zur Informationsfreiheit. Die Einhaltung und Umsetzung der Modelle und Konzepte durch die Einrichtungen der Landesverwaltung Berlin und deren IT-Dienstleistungsunternehmen verhindern Datenschutzverletzungen und tragen durch die Vorgabe von technischen und organisatorischen Maßnahmen wesentlich zum Schutz gegen Cybersicherheitsbedrohungen bei.

Die Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt (LKA) Berlin berät Unternehmen bei Cybervorfällen und kooperiert mit dem ITDZ Berlin sowie der Staatsanwaltschaft Berlin bei Maßnahmen, um Cyberkriminalität zu bekämpfen. Ihre Beratungsdienste und ihre Unterstützung bei der Krisenkommunikation helfen Unternehmen bei der Behandlung von Sicherheitsfragen und beim Melden von Vorfällen.

Die Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin (Abteilung 257) bekämpft Internetkriminalität und arbeitet eng mit der ZAC und dem Verfassungsschutz Berlin zusammen, um Cyberkriminalität strafrechtlich zu verfolgen. Fallbesprechungen und Ermittlungsberichte gewährleisten den Informationsaustausch zwischen den beteiligten Behörden. Diese Spezialabteilung arbeitet mit anderen Akteuren - wie bspw. dem Verfassungsschutz Berlin und IT-Dienstleistern

- zusammen, um länderübergreifende Sicherheitsmaßnahmen miteinander abzustimmen. Der Austausch erfolgt hauptsächlich durch strategische Workshops und Konferenzen, bei denen gemeinsame Sicherheitsmaßnahmen geplant werden.

Der Verfassungsschutz Berlin überwacht Bedrohungen im Cyberraum und arbeitet ebenfalls eng mit der Zentralen Ansprechstelle Cybercrime (ZAC) und der Staatsanwaltschaft Berlin zusammen, um Cyberkriminalität zu bekämpfen.

An der Unterstützung der Gefahrenabwehrbehörden wirken die Einrichtungen der Landesverwaltung Berlin im Rahmen der entsprechenden Strukturen aktiv mit, damit im Ergebnis die stattliche Handlungsfähigkeit gestärkt wird. Die regelmäßige ganzheitliche Lagebilderstellung wird mittels abgestimmten Inhalten sektorspezifischer Teillagebilder unterstützt, die an die zuständigen Stellen verteilt werden.

Die Sektorenverantwortlichen der Handlungsfelder Wirtschaft und Kritische Infrastrukturen (KRITIS) werden durch den Sektor öffentliche Verwaltung im Rahmen des Verwaltungshandelns der Berliner Landesverwaltung unterstützt.

Länderübergreifend werden für Einrichtungen des Sektors Öffentliche Verwaltung die Aktivitäten im Rahmen des IT-Planungsrates und seiner Gremien koordiniert. Für Sachverhalte der Informationssicherheit erfolgt das Verfahren über die als ständiges Gremium etablierte Arbeitsgruppe Informationssicherheit (AG InfoSic), in dem Vertreter der Länder, der FITKO, des BMI und des BSI das für das Handeln des IT-Planungsrates erforderliche Informationssicherheitsmanagement steuern und in Beschlussempfehlungen zur Umsetzung einbringen. Neben Informationssicherheitsleitlinie und Umsetzungsplan werden Normen und Standards zur länder- und ebenenübergreifenden Sachverhalten entwickelt und fortgeschrieben, sowie spezifische Themenschwerpunkte bearbeitet. Die regelmäßige Kommunikation bzw. Berichterstattung mit weiteren übergreifenden Arbeitsgruppen - wie der Länderarbeitsgruppe (LAG) Cybersicherheit der Innenministerkonferenz, dem Verwaltungs-CERT-Verbund und der AG Verbindungsnetz - gehören zu den Aufgaben der AG InfoSic. Die Erarbeitung und Kommunikation erfolgt durch regelmäßige Treffen, Arbeitsgruppen und Berichte sowie über die beim BSI eingerichtete Geschäftsstelle.

Das BSI bietet den Ländern darüber hinaus auch technische Unterstützung und Beratung in IT-Sicherheitsfragen auf der Grundlage des BSI-Gesetzes und im Wege von Kooperationsvereinbarungen an. Das BSI erhält zudem eine zentrale Stellung für die Erfüllung der Melde-Anforderungen, die sich durch die NIS-2-Richtlinie ergeben. Weiterhin kommuniziert das BSI regelmäßig Lageberichte, Sicherheitswarnungen, technische Leitlinien und unterstützt Sachverhalte der Notfallkommunikation.

