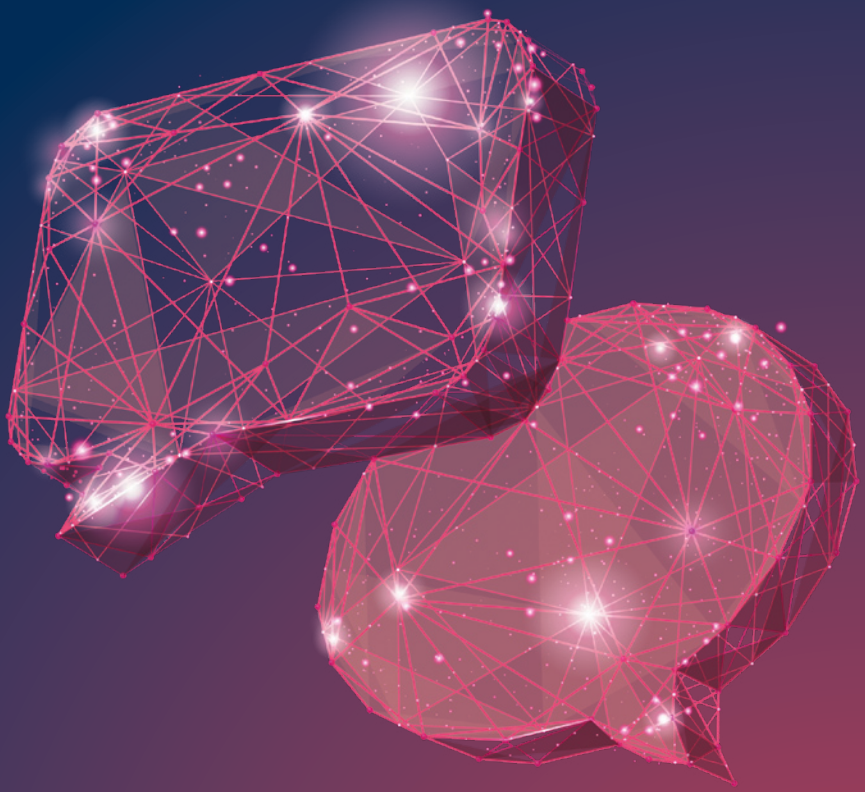
Cybersicherheitsstrategie Niedersachsen

Niedersächsisches Ministerium
für Inneres und Sport



Sehr geehrte Damen und Herren,

die Cyberbedrohungslage ist in Niedersachsen seit Jahren auf einem anhaltend hohen Niveau. Störungen der IT-Infrastrukturen durch Cyberangriffe, Betriebsunterbrechungen, Naturkatastrophen oder geopolitische Entwicklungen sind längst Realität. Die Zeiten, in denen man im Rahmen von Planbesprechungen theoretisch über die Bewältigung solcher Störungen diskutiert hat, sind vorbei. Cyberangriffe können verheerende Folgen für Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft mit sich bringen.

Cyberkriminelle agieren zunehmend professioneller und unabhängig territorialer Grenzen. Den komplexen Bedrohungen kann nur gemeinschaftlich begegnet werden. Eine kooperative und ebenenübergreifende Zusammenarbeit in allen Bereichen ist daher nicht nur ökonomisch sinnvoll, sondern nahezu unerlässlich.

Es besteht daher ein fachlicher, politscher und gesellschaftlicher, länderübergreifender und EU-weiter Konsens darüber, dass zur Stärkung der gesamtstaatlichen Cybersicherheitsarchitektur allen voran Verwaltungen in den Ländern und Kommunen ihre Cyberresilienz deutlich stärken müssen.

Es ist brandgefährlich, Cybersicherheit allein als lästige Aufgabe einer IT-Abteilung zu betrachten. Zur Cybersicherheit gehören nicht nur technische Maßnahmen. Es braucht zudem klare Richtlinien, Schulungen für Mitarbeiterinnen und Mitarbeiter, Ressourcenverteilung und eine durchdachte Incident-Response-Strategie. Cybersicherheit muss Chefinnen- und Chefsache werden.

Alle Akteurinnen und Akteure müssen ein ausgeprägtes Cybersicherheitsniveau vorhalten – dies gilt auch für die Kommunen, Wirtschafts- und Forschungseinrichtungen in Niedersachsen. Die Fähigkeiten und Erfahrungen müssen eingebracht und miteinander geteilt werden, um besser, koordinierter und zielgerichteter gegen Cyberangriffe agieren zu können. Gegenseitiges Vertrauen und intensive Zusammenarbeit sind die notwendige Basis, um bereichsübergreifend diesen Herausforderungen gegenüberzutreten. Daraus muss auch ein zuverlässiges, aktuelles und ganzheitliches Lagebild entstehen, denn dieses ist die grundlegende Voraussetzung für eine erfolgreiche Prävention und Reaktion.

Die öffentliche Verwaltung muss sich in besonderem Maße vor den Bedrohungen aus dem Cyberraum schützen. Unsere Mitbürgerinnen und Mitbürger sowie die Unternehmen vertrauen auf die Arbeitsfähigkeit ihrer Verwaltungen in Land und Kommunen und sind auf sie angewiesen. Niedersachsen zählte bereits vor mehr als einer Dekade zu den ersten Ländern in Deutschland, die sich dem Thema Cybersicherheit mit großem Augenmerk zugewandt hatten und solide Fundamente für eine Informations- und Cybersicherheit gelegt haben. Die Verwaltungen, die Strafverfolgungsbehörden, der Katastrophenschutz, der Verfassungsschutz und auch die Wirtschaft in Niedersachsen reagieren seitdem flexibel und stetig auf die zunehmende Professionalisierung der Cyberkriminellen.

Mit der Fortschreibung der Cybersicherheitsstrategie Niedersachsen tritt die Niedersächsische Landesregierung den stetig wachsenden Herausforderungen gegenüber. Die Ausgestaltung der Handlungsfelder orientiert sich maßgeblich an der Leitlinie für föderale Cybersicherheitsstrategien, wie sie von der „Ständigen Konferenz der Innenminister und -senatoren der Länder“ - kurz Innenministerkonferenz (IMK) empfohlen - worden sind. Die sukzessive Konkretisierung und Umsetzung der adressierten Themenbereiche werden die Cybersicherheitsarchitektur in Niedersachsen weiter stärken.

Daniela Behrens
Ministerin für Inneres und Sport

1 EINLEITUNG

Störungen oder Ausfälle von informationstechnischen Systemen können das gesellschaftliche Leben in Anbetracht wachsender Interdependenzen nachhaltig beeinträchtigen. In der digitalen Welt werden diese Themen ständig neu ausgehandelt und führen zu veränderten Bedingungen für Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft. Die vorliegende Cybersicherheitsstrategie trägt zu einer Stärkung des Cybersicherheitsniveaus in Niedersachsen und der gesamtstaatlichen Cybersicherheitsarchitektur bei. Cybersicherheit ist Aufgabe aller. Es geht um klare Richtlinien, Schulungen für Mitarbeitende, Ressourcenverteilung und eine vorausschauende Resilienz-Strategie. Die Niedersächsische Cybersicherheitsstrategie adressiert unterschiedliche Cybersicherheitsakteure, die gemeinsam zur Stärkung des Cybersicherheitsniveaus in Niedersachsen beitragen.

Die hierbei zu berücksichtigenden Handlungsfelder orientieren sich maßgeblich an der „Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien“, welche die Ständige Konferenz der Innenminister und -senatoren der Länder (Innenministerkonferenz - IMK) entwickelt hat. In ihrer Herbstsitzung 2021 hat die IMK die Länder gebeten, diese Leitlinie bei der Erstellung von Länderstrategien entsprechend zu berücksichtigen.

1.1 MOTIVATION

Die Cybersicherheit in Verbindung mit einem modernen und wirksamen Datenschutz ist eine wesentliche Voraussetzung für das Gelingen der Digitalisierung in unserem Land und nicht zuletzt auch für die Stärkung des Vertrauens in demokratische Prozesse in Deutschland und Europa.

Mit der Digitalisierung rückt auch die Sicherheit in der Cyberwelt in den Fokus, wodurch Informationssicherheit und Datenschutz und der Schutz Kritischer Infrastrukturen (KRITIS) besonders betroffen sind. Mit Blick auf Cybercrime, Angriffe staatlich gesteuerter Gruppen, Terrorismus und Wirtschaftsspionage erweitern sich die Angriffsszenarien permanent.

Die Vernetzung von Informations-, Steuerungs- und Versorgungssystemen über die territorialen Grenzen hinaus vergrößert die mögliche Angriffsfläche, indem in nie dagewesener Form auch kleinste Geräte an das Internet angeschlossen und zugänglich gemacht werden. Eine veränderte Arbeitswelt schafft neue Möglichkeiten und gleichzeitig neue Abhängigkeiten mit entsprechenden Risiken. Die Risiken erstrecken sich von den Schutzzielen der Informationssicherheit über den Schutz personenbezogener Daten, den sicheren Betrieb von Anlagen, welche für die Daseinsvorsorge kritisch sind, bis hin zu Risiken für Leib und Leben. Diesen Bedrohungen muss mit erhöhten Anforderungen an die Informationssicherheit, die Cybersicherheit und den Datenschutz begegnet werden.

Aufgrund des stetigen technologischen und auch geopolitischen Wandels sowie globaler Krisen unterschiedlichster Art ist es wichtig, die Cybersicherheitsstrategie für Niedersachsen aus dem Jahr 2012 fortlaufend an die aktuellen Entwicklungen anzupassen. Dabei ist nicht nur der wirtschaftliche Standort Niedersachsen zu stärken, es ist auch der Schutz der Grundrechte der Bürgerinnen und Bürger im Netz zu garantieren, so dass das Vertrauen in der demokratischen Grundstruktur gegeben ist. Damit kommt der Staat seinen Verpflichtungen nach, ein sicheres und freies Leben in einer digitalisierten Gesellschaft zu ermöglichen.

1.2 KONTEXT

Die Cybersicherheitsstrategie der Europäischen Union für die digitale Dekade wurde am 16. Dezember 2020 vorgelegt. Sie bildet einen der Eckpfeiler des Maßnahmenpakets für die digitale Dekade und benennt konkrete Maßnahmen, die bei der Umsetzung nationaler Cybersicherheitsstrategien zu beachten sind. Daran anknüpfend hat am 8. September 2021 die Bundesregierung ihre überarbeitete Cybersicherheitsstrategie 2021 für Deutschland beschlossen.

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

Die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) ist nach der Veröffentlichung im Amtsblatt der EU am 16.01.2023 in Kraft getreten. Die Mitgliedstaaten müssen die Richtlinie bis zum 17.10.2024 in nationales Recht umsetzen. Gemäß Artikel 7 Absatz 1 der NIS-2-Richtlinie ist jeder Mitgliedstaat verpflichtet, bis zum Ende der Umsetzungsfrist eine nationale Cybersicherheitsstrategie zu formulieren und von der Kommission notifizieren zu lassen. Die nationale Cybersicherheitsstrategie Deutschlands wird die Cybersicherheitsstrategie des Bundes sowie die 16 Cybersicherheitsstrategien der Länder umfassen.

Die einzelnen Strategien müssen insbesondere die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus, umfassen. Im Rahmen der Umsetzung der NIS-2-Richtlinie ist es somit erforderlich, dass Niedersachsen eine aktualisierte Cybersicherheitsstrategie verabschiedet, die diesen Anforderungen genügt.

Mit dem „Masterplan Digitalisierung Niedersachsen" hat die Landesverwaltung in jüngerer Zeit Bestrebungen zur zielgerichteten und kontinuierlichen Umsetzung von Maßnahmen zur Digitalisierung aller Verwaltungsebenen umgesetzt. Basis hierfür war das seit dem 14. August 2017 in Kraft getretene Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG). Am 4. April 2018 hat der Niedersächsische IT-Planungsrat einen ersten Handlungsplan verabschiedet und initiiert, der mit Beschluss vom 19. März 2024 fortgeschrieben worden ist.

