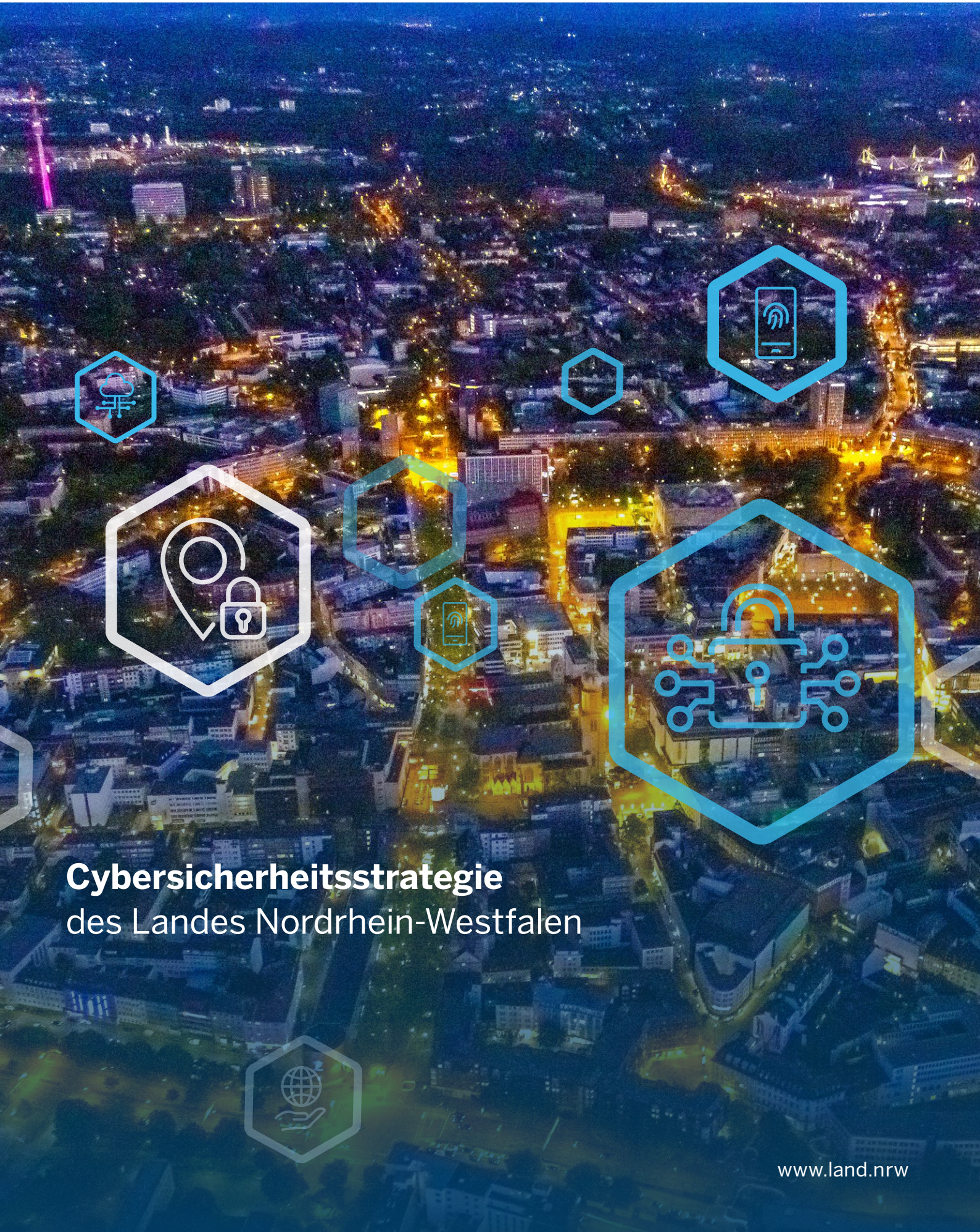
Die Landesregierung
Nordrhein-Westfalen



Cybersicherheitsstrategie
des Landes Nordrhein-Westfalen

www.land.nrw

Vorwort

Die Pandemie hat jedem einzelnen von uns noch einmal deutlich vor Augen geführt, wie wichtig und unverzichtbar digitale Möglichkeiten für unser tägliches Leben sind – beruflich wie privat.

Neben vielen Chancen bringt die zunehmende Digitalisierung aller Lebensbereiche aber auch Risiken und Gefahren mit sich. So sind Cyberangriffe in unserer vernetzten Welt zu einer ernsten und täglichen Bedrohung geworden. Sie betreffen sehr persönliche Daten, sie greifen empfindlich in unser Leben und in die Wirtschaft ein. Ob Diebstahl, Spionage oder Erpressung – Kriminalität findet zunehmend im Internet statt. Schon heute werden weltweit jeden Tag mehr als sechs Millionen Cyberangriffe verübt – und es zeichnet sich ab: Diese Zahl wird in Zukunft weiter steigen. Und noch ein Trend führt dazu, dass diese Bedrohung steigt: Kriminelle im Netz planen zunehmend komplexere Angriffe und führen ihre Taten immer professioneller aus.

Aktuelle Studien zeigen: Die wirtschaftlichen Schäden liegen allein in Deutschland im Milliardenbereich. Angriffe auf vernetzte, kritische Infrastrukturen, wie zum Beispiel Krankenhäuser oder Energiesysteme, können erhebliche Auswirkungen auf das öffentliche Leben haben und sogar Menschenleben gefährden. Und nicht zuletzt ist auch die gezielte Verbreitung von Desinformation, um beispielsweise im Vorfeld von Wahlen politisch Einfluss zu nehmen, eine Bedrohung für unsere freiheitlichen Grundwerte und unsere Demokratie.

Cybersicherheit ist also ein Thema, das uns alle angeht – jede Bürgerin und jeden Bürger genauso wie Wissenschaft, Wirtschaft und Staat. Sie stellt eine sicherheitspolitische Herausforderung für unsere Demokratie und für unseren Wohlstand dar, die wir nur gemeinsam bewältigen können. Nordrhein-Westfalen ist hier bereits auf einem guten Weg. Die von der Landesregierung eingerichtete

HENDRIK WÜST
Ministerpäsident des Landes
Nordrhein-Westfalen

HERBERT REUL
Minister des Innern des Landes
Nordrhein-Westfalen

und im Ministerium des Innern angesiedelte Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen ist ein wichtiger Schritt für mehr Sicherheit im digitalen Raum.

Die neue Cybersicherheitsstrategie geht diesen Weg konsequent weiter. Hierbei verfolgen wir einen vernetzten wie auch integrierten Ansatz. Wir wollen gemeinsam mit allen gesellschaftlichen Akteuren die Cybersicherheit in und für unser Bundesland und seine Menschen erhöhen. Dabei können wir in Nordrhein-Westfalen auf ein enormes Potenzial in Wissenschaft, Zivilgesellschaft und Wirtschaft aufbauen. Information, Prävention und die Stärkung der Resilienz von Personen und Strukturen sind neben der notwendigen Verfolgung von Cyberstraftaten zentrale Faktoren des Erfolges. Und es bleibt wichtig, vorhandene Strukturen und Angebote auszubauen, weiter zu stärken und bekannter zu machen.

Denn: Informierte Menschen sind in der Lage, Gefahren und Risiken besser zu erkennen und aktiv zu handeln. Das gilt sowohl für das Private als auch im beruflichen Kontext. Die Menschen in unserem Land und all jene, die in der Wissenschaft, in Wirtschaftsunternehmen, Behörden und Institutionen Entscheidungen treffen, müssen über Cybersicherheitsrisiken und mögliche Gefahren aufgeklärt sein, um sich selbst, ihre Organisation und die Mitarbeiterinnen und Mitarbeiter angemessen schützen zu können. Wir alle sind hierbei gefragt.

Wir laden Sie also herzlich ein, aktiv an der Verbesserung der Cybersicherheit in und für Nordrhein-Westfalen mitzuwirken!

Hendrik Wüst MdL Herbert Reul

Management Summary

Cybersicherheit bildet das Rückgrat für eine erfolgreiche Digitalisierung. Die anhaltende Beschleunigung und Ausweitung der digitalen Transformation haben das Bewusstsein für eine damit einhergehende, sichere Nutzung des Cyberraums bereits gestärkt. Um für die Zukunft in Nordrhein-Westfalen ein noch höheres Cybersicherheitsniveau zu erreichen, schafft die Landesregierung mit dieser Strategie – auch mit Blick auf die Innere Sicherheit – die Voraussetzungen für eine Schärfung des Bewusstseins als Prävention sowie für eine schnelle Einsatzbereitschaft im Falle digitaler Bedrohungen, einen besseren Schutz vor Cyberangriffen und eine Minderung der daraus resultierenden Folgen.

Dafür hat die Landesregierung Nordrhein-Westfalen folgende Ambition formuliert: „Wir haben das Ziel, gemeinsam mit allen gesellschaftlichen Akteuren das Cybersicherheitsniveau in und für Nordrhein-Westfalen zu verbessern."

Für die Realisierung dieser Ambition benennt die Landesregierung drei Handlungsfelder und sechs strategische Ziele:

ABBILDUNG 1

Die drei Handlungsfelder zur Erhöhung der Cybersicherheit in Nordrhein-Westfalen

Die sechs strategischen Ziele der Landesregierung:

1. Erhöhung der Wahrnehmung von Cybersicherheit
2. Cybersicherheitsprävention für kleine und mittlere Unternehmen
3. Steigerung der Cybersicherheitskompetenzen von Bürgerinnen und Bürgern sowie Unternehmen
4. Steigerung der Effektivität und Effizienz der Kommunikation der Cybersicherheitsakteure im Land und aus dem Land heraus
5. Unterstützung der Forschung und des Ausbaus des Wissenschaftsstandorts Nordrhein-Westfalen
6. Verbesserung der Datenlage im Bereich Cybersicherheit

Diese strategischen Ziele sollen im Rahmen von konkreten Maßnahmen erreicht werden, die den drei Handlungsfeldern zugeordnet werden. Das erste Handlungsfeld **Cybersicherheit in Nordrhein-Westfalen** stellt das bewusste und verantwortungsvolle Handeln einer jeden Person für die individuelle Sicherheit im Cyberraum in den Fokus.

Das zweite Handlungsfeld **Koordination und Kooperation in Nordrhein-Westfalen** bezieht sich auf die effiziente Vernetzung der Cybersicherheitsakteure als ein Lösungsweg für ein erhöhtes Schutzniveau im Land.

Die Erhöhung der Attraktivität Nordrhein-Westfalens als Wirtschafts- und Wissenschaftsstandort wird im Zuge des dritten Handlungsfeldes **Cybersicherheit als Erfolgsfaktor für Nordrhein-Westfalen** angestrebt.

Diese drei Handlungsfelder richten sich an die Zielgruppen Bürgerinnen und Bürger, Wirtschaft, Wissenschaft und die öffentliche Verwaltung.

In den Handlungsfeldern werden konkrete Umsetzungsmaßnahmen beschrieben, die die Zielerreichung unterstützen. Zu den **konkreten Maßnahmen** der Landesregierung zählen insbesondere umfassende Informationsangebote und eine Vielzahl von Programmen zur Steigerung der individuellen Medienkompetenz, um die Prävention vor Cyberangriffen zu fördern. Für eine gesteigerte und effizientere Vernetzung der Cybersicherheitsbehörden mit den vorhandenen Cybersicherheitsakteuren im Land kommt der offenen Kommunikation und der Kooperation eine besondere Bedeutung zu.

Ziel ist es ferner, das **Vertrauen in die staatlichen Institutionen** im Umgang mit Cyberangriffen zu stärken. Angriffe auf die Cybersicherheit werden aus unterschiedlichen Gründen häufig nicht bei staatlichen Stellen gemeldet und auf die Inanspruchnahme von Hilfe verzichtet. Übergreifend strebt das Land Maßnahmen zum Ausbau einer besseren Datenlage der Cybersicherheit an, um die Handlungsfähigkeit und Sicherheit Nordrhein-Westfalens im Cyberraum auch für die Zukunft zu erweitern, Handlungsbedarfe aufzudecken und die Erreichung von strategischen Zielen nachvollziehbarer zu machen.

Da Cybersicherheit **Landes- und Bundesgrenzen überschreitet**, ordnet sich die Strategie für Nordrhein-Westfalen in die strategischen Überlegungen auf Bundes- und EU-Ebene ein. So werden die Vorschläge der Bundes- und der EU-Cybersicherheitsstrategie berücksichtigt, die Zusammenarbeit Nordrhein-Westfalens mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) – insbesondere in dem Bereich Kritische Infrastrukturen (KRITIS) – verstärkt und Nordrhein-Westfalens Mitwirken in landesübergreifenden Kooperationen herausgestellt.

Die Cybersicherheitsstrategie konkretisiert die Digitalisierungsstrategie der Landesregierung in Nordrhein-Westfalen hinsichtlich der Ausgestaltung des Querschnittthemas Cybersicherheit und unterstützt deren Leitlinie, dass Datenschutz, Informationssicherheit und Datensouveränität unserer Bürgerinnen, Bürger und Unternehmen die Grundlage für unsere digitale Gesellschaft sind.

Die Cybersicherheitsstrategie für Nordrhein-Westfalen ist zunächst auf drei Jahre angelegt. Um dem dynamischen Charakter der Cybersicherheitsthematik gerecht zu werden, sollen eine Evaluation und Weiterentwicklung folgen. Anpassungen durch die Landesregierung sind jedoch in Anbetracht des sich rasant entwickelnden Cyberraums auch vor Ablauf der drei Jahre möglich.

Inhaltsverzeichnis

Einleitung

1.0

Die fortschreitende **Digitalisierung** verändert Staat, Wirtschaft und Gesellschaft tiefgreifend. Sie ist sowohl der Schlüssel für die Modernisierung von staatlichen Institutionen, der Bildungs- und Ausbildungslandschaft als auch für die Innovation und Wettbewerbsfähigkeit von Unternehmen. Gleichzeitig birgt die steigende Abhängigkeit z. B. vom „Internet der Dinge“ hohe **Sicherheitsrisiken** für Bürgerinnen und Bürger, Wirtschaft und staatliche Akteure.

Die **Cyber-Bedrohungslage** ist auch in Nordrhein-Westfalen geprägt von einer steigenden Anzahl und stetig komplexeren Cyberangriffen sowie sich ständig wandelnden Bedrohungen. Es gehört zu den Aufgaben des Staates, im Rahmen der Inneren Sicherheit für einen höheren Schutz zu sorgen und dadurch **notwendiges Vertrauen im Cyberraum** zu schaffen. Als bevölkerungsreichstes Bundesland mit den meisten steuerpflichtigen Unternehmen nimmt Nordrhein-Westfalen diese Aufgabe an und veröffentlicht hiermit eine eigene **Cybersicherheitsstrategie**.

Die Landesregierung von Nordrhein-Westfalen steht an der Seite der Bundesregierung und der Europäischen Union, um sich für einen globalen, offenen, stabilen und **sicheren Cyberraum** einzusetzen, der auf **Rechtsstaatlichkeit, Menschenrechten, Grundfreiheiten und demokratischen Werten** beruht. Die nordrhein-westfälische Cybersicherheitsstrategie verpflichtet sich diesen Werten. Diese leiten das Handeln des Landes im Bereich Cybersicherheit in den nächsten drei Jahren und finden sich übersetzt in den geplanten strategischen Maßnahmen wieder.

ABBILDUNG 2

Ambition der Cybersicherheitsstrategie der Landesregierung Nordrhein-Westfalen

> Wir haben das Ziel, gemeinsam mit allen gesellschaftlichen Akteuren das Cybersicherheitsniveau in und für Nordrhein-Westfalen zu verbessern.

Je stärker die digitale Transformation in Gesellschaft und Wirtschaft voranschreitet, desto mehr wird Cybersicherheit zu einem entscheidenden Faktor für deren Gelingen. Mobile Kommunikation, mobiles Arbeiten und digitales Lernen sind mittlerweile in fast allen Gesellschafts- und Wirtschaftsbereichen selbstverständlich. Damit die beschleunigte Digitalisierung gelingt, brauchen Bürgerinnen und Bürger sowie Unternehmen, Schulen und Hochschulen Vertrauen in die Sicherheit der Internetnutzung. Die Zusammenarbeit inner- und außerhalb des Landes ist bei diesem wichtigen Vorhaben zu verstetigen. Damit will die Landesregierung in Zukunft sicherstellen, noch schneller auf digitale Bedrohungen reagieren zu können, den Schutz vor Angriffen insgesamt zu verbessern und deren Folgen zu vermindern.