Zur Verbesserung des Informationsaustauschs und der Reaktionsfähigkeit der Berliner Landesverwaltung als Cybersicherheitsakteur ist eine bessere Vernetzung im Land Berlin und bundesweit notwendig. Durch eine gestärkte Vernetzung wird ermöglicht, Bedrohungen frühzeitig zu erkennen, gemeinsam zu bewältigen und Präventionsstrategien weiterzuentwickeln. Im Rahmen einer effektiven Cybersicherheitsarchitektur ist daher eine klar abgebildete Struktur der Akteure und Kommunikationswege entscheidend, um einen reibungslosen und effizienten Informationsaustausch sicherzustellen.

3.1. Landesverwaltung Berlin, Wirtschaft und KRITIS

Die Herausforderungen im Handlungsfeld Öffentliche Verwaltung, Wirtschaft und KRITIS betreffen verschiedene Aspekte der Digitalisierung und Cybersicherheit. Bezogen auf die Öffentliche Verwaltung erbringt die Wirtschaft zunehmend unterstützende Leistungen für die Verwaltung. Andererseits benötigt die Wirtschaft Leistungen einer handlungsfähigen Verwaltung. Die Sicherstellung funktionsfähiger und sicherer IKT-Systeme ist daher für die Handlungsfähigkeit der Öffentlichen Verwaltung, den Betrieb kritischer Infrastrukturen und die Wertschöpfung bei kleinen und mittleren Unternehmen essentiell.

Betreiber kritischer Infrastrukturen müssen dabei gesetzliche Vorgaben erfüllen, indem sie bestimmte Schwellenwerte erreichen, um den Melde- und Nachweispflichten gemäß den regulatorischen Anforderungen zu genügen. Dabei nutzen die Betreiber hochkomplexe und stark vernetzte Infrastrukturen, die störungsfrei arbeiten müssen.

Der Schutz vor Cyberangriffen ist ebenfalls von großer Bedeutung, da auch Unternehmen, die nicht unter die KRITIS-Regulierung fallen vor Cyberbedrohungen geschützt werden müssen. Für die Mehrzahl dieser Unternehmen werden zumeist die Schwellenwerte der EU NIS-2-Richtlinie wirksam. Insbesondere kleine und mittlere Unternehmen (KMU) sind aufgrund geringerer finanzieller und personeller Ressourcen digital verwundbarer und somit anfälliger für Cyberangriffe. Die Angriffe können dabei unterschiedlich motiviert sein - von der Schädigung der Gesellschaft und politischer Instabilität bis hin zur Erzielung wirtschaftlichen Profits durch Ransomware.

Kleinen und mittleren Unternehmen fehlen jedoch oft das notwendige Know-how und die Ressourcen, um effektiv auf Cyberangriffe reagieren und ihre IT-Systeme schützen zu können. Daher ist es notwendig, deren Cyber-Resilienz zu erhöhen. Unternehmen müssen präventive Sicherheitsmaßnahmen ergreifen und Kapazitäten aufbauen, um Cyberangriffe abwehren und zentrale Prozesse auch unter außergewöhnlichen Umständen aufrechterhalten zu können. Nur so können die Sicherheit und Funktionsfähigkeit der Wirtschaft und der kritischen Infrastrukturen langfristig gewährleistet werden.

Bereits jetzt werden in Berlin in Zusammenarbeit mit verschiedenen Verbänden, Industrie- und Handelskammern, Handwerkskammern und anderen Multiplikatoren gezielte Beratungs- und Präventionsangebote zu IT- und Cybersicherheitsmaßnahmen in Berlin bereitgestellt. Die Digitalagentur Berlin (DAB) bietet eine Vielzahl von Einzelangeboten und Kooperationen mit Akteuren aus dem Cybersicherheitsbereich an. Dialogplattformen zwischen Staat und Wirtschaft, die den Prozess der Stärkung des Sicherheitsniveaus unterstützen, sind ebenfalls vorhanden.

3.2. Schutz vor Spionage und Sabotage

Die Abteilung II der Senatsverwaltung für Inneres und Sport (SenInnS) hat unter anderem die originäre Aufgabe, die Berliner Wirtschaft - einschließlich KRITIS und IT-Dienstleistungseinrichtungen für Einrichtungen der Öffentlichen Verwaltung, sowie Wissenschafts- und Forschungseinrichtungen - vor Spionageaktivitäten von ausländischen Nachrichtendiensten zu schützen. Hierfür wurde die Zentrale Ansprechstelle Wirtschaftsschutz (ZAW) eingerichtet, die verschiedene Sensibilisierungsmaßnahmen anbietet, um die Wirtschaft vor den Gefahren der Spionage zu schützen. Diese Maßnahmen umfassen auch den Schutz vor Sabotage sowie Bedrohungen durch jede Art von Extremismus.