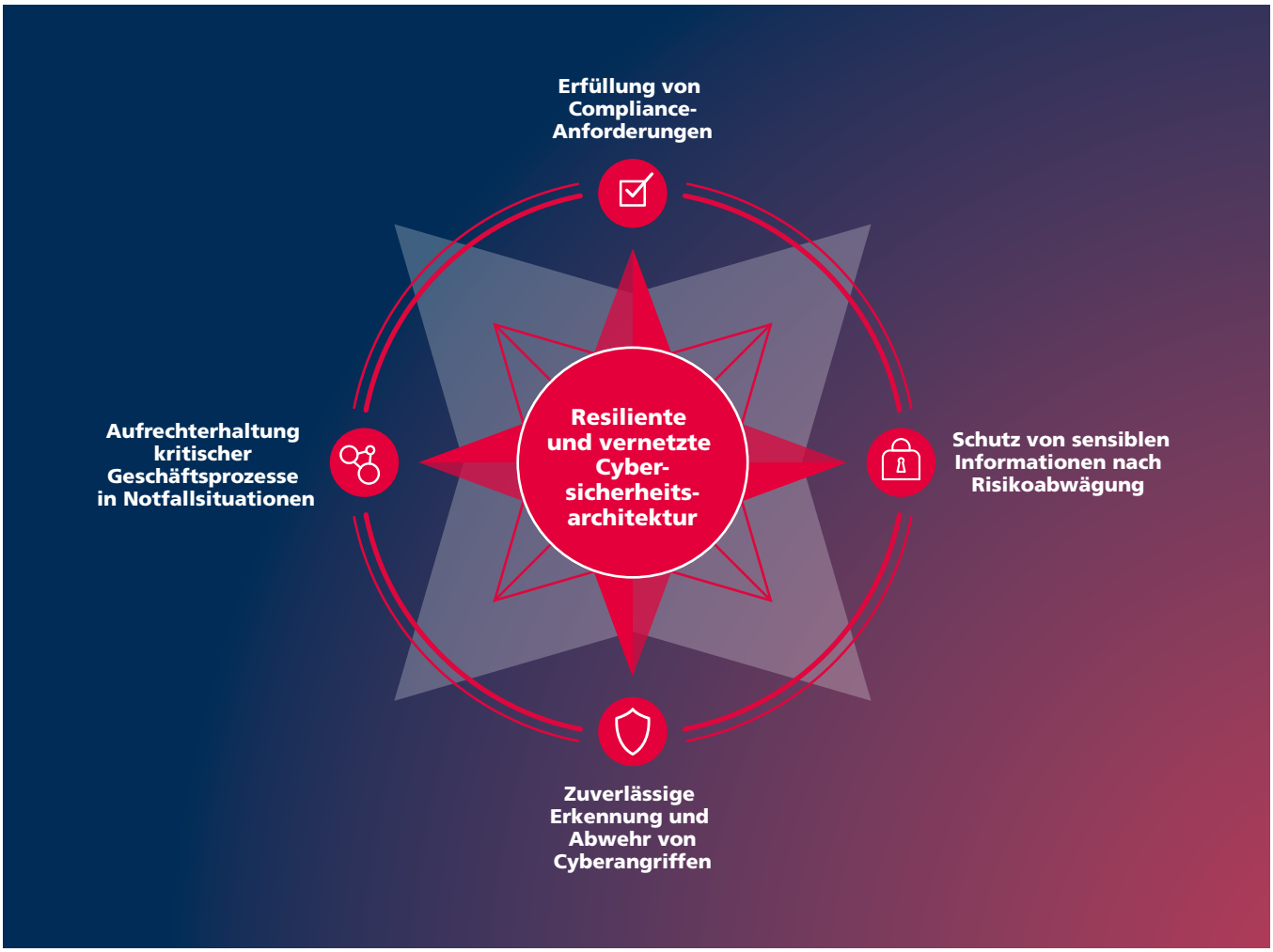
Mit der von der Niedersächsischen Landesregierung beschlossenen „Strategie zur digitalen Transformation der Verwaltung des Landes Niedersachsen – Digitale Verwaltung 2030" werden Anforderungen und Zielsetzungen an die Informationssicherheit für den IT-Einsatz in der Landesverwaltung benannt. Für diese Aufgabe erarbeitet die Niedersächsische Landesregierung eine Informationssicherheitsstrategie, welche die grundsätzlichen Festlegungen zur Messung und Steuerung der Informationssicherheit im Sicherheitsverbund treffen wird.

Eine moderne Cybersicherheitsstrategie muss über die Landesbehörden hinausgehen und in Zeiten geopolitisch veränderter und sich verschärfender Bedrohungslagen auch die Belange aus Gesellschaft, Wirtschaft und Wissenschaft berücksichtigen.

1.3 ZIELDEFINITION

Die Landesregierung wird mit der neuen Cybersicherheitsstrategie für Niedersachsen alle Beteiligten in Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft einbinden und das Cybersicherheitsniveau in und für Niedersachsen nachhaltig verbessern.

Dieses Bekenntnis ist Ansporn, die Cybersicherheitsstrategie in aktives Handeln umzusetzen und mitzuarbeiten, damit in Niedersachsen sowohl die digitale Souveränität als auch die staatliche Handlungsfähigkeit vor dem Hintergrund der Gefahren aus dem Cyberraum auch in Zukunft gewährleistet werden und die Risiken begrenzbar bleiben.



2. HANDLUNGSFELDER

Die nachfolgend adressierten Handlungsfelder der Cybersicherheitsstrategie Niedersachsen orientieren sich an dem zuvor genannten Leitfaden der IMK. Die Handlungsfelder sind:

1. Intensivierung der Vernetzung der Cybersicherheitsakteurinnen und -akteure
2. Staatliche Verwaltung und Kommunen
3. Gefahrenabwehr- und Strafverfolgungsbehörden
4. Spionage- und Sabotageabwehr
5. Kritische Infrastrukturen sowie wesentliche und wichtige Einrichtungen
6. Wirtschaft
7. Öffentlich-Private Partnerschaften
8. Förderung der digitalen Kompetenzen
9. Awareness und Verbraucherschutz
10. Fachkräfte
11. Innovative Forschung und Entwicklung
12. Nationale und internationale Kooperationen

2.1 INTENSIVIERUNG DER VERNETZUNG DER CYBERSICHERHEITSAKTEURINNEN UND -AKTEURE

Zur Verbesserung des Informationsstands und der Reaktionsfähigkeit ist eine Intensivierung der Vernetzung der Cybersicherheitsakteurinnen und -akteure in Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft geboten. Die Cybersicherheitsarchitektur in Niedersachsen soll weiter gestärkt werden, um die verschiedenen Stakeholder bestmöglich miteinander zu vernetzen. Der engen komplementären Zusammenarbeit mit den zuständigen Einrichtungen des Bundes, den Ländern und der Europäischen Union kommt hierbei eine besondere Bedeutung zu. Durch den regelmäßigen Austausch der staatlichen Cybersicherheitsakteurinnen und -akteure ist gewährleistet, dass Bedrohungen frühzeitig erkannt und Präventionsmaßnahmen gezielt (weiter-) entwickelt werden. Das Netzwerk bündelt durch die Heterogenität der Teilnehmenden verschiedene Kompetenzen im Bereich Cybersicherheit und kann durch innovative und interdisziplinäre Herangehensweisen die Cybersicherheit stärken.

Das Niedersächsische Ministerium für Inneres und Sport hat mit seiner Cyberkoordinierungsgruppe eine Informationsdrehscheibe der Akteurinnen und Akteure aus den Organisationseinheiten der Polizei, des Verfassungsschutzes, des Katastrophenschutzes und des Niedersachsen-Computer Emergency Response Team (N-CERT) aufgebaut. Die Mitglieder der Cyberkoordinierungsgruppe sind in ihren fachlichen Zuständigkeiten in und über die Landesgrenzen hinaus vernetzt. Diese bereits bestehenden Strukturen gilt es weiter zu festigen und auszubauen. Insbesondere ist es von hoher Bedeutung, abgestimmte Kommunikationsprozesse und fachliche Austausche fest zu etablieren.

Daneben gilt es, die ressortübergreifende Vernetzung weiter zu verstärken und zu definieren, welche Maßnahmen und Strukturen zur Vernetzung von Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft existieren oder anzustreben sind. Dazu zählen beispielsweise behördeninterne Informations- und Kooperationsplattformen, die der landesinternen Vernetzung der Behörden mit Cybersicherheitsaufgaben oder darüber hinaus einer Abstimmung der strategischen Belange der Cybersicherheit mit allen Mitwirkenden in Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft dienen. Zur Umsetzung dieses Ziels wird in dieser Strategie die Einrichtung eines Cybersicherheitszentrums Niedersachsen vorgestellt (vgl. Abschnitt 3), welches mit den Bereichen der Cybersecurity, Cybercrime sowie Cyberintelligence und weiteren wesentlichen Ergänzungen als Kontakt- und Informationsstelle zum Thema Cybersicherheit dienen soll. Das Cybersicherheitszentrum soll als Kompetenzknotenpunkt ausgebaut und dann sowohl staatlichen Stellen als auch der Wirtschaft, der Wissenschaft und gesellschaftlichen Akteurinnen und Akteure als Anlaufpunkt in Fachfragen rund um das Thema Cybersicherheit zur Verfügung stehen.

Darüber hinaus ist eine komplementäre Zusammenarbeit mit zuständigen Einrichtungen des Bundes, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik (BSI), und den Ländern sowie der Europäischen Union zu festigen.

Vertreten durch das Ministerium für Inneres und Sport hat Niedersachsen im November 2021 als erstes Land eine gemeinsame Kooperationsvereinbarung mit dem BSI geschlossen und somit ein wichtiges Fundament gelegt, um das Cybersicherheitsniveau im Land zu stärken. Bereits im Jahr 2018 wurde eine gemeinsame Absichtserklärung zur vertieften Zusammenarbeit zwischen Niedersachsen und dem BSI unterzeichnet.

Ziel ist es, die Cyber-Sicherheitsarchitektur durch eine verbesserte Bund-Länder-Zusammenarbeit auf allen Ebenen stetig zu verbessern. Neben der gegenseitigen Unterstützung bei herausragenden Cybersicherheitsvorfällen wurden unter anderem ein intensivierter Austausch und eine stärkere Vernetzung mit einem vertieften Wissenstransfer vereinbart. Diese bereits bestehende vertrauensvolle und enge Zusammenarbeit soll durch eine Fortschreibung der Kooperationsvereinbarung künftig weiter gestärkt und verfestigt werden. Darüber hinaus bestehen in all diesen Fragen auch regelmäßige Austausche mit den Sicherheitsbehörden des Bundes – mit dem Bundeskriminalamt, dem Bundesamt für Verfassungsschutz und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Die Vernetzung der Länder in Deutschland erfolgt im Rahmen unterschiedlicher Arbeitsgremien (vgl. Kapitel 2.2). Weiterführende Austauschgremien wie beispielsweise ein juristischer Austausch zum Schwerpunkt Cybersicherheit sollte künftig in den Ländern etabliert werden. Niedersachsen wird sich auch hier aktiv beteiligen. Die Herausforderungen werden in den kommenden Jahren weiter zunehmen, daher ist eine bessere Koordination und Abstimmung von Maßnahmen von Bund, Ländern und Kommunen im Bereich der Cybersicherheit notwendig. Es müssen Lösungen gefunden werden, um einen institutionalisierten Austausch und eine Vernetzung auf allen Verwaltungsebenen zu schaffen.

Cybersicherheitsarchitektur in Niedersachsen

2.2 STAATLICHE VERWALTUNG UND KOMMUNEN

Die Themenbereiche Cybersicherheit und Informationssicherheit haben zahlreiche Schnittmengen auf allen Verwaltungsebenen. Dies zeigt sich auch in der Konstellation und den Aufgaben der beiden zuständigen zentralen Arbeits- und Abstimmungsgremien zwischen den Ländern bzw. zwischen Bund und Ländern – der Länderarbeitsgruppe (LAG) Cybersicherheit der IMK sowie der Arbeitsgruppe Informationssicherheit des IT-Planungsrats Bund/Länder (AG InfoSic).

Die LAG Cybersicherheit fokussiert sich beispielsweise auf den Erfahrungsaustausch und die bessere Vernetzung der Länder über alle Aspekte von Cybersicherheit hinweg. Hier fließen vielfache Aspekte aus den Bereichen der Sicherheitsbehörden, der Wissenschaft, der Kommunen und der Wirtschaft in die Arbeit ein. Auch werden Empfehlungen für die praktische Unterstützung der Kommunen zur Stärkung der Cybersicherheit erarbeitet.

Die AG InfoSic hingegen erarbeitet u. a. Sicherheitsstandards und Sicherheitsstrukturen in der öffentlichen Verwaltung des Bundes und der Länder und legt diese dem IT-Planungsrat Bund/Länder vor. Damit wird ein wichtiger Teil des Auftrages im IT-Staatsvertrag von Bund und Ländern[1] abgedeckt, nämlich die Festlegung übergreifender IT-Interoperabilitäts- und Sicherheitsstandards. Die operative Vernetzung ist mit dem Verwaltungs-CERT-Verbund (VCV) bereits erfolgreich etabliert.

Die in diesem Kapitel enthaltenen Themenblöcke sind weitestgehend in der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018 des IT-Planungsrats Bund/Länder beschrieben. In einem dazu beigeordneten Umsetzungsplan sind die Handlungsfelder mit konkreten Maßnahmen und messbaren Zielen unterlegt sowie ein fortlaufendes jährliches Berichtswesen der AG Informationssicherheit an den IT-Planungsrat Bund/Länder festgelegt. Die darin benannten Arbeitsbereiche sind:

a) Informationssicherheitsmanagement
b) Absicherung der IT-Netzinfrastruktur der öffentlichen Verwaltung
c) Ein einheitliches Sicherheitsniveau für ebenenübergreifende IT-Verfahren und IT-Systeme
d) Gemeinsame Abwehr von IT-Angriffen
e) IT-Notfallmanagement

Alle Verwaltungsebenen spielen in der Cybersicherheitsarchitektur im Land Niedersachsen eine wesentliche Rolle und sind in den Betrachtungen zur Stärkung des Cybersicherheitsniveaus mit einzubeziehen.