Alle Ressorts des Landes Nordrhein-Westfalen beschäftigen sich intensiv mit Digitalisierungsthemen und setzen eigene Digitalisierungsvorhaben um.

Nur wenn Cybersicherheit als eine **Querschnittsaufgabe** verstanden wird, können Chancen und Potenziale der Digitalisierung sicher genutzt werden.

Im Cyberraum entstehen immer neue Bedrohungen, die sich auf alle Lebensbereiche auswirken. Die Landesverwaltung setzt Maßnahmen zur Informationssicherheit nach dem IT-Grundschutz um, um diesen Bedrohungen zu begegnen. Für Bürgerinnen und Bürger sowie Unternehmen existieren weitere geeignete und eigene Möglichkeiten, sich zu schützen. Diese Selbstschutz-Maßnahmen fördern die Resilienz und senken das Risiko von Cyberbedrohungen. Einige dieser Ansätze werden in der Strategie aufgezeigt.

Die Cybersicherheitsstrategie des Landes Nordrhein-Westfalen bildet einen weiten, ressortübergreifenden Rahmen für die Cybersicherheitsaktivitäten der Landesregierung. Sie steht im Einklang mit der Digitalstrategie der Landesregierung und konkretisiert diese hinsichtlich der Ausgestaltung des Querschnittthemas Cybersicherheit.

Um dem dynamischen Charakter des Themas Cybersicherheit gerecht zu werden, bedarf es **regelmäßiger Anpassungen und Fortschreibungen** dieser Cybersicherheitsstrategie. Der ab 2021 jährlich erscheinende Bericht zur Cybersicherheit in Nordrhein-Westfalen verschafft zukünftig einen komprimierten Überblick über den Stand der Cybersicherheit sowie des Umsetzungsfortschritts der Cybersicherheitsstrategie. Die Überprüfung der Entwicklung des Cybersicherheitsniveaus in Nordrhein-Westfalen erfolgt auf der Grundlage eines Datenkonzeptes. Eine strukturierte regelmäßige Datenerhebung und Studien im Auftrag der Landesregierung ergänzen die Darstellung der Cybersicherheitslage in Nordrhein-Westfalen.

Die Strategie wird zudem fortlaufend im Hinblick auf neue Technologien und Erkenntnisse sowie die aktuelle Gefährdungslage und wichtige äußere Umstände (Pandemie, Terrorismus etc.) überprüft werden. Der Zeitraum dieser Cybersicherheitsstrategie umfasst zunächst **drei Jahre (2021–2024)**, wobei Aktualisierungen der Strategie auch vor Ablauf dieses Zeitraums möglich sind.

Die verstärkte Digitalisierung in Gesellschaft, Wirtschaft und Verwaltung macht es erforderlich, dass der Staat – und damit auch die Landesregierung von Nordrhein-Westfalen – konkrete Maßnahmen zur Verbesserung der Sicherheit im Cyberraum ergreift.


od.use_x = False
od.use_y = True
od.use_z = False
ion == "MIRROR_Z":
od.use_x = False
od.use_y = False
od.use_z = True
on at the end -add back the deselected mirror modifier object
lect= 1
select=1
scene.objects.active = modifier_ob
ted" + str(modifier_ob)) # modifier ob is the active ob
ob.select = 0

Ausgangslage der Cybersicherheit und Cybersicherheitsarchitektur in Nordrhein-Westfalen

2.0

Im Jahr 2020 wurde die Digitalisierung in ganz Deutschland, auch aufgrund der Corona-Pandemie, deutlich vorangetrieben und ihre Möglichkeiten in vielen Lebens- und Geschäftsbereichen sichtbarer. Oft konnte die Arbeit ins Homeoffice verlegt, online eingekauft und der private Kontakt über Videokonferenzen gepflegt werden. Universitäten und Schulen sahen sich vielfach dabei gefordert, den Lehrbetrieb kurzfristig auf digitale Formate umzustellen.

Die unterschiedlichen Facetten der Digitalisierung stellen die Menschen vor neue Herausforderungen.

ABBILDUNG 3

Ausgangslage der Cybersicherheit in Nordrhein-Westfalen

Cybersicherheit ist nicht mehr ausschließlich ein Thema für Fachleute. Nordrhein-westfälische Bürgerinnen und Bürger besitzen häufig mehrere internetfähige Geräte, wie Smartphones, Computer und Tablets. Auch andere Geräte wie zum Beispiel Leuchtmittel, Kühlschränke oder Rollläden sind heutzutage digital steuerbar und vernetzt. 95 Prozent der privaten Haushalte in Nordrhein-Westfalen verfügen über einen Internetanschluss. Somit betrifft die digitale Vernetzung, deren Sicherheit ganzheitlich betrachtet werden muss, mittlerweile die große Mehrheit aller Haushalte.

Die zunehmende digitale Vernetzung schafft aber auch eine **größere Angriffsfläche für Cyberkriminelle**. Bedrohungsarten wie Malware, Spam, Phishing und andere Cyberangriffe auf Rechner, Smartphones sowie sonstige internetfähige Endgeräte nehmen weiter zu. Darüber hinaus entstehen auch neue Möglichkeiten für Cyberkriminelle, wie beispielsweise der Betrug mit Corona-Soforthilfen verdeutlicht: Mithilfe von falschen Internetseiten wurden Bürgerinnen und Bürger dazu verleitet, sensible Daten anzugeben, weil sie sich auf einer offiziellen Antragsseite wähnten.

Neben Cyberkriminellen nutzen weltweit auch fremde Nachrichtendienste Cyberangriffe, um sich Zugang zu den IT-Netzen von anderen Nationen, Unternehmen und Institutionen zu verschaffen. Cyberangriffe werden auch zur Einflussnahme auf Wahlen und in Konfliktsituationen eingesetzt. Aus Sicht der Landesregierung wird Cybersicherheit daher auch als ein Teilbereich der Inneren Sicherheit verstanden.

Polizeilich wird zwischen Cybercrime im weiteren und im engeren Sinne unterschieden. Cybercrime im weiteren Sinne umfasst Straftaten, bei denen die Informationstechnik und das Internet als Tatmittel verwendet werden, die eigentliche Tat allerdings nicht im Internet stattfindet. Cybercrime im engeren Sinne umfasst hingegen Straftaten, bei deren Begehung Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind (z. B. Ransomware, Botnetze etc.). Die Fallzahlen für Cybercrime im engeren Sinne sind in Nordrhein-Westfalen von 20.118 Fällen in 2019 auf 24.294 Fälle in 2020 gestiegen. Im Vergleich zum Vorjahr ist dies ein Anstieg um über 20 Prozent. Auf Basis der nur durch Strafanzeigen bekannt gewordenen Fälle bezifferte das Landeskriminalamt NRW (LKA) alleine die durch Computerbetrug und Softwarepiraterie entstandenen Schäden auf rund 18,1 Millionen Euro. Neben diesen offiziell statistisch erfassten Schäden gilt es aber auch auf das grundsätzlich vorhandene, potentielle Schadensvolumen hinzuweisen. Laut der Studie „Wirtschaftsschutz 2021“ des Branchenverbandes BITKOM e. V. entstehen pro Jahr bis zu 223,5 Milliarden Euro an finanziellen Schäden durch Cybercrime in Deutschland. In Relation zu Nordrhein-Westfalen würde das finanzielle Schäden von bis zu 50 Milliarden Euro bedeuten. Die Diskrepanz zur offiziell angezeigten Schadenshöhe macht hierbei sehr deutlich, dass betroffene Unternehmen aus unterschiedlichen Gründen Cyberangriffe nicht anzeigen und dass das Vertrauen in die staatlichen Stellen verbessert werden muss.

Bundesweit geben viele Unternehmen an, nicht ausreichend über Cybersicherheit informiert zu sein. Unaufmerksame Internetnutzende sowie Lücken in der Cybersicherheitsinfrastruktur von Unternehmen eröffnen immer wieder Schwachstellen, die von Cyberkriminellen ausgenutzt werden können. Im Jahr 2020 wurden Cybersicherheitsvorfälle zum ersten Mal

als das größte Geschäftsrisiko für Unternehmen weltweit angesehen. Viele nordrhein-westfälische Unternehmen verfügen über eine ausgezeichnete Expertise in ihrem Wirtschaftszweig und stellen somit zunehmend ein Ziel für Industriespionage via Internet dar.

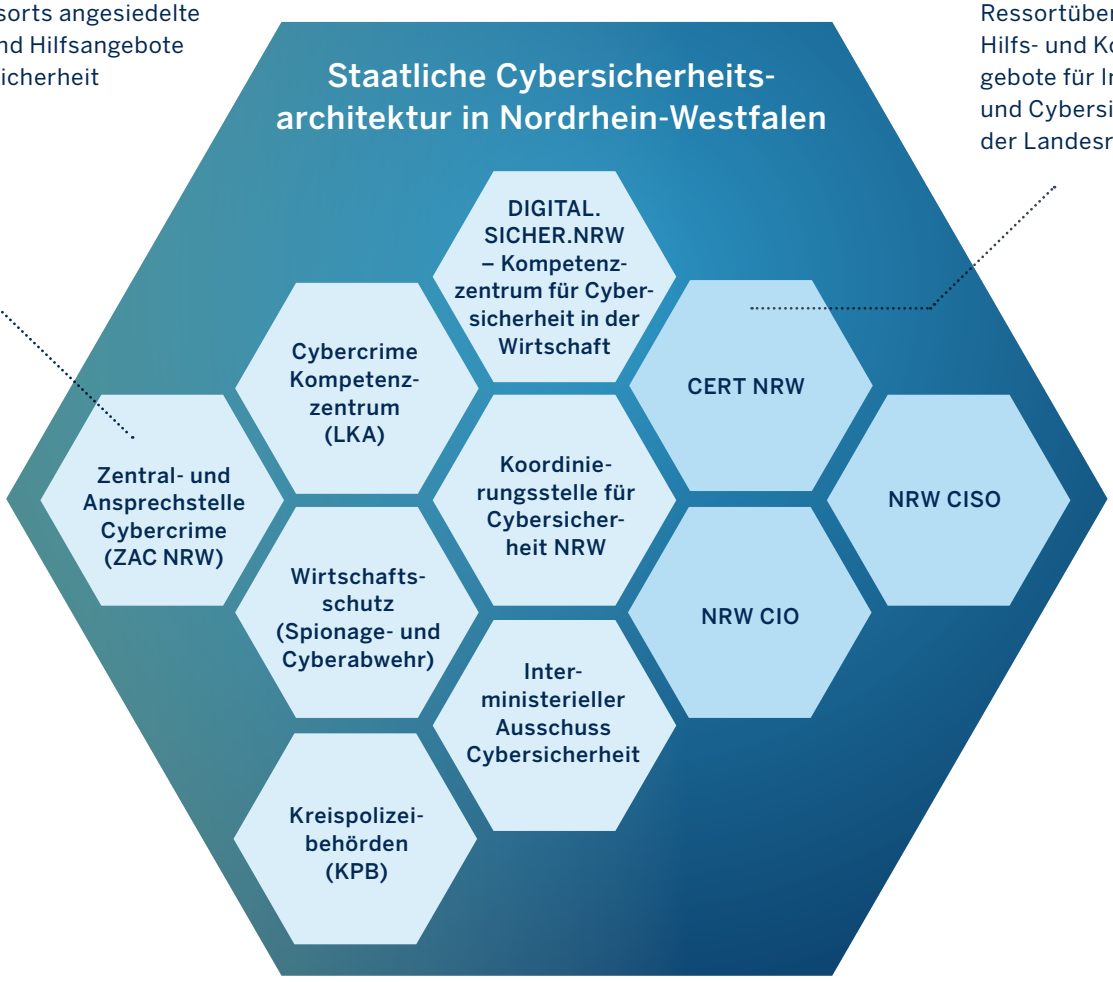
Neben der Wirtschaft sind bereits auch Universitäten, Krankenhäuser und andere öffentliche Institutionen Angriffsziel von Cyberkriminellen geworden. Ein Beispiel ist das Universitätsklinikum Düsseldorf, das 2020 Opfer eines Hackerangriffs wurde. Das dortige IT System wurde folgenschwer gestört, so dass das Klinikum vorübergehend von der Notfallversorgung abgemeldet werden musste.

ABBILDUNG 4

Visualisierung der Cybersicherheitsarchitektur in Nordrhein-Westfalen

Kerninstanzen
In den Ressorts angesiedelte Kontakt- und Hilfsangebote zur Cybersicherheit

Landesverwaltung
Ressortübergreifende Hilfs- und Kontaktangebote für Informations- und Cybersicherheit der Landesregierung



Vielen Herausforderungen im Bereich der Cybersicherheit wird bereits vonseiten des Landes begegnet. Die **Cybersicherheitsarchitektur** in Nordrhein-Westfalen umfasst staatliche Institutionen und staatlich Beauftragte, die sich vorrangig mit dem Thema Cybersicherheit beschäftigen und lässt sich in die Bereiche Kerninstanzen sowie Landesverwaltung aufgliedern (siehe Abbildung 4). Diese engagieren sich für das Querschnittsthema Cybersicherheit aus unterschiedlichen Perspektiven heraus. Handlungsleitend für diese Institutionen ist der staatliche Auftrag, die Innere Sicherheit zu gewährleisten.

Die Cybersicherheitsarchitektur in Nordrhein-Westfalen ist in den letzten Jahren gewachsen und es kamen neue Institutionen hinzu, um die bestehende Architektur zu ergänzen. Die zu den Kerninstanzen gehörenden Behörden sind klassisch im Bereich der Inneren Sicherheit angesiedelt:

- Die **Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)** fungiert als zentrale Ansprechstelle der Justiz im Bereich Cybercrime, insbesondere für Staatsanwaltschaften und Polizeibehörden in Nordrhein-Westfalen. Ihr obliegt die Verfahrensführung u. a. bei Ermittlungen im Bereich herausgehobener Cybercrime.

- Das **Cybercrime Kompetenzzentrum NRW** des LKA zielt auf die Steigerung des Gefahrenbewusstseins und die Vermittlung wirkungsvoller Maßnahmen zur Minimierung von Cybercrime ab.

- Der **Wirtschaftsschutz** im Bereich des Verfassungsschutzes bietet Unternehmen und Forschungseinrichtungen Unterstützung durch Präventionsmaßnahmen und Zusammenarbeit bei Bedrohungen an, die von ausländischen Nachrichtendiensten ausgehen, etwa durch Wirtschaftsspionage oder Cyberangriffe.

Durch das Verständnis von Cybersicherheit als Querschnittsaufgabe sind aber auch aus anderen Bereichen wichtige Beteiligte der Cybersicherheitsarchitektur in Nordrhein-Westfalen aufzuführen:

- Die **Koordinierungsstelle Cybersicherheit NRW** wurde im August 2020 gegründet, um die nordrhein-westfälischen Akteurinnen und Akteure der Cybersicherheit zu koordinieren, zu vernetzen und Synergieeffekte zu schaffen.
- Das Landeskabinett hat 2020 den **Interministeriellen Ausschuss Cybersicherheit (IMA Cybersicherheit)** eingerichtet. Unter Beteiligung aller Ressorts der Landesregierung tauscht sich der IMA Cybersicherheit regelmäßig zu Themen der Cybersicherheit aus und stärkt als Arbeitsgremium des Landes die interne Kommunikation.
- **DIGITAL.SICHER.NRW – Kompetenzzentrum für Cybersicherheit in der Wirtschaft** wurde 2021 zur Unterstützung kleiner und mittlerer Unternehmen (KMU) geschaffen. Zum Aufgabenspektrum gehören das Aufbereiten von Informationen zur Prävention und zielgruppenspezifischen Materialien zu Cybersicherheitsthemen.