In der Präventionsarbeit der ZAW geht es darum, Spionage besser erkennbar zu machen, über Akteure und Methoden zu informieren und realistische Bedrohungsszenarien für ein effektives Risikomanagement bereitzustellen. Zudem werden Hinweise und Erfahrungen aus Wirtschaft und Wissenschaft in den Analyseprozess der Spionageabwehr einbezogen, um so die Sicherheit in Wirtschaft, Wissenschaft und Forschung zu erhöhen. Relevante Unternehmen und andere Einrichtungen werden sowohl anlassbezogen als auch proaktiv kontaktiert, um Informations- und Sensibilisierungsgespräche zu führen. Die ZAW steht gleichzeitig als zentraler Ansprechpartner für Sicherheitsanfragen und Verdachtsfälle zur Verfügung. Sofern konkrete Anhaltspunkte für Spionageaktivitäten vorliegen, wird außerdem die Spionageabwehr der Abteilung II aktiv und übernimmt die reaktive Spionageabwehr.

Wirtschaftsunternehmen, die geheimschutzbedürftige Aufträge von Bundes- und Landesbehörden ausführen, müssen vor Ausspähungen ausländischer Nachrichtendienste besonders geschützt werden. Sie werden deshalb in das Geheimschutzverfahren von Bund und Ländern einbezogen, um sicherzustellen,

dass bestimmte Sicherheitsstandards im Umgang mit Verschlusssachen eingehalten werden. Die Abteilung II ist hierbei die mitwirkende Behörde bei den notwendigen Sicherheitsüberprüfungen.

Die Cyberabwehr in Bezug auf nachrichtendienstlich gesteuerte Cyberangriffe, Cyberspionage und Cybersabotage wird für das Land Berlin aufgrund einer Verwaltungsvereinbarung vollumfänglich vom Bundesamt für Verfassungsschutz (BfV) übernommen. Der Wirtschaftsschutz und die Spionageabwehr der Abteilung II unterstützen das BfV bei Präventionsmaßnahmen, wie der Steuerung von Cybersicherheitshinweisen zu aktuellen Angriffskampagnen und dem Versand von IoC-Listen.

Im Rahmen des personellen Sabotageschutzes führt der Geheimschutz der Abteilung II Überprüfungen nach dem Sicherheitsüberprüfungsgesetz durch, wenn Personen an einer „sicherheitsempfindlichen Stelle einer lebens- oder verteidigungswichtigen öffentlichen Einrichtung beschäftigt sind, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben zahlreicher Menschen zu befürchten ist oder für das Funktionieren des Gemeinwesens unverzichtbar ist“ (§ 2 Abs. 1 Nr. 4 BSÜG). Diese Regelung gilt jedoch bisher nicht für privatrechtlich organisierte Einrichtungen. Sofern es sich um sicherheitsempfindliche Stellen in Privatunternehmen handelt, übernimmt das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) die Durchführung der Sicherheitsüberprüfungen und entscheidet im eigenen Ermessen, welche Stellen als besonders sicherheitsempfindlich gelten und welche Unternehmen in die Betreuung aufgenommen werden.

Da die Daseinsvorsorge auch in Berlin zunehmend privatrechtlich organisiert ist, sollte das Land die Kompetenz besitzen, lebens- und verteidigungswichtige Einrichtungen als solche zu definieren und entsprechende Sicherheitsüberprüfungen durchzuführen, um relevante Unternehmen vor innerbetrieblicher Sabotage schützen zu können.

Im Bereich der Cyberabwehr, insbesondere bei nachrichtendienstlich gesteuerten Cyberangriffen, ist das Bundesamt für Verfassungsschutz die zentrale Ansprechstelle für das Land Berlin. Bei der Berliner Polizei gibt es die ZAC für die Wirtschaft, die sich präventiv und reaktiv mit allgemeiner Cyberkriminalität, wie Ransomware, befasst. Die DAB unterstützt Wirtschaftsunternehmen beim Aufbau eines IT-Sicherheitskonzepts und bietet im Falle eines Cyberangriffs eine Cyberhotline an. Zudem vermittelt sie geeignete IT-Sicherheitsdienstleister und unterstützt Unternehmen bei der Digitalisierung.

3.3. Erhöhung der Resilienz gegen Cyberangriffe

Die Erhöhung der Resilienz gegen Cyberangriffe ist für den Sektor Öffentliche Verwaltung in Berlin ein wichtiges Anliegen. Wirksame Schutzschirme gegen Angriffe aus dem Cyberraum wurden entwickelt, um die Resilienz der Wirtschaftsunternehmen zu verbessern. Die Digitalagentur Berlin (DAB) bietet zahlreiche präventive Maßnahmen für Unternehmen sowie Unterstützung im Falle eines Cyberangriffs. Darüber hinaus existieren verschiedene Projekte, zum Beispiel im Rahmen des Masterplans Industriestadt Berlin, die ebenfalls zur Verbesserung der Cybersicherheit beitragen. Die ZAC für die Berliner Wirtschaft bietet in Vorträgen und Präventionsveranstaltungen umfassende Einblicke in aktuelle Phänomene und Bedrohungen des Cybercrime und gibt wichtige Impulse für den Schutz der Unternehmen.