Ein besonderes Augenmerk liegt auf den IT-betreibenden Stellen der Landes- und Kommunalverwaltung. Aufgrund der heterogenen Strukturen der IT-Betriebe ist es unerlässlich, dass zwischen diesen Stellen ein umfassender, gesicherter Informationsaustausch, insbesondere im Hinblick auf Vorfallsmeldungen, stattfindet. Dazu ist ein geeignetes Kommunikationswerkzeug zu etablieren, welches es Behörden mit unterschiedlichen IT-Dienstleistern erlaubt, Daten auszutauschen. Bei der Fortentwicklung der IT-Infrastruktur muss dies berücksichtigt werden.

Wahlen stehen im Mittelpunkt unseres demokratischen Systems und müssen besonders vor Cyberangriffen geschützt werden. Die Sicherheit und Integrität des Wahlprozesses sind entscheidend für das Vertrauen der Gesellschaft in die Wahlinfrastruktur und das demokratische System insgesamt. Es ist daher sicherzustellen, dass auf diese Informationen nicht von außen, beispielsweise durch Manipulation, eingewirkt werden kann. Deshalb muss dafür Sorge getragen werden, dass mit den IT-Systemen kompetent und sicher umgegangen wird.

[1] *Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG.*

2.2.1 KOMMUNEN UND NACHGEORDNETE BEHÖRDEN

Für ein hohes Sicherheitsniveau in den Kommunen müssen Prozesse und Fachverfahren sowie die jeweiligen IT-Infrastrukturen auf hohem Niveau und stets unter Berücksichtigung aktueller Entwicklungen abgesichert werden. Digitalisierte und noch zu digitalisierende Verwaltungsprozesse können Bürgerinnen und Bürger sowie Unternehmen künftig mittels untereinander vernetzter Verfahren nutzen. Der Grundsatz „Security by Design“ soll bereits bei der Initiierung im Rahmen der Beschaffung und der Planung von IT-Vorhaben stärker berücksichtigt werden, beispielsweise durch den Einsatz von zertifizierten Produkten. An dieser Stelle kommt den Kommunen eine besondere Verantwortung zu, weil diese erste Ansprechstelle für die Menschen vor Ort sind und eine Vielzahl an Verwaltungsdienstleistungen erbringen.

Das Niedersächsische Ministerium für Inneres und Sport hat damit begonnen, den Kommunen in Niedersachsen die Durchführung von Cybersicherheitsanalysen als Unterstützungsangebot anzubieten. Mit Hilfe einer Cybersicherheitsanalyse kann ermittelt werden, ob die bereits getroffenen Schutzmaßnahmen eine ausreichende Widerstandfähigkeit gegen Cyberangriffe gewährleisten. Dazu wurden mit den interessierten Kommunen die wesentlichen technischen und organisatorischen Anforderungen an eine angemessene Absicherung gegen Bedrohungen aus dem Cyberraum untersucht und fachlich bewertet. Diese Leistung ist für die Kommunen kostenfrei und erfolgt auf freiwilliger Basis. Ziel ist es, die Kommunen mit den Ergebnissen und erforderlichen Umsetzungsmaßnahmen zu unterstützen. Darüber hinaus wird die Landesregierung weitere Unterstützungsangebote für die Kommunen entwickeln, um das Cybersicherheitsniveau zu stärken.

2.2.2 INFORMATIONSSICHERHEITSMANAGEMENT

Ein Informationssicherheitsmanagementsystem (ISMS) in Niedersachsen garantiert die langfristige und nachhaltige Informationssicherheit. Das ISMS orientiert sich an der aktuellen Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (Entscheidung 2019/04 des IT-Planungsrats) und dem Umsetzungsplan (Entscheidung 2020/05).

Im Niedersächsischen Gesetz über digitale Verwaltung und Informationssicherheit wird ein Sicherheitsverbund beschrieben (§ 13 NDIG). Die Sicherheitsarchitektur für diesen Verbund wird mit den Zielen Robustheit und Reaktionsfähigkeit weiterentwickelt, so dass die Risiken, die sich aus den organisatorischen Besonderheiten der Landesverwaltung und dem föderierten Sicherheitsverbund ergeben, angemessen reduziert werden können. Die Landesregierung wird eine Informationssicherheitsstrategie erarbeiten, die die Voraussetzung für ein effektives und übergreifendes ISMS schafft. Sowohl für das ISMS als auch für den Sicherheitsverbund sollen in diesem Rahmen weitere strategische Ziele definiert werden, beispielsweise eine Stärkung der Verbundteilnehmenden, eine Kompetenzbündelung oder auch eine Zero-Trust-Architektur.

In der Praxis sollten auch die Kommunen bei der Auswahl eines passenden Vorgehensmodells zur Erstellung eines Informationssicherheitskonzepts unterstützt werden, um ein hohes und möglichst einheitliches Sicherheitsniveau im Land Niedersachsen zu erreichen. Diese Unterstützung zur Erhöhung des Cybersicherheitsniveaus kann in unterschiedlicher Form, etwa durch Beratungsangebote der dafür zuständigen Stellen, in Niedersachsen zur Verfügung gestellt werden.

2.2.3 ANALYSE- UND REAKTIONSFÄHIGKEIT VOR ORT STÄRKEN

Zur Bewältigung der Herausforderungen der gestiegenen Bedrohungslage für informationstechnische Systeme sind die Landesbehörden auf Unterstützung angewiesen. Zentrale Maßnahmen zur Schadensbegrenzung reichen allerdings allein nicht aus, um das Cybersicherheitsniveau aller Beteiligten nachhaltig zu verbessern. Daher sind zusätzliche dezentrale Maßnahmen vor Ort erforderlich, um die Kompetenz und Ressourcen für die IT-Sicherheit zu stärken.

Die Landesregierung prüft zur Stärkung der Analysekompetenz der Fachdienststellen einerseits Fortbildungsmaßnahmen und andererseits den Einsatz von Hard- und Software für eine effiziente Anomalieerkennung zum Schutz der Verwaltung.

2.2.4 NIEDERSACHSEN-COMPUTER EMERGENCY RESPONSE TEAM (N-CERT)

Durch die Zunahme der Anzahl der fortgeschrittenen gezielten Angriffe ist es notwendig, Sicherheitslücken und zielgerichtete Cyberangriffe möglichst frühzeitig zu erkennen. Hierbei hat das N-CERT eine zentrale Rolle: Das N-CERT besteht aus einer Gruppe von Expertinnen und Experten, die ständig die aktuelle Cyber-Sicherheitslage überwacht, um Bedrohungen aus dem Cyberraum frühzeitig zu erkennen und deren Auswirkungen zu bewerten. Es erfüllt seine gesetzlichen Aufgaben als Zentralstelle für Informationssicherheit gem. § 14 NDIG. Als ein landesinternes, koordinierendes CERT richten sich die Leistungen des N-CERT an alle Landes- und Kommunalbehörden und die dort ansässigen IT-Sicherheitsteams. Das N-CERT steht in ständigem und intensivem Austausch insbesondere mit den für Sicherheitsfragen relevanten Bereichen des Landesbetriebes IT.Niedersachsen als Betreiber des Landesdatennetzes sowie weiteren IT-betreibenden Stellen in der Landesverwaltung. Das N-CERT steht in allen Fragen der Cybersicherheit auch unmittelbar der Niedersächsischen Landesregierung zur Verfügung.

Die Einbindung der kommunalen Ebene erfolgt über das N-CERT. Zudem arbeitet es im ständigen direkten Kontakt mit dem Wirtschaftsschutz und der Cyberabwehr des Niedersächsischen Verfassungsschutzes, dem Landeskriminalamt Niedersachsen (Zentrale Ansprechstelle Cybercrime – ZAC) sowie dem Katastrophenschutz zusammen.

Bei Not- und Krisenfällen unterstützt das N-CERT das Notfall- und Krisenmanagement der Landesregierung mit einem IT-Lagebild und steht diesem als Fachberatung zu Fragen der Informationssicherheit zur Verfügung.

Im Rahmen der Umsetzungsverpflichtungen der NIS-2-Richtlinie wird festzulegen sein, welche weiteren Aufgaben das N-CERT übernehmen wird. Nach Art. 10 der NIS-2-Richtlinie benennt jeder Mitgliedstaat ein oder mehrere Computer-Notfallteams (Computer Security Incident Response Teams - CSIRTs) oder richtet diese ein. Da besonders kritische Teile der Landesverwaltung in den Anwendungsbereich der NIS-2-Richtlinie fallen werden, ist ein niedersächsisches CSIRT für die Bewältigung von Sicherheitsvorfällen nach einem genau festgelegten Ablauf zuständig. Das N-CERT bietet sich aufgrund der vorhandenen Expertise hierfür in hervorragender Weise an.

2.2.5 BERICHTSWESEN

Die Bewertung der aktuellen Bedrohungslage soll mit automatischen, ohne zeitliche Verzögerungen generierten Analysen unterstützt werden, um zeitnah auf kritische Bedrohungslagen reagieren zu können. Um dies leisten zu können, soll ein übergreifendes Berichtswesen etabliert und technische Grundlagen für ein übergreifendes Controlling geschaffen werden. Ein übergeordnetes Dashboard, das die einzelnen Analyseergebnisse aus dem Monitoring der IT-betreibenden Stellen sowie aus unterschiedlichen Organisationseinheiten zusammenfassend darstellt, soll als Werkzeug für die Controllingaufgaben herangezogen werden können.

Im Rahmen der technischen Umsetzung eines umfassenden Berichtswesens gilt es, auch die Regelungen des Informationssicherheitsmanagements (z. B. Informationssicherheitsrichtlinien - ISRL) und sonstige Mindestanforderungen zu prüfen und gegebenenfalls anzupassen. In der Folge wird auch ein Monitoring der Umsetzungsgrade im ISMS etabliert.

2.2.6 GANZHEITLICHE LAGEBILDERSTELLUNG

Ein umfassendes Lagebild ist die Grundlage für ein zielgerichtetes Handeln und unerlässlich für die Entscheidungsfindung.

Sowohl die Gefahrenabwehrbehörden als auch die allgemeinen Verwaltungen profitieren von einem umfassenden Lagebild. Auch weitere Interessengruppen können Bedarfe an einem Lagebild zur Cybersicherheit haben (z. B. Wissenschaft, Wirtschaft). Lagebilder entstehen bei den zuständigen Stellen, indem möglichst viele Informationsquellen aus Verwaltung, Wirtschaft und Wissenschaft herangezogen und mit aktuellen Informationen u. a. zu relevanten IT-Sicherheitsvorfällen zusammengeführt werden. Hieraus können zielgerichtete operative Maßnahmen zur Wiederherstellung des Normalzustandes der IT-Services oder strategische Entscheidungen für die jeweilige Stelle abgeleitet werden. Es sind ein strategisches und ein operatives Lagebild vorzuhalten:

- Das strategische Lagebild hat das Ziel, eine Entscheidungshilfe für in die Zukunft gerichtete strategische Entscheidungen zu sein.
- Das operative Lagebild hat das Ziel, Informationen bereit zu stellen, die als Grundlage operativer Entscheidungen in der jeweiligen Situation dienen.

Diese Lagebilder fassen die bereits vorhandenen Informationen zusammen, stellen Querbezüge her und bereiten sie adressatengerecht auf. Unter Berücksichtigung der Vertrauensstufen können die Lagebilder den Stakeholdern in geeigneter Form zur Verfügung gestellt werden. Niedersachsen strebt die automatisierte Erfassung sowie Bündelung der Informationen in einem übergreifenden Cybersicherheitslagebild an.

2.2.7 GEMEINSAME ABWEHR VON IT-ANGRIFFEN

Die Früherkennung von zielgerichteten Cyberangriffen ist im Hinblick auf die Zunahme professioneller und gezielter Angriffe auf die IT-Infrastruktur von besonderer Bedeutung. Die über die Landesgrenzen hinaus etablierte operative Zusammenarbeit von Bund (BSI) und Niedersachsen erfolgt über den Verwaltungs-CERT-Verbund (VCV). Ziel des VCV ist es, ein Netzwerk zu etablieren, in dem ein ständiger Informationsaustausch über relevante Cybersicherheitsthemen stattfindet und von dem die Teilnehmenden Unterstützung anfordern können, um effektiver und schneller auf Cyberbedrohungslagen reagieren zu können. Die Kommunikation im VCV soll weiter verstärkt werden.