Für den Schutz der Landesverwaltung selbst tragen die folgenden Kerninstanzen die Verantwortung für den Bereich der Cyber- und Informationssicherheit:

- Die/Der **Landesbeauftragte für Informationstechnik (NRW CIO)** hat die Aufgabe, die IT der Landesverwaltung bei Fragen der IT-Sicherheit, IT-Plattformen und IT-Verfahren strategisch zu steuern und dabei alle Ressorts mit einzubeziehen.
- Die/Der **Informationssicherheitsbeauftragte (NRW CISO)** unterstützt den/die NRW CIO bei der Aufgabe, die Landesregierung bei Fragen der IT-Sicherheit zu beraten und aufzuklären.
- Das Computer Emergency Response Team **(CERT) NRW** fungiert als zentrale Anlaufstelle der Landesverwaltung und als Informationsschnittstelle zwischen Einrichtungen und Behörden, dem Landesbetrieb IT.NRW sowie bundesweit anderen deutschen CERTs. Es ist für die Prävention und für reaktive Maßnahmen bei konkreten IT-Sicherheitsvorfällen innerhalb der Landesverwaltung verantwortlich.

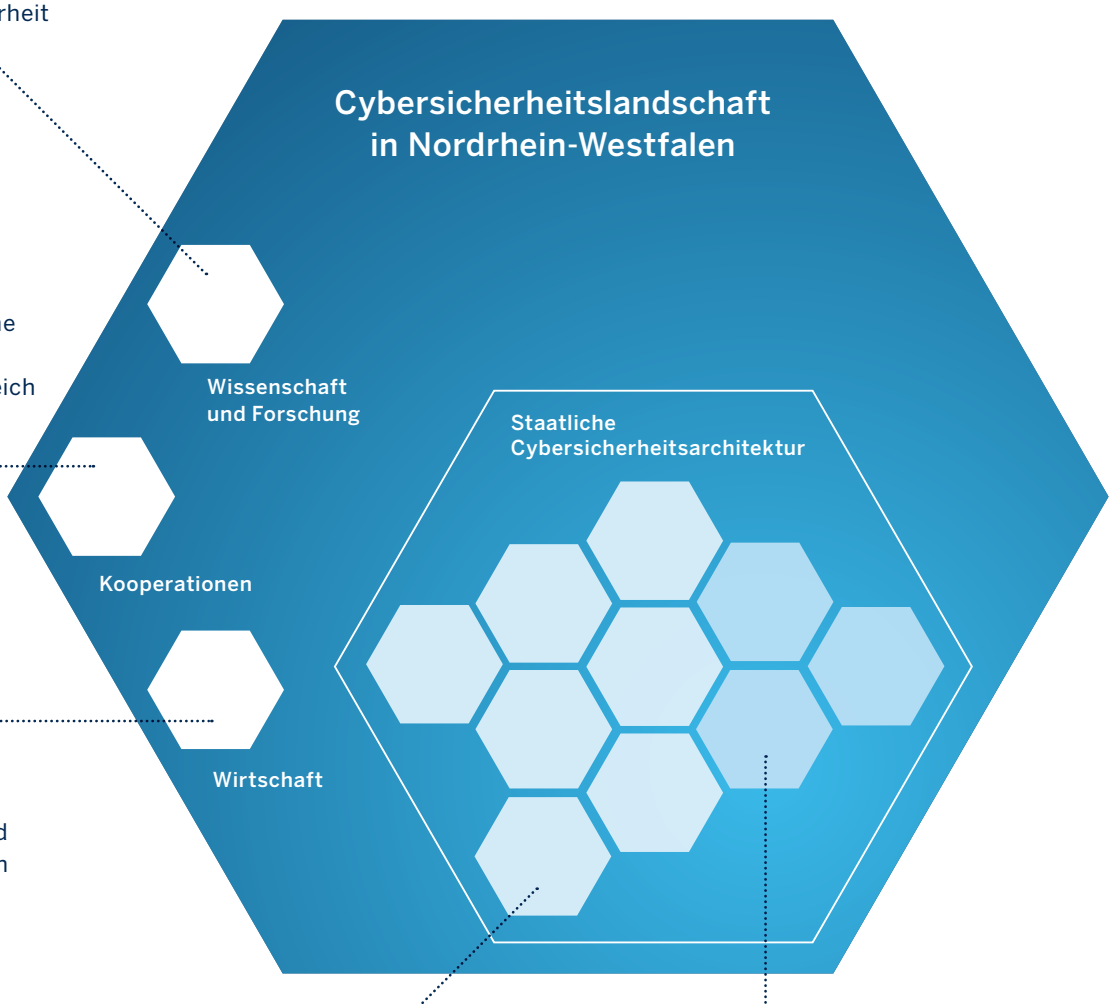
ABBILDUNG 5

Visualisierung der Cybersicherheitslandschaft in Nordrhein-Westfalen

Wissenschaft und Forschung
Rund 30 Hochschulinstitute und außeruniversitäre Forschungseinrichtungen im Bereich Cybersicherheit

Kooperationen
Staatliche, teilstaatliche sowie private Kooperationen im Bereich Cybersicherheit

Wirtschaft
Rund 400 IT-Sicherheitsunternehmen sind in Nordrhein-Westfalen angesiedelt



Kerninstanzen
In den Ressorts angesiedelte Hilfs- und Kontaktangebote für Cybersicherheit

Landesverwaltung
Ressortübergreifende Hilfs- und Kontaktangebote für Informations- und Cybersicherheit der Landesregierung

Die vorgestellte Cybersicherheitsarchitektur des Landes ist Teil der übergreifenden **Cybersicherheitslandschaft in Nordrhein-Westfalen**. Diese umfasst zusätzlich Institutionen aus Wissenschaft und Forschung, der Wirtschaft, Multiplikatoren wie Verbände und private Initiativen (zum Beispiel Cyber Security Cluster Bonn, eurobits e. V.) sowie Kooperationen z. B. der Sicherheitspartnerschaft im Bereich der Cybersicherheit.

Die Cybersicherheits- und IT-Sicherheitsforschung ist ein wichtiger Teil der Cybersicherheitslandschaft in Nordrhein-Westfalen. Das Land verfügt mit mehr als 700 Forscherinnen und Forschern im Bereich der IT-Sicherheit, verteilt auf rund 30 Fachhochschulen, Universitäten und außeruniversitäre Forschungseinrichtungen, über einen der wichtigsten **Forschungsstandorte** für die IT-Sicherheit in Deutschland. In den letzten Jahren hat das Land vermehrt den Bereich Cybersicherheit ausgebaut und in dessen Forschung investiert.

Cybersicherheit ist zudem als wichtige **Wachstumsbranche der Wirtschaft** fest in Nordrhein-Westfalen verankert. So sind im Land mehr als 400 IT-Sicherheitsunternehmen und viele junge Start-ups im Bereich der IT-Sicherheit angesiedelt. Einige der jungen Unternehmen sind Ausgründungen aus Forschungseinrichtungen. Etablierte IT-Sicherheitsunternehmen aus NRW haben sich zu europäischen Marktführenden entwickelt. Dabei ist die strategische und bedeutsame Kooperation zwischen den Wirtschaftsunternehmen – Bedarfsträgerinnen und Bedarfsträgern sowie Anbietenden – und der öffentlichen Verwaltung ein wichtiger Baustein für die Stärkung dieses Wirtschaftszweigs.

Das Zusammenwirken verschiedener Beteiligter der Cybersicherheitslandschaft äußert sich auch durch eine Vielzahl an staatlichen, teilstaatlichen sowie privaten **Kooperationen** im Bereich der Cybersicherheit im Land. Innerhalb der „Sicherheitspartnerschaft NRW“ agieren beispielsweise Wirtschaft, deren Verbände und staatliche Akteure, die gemeinsam gegen Wirtschaftsspionage und Wirtschaftskriminalität vorgehen. Andere regionale Cluster, so beispielsweise das Cyber Security Cluster Bonn oder eurobits e. V. im Ruhrgebiet, schaffen eine enge Verzahnung zwischen Anbieterindustrie und Wissenschaft im engen Dialog mit öffentlichen Einrichtungen des Landes und des Bundes sowie Vernetzung mit anderen europäischen Cybersicherheitsclustern.

Die Herausforderungen der Cybersicherheit werden nicht zuletzt auch durch die Corona-Pandemie deutlich sichtbarer. Die Landesregierung Nordrhein-Westfalen hat bereits mit zahlreichen Akteuren eine Cybersicherheitsarchitektur aufgebaut, die Unterstützungsangebote für Verwaltung, Wirtschaft sowie Bürgerinnen und Bürger bereitstellt.

Ziele der Cybersicherheitspolitik der Landesregierung Nordrhein-Westfalen

3.0

Die Landesregierung hat die Ambition formuliert, gemeinsam mit allen gesellschaftlichen Akteuren, das Cybersicherheitsniveau in und für Nordrhein-Westfalen zu verbessern. Aus dieser Ambition heraus werden die sechs Cybersicherheitsziele für die kommenden drei Jahre abgeleitet:

ABBILDUNG 6

Cybersicherheitsziele für Nordrhein-Westfalen

1. **Erhöhung der Wahrnehmung von Cybersicherheit**
2. **Cybersicherheitsprävention für kleine und mittlere Unternehmen**
3. **Steigerung der Cybersicherheitskompetenzen von Bürgerinnen und Bürgern sowie Unternehmen**
4. **Steigerung der Effektivität und Effizienz der Kommunikation der Cybersicherheitsakteure im Land und aus dem Land heraus**
5. **Unterstützung der Forschung und des Ausbaus des Wissenschaftsstandorts Nordrhein-Westfalen**
6. **Verbesserung der Datenlage im Bereich Cybersicherheit**

Die Erreichung dieser sechs Ziele soll durch die in den drei Handlungsfeldern (siehe Kapitel 4) aufgeführten konkreten Maßnahmen angestrebt werden.

Um das Schutzniveau zu erhöhen und den Cyberraum sicherer für alle Menschen in Nordrhein-Westfalen gestalten zu können, müssen **Cybersicherheitsthemen** präsenter gemacht und das Bewusstsein dafür unter den Technologie-Nutzerinnen und -Nutzern erhöht werden. Allein durch die erhöhte Aufmerksamkeit der Einzelnen für die Gefahrenlage könnte ein nicht unerheblicher Anteil an Cybervorfällen verhindert werden. Die Verhinderung von Cyberangriffen ist prioritär und wird durch eine erhöhte **Cybersicherheitskompetenz** aller Bürgerinnen und Bürger im Land gefördert.

Zusätzlich zur Prävention kommen der Vernetzung und den Kooperationen der Akteure innerhalb der Cybersicherheitsarchitektur eine besondere Bedeutung zu. Nur wenn die Landesverwaltung **effizient kommuniziert**, kann auch effektiv nach einem Cyberangriff geholfen werden. Dieses Ziel wird institutionell, organisatorisch und kulturell in den Blick genommen.

Auch Institutionen der **Wissenschaft und Forschung** sollen weiterhin gezielt **gefördert** und bei der Vernetzung miteinander unterstützt werden, da sie neue Ansätze auf verschiedenen Ebenen

erforschen. Hieraus entstehen Start-ups oder es werden gemeinsam mit der Cybersicherheitsindustrie Lösungen von morgen entwickelt. Diese neuen Erkenntnisse werden die Grundlagen staatlichen und wirtschaftlichen Handelns beeinflussen. Zudem ist die Cybersicherheitsindustrie ein inhärent **wichtiger Wirtschaftszweig** mit enormem zukünftigem Wertschöpfungs- und Wachstumspotenzial, den es zu unterstützen gilt. Nordrhein-Westfalen hat sich in seinem industriepolitischen Leitbild das Ziel gesetzt, die europäische Führungsrolle Nordrhein-Westfalens bei der IT-Sicherheitsforschung und den Wirtschaftsschutz auszubauen sowie die Cybersicherheit in der Wirtschaft zu stärken.

Nur wenn Bürgerinnen und Bürger, Unternehmen und öffentliche Institutionen Cyberangriffe oder Angriffsversuche melden, können staatliche Institutionen auch effektiv helfen und vor neuen Taktiken der Cyberkriminellen warnen. Viele Cyberangriffe werden jedoch aus Sorge vor negativen Konsequenzen nicht gemeldet, beispielsweise bei Ransomware-Angriffen. Die Landesregierung wird daher gezielt vertrauensbildende Maßnahmen unterstützen, die die Wahrnehmung in die fachliche Expertise und Effizienz zuständiger Institutionen stärken.

Übergreifendes Ziel für alle Handlungsfelder ist die Verbesserung der Datenlage. Durch eine Kombination von Kennzahlen und Daten sowie ergänzenden Studien wird künftig regelmäßig ein NRW-spezifisches Lagebild der Cybersicherheit erstellt, der Umsetzungsfortschritt der Cybersicherheitsstrategie gemessen und Handlungsbedarfe identifiziert werden können. Vorrangig sollen nach Möglichkeit vorhandene Datenquellen in der Landesverwaltung und bei Kooperationspartnerinnen und Kooperationspartnern hierfür erschlossen werden. Das dafür erforderliche Datenkonzept wird durch die Koordinierungsstelle Cybersicherheit NRW unter Beteiligung des Interministeriellen Ausschusses erstellt und abgestimmt. Zusätzlich wird die Koordinierungsstelle Studien beauftragen, die Grundlage für die bedarfsgerechte Weiterentwicklung von Maßnahmen sind, damit der Cybersicherheitsstandort Nordrhein-Westfalen weiter gestärkt wird.

Die im Zentrum der Cybersicherheitsstrategie stehenden drei Handlungsfelder umfassen die Zielgruppen Bürgerinnen und Bürger, die Wirtschaft, die Wissenschaft und die öffentliche Verwaltung in Nordrhein-Westfalen.

Die Cybersicherheitsstrategie steht im Einklang mit der Digitalstrategie der Landesregierung. Sie stützt insbesondere die Leitlinien, dass Datenschutz, Cybersicherheit und Datensouveränität für die Bürgerinnen und Bürger und Unternehmen die Grundlage unserer digitalen Gesellschaft sind und dass die Digitalisierung ein Höchstmaß an Sicherheit für die Menschen durch den Ausbau resilienter Infrastrukturen und der Fähigkeit von Staat sowie Bürgerinnen und Bürgern, sich vor Gefahren wie Naturkatastrophen, Pandemien oder kriminellen Tätigkeiten zu schützen, ermöglicht.

Die Cybersicherheitsstrategie konkretisiert die in der Digitalstrategie angesprochenen Handlungsfelder Sicherheit

und Datenschutz hinsichtlich der Cybersicherheit und ergänzt die Digitalisierungsoffensive in den Bereichen Kompetenzförderung, Förderung der Digitalen Sicherheit durch Nutzung vorhandener Kompetenzen, Förderung des Respekts in sozialen Medien und der Informationssicherheit durch konkrete Maßnahmen.

Die sechs Ziele der Cybersicherheitsstrategie stärken das Cybersicherheitsniveau in Nordrhein-Westfalen systematisch und in Einklang mit der Digitalstrategie der Landesregierung.

Die drei Handlungsfelder zur Erhöhung der Cybersicherheit in Nordrhein-Westfalen

4.0

Im Rahmen dieser Cybersicherheitsstrategie werden die sechs strategischen Ziele im Rahmen von drei Handlungsfeldern angestrebt, die das übergeordnete Ziel der Erhöhung von Cybersicherheit in Nordrhein-Westfalen stützen:

Cybersicherheit in Nordrhein-Westfalen
Das Fortschreiten der Digitalisierung in Nordrhein-Westfalen erfordert das bewusste Handeln eines jeden Einzelnen.

Koordination und Kooperation in Nordrhein-Westfalen
Koordination und Kooperation im Bereich Cybersicherheit dienen als Lösungsweg zu einer erhöhten Sicherheit in Nordrhein-Westfalen.

Cybersicherheit als Erfolgsfaktor für Nordrhein-Westfalen
Den kleinen und mittleren Unternehmen muss eine besondere Unterstützung angeboten werden.

ABBILDUNG 7

Die drei Handlungsfelder zur Erhöhung der Cybersicherheit in NRW

Die Handlungsfelder spiegeln die Mehrdimensionalität des Themas Cybersicherheit wider. Sie operationalisieren die strategischen Ziele aus Kapitel 3 und übersetzen diese in konkrete Maßnahmen, die in dem jeweiligen Handlungsfeld vorgestellt werden.

Im Rahmen des ersten Handlungsfeldes **Cybersicherheit in Nordrhein-Westfalen** wird vor allem die Erhöhung der Cybersicherheit durch gesteigerte Präventionsarbeit ins Auge gefasst. Eine Stärkung der individuellen Wahrnehmung von Cybersicherheitsthemen sowie die Steigerung der Medien- und Cybersicherheitskompetenz werden angestrebt. Dabei wird als wichtigste Voraussetzung für Cybersicherheit die achtsame und informierte Internetnutzung jedes und jeder Einzelnen herausgestellt („Faktor Mensch"). Die Landesregierung hat sich daher zum Ziel gesetzt, **die allgemeine Wahrnehmung von Cybersicherheitsthemen der Bürgerinnen und Bürger Nordrhein-Westfalens zu erhöhen**.