Die Erhöhung der Cybersicherheit ist ein Zusammenspiel folgender Institutionen in der Region.

Dazu zählen die

- ZAC (LKA Berlin)
- Senatsverwaltung für Inneres und Sport, Der Regierende Bürgermeister von Berlin – Senatskanzlei, Senatsverwaltung für Wirtschaft, Energie und Betriebe
- it’s.BB e.V.
- Digitalagentur Berlin (DAB)

- Berlin Partner
- Industrie- und Handelskammer (IHK) Berlin
- Handwerkskammer (HWK) Berlin
- ITDZ, BerlinOnline GmbH
- Unternehmen im Bereich KRITIS und Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

Diese Institutionen arbeiten eng zusammen, um die Resilienz der Dienstleistungsunternehmen der Verwaltung und der kleinen und mittleren Unternehmen in der Region gegen Cyberangriffe zu erhöhen und umfassende Unterstützung bei der Entwicklung und Umsetzung von Cybersicherheitsmaßnahmen zu bieten.

3.4. Öffentlich-private Partnerschaften

Öffentlich-private Partnerschaften sind ein zentrales Element zur Stärkung der Cybersicherheit in Berlin. Diese Partnerschaften bündeln die Expertise und Ressourcen von Akteuren aus der Wirtschaft und verschiedenen Verbänden, um gemeinsame Lösungen für die Herausforderungen im Bereich der Cybersicherheit zu entwickeln. Die Zusammenarbeit mit den Einrichtungen der Landesverwaltung Berlin ermöglicht es, Synergien zu nutzen und effektive Strategien gegen Cyberbedrohungen zu formulieren.

Eine der größten Herausforderungen für Berlin ist die Entwicklung eines kohärenten und belastbaren Rahmens für die Cybersicherheit, der sowohl öffentliche als auch private Akteure einbezieht. Das Ziel dieses Handlungsfeldes ist es, eine robuste Zusammenarbeit zu etablieren, die sowohl präventive Maßnahmen als auch schnelle Reaktionen auf Cybervorfälle ermöglicht. Ein zentraler Fokus liegt auf der Vernetzung und dem Wissensaustausch zwischen den verschiedenen Akteuren, um die Resilienz gegen Cyberangriffe zu erhöhen und den Schutz kritischer Infrastrukturen sicherzustellen.

Eine Bestandsanalyse zeigt, dass Berlin bereits einige erfolgreiche öffentlich-private Partnerschaften aufgebaut hat. Ein hervorzuhebendes Beispiel ist die Zusammenarbeit zwischen it's.BB e.V. und der Digitalagentur Berlin. Gemeinsam haben beide Akteure zusätzlich zu den etablierten Formaten des Wissensaustausches die Cyberhotline konzipiert und umgesetzt, die Unternehmen eine zentrale Anlaufstelle bei Cyberangriffen bietet. Diese Hotline stellt eine wichtige Ressource dar, um schnelle und effiziente Unterstützung zu gewährleisten und somit die Cybersicherheit zu verbessern.

Darüber hinaus spielt der Bundesverband IT-Sicherheit e.V. (TeleTrust) eine wichtige Rolle in der Förderung der Cybersicherheit in Berlin. TeleTrust bringt die Perspektiven der IT-Sicherheitsbranche ein und arbeitet eng mit öffentlichen und privaten Partnern zusammen, um Sicherheitsstandards zu entwickeln und zu verbreiten. Der Verband trägt durch verschiedene Initiativen dazu bei, das Bewusstsein für Cybersicherheitsrisiken zu schärfen und die Zusammenarbeit zwischen Wirtschaft und öffentlicher Hand zu stärken.

Zusätzlich engagieren sich das Forschungsforum Öffentliche Sicherheit und das Zukunftsforum Öffentliche Sicherheit in der Förderung von öffentlich-privaten Partnerschaften. Diese Foren bieten Plattformen für den Austausch zwischen öffentlichen Institutionen, Wissenschaft und Wirtschaft. Sie fördern die Entwicklung von innovativen Lösungen und tragen dazu bei, die Cybersicherheitsstrategien kontinuierlich zu verbessern und an die aktuellen Bedrohungen anzupassen.

4. Weitere Handlungsfelder zur kontinuierlichen Verbesserung

4.1. Förderung digitaler Kompetenzen

Die Digitalisierung durchdringt alle Lebensbereiche und erfordert daher ein hohes Maß an digitalen Kompetenzen. Für die Landesverwaltung Berlin ist es daher erforderlich, eine Kultur der kontinuierlichen Fortbildung zu etablieren, die den Entwicklungen in Bezug auf Informations- und Cybersicherheit sowie dem Schutz der zu verarbeitenden Daten entspricht und die Inhalte angemessen vermittelt.