Zur gemeinsamen Abwehr von IT-Angriffen ist eine gute Zusammenarbeit zwischen Erkenntnissen aus den Bereichen Polizei, Wirtschaftsschutz und Cyberabwehr sowie dem Katastrophenschutz erforderlich. Diese Bereiche haben ihrerseits auf Bundesebene entsprechende Pendants, z. B. Bundeskriminalamt (BKA), Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Bundesamt für Verfassungsschutz (BfV). Die Landesregierung wird sich dafür einsetzen, dass in diesen landesinternen Strukturen sowie landesübergreifend (Land-Land, Land-Bund) strategische Ziele für eine gemeinsame Abwehr von Cyberangriffen formuliert werden.

Insgesamt soll die Abwehr von Cyberangriffen effizienter gestaltet werden. Dazu sind Maßnahmenpläne zur Abwehr von Cyberangriffen umfassender mit den beteiligten Bereichen zu verzahnen und an die aktuellen Bedrohungsszenarien anzupassen. Zudem werden die vorhandenen Strukturen und Abläufe auf ihre Wirksamkeit geprüft und je nach Eskalationsstufe und Differenzierung nach Cyberangriff oder Cybercrime optimiert.

2.2.8 VORFALLSBEWÄLTIGUNG

Für eine schnelle Reaktion auf eine eingetretene Cyber-Bedrohungslage bedarf es einer besonderen Ablauforganisation. Diese muss schnell und zuverlässig alle entscheidenden Informationen zur Lage erhalten und über die zu treffenden Gegenmaßnahmen entscheiden können. Das N-CERT ist die zentrale Meldestelle für Sicherheitsvorfälle, die domänenübergreifende oder schwerwiegende Ausfälle haben. Das N-CERT unterstützt die Informationssicherheitsbeauftragten der Sicherheitsdomänen bei der Bewältigung dieser Sicherheitsvorfälle und bei der kontinuierlichen Verbesserung von Sicherheitsmaßnahmen.

Sollte es zu einer massiven Beeinträchtigung der Informationssicherheit bei den IT-Systemen in einer Behörde in Niedersachsen kommen, soll eine Gruppe mobiler Fachkräfte kurzfristig die betroffene Behörde bei der Bewältigung der Störung unterstützen. Dazu soll ein Mobile Incident Response Team (MIRT) aufgebaut werden. Auf Anforderung von Landesbehörden und Kommunen führt das MIRT technische Analysen durch und berät betroffene Organisationen bei der Vorfallsbewältigung vor Ort. So können bei zukünftigen Sicherheitsvorfällen die Teams in der betroffenen Behörde durch fachlich ausgebildetes Personal in kurzer Zeit verstärkt und unterstützt werden. Die Erfahrungen eines MIRT können wesentlich dazu beitragen, gleichgelagerte Störungen oder Ausfällen entgegenzuwirken.

2.2.9 BUSINESS CONTINUITY MANAGEMENT

Es ist Teil der staatlichen Verantwortung, die Funktionsfähigkeit der Landesverwaltung auch in Notfallsituationen gewährleisten zu können. Ein Business Continuity Management System (BCMS) erstellt anhand von Risikoanalysen Handlungspläne, welche auch im Notfall die Aufrechterhaltung bzw. nach Ausfällen innerhalb zugesicherter Zeiträume die Wiederaufnahme insbesondere der kritischen Verwaltungstätigkeiten gewährleisten. Die Landesregierung hat im Jahr 2021 beschlossen, ein strategisches Notfallmanagement (BCM) in der Landesverwaltung zu etablieren. Dieses wird in der Digitalisierungsstrategie „Digitale Verwaltung 2030 – Strategie zur digitalen Transformation der Verwaltung des Landes Niedersachsen“ aufgegriffen und Schnittstellen zum BCM identifiziert.

Die in der Digitalisierungsstrategie benannten Maßnahmen „#35 Ausarbeitung und Verabschiedung verbindlicher Vorgaben für ein strategisches Notfallmanagement für die Niedersächsische Landesverwaltung“ sowie „#36 Erstellung IT-bezogener Notfallkonzepte incl. Schnittstellen zu Krisen- und Katastrophenschutz“ gilt es nun konsequent umzusetzen. Nach Inkrafttreten der Leitlinie für ein BCM in der Landesverwaltung[2] werden zügig die damit verbundenen technischen und organisatorischen Strukturen aufgebaut.

Über das BCM hinaus ist es wichtig, insbesondere bei größeren Schadenslagen, den Katastrophenschutz um den für Cyberlagen notwendigen Sachverstand zu ergänzen. Seine technische Infrastruktur muss möglichst unabhängig von den öffentlichen Kritischen Infrastrukturen ausgelegt werden. Sowohl im Kontext des BCM als auch im Rahmen des Katastrophenschutzes sind Cyberlagen regelmäßig in die bestehenden Übungskalender aufzunehmen.

[2] *Siehe Nds. MBl. 2024 Nr. 300 vom 4. Juli 2024.*

2.2.10 RECHTLICHE RAHMENBEDINGUNGEN

Ein belastbarer normativer Rechtsrahmen ist eine unerlässliche Voraussetzung zur Schaffung notwendiger Befugnisse, um zu einer Erhöhung der allgemeinen Cybersicherheit auf Landesebene beizutragen. Zugleich schafft dieser Handlungssicherheit für alle Akteure der Cybersicherheit.

Niedersachsen wird sich in den Cybersicherheitsdiskurs auf nationaler und supranationaler Ebene einbringen. Bei notwendigen Fortschreibungen der rechtlichen und institutionellen Rahmenbedingungen auf diesen Ebenen gilt es, die besondere Rolle Niedersachsens stets zu bedenken. Insbesondere EU-weite gesetzliche Anforderungen inkl. Marktzugangsregelungen sowie Normen und Standards für Unternehmen im Bereich der Cybersicherheit sind vor dem Hintergrund der Vermeidung von Doppelregulierungen von besonderer Bedeutung.

Die Landesregierung wird überprüfen, inwieweit die bestehenden gesetzlichen Vorgaben den Anforderungen für die Cybersicherheit in Niedersachsen gerecht werden. Ferner wird sie prüfen, inwieweit die Berichtspflichten von Polizei und dem Verfassungsschutz Niedersachsen derart zusammengeführt werden können, dass ein umfangreicheres Lagebild für die Cybersicherheitslage in Niedersachsen erstellt werden kann.

2.2.11 KÜNSTLICHE INTELLIGENZ IN DER VERWALTUNG

Das Thema Künstliche Intelligenz wird in Niedersachen intensiv verfolgt. So hat die Niedersächsische Landesregierung mit ihrer Strategie zur Künstlichen Intelligenz (KI) klare Ziele, Maßnahmen, Budgets und Umsetzungszeiträume formuliert, wobei auch der Einsatz der KI in Verwaltung und Justiz einen wichtigen Schwerpunkt bildet. Für die Landesregierung ist entscheidend, die politischen Rahmenbedingungen im Hinblick auf Datenschutz und Ethik aktiv zu gestalten, ohne dabei die Entwicklung von Innovationen in Wissenschaft und Wirtschaft auszubremsen.

Für den Einsatz der KI in der niedersächsischen Landesverwaltung wurde zudem das KI-Kompetenzzentrum für die niedersächsische Verwaltung (KiKoN) gegründet. Es hat zum Ziel, den Einsatz von KI zu fördern und zu beschleunigen und dabei die bereits vorhandenen Fähigkeiten im Land Niedersachsen zu bündeln und weiter auszubauen.

Der Themenkomplex Cybersicherheit wird von den Entwicklungen in der künstlichen Intelligenz in vielfältiger Weise positiv wie negativ berührt werden. Speziell auf den Bereich Cybersicherheit trainierte Systeme der künstlichen Intelligenz sind eine Möglichkeit, dem Fachpersonalmangel im Bereich der Cybersicherheit entgegenzuwirken. Solche Systeme erlauben es, vorhandenen Fachkräften schneller und zielgerichteter agieren zu können. Damit eignen sie sich aber auch zum Aufspüren von Lücken und der automatisierten Informationsgewinnung aus Sicht der Angreifenden.

Übersetzungs- und Textgenerierungsprogramme eröffnen Angreifenden die Möglichkeit ohne Sprachbarriere und Auffälligkeiten agieren zu können. Eine zielgruppengerechte Ansprache kann ohne Aufwand in großer Zahl automatisch generiert werden und wird die Qualität und Menge bösartiger E-Mails auf ein neues Niveau bringen (Phishing).

Die Generierung von Schadcode mittels Methoden der künstlichen Intelligenz steht noch am Anfang. Es ist absehbar, dass zukünftig weniger technisches Wissen für Angriffe notwendig sein wird und sich damit der Kreis der potentiellen Angreifenden stark erhöht. Vergleichbares gilt auch mit Blick auf die Manipulationsmöglichkeiten von Informationen jeglicher Art, die insbesondere im gesellschaftlichen Raum konsumiert werden; zu nennen wären beispielsweise Deepfakes oder Fake News.

Die Landesregierung wird mit Blick auf die beschriebenen Risiken für die Cybersicherheit die Rahmenbedingungen für einen verantwortungsvollen Einsatz im Sinne der KI-Strategie ausgestalten.

2.3 GEFAHRENABWEHR- UND STRAFVERFOLGUNGSBEHÖRDEN

Der Fortschritt in der digitalen Welt stellt sowohl die Gefahrenabwehrbehörden als auch die Strafverfolgungsbehörden vor ständig neue Herausforderungen. Von zentraler Bedeutung ist, dass Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in der Lage sind, dynamisch auf die sich wandelnden Gegebenheiten und Anforderungen zu reagieren. Dies wird durch stetige Modernisierung und Investitionen in die Handlungsfähigkeit der zuständigen BOS gewährleistet.

Den Bedrohungen aus dem Cyberbereich ist mit einer schlagkräftigen Abwehr, stetiger Aufklärung, effektiver Strafverfolgung und hinreichenden Befugnissen der Sicherheitsbehörden zu begegnen. Diese Herausforderung kann nur als gesamtstaatliche Aufgabe, also in der Zusammenarbeit aller Akteurinnen und Akteure, und unter Stärkung der Strafverfolgungsbehörden sichergestellt werden. Eine enge Zusammenarbeit von Strafverfolgungsbehörden mit betroffenen Unternehmen oder Verwaltungen und anderen Stakeholdern kann im Fall eines Cyberangriffs zu einem besseren gegenseitigen Verständnis und höherem Vertrauen führen.

In diesem Kontext wird auch an die Katastrophenschutzbehörden gedacht. Insbesondere die personellen und technischen Kapazitäten der Strafverfolgungsbehörden zur effektiven Bekämpfung der Cyberkriminalität müssen regelmäßig bewertet und gegebenenfalls angepasst werden, um eine frühzeitige Reaktion an sich ändernde Bedarfe zu ermöglichen. Ein besonderes Augenmerk ist hierbei auf die Justiz zurichten, etwa durch den zusätzlichen Kompetenzerwerb von Digitalexpertise. Neben der Gewinnung des Fachpersonals sind auch die fortlaufende fachliche Qualifikation der Mitarbeitenden insbesondere in den „Cybercrime-Fachdienststellen“ zu gewährleisten. Gleichzeitig gilt es, zur Prävention vor Cyberangriffen das Unterstützungs- und Beratungsangebot des Wirtschaftsschutzes im Niedersächsischen Verfassungsschutz sowie der Zentralen Ansprechstelle Cybercrime (ZAC) im LKA Niedersachsen weiter zu stärken.

Darüber hinaus stellt die Prävention im Kontext hybrider Bedrohungen eine neue, zusätzliche, zentrale Aufgabe dar. Eine illegitime Einflussnahme fremder Staaten kann auf allen Ebenen von Politik und Verwaltung stattfinden und eine große Bandbreite an offenen und verdeckten Mitteln umfassen. Die Möglichkeiten der Einflussnahme sind vielfältig und erstrecken sich unter anderem auf technologische Angriffe auf KRITIS (z. B. Cyberangriffe auf Stromnetze, Wasserversorgung sowie Verkehrsnetze).

Hier ist die Stärkung der Resilienz der eigenen Organisation in geeigneter Weise zu verstetigen. Vor allem wird die Polizei Niedersachsen aber als Netzwerkpartnerin in der Präventionsarbeit auf kommunaler und Landesebene das Themenfeld „Hybride Bedrohungen“ strukturiert in das eigene Angebotsportfolio aufnehmen und folglich in den Präventionsteams vor Ort und im Fachstrang der Präventionsstelle „Politisch Motivierte Kriminalität“ (PPMK) die fortlaufend erforderliche Beratungs- und Handlungskompetenz aufbauen. Ziele sind dabei unter anderem eine fachkompetente Mitwirkung an der Aufklärung der Bevölkerung über die Gefahren hybrider Bedrohungen, die Stärkung der Resilienz der Gesellschaft sowie von KRITIS und die themenorientierte Zusammenarbeit mit anderen Behörden und Organisationen.