Zudem soll innerhalb dieses Handlungsfeldes das Ziel verfolgt werden, **die Cybersicherheitskompetenzen der Bürgerinnen und Bürger sowie Unternehmen zu steigern**. Durch Maßnahmen, wie Medienscouts, Informationskampagnen des Landes Nordrhein-Westfalen sowie Schulungen am Arbeitsplatz soll dieses Ziel gestützt werden (siehe Abschnitt 4.1).

Koordination und Kooperation in Nordrhein-Westfalen bezieht sich vor allem auf die Cybersicherheitsarchitektur und die Cybersicherheitslandschaft in Nordrhein-Westfalen. Im Rahmen dieses zweiten Handlungsfeldes wird die gemeinsame Funktion der staatlichen Akteure als Schutzschirm für die Gesellschaft, Wissenschaft und Wirtschaft in Nordrhein-Westfalen beleuchtet. Zudem werden die Notwendigkeit von mehr Kooperationen und einer gesteigerten Vernetzung im Bereich des Querschnittsthemas Cybersicherheit aufgezeigt, sowie strategische Maßnahmen zum Ausbau der Vernetzung im Land vorgestellt. Beispielsweise stehen das Cybercrime-Kompetenzzentrum des LKA NRW – wie auch das Wirtschafts- und Digitalministerium – im Sinne eines ganzheitlichen Ansatzes mit dem Branchenverband der IT BITKOM e. V., dem Bundesverband der IT-Anwender-Unternehmen VOICE, dem eco-Verband der Internetwirtschaft, in fortwährendem Austausch und sind zudem Teil der Sicherheitspartnerschaft NRW. Weitere Kooperationspartnerschaften in NRW sind zum Beispiel das Cyber Security Cluster Bonn sowie eurobits e. V. im Ruhrgebiet, ASW West oder networker NRW.

Das Handlungsfeld dient auch dem Ziel, die Effektivität und Effizienz der Kommunikation der Cybersicherheitsakteure im Land und darüber hinaus zu steigern. Durch die Identifikation der relevanten Akteure und die Bündelung ihrer Informationsströme sollen Lücken bei den Ansprechstellen geschlossen und das Kontaktangebot für verschiedene Zielgruppen klar zugewiesen werden.

Im Rahmen des dritten Handlungsfeldes wird **Cybersicherheit als Erfolgsfaktor für Nordrhein-Westfalen** vorgestellt. Ausgehend von der spezifischen Bedrohungslage für Unternehmen in Nordrhein-Westfalen, insbesondere für KMU, wird die Relevanz von Cybersicherheit für die Wirtschaft verdeutlicht, um passgenaue Maßnahmen herzuleiten. Zielgruppenspezifische Hilfestellungen sowie Präventionsmaßnahmen des Landes geben Antworten auf die Herausforderungen für die Wirtschaft.

Das dritte Handlungsfeld beschreibt Cybersicherheit als einen wichtigen Erfolgsfaktor für die Digitalisierung in Nordrhein-Westfalen. Cybersicherheit wird vermehrt zu einer notwendigen Voraussetzung für ein erfolgreiches, wirtschaftliches Handeln im Rahmen der Digitalisierung. Zudem spielt die Unterstützung von Hochschulen und anderen Aus- und Fortbildungseinrichtungen und -anbietenden eine wichtige Rolle, da diese die Fachkräfte ausbilden, die dringend für den Schutz der Unternehmen in Nordrhein-Westfalen benötigt werden.

In allen drei Handlungsfelder werden Maßnahmen beschrieben, die zu einer Verbesserung der Datenlage (Ziel 6) führen, um ein NRW-spezifisches Cybersicherheitslagebild zu erstellen. Auf dieser Basis können Maßnahmen angepasst und neue Handlungsbedarfe identifiziert werden.

4.1 Cybersicherheit in Nordrhein-Westfalen: Das Fortschreiten der Digitalisierung erfordert das bewusste Handeln einer jeden einzelnen Person

Ob privat oder beruflich – Cybersicherheit ist immer abhängig von den digitalen Kompetenzen der Internetnutzenden. Daher ist das bewusste **Handeln jeder einzelnen Person** einer der relevantesten Faktoren nicht nur für die **eigene Cybersicherheit**. Durch die zunehmende Bedeutung des Internets und den anhaltenden Digitalisierungsschub geraten Themen der Cybersicherheit privat wie beruflich immer mehr in den Fokus.

Mehr als die Hälfte der Cybersicherheitsvorfälle in Unternehmen in Deutschland lassen sich laut einer aktuellen Studie auf das Fehlverhalten von Mitarbeitenden zurückführen. Dieses meist unbeabsichtigte oder unwissentliche Verhalten äußert sich beispielsweise durch:

- **die Wahl eines unsicheren Passworts,**
- **das Öffnen von Anhängen oder Links aus Phishing-E-Mails,**
- **den Verlust oder Diebstahl der Hardware,**
- **Downloads von nicht vertrauenswürdigen Websites.**

Einzelne Risiken wie die Wahl eines unsicheren Passworts oder das Öffnen von Spam E-Mails, die ggf. Schadcode enthalten können, lassen sich leicht vermeiden. Dennoch war das im Jahr 2020 am häufigsten gewählte Passwort der Welt „123456“. Das BSI hat im Jahr 2020 alleine für die Netze des Bundes 76 % des Emailaufkommens als unerwünschte Spam E-Mails identifiziert. Gegenüber dem Jahr 2019 ist dies ein Anstieg um 7 %, Tendenz steigend. Die Gefährdungslage bleibt weiterhin dynamisch. Durch konkrete Maßnahmen, die ein Bewusstsein für die Gefährdungen schaffen, können diese Risiken gemindert werden.

Die Landesregierung Nordrhein-Westfalen hat die Bedeutung dieses Handlungsfeldes früh erkannt und stellt Bürgerinnen und Bürgern bereits zahlreiche Informations- und Präventionsangebote zur Wahrung und Erhöhung ihrer Cybersicherheit zur Verfügung. Sie bietet allgemeine und kriminalpräventive Präventionsprogramme für Bürgerinnen und Bürger sowie Handlungsempfehlungen, beispielsweise im Rahmen des Projekts „Mach dein Passwort stark“ des Landeskriminalamtes Nordrhein-Westfalen (LKA NRW), an. Ergänzt werden diese Angebote zudem durch Filme des Ministeriums der Justiz des Landes Nordrhein-Westfalen in Zusammenarbeit mit dem Landespräventionsrat. Das LKA NRW bietet auf seiner Webseite bereits Hinweise und Handlungsempfehlungen, damit sich Bürgerinnen und Bürger entsprechend informieren können. Die Zielgruppe der Schülerinnen und Schüler wird durch das Medienscout-Projekt an den Schulen Nordrhein-Westfalens adressiert. Für Unternehmen bietet die Landesregierung zielgruppenspezifische Präventionsprogramme durch den Wirtschaftsschutz und DIGITAL.SICHER.NRW als Kompetenzzentrum für Cybersicherheit in der Wirtschaft an.

Vorhandene Angebote sowie Präventions- und Öffentlichkeitskampagnen sollen hinsichtlich ihres Wirkungs- und Verbreitungsgrades gestaltet und ausgebaut werden, um das Schutzniveau im Cyberraum für die Zielgruppen weiter zu erhöhen. Zur Entwicklung strategischer Maßnahmen ist es daher wichtig, sich diese Zielgruppen und schon bestehende Maßnahmen genau anzuschauen. Ob für Schülerinnen und Schüler, Eltern, Verbraucherinnen und Verbraucher – es sind jeweils dedizierte Inhalte und zielgruppengerechte Kommunikationswege zu wählen, um die Wahrnehmung von Cybersicherheitsthemen zu erhöhen. Ebenso sind bei den Empfehlungen für die Zielgruppen Zukunftstechnologien angemessen zu berücksichtigen.

Inzwischen gibt es – aufsetzend auf den für Schule geltenden Medienkompetenzrahmen NRW, initiiert von der Staatskanzlei Nordrhein-Westfalen und entwickelt von der Gesellschaft für Medienpädagogik und Kommunikationskultur – ein Angebot zur Reflexion der eigenen Medienkompetenz für alle Bürgerinnen und Bürger. Mithilfe des **#DigitalCheckNRW** können Bürgerinnen und Bürger ihre Medienkompetenz testen und daraufhin individualisierte Weiterbildungsangebote erhalten. Die Anbietenden dieser Angebote werden darüber informiert, an welcher Stelle nachgefragte Bildungsangebote fehlen und entwickelt werden

sollten. Dieses Angebot wird um einen **„Cybersicherheitskompetenz-Check“** erweitert. So können Bürgerinnen und Bürger gezielt ihre Kompetenz in diesem Bereich überprüfen und sich erforderliche Kompetenzen aneignen. Um damit Bürgerinnen und Bürger zu erreichen und die Zahl der Nutzenden in den nächsten drei Jahren weiter zu steigern, wird die Koordinierungsstelle Cybersicherheit NRW in Zusammenarbeit mit der Staatskanzlei dieses Angebot entwickeln, intensiver bewerben sowie die Einbindung in andere Angebote des Landes (z. B. Sensibilisierungsmaßnahmen für Unternehmen) oder auch anderer Institutionen (z. B. Volkshochschulen, Fortbildungseinrichtungen, Landesanstalt für Medien NRW) initiieren. Mit dem neuen Angebot **ZEBRA** gibt es seit Januar 2021 eine verlässliche Beratungsstelle der Landesanstalt für Medien NRW (LfM NRW), an die sich Bürgerinnen und Bürger mit konkreten Fragen zur Nutzung digitaler Medien wenden können.

Auch das Projekt **Medienscouts NRW** wird gemeinsam von der LfM NRW und dem Ministerium für Schule und Bildung Nordrhein-Westfalen in den Jahren 2021 bis 2023 weiter ausgebaut. Als das größte Scout-Projekt seiner Art im deutschsprachigen Raum unterstützt Medienscouts NRW Schulen dabei, präventiv Probleme wie Cybermobbing, Hassrede, Cybergrooming, Datenmissbrauch oder exzessive Mediennutzung im schulischen Alltag aufzugreifen und zu bearbeiten. Seit dem Start im Jahr 2011 konnten an ca. 960 Schulen über 4.400 Schülerinnen und Schüler und mehr als 1.900 Beratungslehrkräfte qualifiziert werden.

Im Projekt **Cybercops** werden Jugendliche von der lokalen Polizei zu Medienbetreuenden ausgebildet. Diese sollen nach der Ausbildung in die Lage versetzt werden, Gleichaltrigen digitale Kenntnisse zu vermitteln. Gemeinsam mit der Polizei wird geplant, das bisher nur im Kreis Minden-Lübbecke bestehende Projekt auszubauen und weiter zu fördern.

Die Landesregierung Nordrhein-Westfalen begreift das Thema Cybersicherheit als Querschnittsthema. Aus diesem Grund wurden die Themen bei der Umsetzung des Medienkompetenzrahmens explizit in den Lehrplänen der Schulen der Primar- und Sekundarstufe I verankert. Die Vermittlung von Medienkompetenz an Schülerinnen und Schüler, dazu gehören auch Kompetenzen bezüglich Datenschutz, Datensicherheit und Persönlichkeitsrechten, ist Aufgabe aller Fächer in der Primar- und Sekundarstufe I. Der **„Medienkompetenzrahmen NRW“** ist hierbei verbindliche Grundlage mit dem Ziel, das Lernen und Leben mit digitalen Medien zur Selbstverständlichkeit im Unterricht aller Fächer zu machen und er wirkt darauf hin, dass alle Fächer ihren spezifischen Beitrag zur Entwicklung der geforderten Kompetenzen leisten.

Mit der **LOGINEO NRW Produktfamilie** (www.logineo.nrw.de) hat das Land ein umfassendes digitales Angebot geschaffen, das Schulen, Lehrerinnen und Lehrer sowie Schülerinnen und Schüler beim digitalen Lernen, sei es im Rahmen des Präsenzunterrichts oder in Phasen des Lernens auf Distanz, umfassend unterstützt. Die LOGINEO NRW Produktfamilie besteht gegenwärtig aus drei Modulen, die sicher und datengeschützt sind und von Schulen im Land NRW kostenlos beantragt und genutzt werden können:

– Die **Schulplattform LOGINEO NRW** zur rechtssicheren Kommunikation, Organisation und zum Dateiaustausch per Cloud

– Das **Lernmanagementsystem LOGINEO NRW LMS**

– der **LOGINEO NRW Messenger** zur schnellen und sicheren Kommunikation per Chat und optional auch über die integrierte **Videokonferenzfunktion**

Bereits jetzt bestehen verschiedene Lehrangebote für Schülerinnen und Schüler wie beispielsweise das Projekt „Internet-ABC“ und die Initiative „Klicksafe“. **Das Internet-ABC** ist eine Lernplattform für Eltern, Lehrkräfte und Kinder im Alter von fünf bis zwölf Jahren, die dort zielgruppenspezifisch aufbereitetes Basiswissen über das Internet finden. Zu diesem Zweck stellt das Internet-ABC Kindern, Eltern und Lehrkräften umfangreiche Materialien zur Verfügung, die insbesondere im schulischen Kontext vielseitig Anwendung finden. Als Ratgeber im Netz bietet es Hilfestellung und Informationen über den sicheren Umgang mit dem Internet und nimmt auch sensible Themen wie Cybermobbing und Cybergrooming in den Blick.

„Klicksafe“ ist eine Initiative der EU gegen Hass im Internet die in Nordrhein-Westfalen von der LfM NRW – Eltern und Medien umgesetzt wird. Das Angebot richtet sich an Gruppen von Eltern und kann beispielsweise an Elternabenden vorgestellt werden. Für Jugendliche stehen informative YouTube-Videos sowie weitere Informationsmaterialien zum Thema **„Hate-Speech“** oder **„Hass-Postings“** zur Verfügung. Das Land Nordrhein-Westfalen ist durch seine Kooperation, Expertise und die klaren Zuständigkeiten zudem Vorreiter bei der Bekämpfung von Hasskommentaren im Internet. So sind an dem Projekt **„Verfolgen statt nur Löschen“** neben der LfM NRW auch verschiedene in Nordrhein-Westfalen ansässige Medienunternehmen, von Seiten der Polizei das LKA NRW und seitens der Justiz die ZAC NRW beteiligt. Ziel der Projektarbeit ist die verbesserte Bekämpfung strafbarer Hassrede auf den Präsenzen der Medienunternehmen im Internet im Allgemeinen und in sozialen Medien im Besonderen. Dazu wurde ein elektronisches Anzeigeverfahren implementiert und die Sachbearbeitung standardisiert. Medienverantwortliche wurden und werden geschult, strafbare Hassrede trennscharf von pointierter Meinungsäußerung unterscheiden zu können. Außerdem besteht eine enge Zusammenarbeit mit dem ordnungsbehördlichen Team der LfM NRW. In Zukunft wird die ZAC NRW zusätzlich ihr Online-Angebot erweitern.

STRATEGISCHE ZIELE:

1. Erhöhung der Wahrnehmung von Cybersicherheit
3. Steigerung der Cybersicherheitskompetenzen von Bürgerinnen und Bürgern sowie Unternehmen
6. Verbesserung der Datenlage im Bereich Cybersicherheit

ABBILDUNG 8

In der beruflichen Bildung wird die Förderung digitaler Schlüsselkompetenzen als immanenter Bestandteil der umfassenden Handlungskompetenz in den Dimensionen Medienkompetenz (gesellschaftlich-kulturelle Perspektive), Anwendungs-Know-how (anwendungsbezogene Perspektive) und informatische Grundkenntnisse (technologische Perspektive) verankert. Die digitalen Schlüsselkompetenzen fokussieren die Transformationsprozesse in Arbeit und Gesellschaft. Der Medienkompetenzrahmen NRW kann hier sowohl für die Eingangsdiagnostik durch die Bildungsgänge des Berufskollegs als auch als Ausgangsgröße für die spiralcurriculare Weiterentwicklung von Unterrichtsvorhaben genutzt werden. Die Bildungspläne für die Bildungsgänge in den sieben Fachbereichen des Berufskollegs werden seit 2013 im Rahmen einer systemkoordinierten Bildungsplanentwicklung fortlaufend überarbeitet. Die Einbindung der digitalen Schlüsselkompetenzen erfolgt systematisch.