Aus der steigenden und intensiveren Internetnutzung resultierenden neben den technologisch bedingten Sachverhalten zunehmend auf menschliche Interaktion gerichtete Risiken durch Cyberkriminalität, denen präventiv und auch proaktiv begegnet werden muss. Daher ist es essentiell, dass die Beschäftigten der Verwaltung über die Gefahren im Cyberraum informiert sind und ihr Verhalten entsprechend anpassen, um sich zu schützen und Gefährdungen für die Einrichtungen der Landesverwaltung Berlin zu vermeiden.

Für die Bürgerinnen und Bürger als Kunden der Verwaltung sind geeignete Angebote zu sicherheitsrelevantem Verhalten und zur Stärkung der digitalen Kompetenz durch Dritte z.B. das BSI zugänglich, auf die im Rahmen der digitalen Leistungen Hinweise gegeben werden.

4.2. Awareness

Die Informationssicherheitssensibilisierung für die Einrichtungen der Landesverwaltung Berlin ist der Kernbereich der Cybersicherheits-Awareness. Ziel ist es, ein umfassendes Verständnis für die Risiken und Schutzmaßnahmen zu entwickeln und zu fördern. Damit soll ein ausgeprägtes und aktuelles Bewusstsein für Cyber- und Informationssicherheit erreicht werden, um ein hohes Sicherheitsniveau zu gewährleisten. So wird die Fähigkeit entwickelt und trainiert, bei Cybersicherheitsvorfällen sachgerecht zu agieren. Die begonnenen Prozesse der Bereitstellung von landesweiten Fortbildungs- und Trainingsangeboten sind auf der Basis landesweiter Konzepte und mittels kontinuierlicher Verbesserungsprozessen fortzuführen.

Die Sensibilisierung der Bürgerinnen und Bürger für Sicherheitsaspekte im digitalen Raum ist aus Sicht der Landesverwaltung Berlin im Zusammenhang mit der Leistungserbringung im Rahmen digitaler Verwaltungsangebote ein bedeutsamer Aspekt. Diese Sensibilisierung ist mit Hinweisen auf geeignete vorhandene Unterstützungsangebote begleitend im Kontext digitaler Dienstleistungen zu unterstützen.

4.3. Innovative Forschung und Entwicklung

Eine aktuelle Bestandsanalyse zeigt, dass spezielle Fördermaßnahmen für Start-up-Unternehmen im Bereich der IT-Sicherheit bisher begrenzt sind. Entwickelte Angebote sind nicht spezifisch konzeptionell orientiert und bedürfen einer gezielten Ausrichtung auf die Bedürfnisse der der Landesverwaltung Berlin.

Auf nationaler und europäischer Ebene bestehen unterschiedliche Forschungsverbünde und Netzwerke, die sich mit Cybersicherheit beschäftigen, jedoch dominieren eher regionale Reallabore das Bild.

In Bezug auf prozessorientierte und plattformunterstützte Lösungen für die Zusammenarbeit von Wissenschaft und Wirtschaft gibt es verschiedene Veranstaltungen und Foren - wie beispielsweise den IT-Sicherheitstag der IHK Berlin und der HWK Berlin sowie das Forschungsforum Öffentliche Sicherheit. Diese Plattformen fördern den Austausch und die Entwicklung von innovativen Lösungen, die sowohl wissenschaftliche Erkenntnisse als auch praktische Anwendungen für die Partizipation durch Cybersicherheitsakteure ermöglichen.

Das CityLAB Berlin als Berlins öffentliches Innovationslabor unterstützt die Umsetzung der Smart City- und Digitalstrategie „Gemeinsam Digital: Berlin“ durch die Entwicklung und Förderung innovativer Projekte und Lösungen für die Stadt. In Bezug auf den Sektor Öffentliche Verwaltung in Berlin stellt die Entwicklung resilienter bürgerorientierter Verwaltungsprozesse ein spezifisch zu gestaltendes Themenfeld dar, um die Anforderungen der Cybersicherheit geeignet umzusetzen.

4.4. Kooperationen

Der Cyberraum kennt keine geografischen Grenzen. Schwachstellen in Software oder Hardware stellen damit potentiell globale Risiken dar. Behörden, Unternehmen und Privatpersonen stehen somit vor ähnlichen Herausforderungen, die es zu bewältigen gilt.

Aus diesem Grund sind Kooperationen von entscheidender Bedeutung für die Cybersicherheit. Schwachstellen in Anwendungen können stufenweise Auswirkungen haben, die durch Kooperationsnetzwerke, in denen Informationen und Wissen ausgetauscht werden, besser erkannt und bewertet werden können. Diese Netzwerke helfen dabei, Risiken zu mindern und Abhängigkeiten zu identifizieren. Auch die Vernetzung staatlicher Akteure auf internationaler Ebene ist dabei von großer Bedeutung.