2.4 SPIONAGE- UND SABOTAGEABWEHR

Angriffe ausländischer Nachrichtendienste stellen eine Bedrohung für die deutsche Politik, die kritischen Infrastrukturen, die sonstige Wirtschaft sowie für die Wissenschaft dar. Insbesondere Cyberangriffe sind für ausländische Nachrichtendienste ein effektives Mittel, um Informationen auf digitalem Weg zu beschaffen, politisch Einfluss zu nehmen oder Sabotage zu verüben. Dem Themenfeld kommt gerade in politischen Krisenzeiten mehr Bedeutung zu.

Mit der niedersächsischen Verfassungsschutzbehörde und den Polizeibehörden in Niedersachsen gibt es bereits etablierte Akteurinnen und Akteure, die potentiell betroffene Stellen bei der Prävention, Aufklärung und Bewältigung von elektronischen Angriffen mit Spionage- oder Sabotagehintergrund unterstützen. Der Verfassungsschutz hat bedingt durch seinen Auftrag weitergehende Befugnisse und darauf basierend nachrichtendienstlich gewonnene Erkenntnisse, über die andere Stellen und Teile der Verwaltung nicht verfügen. Zudem unterliegt dieser im Unterschied zu den Polizeibehörden nicht dem Legalitätsprinzip und kann so einen weiteren Beitrag zur Aufhellung des Dunkelfelds leisten. Die im Aufbau befindliche Cyberabwehr des niedersächsischen Verfassungsschutzes hat die Aufgabe, Cyberangriffe zu erkennen und diese einer betroffenen Behörde oder Institution zuzuordnen. Um auch der steigenden Bedrohungslage von ausländischen Akteurinnen und Akteure entgegentreten zu können, wird die Landesregierung die Cyberabwehr in ihren Fähigkeiten weiter stärken.

Die Sensibilisierung gefährdeter Stellen ist je nach Erkenntnislage bzw. Betroffenen ein Gemeinschaftsprodukt von Polizei, N-CERT, Cyberabwehr und Wirtschaftsschutz des niedersächsischen Verfassungsschutzes.

2.5 KRITISCHE INFRASTRUKTUREN SOWIE WESENTLICHE UND WICHTIGE EINRICHTUNGEN

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungs- oder Entsorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit eintreten.[3] Zur Stärkung der Resilienz von KRITIS traten im Januar 2023 zwei EU-Richtlinien in Kraft: Die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) sowie die Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie). Während die Vorschriften der CER-Richtlinie die physische Widerstandsfähigkeit von KRITIS gegenüber Bedrohungen in Form von etwa Naturkatastrophen, Terroranschlägen oder Sabotage betreffen, enthält die NIS-2-Richtlinie Vorschriften zur Sicherheit von Netz- und Informationssystemen.

Die NIS-2-Richtlinie klassifiziert Unternehmen innerhalb ihres Anwendungsbereichs in „essential und important entities" (wesentliche und wichtige Einrichtungen). Daraus erwachsen unterschiedliche Verpflichtungen sowie Aufsichts- und Durchsetzungsbefugnisse der zuständigen Behörden. Anhang I („essential") der NIS-2-Richtlinie umfasst elf Sektoren und Anhang II („important") der NIS-2-Richtlinie umfasst sieben Sektoren. Diese insgesamt 18 Sektoren decken die deutschen KRITIS-Sektoren sowie Unternehmen im besonderen öffentlichen Interesse ab und gehen noch darüber hinaus. Dadurch können auch kommunale Unternehmen und kommunale Eigenbetriebe betroffen sein. Zudem werden Behörden der unmittelbaren Landesverwaltung, die nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben, als wichtige Einrichtungen in den Anwendungsbereich der NIS-2-Richtlinie fallen und Cybersicherheitsmindestanforderungen erfüllen müssen.

Im Zuge der Implementierung des Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz von Betreibern kritischer Anlagen muss überprüft werden, inwieweit Anpassungsbedarfe für die landesrechtlichen Regelungen bestehen. Hierbei nimmt der Interministerielle Arbeitskreis „Schutz Kritischer Infrastrukturen in Niedersachsen" (IMAK KRITIS) eine maßgebliche Rolle ein. Auf Landesebene wurde mit dem § 5 a NKatSG bereits frühzeitig eine Grundlage zur Identifizierung und zum Schutz von KRITIS geschaffen. Da die Zuständigkeit für die verschiedenen KRITIS-Sektoren wie Energie, Transport und Verkehr oder Gesundheit dem Ressortprinzip folgend bei verschiedenen Ministerien liegt, wurde weiterhin im Niedersächsischen Ministerium für Inneres und Sport bereits vor mehreren Jahren eine Koordinierungsstelle Kritische Infrastruktur (KOST KRITIS) eingerichtet, welche als Informationsdrehscheibe die Fäden aus den unterschiedlichen Ressorts zusammenführt und unter anderen mit dem Bund und den Ländern vernetzt ist.

Die Landesregierung wird sowohl solche Unternehmen bei der Umsetzung von Cybersicherheitsmindestanforderung unterstützen, die von regulatorischen Vorgaben betroffen sind, als auch solche Einrichtungen, die ihre Aufgaben der (regionalen) Daseinsvorsorge unterhalb regulatorischer Schwellenwerte wahrnehmen.

[3] *Siehe auch § 5a Niedersächsisches Katastrophenschutzgesetz (NKatSG).*

2.6 WIRTSCHAFT

Cybervorfälle wie Ransomware-Angriffe, Datenschutzverletzungen und IT-Unterbrechungen sind laut Allianz Risk Barometer im Jahr 2024 die größte Sorge für Unternehmen weltweit. Das BSI hat in seinem aktuellen Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“ eine Verlagerung der Angriffsziele feststellen können: Nicht nur große, finanzstarke Unternehmen stehen im Mittelpunkt der Angriffsvektoren, sondern zunehmend auch kleine und mittlere Organisationen und staatliche Institutionen und Kommunen.[4]

Zahlreiche Faktoren verschärfen die ohnehin angespannte Cyberbedrohungslage für die Wirtschaft. Dazu zählen beispielsweise zunehmend hybrid geführte Kriege, ein fortdauernder „Systemwettbewerb“ mit staatlich gelenkten Wirtschaftssystemen, ein hohes Niveau an mobilem Arbeiten sowie die zunehmende Verbreitung des Internet of Things (IoT) oder die Entwicklungen in den Bereichen KI und Quantencomputer. Aufgrund dieser Bedrohungslage ist ein hohes Sicherheitsniveau für Unternehmen, insbesondere für wesentliche und wichtige Einrichtungen sowie kritische Anlagen zu schaffen und im Sinne der Daseinsvorsorge auch die Handlungsfähigkeit des Staates zu schützen.

Der Sensibilisierung der Managementebene kommt eine besondere Bedeutung zu, weil Cybersicherheit kein Thema der IT-Abteilungen ist, sondern als Querschnittsaufgabe in allen Organisationsbereichen berücksichtigt werden muss. Hierbei gilt es, unter anderem nachfolgende Parameter zu berücksichtigen:

(1) Awareness in der Unternehmenskultur etablieren,
(2) Investitionen für Cybersicherheitsmaßnahmen erhöhen, denn Investitionen in präventive Cybersicherheitsmaßnahmen steigern die betriebswirtschaftliche Attraktivität von Investitionen in einer mittel- bis langfristigen Perspektive als Schadensverhütung und werden etwaige spätere finanzielle Schäden maßgeblich reduzieren,
(3) eine übergreifende Kooperation zur Stärkung der Cybersicherheit verschiedener Unternehmensbranchen.

Gezielte Beratungs- und Präventionsangebote zu IT- und Cybersicherheitsmaßnahmen in Zusammenarbeit mit Verbänden und Kammern oder anderen Multiplikatoren können Bausteine zur Stärkung des Sicherheitsniveaus sein. Dialogplattformen zwischen Staat und Wirtschaft können diesen Prozess unterstützen. Vor allem kleine und mittlere Unternehmen (KMU) sollen zum Abruf von nationalen und EU-weiten Fördermaßnahmen unterstützt und beraten werden, damit auch sie ihrer Verantwortung im Bereich Cybersicherheit gerecht werden können.

Als Ansprechpartnerin für die Unternehmen in Niedersachsen fungieren vor allem die Digitalagentur Niedersachen gemeinsam mit dem Niedersächsischen Ministerium für Wirtschaft, Bauen, Verkehr und Digitalisierung sowie die Mittelstand-Digitalzentren. Hier erhalten Unternehmen unterschiedliche Informations- sowie Unterstützungsangebote sowie Fördermöglichkeiten im Bereich Cybersicherheit. Diese werden weiter bedarfsgerecht ausgebaut. Strategische Impulse und Vorschläge für konkrete Maßnahmen für eine bessere Cybersicherheit in Niedersachsen kommen aus dem Arbeitskreis IT-Sicherheit, den die Digitalagentur im Auftrag des niedersächsischen Wirtschaftsministeriums koordiniert. Hier sind Perspektiven von Wirtschaft über Unternehmensverbände, die Industrie- und Handelskammer (IHK) und IT-Sicherheitsunternehmen, Wissenschaft, Ministerien und IT-Sicherheitsbehörden sowie Transfer- und Beratungsstellen vereint. Mittels des Arbeitskreises besteht zudem eine Austauschmöglichkeit mit Arbeitsgruppen und Stellen der Cybersicherheit in Unternehmensverbänden und IHKn. Für Beratung, Information

[4] *Quelle: Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2023, verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=6 (Oktober 2024).*

und Warnung kann auf die umfangreichen Angebote des Bundesamtes für die Sicherheit in der Informationstechnik zurückgegriffen werden. Darüber hinaus bietet das LKA Niedersachsen mit der ZAC einen polizeilichen Ansprechpartner bei der Prävention von Cyberkriminalität sowie im Schadenfall für niedersächsische Unternehmen an. Um den Herausforderungen zukünftig effektiv zu begegnen, sind neben präventiven Maßnahmen, das Anzeigeverhalten und die vertrauensvolle Zusammenarbeit mit betroffenen Unternehmen zu stärken.

Die vom Bund finanzierte Transferstelle Cybersicherheit wird den begonnenen Aufbau ihres Informationsangebotes in Kooperation mit den niedersächsischen Akteurinnen und Akteure fortsetzen. So werden vor allem KMU in der Vorsorge gegen und Reaktion auf Cyberangriffe gestärkt.

Um allen voran KMU zur Prävention von schädigenden Cyberattacken bzw. im Fall eines Cyberangriffs eine Orientierung von IT-Sicherheitsdienstleistern, die die Expertise zur Herstellung ihrer Systeme haben, zu verschaffen, wird die Transferstelle Cybersicherheit den begonnenen Aufbau eines entsprechenden Informationsportals weiter fortsetzen.

Die Lage der IT-Sicherheit in Deutschland 2023

Quelle: Bitkom Wirtschaftsschutz-Bericht 2023, https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf

Im Austausch mit den Stakeholdern aus Wirtschaft, Wissenschaft und Verwaltung sollen die Angebote weiterentwickelt und in konkrete Maßnahmen überführt werden. Die wesentlichen Ziele und Maßnahmen sind vor diesem Hintergrund für die nächsten Jahre:

- Awareness bei den relevanten Stellen in den Unternehmen schaffen, um das Thema in den Unternehmenskulturen weiter zu etablieren und zu verfestigen.
- Ein weiterer Ausbau sowie Verzahnung des bestehenden Beratungs- und Präventionsangebots.
- Erfolgreiche Formate wie Informations- und Diskussionsveranstaltungen sollen als Dialogplattformen fortgesetzt und ausgebaut werden.
- Bereits bestehende Qualifizierungsangebote müssen transparenter gemacht werden. Die Qualifizierung von Personal ist zentral für die Gewährleistung eines hohen Cybersicherheitsniveaus in Unternehmen. Es soll deshalb das Auffinden guter Qualifizierungsangebote erleichtert werden.
- Kooperation von Wissenschaft, Cyber-Sicherheitsbehörden und Multiplikatoren sowie Transferstellen in die Wirtschaft sollen weiter ausgebaut werden, um neueste Erkenntnisse zu Angriffsvektoren und gelingenden Sicherheitsmaßnahmen bestmöglich in die Praxis zu bringen.

2.7 ÖFFENTLICH-PRIVATE PARTNERSCHAFTEN

Zur Stärkung der Cybersicherheitsarchitektur ist es unerlässlich, dass öffentliche und private Akteurinnen und Akteure eng zusammenarbeiten. Der schnelle technologische Wandel und der Fachkräftemangel erfordern ein gemeinsames koordiniertes Vorgehen, bei dem sich Verwaltung und Wirtschaft als Partner verstehen sollten. Beispielsweise befindet sich die Mehrheit der Kritischen Infrastrukturen in der Hand privater Unternehmen. Eine kooperative und vertrauensvolle Zusammenarbeit bei der Prävention flankiert die bereits bestehenden Maßnahmen mit dem Ziel, ein hohes Cybersicherheitsniveau in Niedersachsen zu erreichen. Die Reaktion auf Cyberangriffe oder andere größere Krisenfälle stellt selbst größere Organisationen auch außerhalb der KRITIS-Sektoren vor erhebliche Herausforderungen. Vorab geschlossene Partnerschaften können ein Modell sein, um geeignete Reaktionskräfte effizient zu organisieren.