Zur Stärkung des Unterrichtsangebots zur Förderung digitaler Schlüsselkompetenzen in der beruflichen Bildung wurde mit einem namhaften Hersteller von Netzwerktechnik eine Kooperationsvereinbarung hinsichtlich der Nutzung der E-Learning-Plattform für die Berufskollegs in Nordrhein-Westfalen geschlossen. Das Thema Cybersicherheit wird explizit in einzelnen Kursangeboten auf der E-Learning-Plattform aufgegriffen.

Zudem können die Berufskollegs den Schülerinnen und Schülern ihrer Schule im Rahmen des staatlichen EDV-Führerscheins NRW erworbene EDV-Kenntnisse zertifizieren. Auch hier wird das Thema Datenschutz und Datensicherheit von einem Modul abgedeckt.

Das Ineinandergreifen von Präventionsmaßnahmen und konkreten Hilfsangeboten für Bürgerinnen und Bürger, für Eltern und Jugendliche und Unternehmen ist eine wichtige Voraussetzung für eine nachhaltig wirkende Aufklärung und Kompetenzerweiterung. Im Zuge der Cybersicherheitsstrategie greift die Landesregierung diesen Aspekt auf und reflektiert die vorhandenen Maßnahmen und ihre jeweilige Wirkung. Dazu wird durch die Koordinierungsstelle Cybersicherheit NRW, in Abstimmung mit dem IMA Cybersicherheit, eine Studie in Auftrag gegeben, die weitere Handlungsbedarfe identifizieren soll.

Die Beteiligten der Cybersicherheitsarchitektur unterstützen mit ihren Aufklärungs- und Präventionsprogrammen sowohl Bürgerinnen und Bürger, Wirtschaft, Wissenschaft und Staat in der Befähigung, die digitalen Möglichkeiten zu nutzen, Risiken zu erkennen und diese abwägen zu können. Die Landesregierung kann zwar **keine vollständige Sicherheit** des Cyberraums für NRW gewährleisten. Sie hat sich jedoch zum Ziel gesetzt, die **Eigenverantwortung** aller durch diese Angebote zu unterstützen.

4.2 Koordination und Kooperation in Nordrhein-Westfalen: Gesteigerte Zusammenarbeit im Bereich Cybersicherheit dient als Lösungsweg für eine erhöhte Sicherheit

Das Aufgabenspektrum des Landes mit Bezug zu Cybersicherheit ist vielseitig, entwickelt sich stetig fort und reicht von der Prävention über die Gefahrenabwehr bis hin zur Strafverfolgung. Eine effiziente und effektive **Cyberabwehr und -prävention** bedingt eine strukturierte politische Herangehensweise.

Die Landesregierung setzt hierfür einen Schwerpunkt auf die Verbesserung der Zusammenarbeit und Koordination der staatlichen Akteure sowie den Ausbau von Kooperationen zwischen relevanten Institutionen in Nordrhein-Westfalen. Ziel ist es, die Vielzahl der Akteurinnen und Akteure effektiv zu verzahnen, um Informationsflüsse und Aufgabenfelder besser aufeinander abzustimmen und langfristig Synergie- und Skaleneffekte erzielen zu können.

Für die Erhöhung der Cybersicherheit in Nordrhein-Westfalen ist es wesentlich, die Zusammenarbeit der staatlichen Institutionen innerhalb der Cybersicher-sicherheitsarchitektur in Nordrhein-Westfalen besser zu koordinieren. Dies führt zum Schließen von Lücken im Sicherheitsangebot sowie zur Zuständig-

keitsklärung und unterstützt damit ein verbessertes Schutzniveau auch im Sinne der Inneren Sicherheit im Land.

Die Landesregierung hat diese Notwendigkeit der intensiveren Koordinierung bereits erkannt und als Reaktion im August 2020 die **Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen** gegründet. Mit der Koordinierungsstelle wurde bereits jetzt eine zentrale Instanz geschaffen, die unter Berücksichtigung der Ressortzuständigkeiten auch die Koordinierung und Strukturierung der Kommunikationsflüsse zwischen den Beteiligten der Cybersicherheitsarchitektur des Landes Nordrhein-Westfalen zur Aufgabe hat.

Zusätzlich setzt die Landesregierung auf die stärkere Vernetzung und Förderung der Kooperation innerhalb der bereits **vorhandenen Cybersicherheitsarchitektur** in Nordrhein-Westfalen und wird diese nur bedarfsgemäß ergänzen anstatt diese stetig um eine Vielzahl neuer Institutionen zu erweitern. Vorhandenes Wissen soll effizienter ausgetauscht, Doppelstrukturen vermieden und das Voneinander-Lernen gefördert werden.

So sollen in Zukunft bereits vorhandene Kapazitäten für Expertenvorträge des LKA NRW, des Wirtschaftsschutzes, der ZAC NRW und weiterer Institutionen effizienter genutzt werden. Es soll ein **Referenten-Pool** aus den vorhandenen Referentinnen und Referenten der einzelnen Institutionen entstehen. Unternehmen können dann sicher sein, dass bei einer Anfrage an eine der zuvor genannten Institutionen der gesamte Referenten-Pool genutzt wird, um freie Kapazitäten zu finden. Unternehmen erhalten dabei von staatlicher Seite Informationen, um ihre **Belegschaft und das Führungspersonal für das Thema Cybersicherheit zu sensibilisieren und bekommen verwaltungsseitige Ansprechstellen aufgezeigt**. Denn zur Erhöhung der Cybersicherheit muss von Unternehmen auch **aktiv kommuniziert** werden, dass ein Cyberangriff oder Angriffsversuch erfolgt ist („Need to know – need to share"-Grundsatz), da nur so die Handlungsfähigkeit und Effizienz in einem akuten Angriffsfall gesteigert werden kann. In den Vorträgen werden die staatlichen Unterstützungsangebote vorgestellt und es wird insbesondere der Aspekt der Vertraulichkeit der Informationen angesprochen. Der Aufbau des Referenten-Pools wird von der Koordinierungsstelle Cybersicherheit organisiert, um den Einsatz der Referentinnen und Referenten der verschiedenen Institutionen zu optimieren.

Cybersicherheit und Vernetzung der staatlichen Stellen spielen auch im Umgang mit Naturkatastrophen, wie der unter anderem in Nordrhein-Westfalen im Juli 2021 eingetretenen Hochwasserkatastrophe, eine immer wichtigere Rolle. Zur besseren Bewältigung solcher Extremsituationen wurde das Projekt **„Vernetzung von Informationen zur Darstellung der Landeslage" (VIDaL)** ins Leben gerufen, dessen Ziel es ist, alle Beteiligten des Krisenmanagements und Katastrophenschutzes zu vernetzen. VIDaL soll in Krisen alle Informationen zur Darstellung der Landeslage – egal ob sie aus den Leitstellen der Kreise und kreisfreien Städte oder den Krisenstäben des Landes oder der Bezirksregierungen kommen – miteinander verknüpfen und eine sichere Kommunikation zwischen den jeweiligen Krisenstäben ermöglichen. Das Projekt tritt 2022 in die Pilotphase. Damit solch eine Krisenkommunikation sicher und stabil funktionieren kann, gilt es dabei von vorneherein Cybersicherheit mitzudenken. Die über VIDaL kommunizierten Daten und Informationen müssen sowohl sicher vor externem Zugriff sein, als auch verlässlich ankommen.

Zur Weiterentwicklung der Cybersicherheitsarchitektur des Landes Nordrhein-Westfalen wählt die Landesregierung einen kooperativen Ansatz. Gemäß der gesteigerten **Dynamik der Digitalisierung** muss diese Architektur kontinuierlich angepasst und den technischen Entwicklungen angeglichen werden. Der IMA Cybersicherheit NRW, als ressortübergreifendes Arbeitsgremium, wird unter Berücksichtigung der Ressortzuständigkeiten diese Entwicklungen begleiten und Vertretende aus Wissenschaft und Wirtschaft in die Beratungen einbeziehen.

Um **Kooperationen und Vernetzung** innerhalb der breiteren Cybersicherheitslandschaft in Nordrhein-Westfalen zu unterstützen, werden die Partizipations- und Informationsprozesse innerhalb der bestehenden Cybersicherheitsstruktur Nordrhein-Westfalens weiterentwickelt und kontinuierlich verbessert. Strukturierte Austauschformate wie beispielsweise runde Tische und Beteiligung an Fachgremien ermöglichen eine interdisziplinäre Zusammenarbeit zwischen Landesverwaltung, Institutionen und Verbänden sowie Unternehmen der Kommunikations- und Cybersicherheitswirtschaft. Das Land fördert die übergreifende Zusammenarbeit um vorhandenes Wissen und Informationen verfügbar zu machen und Maßnahmen zur Verbesserung der Cybersicherheit auf unterschiedlichen Ebenen abzustimmen. Der kooperative Ansatz wird auch Datenquellen außerhalb der öffentlichen Verwaltung für das Cybersicherheitslagebild in Nordrhein-Westfalen erschließen, die die Handlungsmöglichkeiten zur Verbesserung der Cybersicherheit erweitern helfen. Die Stärkung der Zusammenarbeit auf allen Ebenen kann als **Schlüssel zum Aufbau von Cybersicherheitsfähigkeiten** und zur Verbesserung der Sicherheit im Gesamten gesehen werden. Kooperationen im Bereich der Cybersicherheit werden daher vom Land weiter forciert, verstetigt und ausgebaut.

Bereits jetzt ist Nordrhein-Westfalen über das Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie Teil der **Allianz für Cybersicherheit** – einer kooperativen Plattform des BSI, über die zahlreiche kleine und mittelständische Unternehmen zielgerecht in Fragen der Cybersicherheit erreicht und beraten werden.

Wichtige Kooperationspartnerinstitutionen sind die Hochschulen des Landes Nordrhein-Westfalen. Bereits 30 Hochschulinstitute und außeruniversitäre Einrichtungen in Nordrhein-Westfalen sind in der IT-Sicherheitsforschung tätig. **Innovative Forschung und Projekte** werden unter anderem von staatlicher Seite finanziert und im Bereich der Cybersicherheit hat sich die Förderung des Landes in den letzten Jahren intensiviert. Die Digitalstrategie des Landes NRW enthält zahlreiche Förderprogramme für Forschungsprojekte zur Förderung der Digitalisierung in Nordrhein-Westfalen, die auch den Aspekt Cybersicherheit berücksichtigen werden.

Die Kooperation der öffentlichen Verwaltung mit den Hochschulen und der Wirtschaft ist ein wichtiger Baustein für die Weiterentwicklung einer zukunftsorientierten Cyberabwehr. Ein Beispiel ist die **Nutzung künstlicher Intelligenz (KI)**. Hochschulen des Landes haben diesen Forschungsbereich mit unterschiedlichen Schwerpunkten in den vergangenen Jahren ausgebaut. Die Ergebnisse fließen in die Digitalisierungs- und Cybersicherheitsstrategie des Landes Nordrhein-Westfalen ein und unterstützen die zukunftsorientierte Weiterentwicklung der Umsetzungsmaßnahmen. Die Landesregierung wird die Hochschulen bei der Intensivierung und Erweiterung von Forschungsbereichen zur Cybericherheit unterstützen.

Das **Thema Künstliche Intelligenz** wird überdies als wichtiger Aspekt der **Zukunftsfähigkeit der Justiz** betrachtet. Dieser Einschätzung folgend hat die ZAC NRW u. a. in Zusammenarbeit mit Unternehmen, Wissenschaftlern und dem Deutschen EDV-Gerichtstag e. V. ein Grundlagenprojekt im Themenfeld „Bekämpfung der digitalen Kinderpornographie“ initiiert. Dieses Projekt diente der Erforschung des Einsatzes von künstlicher Intelligenz mit dem Ziel der beschleunigten Erkennung und Auswertung kinder- und jugendpornographischen Bildmaterials im Bereich der Strafverfolgung. Es hat den Nachweis erbracht, dass ein hybrides Cloudszenario grundsätzlich geeignet ist, ein entsprechend angelegtes neuronales Netzwerk auszubilden. Die entwickelte KI-Infrastruktur hat hier den Projektnamen „AIRA“ (AIenabled Rapid Assessment) erhalten. Ein funktionsfähiger Prototyp ist bei der ZAC NRW implementiert.

Die im Anschluss an die Forschungsphase erforderliche Beauftragung geeigneter Unternehmen mit der Umsetzung wird derzeit vorbereitet. Um den Übergang wichtiger Forschungsergebnisse in das Land Nordrhein-Westfalen zu gewährleisten, wird die Landesregierung die Kooperation zwischen Wissenschaft, Verwaltung und Wirtschaft weiter ausbauen.

Nordrhein-Westfalen ist ein Standort für internationale Spitzenforschung. Rund 70 Universitäten und Hochschulen mit etwa 772.300 Studierenden (Wintersemester 2018/2019), circa 100 an Hochschulen angesiedelten Forschungsinstituten und mehr als 50 außeruniversitären Forschungseinrichtungen sind im Bundesland präsent. Somit besitzt Nordrhein-Westfalen die dichteste Wissenschafts- und Forschungslandschaft Europas. Die Landesregierung hat es sich zum Ziel gemacht, den Schutz des Wissenschaftsstandorts Nordrhein-Westfalen aktiv zu stärken und die Forschung im Land weiter zu fördern.

Hochschulen werden zunehmend zu Zielen für Angriffe im IT-Bereich. Daher bekommt Informationssicherheit im Hochschulumfeld eine immer größer werdende Relevanz. Aufgrund ihrer offenen Struktur und ihrer systemisch bedingten heterogenen IT-Landschaften sehen sich Hochschulen hier einer besonderen Herausforderung gegenübergestellt, die nicht mit denen geschlossener Behörden- oder Firmennetzwerke vergleichbar sind. Diesen besonderen Bedarf haben die Hochschulen erkannt und beschlossen – begleitend zu lokalen Maßnahmen zur Informationssicherheit, wie beispielsweise dem Einsatz lokaler IT-Sicherheitsbeauftragter und IT-Sicherheitskonzepte – auch weitere kooperative Maßnahmen zu ergreifen und so die lokalen Aktivitäten zu stärken. In der Vereinbarung zur Digitalisierung haben sich die Hochschulen dazu verpflichtet, mindestens die Basis-Absicherung nach BSI IT-Grundschutz oder das „IT-Grundschutz-Profil für Hochschulen“ des Zentrums für Kommunikation und Informationsverarbeitung e. V. (ZKI e. V.) anzuwenden und zu erfüllen. Vorrangig sollen hierbei die Maßnahmen zum Schutz von Services der zentralen Rechenzentren und der Verwaltungs-IT im Fokus stehen.

Zudem unterstützt das Land die Hochschulen auch bei der Sensibilisierung der Studierenden und des Hochschulpersonals zum Thema „Cyber- und Informationssicherheit“. Hierzu wurde kürzlich die Förderausschreibung „Cyber- und Informationssicherheit“ für digitale Selbstlernangebote veröffentlicht, deren Inhalte modular auch in anderen Projekten an den Hochschulen, z. B. in der Fortbildung zur Entwicklung digitaler Kompetenzen in der Hochschulverwaltung (Digi-V.nrw) oder dem Erwerb Digitaler Kompetenzen für Studierende (digi-komp.nrw), integriert werden.

Aus Mitteln der Digitalisierungsoffensive fördert das Land zudem eine hochschultypübergreifende Struktur an der Digitalen Hochschule NRW (DH.NRW), die die Hochschulen bei der Umsetzung der Absicherung nach BSI-Methodik und im Falle einer Havarie fachlich unterstützt. Weiterhin erarbeiten die Hochschulen über die DH.NRW gemeinsame Sicherheits- und Schulungskonzepte, implementieren dieselben und werden sich gegenseitig untereinander und mit dem CERT NRW austauschen. Dabei werden die Hochschulen über die DH.NRW auch länderübergreifend zusammenarbeiten.