Im Bereich der nationalen und internationalen Kooperationen stehen für Berlin verschiedene Herausforderungen und Ziele im Fokus. Eine genaue Bestandsanalyse zeigt aktuell keine bestehenden Kooperationen oder Kooperationsvereinbarungen mit Gremien.

Auf nationaler Ebene arbeitet Berlin eng mit dem Bund und den anderen Bundesländern zusammen. Die Zusammenarbeit erfolgt im Rahmen der Teilnahme an Fachministerkonferenzen und mit Bezug auf den Sektor Öffentliche Verwaltung in den Gremien des IT-Planungsrat, insbesondere im Rahmen der permanent etablierten Arbeitsgruppe Informationssicherheit (AG InfoSic) und zum Schwerpunktthema Informationssicherheit.

5. Fazit und Ausblick

Die fortschreitende Digitalisierung und die zunehmende Komplexität der Bedrohungslage im Cyberraum stellen auch die Landesverwaltung Berlin vor große Herausforderungen. Cyber- und Informationssicherheit bleiben daher ein zentrales Handlungsfeld der Berliner Verwaltung, das kontinuierlich weiterentwickelt werden muss, um den wachsenden Anforderungen gerecht zu werden. Die vorliegende Cybersicherheitsstrategie setzt hier an und legt den Grundstein für eine systematische und koordinierte Herangehensweise, die an die spezifischen Gegebenheiten der Landesverwaltung der Hauptstadt angepasst ist.

Mit Bezug auf den Sektor Öffentliche Verwaltung wurde mit der vorliegenden Cybersicherheitsstrategie ein Überblick und die Einordnung der bestehenden Initiativen und Akteure im Bereich der Cybersicherheit wiedergegeben. Die Strategie ist das Ergebnis der abgestimmten sektoralen Zuständigkeit, mit der Doppelstrukturen vermieden und eine effiziente und zielgerichtete Umsetzung der Maßnahmen gewährleistet werden soll. Von großer Bedeutung für die zukünftige Entwicklung wird die weitere Intensivierung des bestehenden Vorgehens im Rahmen kontinuierlicher Verbesserungsprozesse sein - sowie das Engagement als Cybersicherheitsakteur des Sektors Öffentliche Verwaltung.

Für Berlin ist es essentiell, die Zusammenarbeit zwischen Bund, Land, Kommunen sowie der Wirtschaft und den Bürgerinnen und Bürgern zu stärken. Es gilt sicherstellen, dass alle Akteure von den Vorteilen der Digitalisierung profitieren und gleichzeitig vor den Risiken des Cyberraums geschützt bleiben. Ein besonderes Augenmerk liegt dabei auf der Unterstützung von Unternehmen, insbesondere von kleinen und mittleren Unternehmen, die bei Cyberangriffen verstärkt Hilfsangebote erhalten sollen. Darüber hinaus wird der Einsatz neuer Technologien, wie das Internet der Dinge und Künstliche Intelligenz, in die Sicherheitsstrategien integriert, um zukünftigen Herausforderungen proaktiv begegnen zu können.

Die Berliner Cybersicherheitsstrategie erkennt die Bedeutung einer fortlaufenden Evaluierung und Anpassung an neue Entwicklungen. Angesichts der dynamischen Bedrohungslage und des rasanten technologischen Fortschrittes ist es unerlässlich, flexibel auf neue Herausforderungen zu reagieren. Dies umfasst die regelmäßige Überprüfung der Strategie sowie die Einbindung der Öffentlichkeit und relevanter Interessengruppen. Dadurch soll sichergestellt werden, dass die Maßnahmen den tatsächlichen Bedürfnissen der Berliner Bevölkerung und Wirtschaft entsprechen.

Geplant ist, die Kooperation und den Informationsaustausch zwischen allen beteiligten Akteuren weiter zu intensivieren. Durch proaktive Kommunikation und Transparenz im Prozess soll eine breite Akzeptanz geschaffen und eine konstruktive Zusammenarbeit weiter gefördert werden. Oberstes Ziel bleibt es, die digitale Resilienz aller Akteure in Berlin zu stärken und die Cybersicherheitsgefahren zu minimieren.

Die vorliegende Cybersicherheitsstrategie stellt damit einen wichtigen Schritt in einem fortlaufenden Prozess dar, der regelmäßig überprüft und weiterentwickelt wird, um den Herausforderungen der digitalen Welt in Berlin erfolgreich zu begegnen.