Im Rahmen der vertrauensvollen Zusammenarbeit zwischen der Wirtschaft und den staatlichen Sicherheitsbehörden soll der Informationsaustausch verstetigt und die Sensibilisierung für ein vorhandenes Gefahrenpotenzial erhöht werden. Die in Niedersachsen vorhandenen Netzwerke sollen stärker zusammengebracht und in weiten Teilen des Landes sichtbarer gemacht werden. Die Landesregierung wird prüfen, ob eine Öffentlich-Private-Partnerschaft als Instrument für diesen Kontext förderliche Aufgaben übernehmen kann.

2.8 FÖRDERUNG DER DIGITALEN KOMPETENZEN

Die Digitalisierung durchdringt alle Lebensbereiche bis hinein ins Private. Durch die Stärkung der digitalen Kompetenzen werden die Menschen in Niedersachsen auf dem Weg zu einer digitalen Souveränität unterstützt. Ein Netzwerk von Anlauf- und Beratungsstellen für Bürgerinnen und Bürger ist zu fördern, um diese im Hinblick auf Informationssicherheit direkt vor Ort zu beantworten. Eine angemessene digitale Kompetenz ist eine wichtige Voraussetzung dafür, dass die Menschen in Niedersachsen besser mit Cybersicherheitsrisiken umgehen können. Neben klassischen Schulungsangeboten erhalten digitale Lernplattformen eine immer größere Bedeutung, um möglichst viele Menschen zu erreichen.

Der Digital Campus Niedersachsen ist eine seit 2022 öffentlich zugängliche digitale Lernplattform für alle Interessierten, die ihre digitalen Kenntnisse aufbauen oder verbessern wollen. Hinter diesem Projekt stehen das Land Niedersachsen sowie die Einrichtungen der öffentlich geförderten Erwachsenenbildung mit ihren Mitgliedern (insb. die Volkshochschulen).

Durch innovative Bildungsangebote werden digitale Grundkompetenzen und die Steigerung von vorhandenen digitalen Kompetenzen vermittelt. Ein sogenannter „Digital-Check“ auf Grundlage der fünf Kompetenz-Kategorien des Europäischen Referenzrahmens hilft dabei, die eigenen Kompetenzen einzuordnen. Auf Basis der Auswertung werden dann individuelle Lernvorschläge unterbreitet – von niedrigschwelligen Angeboten bis hin zu weiterführenden Formaten. Der Schwerpunkt liegt auf der Vermittlung digitaler Prozesse und der nachhaltigen Veränderung in der Nutzung digitaler Tools und Angebote. Gleichzeitig soll eine Sensibilisierung der Öffentlichkeit für die digitale Bildung erreicht werden.

Im Hinblick auf den digitalen Schulalltag ist auf den Einsatz von IT an Schulen ein besonderes Augenmerk zu legen. Das Grundverständnis für Prävention und Reaktion in der Cybersicherheit sowie bei der Informationssicherheit und beim Datenschutz wird bereits hier geschaffen. Insbesondere Lehrkräfte müssen zuvorderst selbst in Ihren Kompetenzen gestärkt werden, um entsprechende Inhalte in den Unterricht einfließen zu lassen. Eine besondere Herausforderung stellt hierbei insbesondere die geteilte Verantwortung einerseits für die IT-Infrastruktur der Schulen beim Schulträger (vorwiegend Kommune) und andererseits Zuständigkeit für Lehrkräfte, Schülerinnen und Schüler sowie Unterrichtsinhalte durch das Land dar. Hinsichtlich rechtlicher Rahmenbedingungen ist zu prüfen, inwieweit Anpassungen beispielsweise der Informationssicherheitsleitlinie (ISLL) oder weiterer Normensetzungen in Niedersachsen vorgenommen werden müssen.

2.9 AWARENESS UND VERBRAUCHERSCHUTZ

Um Cybersicherheitsrisiken rechtzeitig zu erkennen sowie früh und angemessen darauf zu reagieren, sollen nicht nur die digitalen Kompetenzen, sondern auch das Bewusstsein (Awareness) über Cyberrisiken erhöht werden. Präventionsmaßnahmen, die zum Thema Cybersicherheit sensibilisieren und schulen, leisten einen entscheidenden Beitrag hierfür.

Eine fehlende Awareness sowie mangelnde Resilienz sind häufige Einfallstore für Cybersicherheitsvorfälle. Komplexe Systeme und zum Teil Unbedarftheit erschweren einen sicheren Umgang mit IT. Gerade im Bereich der Verbraucherendgeräte erwachsen zahlreiche Sicherheitsrisiken aus einer weit verbreiteten digitalen Unbekümmertheit der Anwendenden sowie unberücksichtigter Sicherheitsanforderungen bei der Herstellung der Produkte. Kosteneffizienz und Sicherheit stehen dabei oft in direkter Konkurrenz. Schnell werden dadurch Endnutzende zum Ziel eines Cyberangriffs. Sicher konzipierte („Security by Design“) und sicher konfigurierte („Security by Default“) Geräte und Verfahren sind neben einer kontinuierlichen Awareness Ansätze, dem entgegenzuwirken.

Bei der Vermittlung kommt den Verbraucherzentralen eine besondere Bedeutung zu. Klassische Schulungsangebote wie etwa Präsenzschulungen erreichen nur wenige Menschen gleichzeitig bei relativ hohem Aufwand für die Lehrenden. Es müssen somit alternative Lehrformen und Lernkonzepte unterstützt werden, die besser skalieren. Als Lehrformen sind beispielsweise Lernvideos, Web-Based-Trainings und weitere E-Learning-Angebote geeignet. Der Einsatz von Lernplattformen, mit denen die Organisation, die Durchführung und der Abschluss solcher Lehrangebote effizient durchgeführt werden können, muss aufgebaut und gefördert werden. Mit Blick auf die Verwaltung sind kontinuierliche Investitionen in die Steigerung der Awareness und Ausbildung der Mitarbeitenden hierbei von großer Bedeutung.

Das Ministerium für Inneres und Sport führt regelmäßig Cybersicherheitstage für unterschiedlichste Zielgruppen durch. Auch die ZAC des LKA sowie der Wirtschaftsschutz des Niedersächsischen Verfassungsschutzes führen regelmäßige Veranstaltungen durch und halten zielgruppenorientierte Informationsangebote vor.

Die Landesregierung wird diese Angebote weiterentwickeln und ausbauen. Hierfür sollen unter anderen spezielle Sensibilisierungskampagnen sowie ressortspezifische Awarenessmaßnahmen durchgeführt werden. Zudem soll ein digitales Informationsportal bereitgestellt werden.

2.10 FACHKRÄFTE

Es werden zunehmend hochqualifizierte Fachkräfte für Wirtschaft und Verwaltung benötigt. Cybersicherheit wird in Studien- und Ausbildungsgängen für unterschiedliche Zielgruppen stärker verankert oder neue Angebote werden implementiert. Die Gewinnung und Bindung von qualifiziertem Fachpersonal bei Staat und Wirtschaft ist eine zentrale Herausforderung. Zielgruppenorientierte Personalgewinnungs- und Entwicklungskonzepte müssen entwickelt, landesweit aufeinander abgestimmt und umgesetzt werden. Durch die Entwicklung von Personal im Kreislauf von Schule, Wissenschaft, Start-ups und Unternehmen wird als positiver Nebeneffekt der Fachkräftemangel auch an anderen Stellen gesenkt und das Innovationspotenzial gefördert. Verbesserte staatliche Anreize werden die Gewinnung von Fachkräften im öffentlichen Dienst zusätzlich vereinfachen. Der Fokus muss aber auch auf dem Ausbau von Ausbildungskapazitäten für Fachkräfte liegen, damit die positive Entwicklung von zukünftigem Fachpersonal nachhaltig und wettbewerbsfähig bleibt.

Ein hohes Niveau an Cybersicherheit bedarf entsprechender Fachkräfte.

Gut ausgebildete Fachkräfte sind heute wie auch in Zukunft elementar für die Cybersicherheit im Land. Dem IT-Fachkräftemangel muss aktiv entgegengewirkt werden, um die Cybersicherheit für die Zukunft zu garantieren. Bereits heute besteht ein diesbezüglicher Mangel, der sich absehbar verschärfen wird. Davon sind die Wirtschaft und der Staat gleichermaßen betroffen. In verschiedenen Bereichen muss diese Herausforderung adressiert werden, in der Aus- und Weiterbildung, der Gewinnung einschließlich dem Anwerben im internationalen Kontext und beim Halten von Fachkräften in der Organisation.

Dabei geht es neben der Verfügbarkeit von Fachkräften auch darum, ein Grundverständnis für IT-Systeme und IT-Sicherheit auf Leitungsebenen und an Schnittstellen sicherzustellen. Als Basis dient die Förderung digitaler Kompetenzen (s. o. Kapitel „digitale Kompetenzen“). Vor diesem Hintergrund werden folgende Ziele und Ansätze verfolgt:

Im Unterrichtsfach Informatik soll allen Schülerinnen und Schülern ein Mindestmaß an IT-Wissen vermittelt werden, einschließlich System- und Sicherheitsgrundlagen. Die curricularen Vorgaben für das Fach Informatik sowie die Lehrerausbildung werden daraufhin geprüft, ob die Cybersicherheit ein Bestandteil des Unterrichts ist. Weiterhin muss es ausreichend Möglichkeiten der Fort- und Weiterbildung geben, damit möglichst viele Lehrkräfte für den Informatikunterricht qualifiziert und für die Cybersicherheit sensibilisiert werden.

Ausbildungsmöglichkeiten im Bereich Cybersicherheit sollen ausgeweitet werden und Bewerbungskampagnen der Wirtschaft unterstützt werden. Im öffentlichen Dienst werden mehr Fachkräfte ausgebildet.

Unsere Hochschulen sind von grundlegender Bedeutung für die Ausbildung von IT-Fachkräften. Ziel muss es daher sein, dem IT-Fachkräftemangel wirksam zu begegnen, um einerseits den Wissenschaftsstandort Niedersachsen zu festigen und andererseits die Cybersicherheit im Land durch kompetentes Fachpersonal langfristig zu sichern. Eine wesentliche Herausforderung ist dabei, diese Fachkräfte für die Verwaltung zu gewinnen. Mit dem Stipendienmodell des Landes Niedersachsen als Kooperation mit der Hochschule Hannover werden im Rahmen des Dualen Studiums „Verwaltungsinformatik“ (B. Sc.) Fachkräfte direkt dort ausgebildet, wo sie langfristig für die Entwicklung und den Betrieb von IT-Systemen notwendig sein werden.

Als attraktiver Arbeitgeber muss sich das Land insbesondere dem demografischen Wandel und der zunehmenden Digitalisierung stellen. Hierzu entwickelt das Land die Rahmenbedingungen für attraktive Arbeitsplätze von IT-Fachkräften laufend weiter.

Als Ausbildungsstätten der akademisch qualifizierten Fach- und Führungskräfte von morgen sowie als zentrale Orte des Erkenntnisgewinns über die Digitalisierung spielen die Hochschulen eine entscheidende Rolle für den langfristigen Erfolg des Landes in einer digitalen Welt. Zur Bewältigung dieser zentralen Herausforderung im Zuge der Digitalisierung stärkt das Land die niedersächsischen Hochschulen in staatlicher Verantwortung seit 2018 nachhaltig durch 50 neue, auf Dauer eingerichtete Digitalisierungsprofessuren, die mit einem Aufwuchs an Studienkapazitäten verbunden sind.

Die Förderung von IT- und Datenkompetenz bei Studierenden und Mitarbeitenden der Hochschulen fördert die Qualifizierung und reduziert zugleich das Risiko von nutzer-induzierten Cyber-Sicherheitsvorfällen.

Qualifizierungsangebote für Unternehmen sollen transparenter gemacht werden und mit Blick auf Qualitätskriterien soll eine Auswahl erleichtert werden. Hier könnte die Idee einer neutralen Plattform greifen, die alle Schulungsangebote auflistet, nach Kategorien und Zielgruppen strukturiert und kriterienbasierte Bewertungen ermöglicht.

Die Anwerbung ausländischer Fachkräfte soll mit einem Fokus auch auf Cybersicherheitsexpertise erfolgen.

2.11 INNOVATIVE FORSCHUNG UND ENTWICKLUNG

Die IT-Sicherheitsforschung in den Ländern ist Quelle und Treiber für Innovationen. Junge Unternehmen müssen gefördert und bei ihrer Entwicklung zu einer schnellen Marktreife im Rahmen der rechtlichen Möglichkeiten unterstützt werden. Forschungsverbünde sollen sich unter Einschluss der nationalen und europäischen Ebene vernetzen. Die Start-up-Szene selbst ist, durch ihre Innovationskraft, ein besonders schützenswerter Bereich.