Hochschulen sind zudem **wichtige Kooperationspartner des Landes für die Ausbildung von IT-Fachkräften**. Ziel ist es, dem bestehenden IT-Fachkräftemangel wirksam zu begegnen, um einerseits den Wissenschaftsstandort zu festigen und andererseits die Digitalisierung und die Cybersicherheit im Land langfristig durch gut ausgebildetes Fachpersonal zu sichern. Hierbei sollte außerdem die Chance genutzt werden, um durch spezielle Bildungsangebote zum Thema Cybersicherheit für Frauen und Mädchen nicht nur eine Sensibilisierung zu fördern, sondern auch dazu beitragen, dem Digital Gender Gap

entgegenzuwirken. Mehr Frauen auf diesem Wege für das Thema Cybersicherheit zu begeistern und zu gewinnen, stellt eine wichtige Maßnahme zur Weiterqualifikation und Fachkräftegewinnung dar. Für den Bereich der öffentlichen Verwaltung erfolgte bei der Hochschule für Polizei und öffentliche Verwaltung (HSPV) zum Studienjahr 2020/2021 die Einrichtung eines neuen Bachelorstudiengangs „Verwaltungsinformatik“ (B.A.), welcher neben Rechts-, Verwaltungs-, Wirtschafts- und Sozialwissenschaften auch Grundlagen der Informatik, der IT-Anwendungsentwicklung und des IT-Management vermittelt. Im Rahmen einer Kooperation zwischen der Hochschule Rhein-Waal und dem Wirtschaftsministerium wird seit dem Wintersemester 2020/21 ein weiterer dualer Studiengang „Verwaltungsinformatik – E-Government“ (B.Sc.) mit Schwerpunkt Informatik, IT-Sicherheit, Datenschutz und Datensicherheit, E-Government, IT-Administration sowie Softwareanpassung und -entwicklung Studierenden angeboten.

Die Cybersicherheitsarchitektur und die erweiterte Cybersicherheitslandschaft Nordrhein-Westfalens bieten ein gutes Fundament zur Förderung und Steigerung der Cybersicherheitskompetenz des Landes. Mit Blick auf weitere zukünftige KI-Nutzung legt das Land besonderen Wert auch auf die ethischen Aspekte von KI wie sie in der EU guideline on ethics in artificial intellligence (Stand 2019) beschrieben sind. Durch die geplante **Fokussierung auf eine erhöhte Koordinierung**, eine **gesteigerte Kooperation** zwischen staatlichen und nichtstaatlichen Institutionen sowie die **Umsetzung der konkreten Maßnahmen** wird die Cybersicherheit wirksam gefördert.

STRATEGISCHE ZIELE:

4. Steigerung der **Effektivität** und **Effizienz der Kommunikation** der Cybersicherheitsakteure im Land und aus dem Land heraus
5. Unterstützung der Forschung und des Ausbaus des **Wissenschaftsstandorts** Nordrhein-Westfalen
6. **Verbesserung der Datenlage** im Bereich Cybersicherheit

ABBILDUNG 9

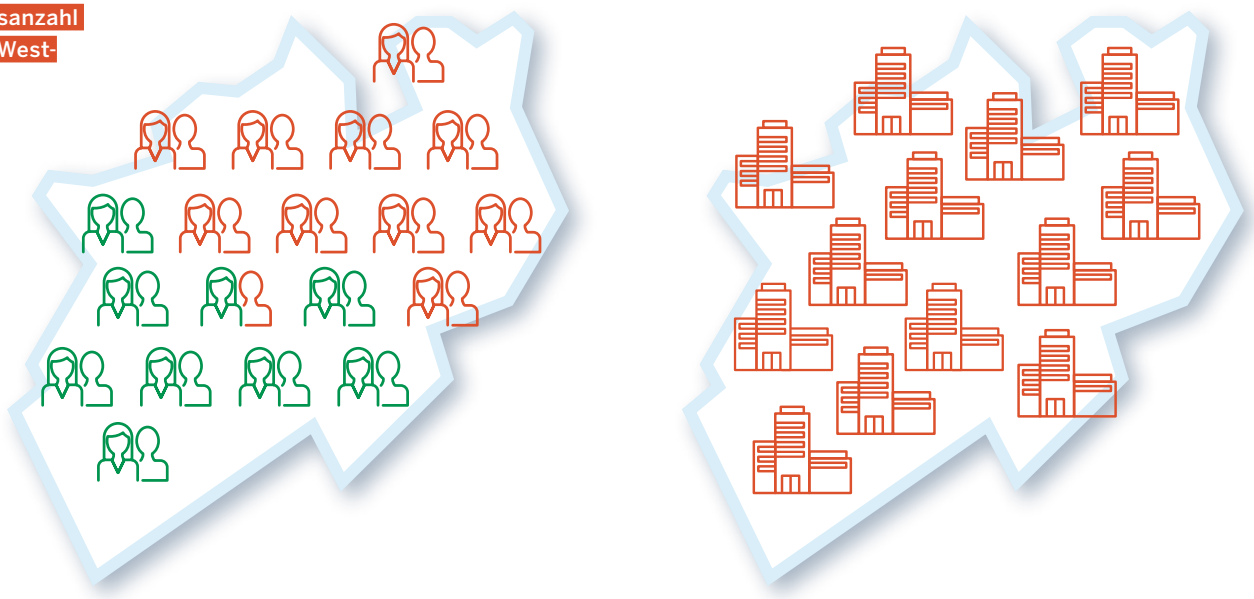
4.3 Cybersicherheit als Erfolgsfaktor Nordrhein-Westfalens: Den kleinen und mittleren Unternehmen muss eine besondere Unterstützung angeboten werden

Die mehr als 700.000 nordrhein-westfälischen Unternehmen erwirtschafteten im Jahr 2019 mehr als 1,6 Billionen Euro Umsatz. Für diese Unternehmen ist Cybersicherheit neben einer Notwendigkeit auch ein wichtiger Erfolgsfaktor. Dies wird besonders daran deutlich, dass laut des Branchenverbands BITKOM e. V. durch Diebstahl, Spionage und Sabotage der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro entsteht. Damit haben kriminelle Attacken erneut für Rekordschäden gesorgt: Die Schadenssumme ist mehr als doppelt so hoch wie in den Jahren 2018/2019, als sie noch 103 Milliarden Euro p. a. betrug.

Kleine und mittlere Unternehmen bilden mit 99,5 Prozent der Unternehmen des Landes das Rückgrat der nordrhein-westfälischen Wirtschaft. Sie beschäftigen rund 53,5 Prozent aller sozialversicherungspflichtig angestellten Personen in Nordrhein-Westfalen.

ABBILDUNG 10

Anzahl der sozialversicherungspflichtig Beschäftigten und Anteil von KMU an der gesamten Unternehmensanzahl in Nordrhein-Westfalen (2017)



Kleine und Kleinst-Unternehmen in Deutschland wurden in den letzten Jahren vermehrt Ziel von Cyberangriffen. Sie sind in der Regel hoch spezialisiert, arbeiten häufig eng mit großen Unternehmen zusammen, verfügen jedoch nicht in jedem Fall über die notwendigen Ressourcen und das Wissen, um sich bestmöglich vor Cyberangriffen zu schützen. Hinzu kommt, dass viele Unternehmerinnen und Unternehmer ihren Betrieb für zu klein halten, um Opfer von Cybercrime zu werden, was sich oft als Fehleinschätzung erweist.

Laut einer Untersuchung des BSI würde jeder sechste Mitarbeitende sensible Unternehmensinformationen als Reaktion auf eine gefälschte E-Mail der vermeintlichen Vorgesetzen weitergeben. Somit bleibt der **„Faktor Mensch“** auch im Unternehmensumfeld weiterhin die größte Angriffsfläche für Cyberkriminelle. Gerade KMU müssen in die Lage versetzt werden, sich wirksam vor den Gefahren im und aus dem Cyberraum zu schützen, um die mit der Digitalisierung verbundenen Chancen in vollem Umfang nutzen zu können.

Als Reaktion auf die geschilderte Gefährdungslage bietet das Land bereits zahlreiche Angebote zur Cybersicherheit wie beispielsweise Präventionsprogramme für Unternehmen an.

Das Ministerium für Wirtschaft, Industrie, Digitalisierung und Energie hat zu Anfang des Jahres 2021 **DIGITAL.SICHER.NRW** als **Kompetenzzentrum für Cybersicherheit in der Wirtschaft** ins Leben gerufen.

Das Kompetenzzentrum wird den Mittelstand Nordrhein-Westfalens bei der Erhöhung seiner digitalen Sicherheit unterstützen und bietet künftig schnellen und unkomplizierten Zugang zu Informationen und Ressourcen zum Thema. Alle Leistungen und Unterstützungsangebote, die das Kompetenzzentrum anbietet, sind dabei für nordrhein-westfälische KMU kostenfrei.

Im Fokus der Aktivitäten stehen die **Förderung von Austausch und Vernetzung** sowie Angebote für Ausbildung und Prävention zum Thema Cybersicherheit. Eine wichtige Rolle spielt dabei die Zusammenarbeit mit anderen Beteiligten der Cybersicherheitsarchitektur Nordrhein-Westfalens, wie LKA NRW, ZAC NRW und CERT sowie relevanten Akteurinnen und Akteuren aufseiten der Zielgruppe, bspw. die lokalen oder regionalen IT-Dienstleister. Das Kompetenzzentrum agiert als Erstanlaufstelle mit besonderem Fachwissen zu KMU-Strukturen und gleichzeitig als Multiplikator zu den Bedarfstragenden im Sinne der Zielgruppen. Dazu gehören beispielsweise die IHK, nordrhein-westfälische Unternehmerverbände, Handwerkskammern sowie auch Sparkassenverbände mit einem breiten Zugang zu den KMU in NRW.

DIGITAL.SICHER.NRW wird zudem eng mit der **„Allianz für Cybersicherheit“** des BSI zusammenarbeiten. Mit dieser Kooperation wird der unkomplizierte Zugriff auf die Angebote des BSI für nordrhein-westfälische Unternehmen gewährleistet.

Jährlich soll durch DIGITAL.SICHER.NRW ein **landesweites Kompetenztreffen** zur Cybersicherheit veranstaltet werden. Das Kompetenztreffen soll zu einer der zentralen Austausch- und Vernetzungsveranstaltungen rund um das Thema Cybersicherheit in Nordrhein-Westfalen ausgebaut werden. Bis zu 300 Teilnehmende sollen dabei zudem über den aktuellen Stand der Cybersicherheitsforschung und -entwicklung in Nordrhein-Westfalen informiert werden. Mit Maßnahmen wie einem Cybersicherheits-Roundtable, öffentlichen, regionalen Technologiestammtischen oder einer intensiven Kommunikation über die Homepage www.digital-sicher.nrw wird das Kompetenzzentrum zum einen die gesamte Tiefe der Wertschöpfungsketten in NRW ansprechen und zugleich zielgerichtet lokal agieren können.

Zur Profilierung des Wirtschaftsstandortes und zur Vernetzung insbesondere von kleinen und mittleren Unternehmen wird DIGITAL.SICHER.NRW auf Messen und Veranstaltungen das Thema **„Cybersicherheit im Mittelstand“** in den Mittelpunkt stellen. Mithilfe von Status-quo-Befragungen und der Einrichtung von entsprechenden Panels wird „DIGITAL.SICHER.NRW“ dazu beitragen, die Datenlage im Themenfeld der Cybersicherheit für Nordrhein-Westfalen zu verbessern. Zudem ist das Angebot kostenfreier leicht zugänglicher praxisorientierter Formate wie Webinarreihen, die den Zugang zum gesamten Themenkomplex der Cybersicherheit erleichtern, geplant.

Neben den Aktivitäten des Kompetenzzentrums werden im Rahmen der **Innovationsstrategie für Nordrhein-Westfalen** Forschung und Entwicklung im Bereich der Cybersicherheit des Landes gezielt im Rahmen von Förderwettbewerben finanziell unterstützt. Unter anderem in dem Innovationsfeld „Schlüsseltechnologien der Zukunft, IKT“, aber auch in den Bereichen „Digitalisierung“ und „Forschungsinfrastruktur“ werden innovative Vorhaben der Cybersicherheitsforschung und -anwendung ihren Platz finden können.

Das Förderprogramm Mittelstand Innovativ & Digital (MID) fördert mit den Bausteinen MID-Gutscheine und MID-

Assistent/in branchenoffen die Entwicklung und Optimierung digitaler Produkte, Dienstleistungen und Produktionsverfahren. Der neue Baustein „MID-Invest“ setzt weitere Anreize bei kleinen und mittleren Unternehmen, sich digital aufzustellen und Anschaffungen in technologiebasierte Soft- und Hardware vorzunehmen. Diverse Investitionen zur Stärkung der IT-Sicherheit der Unternehmen (u. a. Penetrationstest und Virenschutzsoftware, Firewall) sind hier ebenfalls förderfähig.

Die ZAC NRW hat insbesondere mit Unternehmen aus dem Bereich der Kritischen Infrastrukturen ein enges Netzwerk gebildet. Nach den bisherigen Erfahrungen ist dieses Netzwerk eine tragfähige Grundlage für eine verbesserte Zusammenarbeit bei Cybersicherheitsvorfällen und hat in der Vergangenheit erheblich dazu beigetragen, die Bereitschaft zur Erstattung von Strafanzeigen durch die Unternehmen zu erhöhen. Der Bereich Kritische Infrastrukturen ist ein in besonderem Maße vertrauensbezogenes Wirtschaftsfeld, in dem ohne den Aufbau belastbarer Vertrauensbeziehungen eine wirksame Ermittlungsarbeit kaum denkbar erscheint.

Bei ihrer Netzwerkarbeit greift die ZAC NRW auf verschiedene Formate zurück. So ist sie zunächst Mitglied im **Netzwerk Wirtschaftskriminalität** des Bundeskriminalamtes. In diesem Verbund sind vor allem DAX-Konzerne engagiert. Ferner trägt die ZAC NRW regelmäßig auf Schulungen und Tagungen der Wirtschafts- und Unternehmensverbände vor und ist über eine besondere 24/7-Hotline jederzeit für die Unternehmen erreichbar. Mit dem **„ZAC Talk“** ist schließlich eine Veranstaltung etabliert, in der Unternehmen und Strafverfolgende in unmittelbaren Austausch treten können. Darüber hinaus berät auch die Polizei NRW auf Wunsch die Unternehmen.

Die Landesregierung wird ihre Sensibilisierungs- und Unterstützungsangebote für die Führungs- und Beschäftigtenebene der nordrhein-westfälischen Wirtschaft weiter ausbauen und soweit erforderlich fachspezifisch ausrichten. In Kooperation mit Interessenverbänden werden neue Kommunikationswege erschlossen. So werden die Präventionsangebote des LKA NRW und des Fachbereichs Wirtschaftsschutz des Verfassungsschutzes noch stärker als bisher über die regionalen und lokalen Strukturen der Beteiligten in der **„NRW-Sicherheitspartnerschaft gegen Wirtschaftsspionage und Wirtschaftskriminalität“** (IHK, Verband der Wirtschaftsförderungsgesellschaften und ASW) publik gemacht, um das Angebot „vor Ort“ zu bewerben. Die Initiative des Ministeriums für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz bietet Unterstützung bei der Durchführung von Cybersicherheitsmaßnahmen im Sinne des Störfallrechts im Bereich der Anlagensicherheit an.

Wie gut kleine und mittlere Unternehmen in Nordrhein-Westfalen vor Spionage, Sabotage und Cyberangriffen geschützt sind, lässt der **nordrhein-westfälische Verfassungsschutz** 2021 im Rahmen der Fortschreibung des **Lagebilds Wirtschaftsschutz** untersuchen. Das erste Lagebild aus dem Jahr 2019 hatte gezeigt, dass mehr als ein Drittel der mittleren Unternehmen kaum gegen Angriffe geschützt sind und das Schutzniveau insgesamt stark ausbaufähig ist. Als eine der strategischen Maßnahmen zur Verbesserung der Datenlage im Bereich der Cybersicherheit ist geplant, das Lagebild Wirtschaftsschutz in einem zweijährigen Rhythmus zu aktualisieren und fortzuschreiben. Das Lagebild Wirtschaftsschutz ist ein Präventionsprojekt der **Sicherheitspartnerschaft NRW**. Verantwortlich für das Lagebild ist der Verfassungsschutz. Er kooperiert dabei mit der Fachhochschule des

Mittelstands (FHM) in Bielefeld, um die Datenlage im Bereich der Cybersicherheit zu verbessern. Zur Sicherheitspartnerschaft NRW gehören seit 2001 neben Innen- und Wirtschaftsministerium, der ASW West – Allianz für Sicherheit in der Wirtschaft und die IHK NRW. Neues Mitglied ist seit dem Jahr 2020 der Verband der Wirtschaftsförderungs- und Entwicklungsgesellschaften NRW.