Anhang: Operationalisierung mit Umsetzungsvorschlägen

Landesverwaltung Berlin – Cybersicherheitsakteur des Sektors öffentliche Verwaltung des Landes Berlin

A.1.1 Informationssicherheitsmanagement

Die gesetzlich vorgegebene Umsetzung des Informationssicherheitsmanagements (ISM) nach den Standards des BSI in allen Einrichtungen der Berliner Landesverwaltung bildet die elementare Grundlage für die Cybersicherheit des Sektors Öffentliche Verwaltung in Berlin. Die kontinuierliche Verbesserung wird orientiert an den Ergebnissen der jährlichen Berichte umgesetzt.

Für die kontinuierlichen Verbesserung der Informations- und Cybersicherheit werden die Einrichtungen der Landesverwaltung mittels mandantenfähig bereitgestellter Werkzeuge zur Dokumentation und Steuerung des Informationssicherheitsmanagementsystems (ISMS) unterstützt. Die Werkzeuge unterstützen die Bereitstellung einheitlicher spezifischer Bausteine in einer geeignet abbildbaren Struktur der Informationsverbünde.

Die bisherige BSI-Zertifizierung von insbesondere landesweit genutzten Informationsverbünden im ITDZ Berlin, wird fortgeführt. Die Erweiterung bzw. weitere Zertifizierung im Kontext der Erhöhung der Netzwerk- und Informationssicherheit wird mit Bezug auf die Mandantenzugänge der Einrichtungen zum Berliner Landesnetz so weiterentwickelt, das eine äquivalente Auditierung nachgewiesen wird.

A.1.2 Analyse- und Reaktionsfähigkeit vor Ort stärken sowie gemeinsame Abwehr von IT-Angriffen gewährleisten

Das Berlin-CERT wird als Computer Security Incident Response Team (CSIRT) der Berliner Landesverwaltung Verwaltung etabliert und die bisherigen Leistungen werden anforderungsgerecht qualitativ und quantitativ weiterentwickelt.

Das Berlin-CERT beteiligt sich aktiv am Verwaltungs-CERT-Verbund das als sektorspezifisches Kooperationsnetz Teil des internationalen CSIRT-Netzwerkes ist. Mittels der raschen und wirksamen operativen Zusammenarbeit sowie dem darüber möglichen Informationsaustausch zwischen den am Netzwerk beteiligten Einrichtungen wird zur Stärkung des Vertrauens beigetragen.

Das Handeln des Berlin-CERTs wird durch das Cyber Defense Center der Landesverwaltung (CDC-LV) unterstützt. Etablierte Vorgehensweisen (z.B. regelmäßige Schwachstellenscans mit anschließender Beratung und Maßnahmenplanung) werden fortgeführt und weiterentwickelt. Mit Unterstützung des CDC-LV werden Maßnahmen zum Ausbau des Schwachstellenmanagements, zur Ausstattung mit modernen Technologien der Cybersicherheitsprävention und auch zum Ausbau der automatisierten Überwachungssysteme realisiert.

Mittels regelmäßiger Übungen und Simulationen von Cyberangriffen wird die kontinuierliche Verbesserung der Einsatzbereitschaft und der Reaktionsfähigkeit der beteiligten Akteure trainiert.

Das Land Berlin schließt eine Kooperationsvereinbarung mit dem BSI ab.

A.1.3 IKT-Business Continuity Management (IKT-BCM)

Das bestehende IKT-Notfallmanagement ist zum IKT-BCM weiterzuentwickeln, das integraler Bestandteil des Business Continuity Management Systems (BCMS) des Landes wird.

Operatives Ziel ist es, zeitnah ein BCMS mit der Stufe Aufbau umzusetzen, in dem wesentliche Prozesse und Dokumentationen (z.B. Meldestrukturen) dokumentiert sind und regelmäßig geübt werden.

Die Teilnahme an länderübergreifenden Übungsformaten (z.B. LÜKEX) erfolgt sektorspezifisch. Mittels der Teilnahme an vorbereitenden Schulungen und Unterweisungen werden die Fähigkeiten für das Zusammenwirken bei sektorübergreifend wirksamen Prozessen zur Cybersicherheit gemäß den jeweiligen Ressortzuständigkeiten weiterentwickelt und trainiert.

A.1.4 Rechtliche Rahmenbedingungen für den Sektor Öffentliche Verwaltung

Mittels der begonnenen Digitalgesetzgebung wird die Fortschreibung und Verbesserung der rechtlichen und institutionellen Rahmenbedingungen zur Stärkung der Cybersicherheit auf allen Ebenen umgesetzt.

Vernetzung mit Cybersicherheitsakteuren intensivieren

Die Einrichtungen der Berliner Landesverwaltung sind sektorspezifische Cybersicherheitsakteure und bringen ihre Kompetenzen im Rahmen der Vernetzung der Cybersicherheitsakteure ein. Die Intensivierung der Vernetzung u.a. durch Plattformen zum vertraulichen Austausch spezifischer Inhalte (z.B. Indicators of Compromise [IoC]) wird im Sinne der gegenseitigen Wirksamkeit unterstützt.