Die innovativen Forschungen der Hochschulen und der außeruniversitären Forschungseinrichtungen zu Cybersicherheitstechnologien leisten einen wichtigen Beitrag zur Cybersicherheit. Mit prozessorientierten und plattformunterstützten Lösungen müssen die Zusammenarbeit von Wissenschaft und Wirtschaft gestärkt und Cybersicherheit zu einem Markenkern in Niedersachsen weiterentwickelt werden. So müssen Cybersicherheit, Informationssicherheit und Datenschutz als Wettbewerbsvorteil bei Produkten und Dienstleistungen „Made in Niedersachsen“ etabliert und die Innovations- und Wertschöpfungspotenziale in diesen Bereichen gehoben werden.

Durch gezielte Impulse gilt es, die vorhandenen Strukturen in Niedersachsen zu stärken. Diese Kristallisierungspunkte können so eine Anziehungskraft für die Ansiedlung weiterer Organisationen und Unternehmen entfalten. Dies ermöglicht es, Fachkräften Perspektiven und Entwicklungsmöglichkeiten zu bieten und sie langfristig an den Standort Niedersachsen zu binden. Besonders die großen Forschungs- und Entwicklungsstandorte in Niedersachsen sollen noch weiter vernetzt werden, um eine kooperative Zusammenarbeit herbeizuführen.

Zur Stärkung der Cybersicherheitslandschaft in Niedersachsen sind Gesellschaft, Wirtschaft und Verwaltung auf den Transfer von wissenschaftlichen Erkenntnissen der Hochschulen und außeruniversitären Forschungseinrichtungen angewiesen.

Forschung und Entwicklung „Made in Niedersachsen“ ist ein Standortvorteil: Mit 20 Universitäten und Hochschulen und etwa 196.665 Studierenden (Wintersemester 2022/2023) ist Niedersachsen ein Forschungsland. Durch ihre Forschung und Expertise sind die Hochschulen im Land zentrale Akteurinnen und Akteure zum Aufbau von Cybersicherheitskompetenzen. Zahlreiche Hochschulen und außeruniversitäre Forschungseinrichtungen in Niedersachsen sind in der IT-Sicherheitsforschung tätig.

Wir stärken den Wissenschaftsstandort Niedersachsen und fördern den wechselseitigen Wissenstransfer zwischen Wissenschaft und Wirtschaft im Land weiter.

Mit der Errichtung einer Betriebsstätte des Helmholtz-Zentrum für Informationssicherheit (CISPA) an der Leibniz Universität Hannover stärkt Niedersachsen seine Kompetenzen in diesem Bereich und fördert den Aufbau mit 4,5 Mio. Euro. Themenschwerpunkte sind insbesondere „Usable Security and Privacy“ sowie „Industrial Security“.

Zudem wird mit dem „Digital Innovation Campus KI und Sicherheit“ an der Leibniz Universität Hannover ein zentraler Wissenschafts- und Ausbildungsnukleus in Niedersachsen für die zukunftsweisende Technologie der Künstlichen Intelligenz geschaffen, u. a. in Zusammenarbeit mit dem CISPA. Das Land Niedersachsen gibt hierfür einen Zuschuss von ca. 20,9 Mio. Euro. Mit dem seit 2022 verstetigten Standort Niedersachsen des Deutschen Forschungszentrums für Künstliche Intelligenz in Osnabrück und Oldenburg (Aufbauförderung durch das Land 19,6 Mio. Euro), dem landesfinanzierten Informatik Institut OFFIS in Oldenburg und dem institutionell geförderten Forschungszentrum L3S an der Leibniz Universität Hannover sowie den weiteren Arbeitsgruppen an Hochschulen besteht darüber hinaus ein landesweites Netzwerk der Forschung und Entwicklung, das weiter ausgebaut werden soll. Eine verstärkte Einbindung weiterer Hochschulen in Niedersachsen in diese Aktivitäten verstärkt die Breitenwirkung der Initiativen und sichert den Erfolg weiter ab.

Gleichzeitig werden Hochschulen zunehmend zu Angriffszielen im IT-Bereich. Gerade vor dem Hintergrund der Freiheit von Forschung und Lehre stellt diese Bedrohung unsere Hochschulen vor eine besondere Herausforderung. Diese Angriffe können im ungünstigsten Falle den gesamten Hochschulbetrieb über Wochen und Monate gravierend beeinträchtigen. Der unberechtigte Zugriff auf Forschungsdaten stellt eine weitere Bedrohung unserer Hochschulen als Forschungseinrichtungen dar. Im Rahmen der Dachinitiative „Hochschule.digital Niedersachsen“ ergreifen die Hochschulen jenseits der lokalen Aktivitäten zur Informationssicherheit weitere standortübergreifende Maßnahmen zur Vertiefung der Zusammenarbeit im Bereich der Cybersicherheit. In diesem Kontext werden Mittel des Programms „zukunft.niedersachsen“ der VolkswagenStiftung und des Niedersächsischen Ministeriums für Wissenschaft und Kultur in Höhe von 10 Mio. Euro für die Stärkung der Cyberresilienz an den niedersächsischen Hochschulen eingesetzt.

Die Landesregierung unterstützt diese Aktivitäten und durch Bereitstellung einer zentralen Koordination durch das Land Niedersachsen und die Unterstützung bei der Vernetzung mit den bereits genannten Forschungsaktivitäten im Land Niedersachsen.

Zudem sollen Einrichtungen der Wissenschaft und Forschung in Niedersachsen bei der anwendungsorientierten Forschung und bei der Vernetzung unterstützt werden. Die Landesregierung wird die Kooperation zwischen Wirtschaft, Verwaltung und Wissenschaft weiter ausbauen, um den wichtigen wechselseitigen Transfer von Erkenntnissen zu fördern. Wesentlicher Treiber dieses Innovationstransfers sind Start-ups, die nicht nur Arbeitsplätze vor Ort schaffen, sondern gleichzeitig auch die Innovationsfähigkeit des Wissenschaftsstandorts Niedersachsen fördern.

Mit Blick auf die Wirtschaftsspionage sei darauf hingewiesen, dass hier ein großes Gefährdungspotenzial entstehen kann, da andere Staaten häufig an innovativem Wissen interessiert sind. Hierbei sollte bedacht werden, dass ein Informationsabfluss gerade im Bereich der innovativen Technologien schnell stattfinden kann und Mitarbeitende aus Sicherheitssicht grundsätzlich kritisch und individuell überprüft werden sollten. So kann es im Rahmen der Ausspähung dieses Wissens zu enormen reputativen und zukünftigen finanziellen Schäden kommen, sodass eine frühestmögliche Sensibilisierung und Fokussierung unter anderem auf das Thema Cybersicherheit angeraten wird. Der Wirtschaftsschutz steht hierbei beratend, wie im Handlungsfeld 2.4 bereits erläutert, zur Verfügung.

2.12 NATIONALE UND INTERNATIONALE KOOPERATIONEN

Der Cyberraum macht nicht vor nationalen oder internationalen Grenzen halt. Eine tiefergehende Vernetzung der beteiligten Akteurinnen und Akteure von Bund und Ländern ist daher eine Notwendigkeit zum effektiven und effizienten Austausch zur Prävention und Bewältigung von Herausforderungen der Cybersicherheit. Das Land Niedersachsen hat daher bereits im Jahr 2018 gemeinsam mit dem BSI eine Absichtserklärung zur vertieften Kooperation beider Parteien unterzeichnet. Die vertrauensvolle und enge Zusammenarbeit wurde im Jahr 2021 durch eine gemeinsame Kooperationsvereinbarung weiter gefestigt und soll weiterhin ausgebaut werden. Ziel ist es, eine leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur und eine Stärkung der Bund-Länder-Zusammenarbeit voranzubringen.

Der Koalitionsvertrag 2021-2025 zwischen SPD, Bündnis 90/Die Grünen und FDP auf Bundesebene sieht einen strukturellen Umbau der IT-Sicherheitsarchitektur vor. Im Zuge dessen soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger aufgestellt und als zentrale Stelle im Bereich IT-Sicherheit ausgebaut werden. Die Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat konkretisiert dieses Vorhaben und führt aus, dass das BSI zu einer dritten Säule – neben dem BKA im Polizeiwesen und dem BfV im Verfassungsschutzbund – einer föderal integrierten Cybersicherheitsarchitektur ausgebaut werden soll. Eine Zentralstelle erlaubt die institutionalisierte Zusammenarbeit in Form einer auf Dauer angelegten Kooperation, z. B. durch laufende gegenseitige Unterrichtung und Auskunftserteilung, wechselseitige Beratung, gegenseitige Unterstützung und Hilfeleistung in den Grenzen der je eigenen Befugnisse und Einrichtung organisatorischer Verbindungen, gemeinschaftlicher Einrichtungen und gemeinsamer Informationssysteme. Insbesondere eine umfassende Lagebilderstellung würde für Niedersachsen einen erheblichen Mehrwert bieten. Das Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) hat bereits bei seiner Verabschiedung in bestimmten Fällen eine engere Zusammenarbeit mit dem BSI eröffnet.

Ein weiterer Eckpunkt einer gesamtstaatlichen Cybersicherheitsarchitektur ist eine flächendeckende Umsetzung der vom BSI und IT-Planungsrat empfohlenen Standards und Maßnahmen. Darüberhinausgehende Empfehlungen für eine ganzheitliche Cybersicherheit von EU, Vereinten Nationen, OSZE, NATO, OECD, Europarat sowie multilaterale Foren (Global Conference on Cyberspace, Central European Cyber Security Platform, Freedom Online Coalition) müssen periodisch mit dem Ziel der Umsetzung von Maßnahmen zur Erhöhung der Cybersicherheit in Niedersachsen ausgewertet werden.

Für den Bereich der strafrechtlichen Rechtshilfe ist auszuführen, dass es in der Zuständigkeit des Bundes liegt, entsprechende völkerrechtliche Verträge oder sonstige Rechtsakte in diesem Bereich abzuschließen. Die Landesregierungen begleiten etwaige Vertragsverhandlungen oder sonstige Rechtakte und setzen diese später – sofern erforderlich – um. So ist das Übereinkommen über Computerkriminalität vom 23. November 2001 (BGBl. II 2008, 1243) zwischen den Mitgliedstaaten des Europarats und weiteren Staaten (Eu-ComputerÜbk2001; Cybercrime-Convention; Budapest-Konvention) für Deutschland seit dem 01.07.2009 in Kraft. Das Übereinkommen ist eine internationale Vereinbarung über mittels Internet oder sonstiger Computernetze begangener Straftaten (sog. Cybercrimes), insbesondere Verletzungen des Urheberrechts, Betrug per Computer, Kinderpornographie und Verstöße gegen die Sicherheit von elektronischen Netzen. Das Übereinkommen zielt auf einen Mindeststandard bei den Strafvorschriften

über bestimmte schwere Formen der Computerkriminalität ab. Darüber hinaus enthält es Vorgaben für das Strafverfahrensrecht, die internationale Zusammenarbeit und zur Rechtshilfe. Soweit also Übereinkommen oder andere Rechtsakte die Einrichtung spezieller Stellen mit Ansprechpersonen etc. vorsehen, werden diese Vorgaben im Bereich des Strafrechts und der internationalen Rechtshilfe in Strafsachen umgesetzt. Dies gilt beispielsweise auch mit Blick auf das Europäische Justizielle Netz für Cyberkriminalität (EJCN). Das EJCN ist ein Netzwerk von Staatsanwältinnen und Staatsanwälten und Ermittlungsrichterinnen und Ermittlungsrichtern, die auf Cyberkriminalität, durch Cyberspace ermöglichte Kriminalität und strafrechtliche Ermittlungen im Cyberspace spezialisiert sind. Das EJCN wurde durch die Schlussfolgerung des Rates der Europäischen Union vom 9. Juni 2016 (10025/16) mit dem Ziel eingerichtet, den Austausch von Fachwissen und bewährten Praktiken zu erleichtern, die Zusammenarbeit zwischen den zuständigen Justizbehörden zu verbessern und den Dialog zur Gewährleistung der Rechtsstaatlichkeit im Cyberspace zu fördern. Jeder Mitgliedstaat soll entsprechend seiner einzelstaatlichen Verfahren mindestens einen nationalen Vertreter der Justizbehörden mit einschlägiger Erfahrung für die Teilnahme an dem Netz benennen. Eurojust hat die Aufgabe, das Netzwerk zu unterstützen.

Das Land Niedersachsen wird auch künftig bei nationalen und internationalen Rechtsetzungsverfahren die erforderlichen Impulse geben, um die gesamtstaatliche Cybersicherheitsarchitektur zu stärken.