Ein besonderes Augenmerk wird auch auf Unternehmen zu richten sein, die noch nicht über die notwendigen finanziellen Mittel zum Aufbau einer IT-Sicherheitsinfrastruktur verfügen. Der Schutz deren Know-hows vor Cyberangriffen, Wirtschafts- oder Industriespionage ist wichtig für die Attraktivität des Wirtschaftsstandorts Nordrhein-Westfalen.

Die aktuellen Statistiken über erfolgreiche Cyberangriffe auf Unternehmen stehen unter dem Vorbehalt, dass viele erfolgreiche Angriffe nicht bekannt werden. Unternehmen scheuen teilweise – aus Sicht der Ermittlungs- und Verfolgungsbehörden – eine Einbindung von Polizei und Staatsanwaltschaft. In der akuten Situation ist die Beteiligung der Polizei zur Bekämpfung des Angriffs, der Abwehr weiterer Gefahren und folgend einer konsequenten Strafverfolgung jedoch ein wichtiges Instrument, um Unternehmen vor wirtschaftlichen Schäden zu schützen oder diese zumindest zu verringern. Für die Erhöhung der Reaktionsfähigkeit und der Chancen einer Strafverfolgung ist daher wesentlich, dass möglichst alle Unternehmen – nicht nur KRITIS-Unternehmen – bei Cyberangriffen unverzüglich die zuständigen Stellen informieren und Unterstützung bei der Bewältigung des Angriffs anfordern. Langfristig strebt die Landesregierung Nordrhein-Westfalen im Bereich der Inneren Sicherheit an, das Vertrauen der Unternehmen in die Cybersicherheitsangebote von Polizei, Justiz und Wirtschaftsschutz weiter zu erhöhen, um die **Anzeigebereitschaft** zu steigern und verstärkt **präventiv** wirken zu können.

Dies erfordert auch Investitionen in die staatliche Cybersicherheitsarchitektur. Die Polizei in Nordrhein-Westfalen hat durch ein umfangreiches Maßnahmenbündel, angefangen von der Stärkung der virtualisierten Zusammenarbeit der Kreispolizeibehörden, über zentral geführte Ermittlungen gegen weltweit operierende Tätergruppen bis hin zur Bildung von hochqualifizierten Cyberspezialisten-Teams die Kapazitäten zur Bekämpfung der Cyberkriminalität erheblich ausgebaut. Die Landesregierung fördert konsequent den weiteren Ausbau, beispielsweise durch Neueinstellungen von IT-Spezialistinnen und -Spezialisten. Der zusätzliche Ressourcenaufbau unterstützt die Detektion und Reaktion bei gemeldeten Cyberangriffen und stärkt das Vertrauen in die Expertise und Effizienz der Polizeibehörden.

Einen erheblichen Ausbau ihrer Kapazitäten im Bereich der Bekämpfung der Cybercrime hat auch die Justiz in Nordrhein-Westfalen erfahren. So ist die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) im Jahre 2020 personell erheblich aufgestockt worden und hat sich als bundesweit größte Cybercrime-Einheit der Justiz etabliert. Sie steht in engem Austausch unter anderem mit den Zentralstellen für Cybercrime in anderen Bundesländern, mit Unternehmen, anderen Einrichtungen und zu den Strafverfolgungsbehörden in anderen Staaten. Neben der ZAC NRW verfügen auch die weiteren Staatsanwaltschaften des Landes über Spezialistinnen und Spezialisten für den Bereich Cybercrime. Die Landesregierung fördert auch im Bereich der Justiz konsequent den weiteren Ausbau der erforderlichen Strukturen.

Der Kulturwandel hin zu einer offenen und partnerschaftlich geprägten Kommunikation zwischen Unternehmen und Behörden gelingt mit einem kontinuierlichen Austausch sowie **Transparenz des behördlichen Handelns**. Dies ist ein wesentlicher Bestandteil der Kooperation des Cybercrime-Kompetenzzentrums des LKA NRW mit den Verbänden. Die fachlich zuständigen Ressorts werden dazu gemeinsam mit dem Wirtschaftsschutz, der Polizei und der Justiz das Sensibilisierungsangebot zum Umgang mit Cyberangriffen und deren Folgenbewältigung intensivieren. Gleichzeitig ergeben sich weitere Erkenntniswerte für die Cybersicherheitslage in Nordrhein-Westfalen in den kommenden Jahren.

Eine besondere Relevanz entfaltet **Cybersicherheit** für **Kritische Infrastruktur-Unternehmen (KRITIS)**. Kritische Infrastrukturen sind Unternehmen oder Einrichtungen, die wichtige Funktionen für die Versorgung der Allgemeinheit sowie für die Wahrung öffentlicher Ordnung und Sicherheit erfüllen. Durch ihre Abhängigkeit von der Informationstechnologie sind auch sie ins Visier von Cyberkriminellen geraten. Die enge Verflechtung und sich bedingende Abhängigkeiten der jeweiligen Bereiche und Dienste erhöhen die Verwundbarkeit und das mögliche Schadenspotenzial durch Cyberangriffe beträchtlich.

Aus Gründen der Daseinsvorsorge besteht seitens der Landesregierung ein hohes Interesse daran, dass diese Organisationen uneingeschränkt ihre Leistungen für die Allgemeinheit erbringen können und sich durch bedarfsgerechte Sicherheitsmaßnahmen vor Störfällen, wie beispielsweise Cyberangriffen, schützen können. Die **Erhöhung der Cyberresilienz** ist daher nicht nur wichtig für Betreibende kritischer Infrastrukturen, denen gemäß der BSI-KRITIS-Verordnung aufgrund des Überschreitens von Schwellenwerten ein bedeutender Versorgungsgrad zugeschrieben wird.

Auch Betriebsstörungen lokaler Versorgungsunternehmen als Teil einer Lieferkette können zu signifikanten Versorgungslücken und Schäden führen. Unternehmen, die zwar den KRITIS-Sektoren zuzuordnen sind, jedoch nicht die Schwellenwerte der KRITIS-Verordnung erreichen, haben dennoch für Nordrhein-Westfalen zum Beispiel als lokale Wasserversorgungsunternehmen eine hohe Bedeutung. Diese Unternehmen unterliegen nicht einer Registrierungspflicht beim BSI und profitieren nur dann von dem dort eingerichteten Warn- und Meldedienst, wenn sie sich freiwillig registrieren lassen.

Die Landesregierung hat sich zum Ziel gesetzt, durch Unterstützungsangebote diesen Unternehmen zu helfen, ihre Resilienz und ihre Fähigkeit zur Reaktion auf Sicherheitsvorfälle weiter zu verbessern. Ein wichtiger Baustein ist die **Optimierung der Melde- und Informationswege**. Laut aktuellen Umfragen geben 53 Prozent der deutschen KRITIS-Unternehmen an, nicht oder nicht ausreichend von staatlichen Stellen über die aktuelle Bedrohungslage durch Cybervorfälle informiert worden zu sein. Hier gilt es, auf die vorhandenen Informationsmöglichkeiten, wie die Warn- und Informationsdienste des BSI, des UP-KRITIS und der Allianz für Cybersicherheit, hinzuweisen und an die **Eigenverantwortung der KRITIS-Unternehmen** zu appellieren.

Die beim Ministerium des Innern eingerichtete **zentrale Kontaktstelle des Landes (ZKL)** wird gemeinsam mit dem BSI und in Abstimmung mit den fachlich zuständigen Ressorts die Informations- und Kommunikationswege so ausgestalten, dass Betreibende von kritischen

Infrastrukturen schnellstmöglich über Cyberangriffsvektoren unterrichtet und damit Reaktionszeiten verkürzt werden.

Die ZKL wird gemeinsam mit den kommunalen Spitzenverbänden die Möglichkeiten prüfen, wie auch regionale und kleinere KRITIS-Versorgungsunternehmen in kommunaler Hand in dieses Informationssystem eingebunden werden können. Die Erhöhung der Cyberresilienz erfordert sowohl infrastrukturelle Schutzmaßnahmen, als auch die Sensibilisierung und Schulung der Beschäftigten in diesen Unternehmen.

Nordrhein-Westfalen wird diese Anstrengungen der Betreibenden durch zusätzliche Beratungsangebote zu bereichsspezifischen Schutzmaßnahmen der IT-Infrastruktur sowohl über staatliche Stellen, wie beispielsweise die ZAC NRW oder das LKA NRW, als auch über Zentren wie DIGITAL.SICHER.NRW – Kompetenzzentrum für Cybersicherheit in der Wirtschaft, unterstützen. Die ZAC NRW wird ihre vielfältige Netzwerkarbeit mit Wissenschaft und Wirtschaft weiter ausbauen. Dazu gehört auch ein erweitertes Informationsangebot in digitalen Medien.

Um die Kompetenzen zur agilen Gestaltung der Digitalisierung (z. B. der Wasserwirtschaft, insbesondere in Nordrhein-Westfalen) weiterzuentwickeln und aktiv zu gestalten, hat das Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz zusammen mit mehreren Wasserwirtschaftsunternehmen das Kompetenzzentrum Digitale Wasserwirtschaft geschaffen.

Der Austausch und die Kooperation der KRITIS-Unternehmen, insbesondere, wenn gegenseitige Abhängigkeiten bestehen, wird die Koordinierungsstelle Cybersicherheit NRW gemeinsam mit den zuständigen Ressorts im Rahmen von Netzwerken, Tagungen und anderen Formaten fördern und fachlich begleiten.

STRATEGISCHE ZIELE:

2 Cybersicherheitsprävention für kleine und mittlere Unternehmen

5 Unterstützung der Forschung und des Ausbaus des Wissenschaftsstandorts Nordrhein-Westfalen

6 Verbesserung der Datenlage im Bereich Cybersicherheit

ABBILDUNG 11

Die drei Handlungsfelder ermöglichen die Umsetzung der sechs Ziele der Landesregierung. Mit Hilfe zielgruppengerechter Maßnahmen will die Landesregierung in den kommenden Jahren gemeinsam mit allen gesellschaftlichen Akteuren das Cybersicherheitsniveau in und für Nordrhein-Westfalen gezielt verbessern.

Die Einflüsse der Europäischen Union, des Bundes, der anderen Bundesländer und der Kommunen für die Cybersicherheit in Nordrhein-Westfalen

5.0

Die Digitalisierung überschreitet Landes- und Bundesgrenzen. Daher muss **auch Cybersicherheit über die Grenzen Nordrhein-Westfalens** hinausgedacht werden. Cybersicherheit kann nur funktionieren, wenn **Kommunen, Länder, Bund und EU** zusammenarbeiten. Die sechs strategischen Ziele der Cybersicherheitsstrategie für Nordrhein-Westfalen unterstützen daher die vom Bund definierten Handlungsfelder und Leitlinien der Cybersicherheitsstrategie für Deutschland 2021.

Die **öffentliche Verwaltung** Nordrhein-Westfalens agiert täglich als wichtige Partnerin und Dienstleisterin für Bürgerinnen und Bürger, Unternehmen und Wissenschaft.

Für Bürgerinnen und Bürger sowie Unternehmen sind die 427 Kommunen in Nordrhein-Westfalen meistens die erste Ansprechstelle als öffentliche Verwaltung. Zudem betreiben sie häufig Einrichtungen oder Unternehmen (z. B. Stadtwerke), die den **KRITIS-Sektoren** zuzuordnen sind. Die Digitalisierung der kommunalen Verwaltung wird auch durch das Onlinezugangsgesetz (OZG), das den Online-Zugang für alle Verwaltungsleistungen bis Ende 2022 vorschreibt, entscheidend geprägt und vorangetrieben. Die Kommunen haben die meisten direkten Kontakte zu den Bürgerinnen und Bürgern. In allen Lebenslagen stellen sie daher bei der Digitalisierung der Gesellschaft eine besonders wichtige Schnittstelle zwischen den Bürgerinnen und Bürgern und der Verwaltung dar.

Die Landesregierung ist den Kommunen und kommunalen Unternehmen eine **starke Partnerin** in Sachen Cybersicherheit. In den kommenden drei Jahren wird die Landesregierung den engen Austausch mit der kommunalen Familie intensivieren, um gemeinsame Ziele für die Erhöhung der Cybersicherheit abzustimmen und eine gemeinsame Umsetzungsstrategie zu entwickeln. Vorrangig werden jedoch kurzfristige Verbesserungen der Informationslage zur Cybersicherheit für die Kommunalbehörden angestrebt.

Der **NRW CISO** wird mit den kommunalen Partnerorganisationen im Rahmen des E-Government-Gesetzes die Einbindung in den **Warn- und Informationsdienst des CERT NRW** prüfen und perspektivisch die Zusammenarbeit im CERT-Verbund mit den Kommunen und deren Rechenzentren weiter ausbauen.

Der Beauftragte der Landesregierung für Informationstechnik (CIO) hat die Voraussetzungen geschaffen, dass das Computer Emergency Response Team der Landesverwaltung (CERT NRW) für alle Kommunen in NRW schrittweise CERT-Dienstleistungen anbieten kann. Das erfolgt in drei Stufen:

— Im ersten Schritt bietet das Land bereits jetzt die **Weiterleitung sämtlicher Warn- und Informationsmeldungen**, die ihm selbst zur Verfügung stehen, in Richtung der Kommunen an. Das ist der kommunale Warn- und Informationsdienst – **KWID**.

— Danach wird, in Abstimmung mit den Kommunen, auch ein **Rückmeldekanal** angeboten, sodass das CERT NRW auch Sicherheitsmeldungen annehmen und an die angeschlossenen CERT-Verbünde zur Warnung und zum Erfahrungsaustausch weiterleiten kann.

— In einem dritten Schritt baut das CERT NRW ein **Mobile Incident Response Team** auf, ein sogenanntes „MIRT“. Auf Anforderung von Landesbehörden und NRW-Kommunen wird dann Hilfestellung vor Ort angeboten. So können bei zukünftigen Sicherheitsvorfällen die Teams in der betroffenen Behörde durch fachlich ausgebildetes Personal in kurzer Zeit verstärkt und unterstützt werden.

Das Land NRW hat somit im Zusammenwirken mit den Kommunalen Spitzenverbänden und der Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (KDN) die **Grundlage für eine dauerhafte Kooperation** der Verwaltungsebenen gelegt. Somit unterstützt die Landesregierung die Kommunen in NRW für eine bessere Cybersicherheit.

Im Kontext der **Länder, des Bundes und der Europäischen Union** fungiert Nordrhein-Westfalen als wichtiger Wirtschaftsstandort und fühlt sich verpflichtet, die Cybersicherheit auch über seine Landesgrenzen hinweg zu unterstützen. Nordrhein-Westfalen hat erkannt, dass Cybersicherheit für Europa nur in Zusammenarbeit mit den unterschiedlichen Ebenen innerhalb Europas gefördert werden kann. Auch wenn sich diese Ebenen stark unterscheiden, will sich Nordrhein-Westfalen im Rahmen von Partnerschaften und anderen Kooperationen einbringen.

Die vorliegende **Cybersicherheitsstrategie des Landes Nordrhein-Westfalen** soll als Anknüpfungspunkt für Partnerschaften auf Landes- und Bundesebene dienen. Um die Rolle Nordrhein-Westfalens in Cybersicherheitsthemen deutlich zu stärken, strukturiert und koordiniert die Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen künftig im Vorfeld von Entscheidungen in den Länderministerkonferenzen und länderübergreifenden Gremien die Abstimmung von Positionen Nordrhein-Westfalens im Bereich Cybersicherheit auf der Arbeitsebene. Der

Informationsfluss aus dem Land heraus und ins Land zurück wird kontinuierlich durch die Koordinierungsstelle verbessert. Damit steigen sowohl die Effizienz der Abstimmung, als auch die Handlungsfähigkeit der Landesregierung in den kommenden Jahren.

Bereits jetzt besteht ein regulärer **länderübergreifender Austausch** im Rahmen von Fachministerkonferenzen und insbesondere über das Gremium der Bund-Länder-Arbeitsgruppe zu Cybersicherheit. Dort beteiligt sich das Land Nordrhein-Westfalen am stetigen Wissenstransfer und dem Ausbau von Kooperationen. Entwicklungen und Trends im Bereich Cybersicherheit werden durch die Intensivierung der länderübergreifenden Gremienarbeit frühzeitiger erkannt und diese Informationen im Rahmen der Kommunikations- und Präventionsarbeit der Koordinierungsstelle für alle Betroffenen verfügbar gemacht.