An der Unterstützung der Gefahrenabwehrbehörden wird im Rahmen der entsprechenden Strukturen aktiv mitgewirkt, damit im Ergebnis die stattliche Handlungsfähigkeit gestärkt wird.

Die regelmäßige ganzheitliche Lagebilderstellung wird mittels abgestimmten Inhalten sektorspezifischer Teillagebilder unterstützt. Die sektorspezifische Verteilung der Lagebilder erfolgt an die zuständigen Stellen.

Die Unterstützung des Handlungsfeldes Wirtschaft und KRITIS erfolgt im Rahmen des Verwaltungshandelns der Berliner Landesverwaltung.

Förderung der digitalen Kompetenzen

Kompetenzen mit Bezug zur Cybersicherheit sind Teil einer umfassenden Medienkompetenz. Daher ist es wichtig, diese Kompetenzen zum Schutz vor den ständig wachsenden Bedrohungen im digitalen Raum durch kontinuierliche berufliche Weiterbildung und Ausbau der digitalen Fähigkeiten zu verbessern. Das wird im Rahmen der Bildungsangebote für die Landesverwaltung durch die Aufnahme und Ausweisung von Inhalten der Informationssicherheit und zur präventiven Cybersicherheit unterstützt.

Awareness

Ein ausgeprägtes und aktuelles Bewusstsein für Cyber- und Informationssicherheit ist essentieller Bestandteil zur Gewährleistung eines hohen Niveaus der Cyber- und Informationssicherheit und der Fähigkeit bei Cybersicherheitsvorfällen sachgerecht zu agieren. Durch die weitere Entwicklung landesweiter Bildungsprogramme und Kampagnen soll das Niveau weiter gesteigert und aktuell ausgeprägt werden. Zusätzlich sind zunehmend spezielle, adressatengerechte

Angebote für Führungskräfte, Beschäftigte mit IT-Bezug bzw. andere Stellen mit spezifischen Gefährdungen aus dem Cyberraum zu entwickeln und bereitzustellen.

Als weitere Formate werden Live-Hacking-Angebote sowie Angebote im Rahmen des Europäische Monat der Cybersicherheit (European Cyber Security Month, kurz ECSM), in dem jährlich im Oktober u. a. das Thema Cybersicherheit mit verschiedenen Veranstaltungen und Publikationen nähergebracht wird, genutzt.

Innovative Forschung und Entwicklung

Im Rahmen der fortschreitenden Digitalisierung wird die Entwicklung resilienter bürgerorientierter Verwaltungsprozesse in eine engere Zusammenarbeit zwischen der Landesverwaltung mit GovTech-Campus und CityLab Berlin gefördert, die Anforderungen der Cybersicherheit spezifisch unterstützen.

Kooperationen

Zur Erhöhung der gemeinsamen Cybersicherheitsfähigkeiten sollen seitens der Berliner Landesverwaltung Kooperationen oder Kooperationsvereinbarungen mit dem BSI und weiteren möglichen Gremien geschlossen werden

Abkürzungsverzeichnis

Abkürzung	Erläuterung
AG InfoSic	Arbeitsgruppe Informationssicherheit des IT-Planungsrates
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	Business Continuity Management
BeLa	Berliner Landesnetz
Berlin-CERT	Computer Emergency Response Team des Landes Berlin
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDC-LV	Cyber Defense Center der Landesverwaltung
CDO	Chief Digital Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team
DAB	Digital Agentur Berlin
DsiN	Deutschland sicher im Netz
E-GovGBln	E-Government Gesetz Berlin
FITKO	Föderale IT-Kooperation
HWK	Handwerkskammer
HWR Berlin	Hochschule für Wirtschaft und Recht Berlin
IHK	Industrie- und Handelskammer
IKT	Informations- und Kommunikationstechnologie
IKT-BCM	Business Continuity Management zur Informations- und Kommunikations-technologie
IMK	Innenministerkonferenz
IoC	Indicators of Compromise
ISMS	Informationssicherheitsmanagementsystem
IT-PlR	IT-Planungsrat
ITDZ Berlin	IT-Dienstleistungszentrum Berlin
KMU	kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen
LAG	Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz
LKA	Landeskriminalamt

LÜKEX	Länder- und Ressortübergreifenden Krisenmanagement-Übung
MISP	Malware Information Sharing Platforms
NIS-2 RL	Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau (Netzwerk- und Informationssicherheits-RL)
SenInnSport	Senatsverwaltung für Inneres und Sport
SenWEB	Senatsverwaltung für Wirtschaft, Energie und Betriebe
SOC	Security Operations Center
TeleTrust	Bundesverband IT-Sicherheit e.V.
VCV	Verwaltungs-CERT-Verbund
ZAC	Zentrale Ansprechstelle Cybercrime