3 CYBERSICHERHEITSZENTRUM NIEDERSACHSEN

Zur besseren Koordinierung von Cybersicherheitsaktivitäten im Niedersächsischen Ministerium für Inneres und Sport wurde im Januar 2014 die Cyberkoordinierungsgruppe gegründet. Der Mitgliederkreis setzt sich aus den Fachreferaten des Niedersächsischen Ministeriums für Inneres und Sport zusammen, die mit diesem Themenumfeld betraut sind. In der Cyberkoordinierungsgruppe informieren sich die Mitglieder über aktuelle Geschehnisse, stimmen gemeinsame Bedarfe, Positionen und Vorgehensweisen ab. Hierbei wird sichergestellt, dass die Informationsflüsse seitens des Bundes und der Länder in Niedersachsen an einer Stelle zusammengeführt und zu einer Lagebewertung bereitstehen.

Um die niedersächsische Landes- und Kommunalverwaltung gegen Cyberangriffe zu schützen, ist es erforderlich, dass Akteurinnen und Akteure der Cybersicherheit auf allen Ebenen institutionalisiert und kooperativ zusammenarbeiten (vgl. Kapitel 2.1 Intensivierung der Vernetzung der Cybersicherheitsakteure). Insbesondere sind hierbei eine ganzheitliche Lagebilderstellung sowie etablierte Informationsflüsse in Echtzeit von elementarer Bedeutung (vgl. Kapitel 2.2.6 Ganzeinheitliche Lagebilderstellung). Neben der technischen Absicherung ist auch der souveräne Umgang mit technischen Systemen durch Nutzende sowie eine durchdachte Incident-Response-Strategie von besonderem Belang, um eine umfassende Resilienzstrategie verfolgen zu können (vgl. 2.2.8 Vorfallsbewältigung, 2.2.9 Notfallmanagement). Auch die Wirtschaft in Niedersachsen sowie Betreibende kritischer Anlagen, wesentlicher und wichtiger Einrichtungen (i. S. NIS-2-RL) können davon profitieren (vgl. 2.5 Kritische Infrastrukturen sowie wesentliche und wichtige Einrichtungen, 2.6 Wirtschaft). Die Fachgebiete „Cybersecurity“ (CERT-Leistungen), „Cybercrime“ (polizeiliche Aspekte), „Cyberintelligence“ (nachrichtendienstliche Aspekte, Verfassungsschutz Niedersachsen) und Katastrophenschutz gehören zu den Kernbereichen der institutionalisierten Zusammenarbeit. Die zuständigen (Schwerpunkt-) Staatsanwaltschaften in Niedersachsen werden in die Zusammenarbeit einbezogen.

Im Rahmen des Koalitionsvertrages 2022 zwischen der SPD und Bündnis 90/Die Grünen wurde festgelegt, ein robustes Cybersicherheitszentrum einzurichten. Beschlüsse der Landesregierung zur „Digitalen Verwaltung 2030“ und zur Umsetzung durch den „Handlungsplan Digitale Verwaltung Niedersachsen“ greifen dieses Vorhaben auf.

Um diese Ziele erreichen zu können, werden in Niedersachsen die Strukturen im Bereich Cybersicherheit durch die Errichtung eines Cybersicherheitszentrums gestärkt und ausgebaut. Das Cybersicherheitszentrum soll dabei unterstützen, Cyberangriffe auf die Infrastrukturen der niedersächsischen Landesverwaltung zu verhindern und für die kommunalen Verwaltungen, die Wirtschaft und Betreibende kritischer Anlagen und weiteren Zielgruppen in Niedersachsen praktische Unterstützungsangebote vorhalten und die Nachwuchsgewinnung fördern. Es bildet ein attraktives Arbeitsumfeld für die unterschiedlichen Beteiligten durch die Möglichkeit des Austausches und der Spezialisierung. Damit können dauerhaft Kompetenzen aufgebaut werden, die in den einzelnen Organisationseinheiten nur schwer langfristig gebunden werden können.

Im Rahmen einer Cyberakademie als weiteren wichtigen Bestandteil des Cybersicherheitszentrums können die Aufgaben Beratung, Fortbildung und Schulung angesiedelt und praktische Angebote für Landes- und auch Kommunalbedienstete bereitgestellt werden. Eine enge Verbindung mit universitären Einrichtungen wie dem CISPA – Helmholtz-Zentrum für Informationssicherheit in Hannover und anderen Bildungsträgern sorgt für einen intensiven Transfer und ermöglicht, attraktive Aus-, Weiter- und Fortbildungsangebote zu entwickeln.

Mit seinen Diensten, seiner Expertise und seinen Ressourcen stellt das Cybersicherheitszentrum eine kompetente Anlaufstelle für die Unterstützung bei der Prävention sowie der Bewältigung von Cybersicherheitsvorfällen dar. Durch die Schwerpunktbildung kann das Cybersicherheitszentrum die Sichtbarkeit des Themas Cybersicherheit dauerhaft verankern. Schlussendlich wird eine zentrale, effiziente und umfassende Stärkung der Cybersicherheit in Niedersachsen hergestellt. Die bisherigen konzeptionellen Ausarbeitungen werden im Niedersächsische Ministerium für Inneres und Sport zur Umsetzungsreife fortgeführt.

4 GLOSSAR

Awareness
Awareness beschreibt das Bewusstsein einer Person oder Organisation für bestimmte Risiken, Bedrohungen oder Chancen. Im Bereich der Cybersicherheit ist Awareness besonders wichtig, um die Nutzenden von Computersystemen auf die Gefahren von Cyberangriffen und anderen Bedrohungen aufmerksam zu machen und sie dazu zu bewegen, sich sicherheitsbewusst zu verhalten.

Business Continuity Management (BCM)
Die Fortführung oder Wiederaufnahme aller zeitkritischen Geschäftsprozesse nach Schadensereignissen, um die Arbeitsfähigkeit und die wirtschaftliche Existenz einer Institution zu sichern, wird als Business Continuity (BC) bezeichnet. Die Steuerung sämtlicher Aktivitäten, die eine geordnete Geschäftsfortführung nach Schadensereignissen zum Ziel haben, ist Aufgabe des Business Continuity Management (BCM) und wird im BSI Standard 200-4 BCM beschrieben.

Chief Information Security Officer (CISO) des Landes Niedersachsens
Der Chief Information Security Officer des Landes Niedersachsens ist der oder die Informationssicherheitsbeauftragte der Landesverwaltung und ist für die Koordinierung des ressortübergreifenden Informationssicherheitsmanagementsystems und für die strategische, ressortübergreifende Planung und Steuerung des Informationssicherheitsprozesses in der gesamten Landesverwaltung zuständig.

Computer Emergency Response Team (CERT)
Das Niedersachsen-CERT (N-CERT), welches sich aus IT-Spezialistinnen und -Spezialisten zusammensetzt, agiert in Niedersachsen als koordinierendes CERT. In vielen Unternehmen und Institutionen sind mittlerweile CERTs etabliert, die sich um die Abwehr von Cyberangriffen, die Reaktion auf IT-Sicherheitsvorfälle sowie um die Umsetzung präventiver Maßnahmen kümmern.

Cybercrime
Die Motivation von Cyber-Kriminellen ist es, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Die Bandbreite reicht von einfacher Kriminalität mit geringen Schäden bis hin zu organisierter Cyber-Kriminalität. Organisierte Cyber-Kriminalität reicht vom Identitätsdiebstahl mit Warenbetrug über den Diebstahl von Geld durch Missbrauch von Bankdaten bis hin zur Erpressung. Organisierte Cyber-Kriminelle nutzen die genannten Vorteile von Cyber-Angriffen bei ihren Aktivitäten mit hoher Professionalität aus. Im Gegensatz zur organisierten Kriminalität sind einfache Cyber-Kriminelle meist Einzelpersonen oder kleine Gruppen, die sich durch geringere Professionalität in ihrem Handeln auszeichnen. Dementsprechend ist auch die Auswahl der Angriffsziele eingeschränkt und der verursachte Schaden typischerweise geringer.

Cyberintelligence
Cyberintelligence aggregiert Informationen mit dem Ziel, digitale Infrastrukturen und Daten zu schützen. Aufgabe der Cyberintelligence ist es, Schwachstellen, Angriffe und aktuelle Bedrohungslagen im Cyberbereich zu erkennen und effizient und umfassend zu bewerten (vgl. N-CERT-Aufgaben).

Cyberraum
Mit dem Begriff „Cyberraum" bezeichnet man die virtuelle Welt aller vernetzten IT-Systeme im Internet. Im Cyberraum gibt es keine physischen Distanzen oder zeitliche Verzögerungen zwischen den vernetzten IT-Systemen. Alle IT-Systeme sind weltweit und zu jeder Zeit erreichbar und können miteinander kommunizieren und agieren. IT-Systeme, die nicht direkt an das Internet angeschlossen sind, aber mit solchen verbunden sind oder Daten austauschen, werden zum Cyberraum gezählt. In diesem sehr weit gefassten und allumspannenden Cyberraum ergeben sich neue und aber zumeist veränderte Bedrohungen, die mit dem Begriff „Cyberbedrohungen" belegt werden.

Cybersicherheit / Cybersecurity
Cybersicherheit bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzenden solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen. Besondere Bedeutung hat dabei der Schutz der wesentlichen und wichtigen Einrichtungen sowie der kritischen Anlagen.[5]

[4] Siehe EU NIS-2-RL.
[5] Siehe Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (EU NIS-2-RL).

Cybersicherheitsarchitektur
Die Cybersicherheitsarchitektur beschreibt das Zusammenspiel der Akteurinnen und Akteure, Prozesse und Einrichtungen sowohl auf organisatorischer wie auch auf technischer Ebene in Bezug auf die Erreichung eines hohen Cybersicherheitsniveaus. Die Cybersicherheitsarchitektur stellt über ein gemeinsames Bild sicher, dass die einzelnen Bausteine der Cybersicherheit zusammenwirken und sich ergänzen können.

Informationssicherheit
Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in IT-Systemen oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Es können auch weitere Grundwerte einbezogen werden.

Informationssicherheitsmanagementsystem (ISMS)
Das ISMS legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).

Internet of Things
„IoT" steht für Internet of Things, also das Internet der Dinge. Im Gegensatz zu „klassischen" IT-Systemen umfasst das Internet der Dinge „intelligente" Gegenstände, die zusätzliche „smarte" Funktionen enthalten. Diese Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden.[6]

IT-Sicherheit
IT-Sicherheit kümmert sich um die technisch-organisatorischen Maßnahmen zur Sicherstellung der Informationssicherheit bei IT-Systemen.

IT-Systeme
IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.[7]

Mobile Incident Response Team (MIRT)
Mobile Incident Response Teams sind spezialisierte Teams, die in Notfällen schnell reagieren können, um IT-Sicherheitsvorfälle zu untersuchen und zu beheben. MIRT sind mobil und können bei Bedarf an den Ort des Vorfalls reisen, um schnell und effektiv zu handeln.

Security by Default
Produkte, Anwendungen und Verfahren sind im Normalzustand mit sicherheits- und datenschutzfreundlichen Einstellungen belegt.

Security by Design
Security by Design ist ein in der Hard- und Softwareentwicklung angewandtes Designkonzept. Die Sicherheit der Hard- oder Software wird bereits im Entwicklungsprozess berücksichtigt und in den kompletten Lebenszyklus eines Produkts integriert. Zu den Designkriterien zählen beispielsweise die Minimierung der Angriffsfläche, der Einsatz von Verschlüsselung und Authentifizierung und die Isolation sicherheitsrelevanter Bereiche. Die Sicherheit wird kontinuierlich getestet.

Zero-Trust-Architektur
Zero Trust Architektur ist ein modernes IT-Sicherheitskonzept, das auf der laufenden Kontrolle sämtlicher Transaktionen und Interaktionen im Netzwerk basiert. Im Gegensatz zu traditionellen Sicherheitsmodellen, die auf einer impliziten Vertrauensbasis aufbauen, geht Zero Trust davon aus, dass jeder Anwendende, jede Verbindung und jedes Asset als nicht vertrauenswürdig gilt, bis die Verifizierung erfolgt ist.

[6] Siehe EU NIS-2-RL.
[5] Gemäß Glossar der Allianz für Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de (Oktober 2024).
[7] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, verfügbar unter: https://www.bsi.bund.de (Oktober 2024).

Impressum

Herausgeber:
Niedersächsisches Ministerium für Inneres und Sport
Schiffgraben 12
30159 Hannover
pressestelle@mi.niedersachsen.de
www.mi.niedersachsen.de

Bilder von stock.adobe.com: S. 4: ©Seventyfour; S. 6: ©sebra; S. 7: ©Andrey Popov; S. 11: ©bernardbodo; S. 15: ©amnaj; S. 16: ©Urupong; S. 17: ©ASDF; S. 18: ©joyfotoliakid; S. 21: ©Gorodenkoff; S.23: ©NDABCREATIVITY; S. 24: ©Waldteufel; S. 27: ©Creator88; S. 28: ©Funtap; S. 31: ©lemoncraft; S. 33: ©NAMPIX; S. 34: ©Gorodenkoff; S. 37: ©Dan Dalton/KOTO; S. 41: ©alfa27; S. 43: ©Michael C/peopleimages.com;

Hannover, November 2024

Niedersächsisches Ministerium
für Inneres und Sport