Ein Beispiel für die erfolgreiche Zusammenarbeit zwischen dem Bund und Nordrhein-Westfalen ist auch die aktuell laufende **Pilotphase zwischen dem Nationalen Cyber-Abwehrzentrum (Cyber-AZ) und den Staatsanwaltschaften der Länder, darunter der ZAC NRW**. Ziel ist eine Steigerung der Effektivität durch Verbesserung des Informationsflusses und der Koordinierung zwischen den Beteiligten im Falle von Cyberangriffen. Das Cyber-AZ wurde 2011 im Rahmen der Umsetzung der Cybersicherheitsstrategie in Bonn gegründet. Es besteht bislang aus acht Kernbehörden des Bundes. Das Abwehrzentrum ist die Kooperations-, Kommunikations- und Koordinationsplattform der relevanten (Sicherheits-)Behörden und trägt im Krisenfall zur Handlungsfähigkeit der Bundesregierung bei.

Auch international etabliert sich die ZAC NRW als landesweit zuständige Zentralstelle für **Rechtshilfeersuchen anderer Staaten** bei herausgehobener Cyberkriminalität. Sie unterhält ein enges Netzwerk an Kontakten insbesondere mit europäischen und US-amerikanischen Partnerinnen und Partnern und kooperiert darüber hinaus mit internationalen NGOs aus unterschiedlichen Themenfeldern der Cybersicherheit und weiteren internationalen Behörden, wobei eine besonders aktive Zusammenarbeit mit den britischen Institutionen besteht. Für einen tiefergehenden Austausch beteiligt sich die ZAC NRW zudem regelmäßig an internationalen Tagungen und Konferenzen.

Auch aktuelle **Gesetzgebungsvorhaben des Bundes**, die die Cybersicherheit in Nordrhein-Westfalen betreffen, werden im Land aktiv begleitet. Fortlaufend überprüft der IMA Cybersicherheit NRW diese auf Handlungsnotwendigkeiten und stimmt die landesweiten Positionen zu Änderungsvorhaben ab. Als Beispiel für diesen Fall kann das IT-Sicherheitsgesetz 2.0 genannt werden.

Mit ihrer am 16. Dezember 2020 vorgelegten Cybersicherheitsstrategie will die EU-Kommission die kollektive Abwehr gegen Cyberbedrohungen etwa in den Bereichen Binnenmarkt, Strafverfolgung, Diplomatie und Verteidigung stärken und ein globales, offenes und sicheres Internet gewährleisten. Die EU-Cybersicherheitsstrategie bietet der Europäischen Union die Möglichkeit, ihre Führungsrolle bei internationalen Normen und Standards im Cyberraum zu festigen und die Zusammenarbeit mit Beteiligten in der ganzen Welt zu stärken, um sich für einen **sicheren Cyberraum** einzusetzen, der auf **Rechtsstaatlichkeit, Menschenrechten, Grundfreiheiten und demokratischen Werten** beruht. Die nordrhein-westfälische Cybersicherheitsstrategie verpflichtet sich diesen Werten. Sie leiten das Handeln des Landes im Bereich Cybersicherheit in den nächsten drei

Jahren und finden sich übersetzt in den geplanten strategischen Maßnahmen wieder.

Da nicht wenige Cybersicherheitsbedrohungen ihren Ursprung außerhalb der Europäischen Union haben, bedarf es auch eines erhöhten Engagements für die internationale Zusammenarbeit. Daher wird sich Nordrhein-Westfalen verstärkt für eine Zusammenarbeit des Bundes und der Europäischen Union mit Drittländern für eine grenzüberschreitend technische Hilfe und Unterstützung bei der Strafverfolgung einsetzen.

Digitale Souveränität soll in Deutschland und Europa aus Sicht der Bundesregierung als Leitbild etabliert werden. Die Landesregierung Nordrhein-Westfalen versteht Digitale Souveränität als Querschnittsthema und betont ihre Bedeutung auch für die Cybersicherheit. Sie teilt die Definition des Bundes und begreift Digitale Souveränität als die „Fähigkeit und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“. Das betrifft einerseits den Schutz von Daten sowie von Anwendungen vor unbefugten Zugriffen und Abflüssen und andererseits die Unabhängigkeit von Unternehmen. Die Landesregierung hat die Ambition, jederzeit die vollständige Verfügungsgewalt über die eingesetzten IT-Arbeitsmittel zu behalten.

Die Nutzung sicherer und vertrauenswürdiger Cloudtechnologien durch kleine und mittlere Unternehmen kann ein entscheidender Wirtschaftsfaktor für die Zukunft sein. Die dabei angestrebte Nutzung von in NRW, Deutschland und Europa entwickelten Technologien wird ein innovativer Meilenstein zu mehr digitaler Souveränität in NRW werden. Die Beteiligten der Cybersicherheitsarchitektur unterstützen mit ihren Aufklärungs- und Präventionsprogrammen sowohl Bürgerinnen und Bürger, Wirtschaft, Wissenschaft und Staat in der Befähigung, die digitalen Möglichkeiten zu nutzen, Risiken zu erkennen und diese abwägen zu können. Die Landesregierung setzt sich bereits jetzt im Rahmen des IT-Planungsrats aktiv zusätzlich für die Entwicklung einer Deutschen Verwaltungscloudlösung ein, in der die öffentlich-rechtlichen Rechenzentren auf standardisierten Infrastrukturen ihre Ressourcen bündeln und einen gemeinsamen Cloud-Verbund bilden können, damit sie unabhängiger von externen und privatwirtschaftlichen Cloudanbietern aus Drittstaaten werden. Insbesondere für die Sicherheitsbehörden in Nordrhein-Westfalen hat dieses Projekt eine hohe praktische Bedeutung. Durch die Förderung der Forschung und Entwicklung zu sicheren IT-Produkten in Nordrhein-Westfalen kann darüber hinaus ein Beitrag zur angestrebten Digitalen Souveränität auf nationaler und europäischer Ebene aus Nordrhein-Westfalen heraus geleistet werden.

Der digitalisierte Raum kennt keine Landesgrenzen. Aus diesem Grund arbeitet die Landesregierung Nordrhein-Westfalen nicht nur mit den nordrhein-westfälischen Kommunen, sondern auch mit anderen Ländern, dem Bund und der Europäischen Union zusammen.

Ausblick

6.0

Um die Potenziale des raschen Digitalisierungsschubs sicher nutzen zu können, stärkt Nordrhein-Westfalen die Cybersicherheit im Rahmen der Umsetzung dieser Strategie über die kommenden drei Jahre kontinuierlich. Nordrhein-Westfalen arbeitet bereits in den Bereichen der Strafverfolgung, Spionage- und Cyberabwehr, Forschung und Entwicklung, Ansprechstellen und Ausbildungen durch Präventions- und Informationsarbeit sowie Vernetzung an einer **nachhaltigen Erhöhung des Cybersicherheitsniveaus**. Weitere Beteiligte der Cybersicherheitsarchitektur des Landes wie der IMA Cybersicherheit und die Koordinierungsstelle Cybersicherheit fördern zudem die Kommunikation und Koordination der relevanten Stellen im Land und über die Landesgrenzen hinaus.

Die Landesregierung wird als zusätzliche strategische Maßnahme die Hilfsangebote an Unternehmen bei Cyberangriffen, insbesondere bei solchen auf KMUs, durch Polizei, Justiz und Wirtschaftsschutz stärken. Dies umfasst die Unterstützung der Unternehmen bei der Schadensbegrenzung ebenso wie bei der Betriebswiederherstellung etwa unter dem Aspekt der Prävention vor weiteren Angriffen.

Die Weiterentwicklung zahlreicher Technologien wird die nächste Generation der Cybersicherheit beeinflussen. Die **Internet-der-Dinge-Technologie** ist nur ein Beispiel, das vermehrt in der Fertigungsindustrie eingesetzt wird und für die ein neuer Sicherheitsrahmen entwickelt werden muss. Der Einsatz neuer Technologien bedeutet auch die konstante Weiterentwicklung der rechtlichen Rahmenbedingungen, um deren Nutzung rechtssicher zu ermöglichen. Neue Gefahren müssen frühzeitig erkannt, innovative Lösungen erforscht und entwickelt werden, weswegen der Forschungsstandort Nordrhein-Westfalen und die Cybersicherheitswirtschaft einer besonderen Förderung und eines besonderen Schutzes bedarf. Es wird zu den künftigen Aufgaben der Landesregierung gehören, hier Schritt zu halten und gleichzeitig eine Führungsposition in Modernität und Innovation einzunehmen. Die Förderung der Innovationsbereitschaft der Wirtschaft bei Schlüsseltechnologien (Quantentechnologien, KI, Kryptografie) wird weitere technologische Verbesserungen der Sicherheitsverfahren zukünftig bewirken. Hierdurch werden neue Möglichkeiten zur erfolgreichen und nachhaltigen Cybersicherheit entwickelt, die „sicherheitstechnische Strukturwandel“ in Nordrhein-Westfalen bewirken können.

Die sich stetig **ändernden Rahmenbedingungen** machen es erforderlich, Anpassungen an der Cybersicherheitsstrategie auch vor Ablauf des geplanten 3-Jahres-Zeitraums zu ermöglichen. Die Landesregierung und alle Beteiligten der Cybersicherheitsarchitektur des Landes haben daher die Aufgabe, nachzusteuern und Impulse in den laufenden Fortschreibungsprozess der Strategie einzubringen, wenn einschneidende Ereignisse für die Cybersicherheit in Nordrhein-Westfalen zu verzeichnen sind.

Im Rahmen der Fortschreibung dieser Strategie in drei Jahren bietet eine **Öffentlichkeitsbeteiligung**, beispielsweise durch ein öffentliches Forum, Workshops oder einen Runden Tisch mit ausgewählten Interessensvertretungen, die Möglichkeit, Impulse aus der Gesellschaft, Wirtschaft, Anbieterinnen und Anbietern sowie Wissenschaft aufzunehmen. Durch Rückmeldungen kann danach noch zielgerichteter auf die Bedarfe der Öffentlichkeit eingegangen werden. Diese werden dazu beitragen, den Cyberraum für die Menschen im Land sicherer zu gestalten.

In Zukunft will die Landesregierung regelmäßig ein umfassendes Cybersicherheitslagebild erstellen, das Grundlage der weiteren strategischen Überlegungen zur Verbesserung der Cybersicherheit sein wird. Darüber hinaus sollen die Zusammenarbeit, die Koordinierung und der Informationsaustausch weiter verstärkt und sichergestellt werden.

Bürgerinnen und Bürger des Landes sollen im Cyberraum sicher, frei und selbstbestimmt agieren können, insbesondere, wenn sie die Technologien und die mit deren Einsatz verbundenen Risiken aufgrund steigender Komplexität nicht im Einzelnen nachvollziehen können. Mit der Weiterentwicklung der Cybersicherheitsarchitektur und dem Ausbau der landeseigenen Angebote leistet die Landesregierung einen Beitrag zu einer verbesserten Informationslage bei der Bekämpfung von Cybercrime sowie einer vereinfachten Übersicht über wichtige Ansprechstellen und Kontakte. Die Cybersicherheitsstrategie bringt Nordrhein-Westfalen einen Schritt weiter, um den **Erfolgsfaktor Cybersicherheit** auch in der Wirtschaft nachhaltig zu fördern.

Das Gesamtziel, einen Beitrag zur gezielten Verbesserung des Cybersicherheitsniveaus in und für Nordrhein-Westfalen zu leisten, steht bei der Umsetzung und Verfolgung der Strategie immer im Vordergrund.

Die Landesregierung Nordrhein-Westfalen treibt konsequent die Digitalisierung des Landes voran und fördert die Cybersicherheit als wichtigen Erfolgsfaktor. Die Umsetzung der Cybersicherheitsstrategie und eine stetige Anpassung an den technologischen Fortschritt unterstützen dieses Ziel.

Zuständigkeiten der Ressorts

Ministerien des Landes Nordrhein-Westfalen	Zuständigkeiten der Ressorts im Bereich der Cybersicherheit	Kontakt
Staatskanzlei		https://www.land.nrw/de
	#DigitalCheckNRW	https://www.digitalcheck.nrw
Ministerium für Kinder, Familie, Flüchtlinge und Integration		https://www.mkffi.nrw
Ministerium der Finanzen		https://www.finanzverwaltung.nrw.de/
Ministerium des Innern	Referat 73 – Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen	https://www.cybersicherheit.nrw
	Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz (LAG-Cybersicherheit)	
	Kriminalitätsbekämpfung, Cybercrime	https://www.polizei.nrw/cybercrime
	Cybercentrum für Analyse, Prävention, Abwehr	https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/spionageabwehr E-Mail: kontakt.verfassungsschutz@im1.nrw.de
	Sicherheitspartnerschaft NRW	https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/sicherheitspartnerschaft-nordrhein
	Wirtschaftsschutz, Sicherheitspartnerschaft	https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/wirtschaftsschutz E-Mail: wirtschaftsschutz@im1.nrw.de Telefon: 0211 871-2821
	LKA NRW: Abteilung IV Cybercrime (Competence Center Cybercrime CCCC)	https://lka.polizei.nrw/artikel/abteilung-4 E-Mail: cybercrime.lka@polizei.nrw.de Telefon: 0211 939-4040
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie	Informationssicherheit in der Landesverwaltung	https://www.wirtschaft.nrw/sicherheit-der-informationstechnik
	CIO der Landesregierung (Abteilung II)	https://www.wirtschaft.nrw/cio-nrw
	IT-Sicherheit in der Landesverwaltung (NRW-CISO, Referat II B 4)	
	IT.NRW: IT-Planung und Steuerung, IT-Sicherheit, Infrastrukturdienste, Sicherheitsinfrastrukturen, Trustcenter	https://www.it.nrw/sicherheit
	CERT NRW	https://www.it.nrw/cert-nrw-91640 E-Mail: cert@it.nrw.de Telefon: 0211 9449-2124

Ministerien des Landes Nordrhein-Westfalen	Zuständigkeiten der Ressorts im Bereich der Cybersicherheit	Kontakt
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie	Cybersicherheit in der Wirtschaft (Prävention, Sensibilisierung, Transfer – Referat IV A 3)	https://www.wirtschaft.nrw/cybersicherheit
	DIGITAL.SICHER.NRW – Kompetenzzentrum für Cybersicherheit in der Wirtschaft	https://www.digital-sicher.nrw/ E-Mail: info@digital-sicher.nrw Telefon: 0234 5200-7334
	Sicherheitspartnerschaft	https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/sicherheitspartnerschaft-nordrhein
Ministerium für Arbeit, Gesundheit und Soziales	Digitalisierung im Gesundheitswesen, Gesundheitswirtschaft	https://www.mags.nrw/
Ministerium für Schule und Bildung		https://www.schulministerium.nrw/
	Programm LOGINEO NRW	www.logineo.nrw.de
Ministerium für Heimat, Kommunales, Bau und Gleichstellung		https://www.mhkbg.nrw/
Ministerium der Justiz	Strafrechtspflege: Cybercrime	https://www.justiz.nrw.de/Gerichte_Behoerden/zahlen_fakten/statistiken/strafrechtspflege/index.php
	Landespräventionsrat Nordrhein-Westfalen: Prävention der Internet- und Computerkriminalität	https://www.lpr.nrw.de/aufgaben/Computerkriminalitaet/index.php
	ZAC: Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen bei der Staatsanwaltschaft Köln	https://www.justiz.nrw.de/JM/schwerpunkte/zac/index.php E-Mail: zac@sta-koeln.nrw.de Telefon: 0211 477-4922
Ministerium für Verkehr		https://www.vm.nrw.de
Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz		https://www.umwelt.nrw.de
	Wirtschaftlicher Verbraucherschutz, Verbraucherzentrale NRW	https://www.verbraucherzentrale.nrw/ E-Mail: service@verbraucherzentrale.nrw Telefon: 0211 3399-5845
	Kompetenzzentrum Digitale Wasserwirtschaft	https://www.kompetenzzentrum-digitale-wasserwirtschaft.de/w E-Mail: info@kdw-nrw.de Telefon: 0201 4758-9020
Ministerium für Kultur und Wissenschaft	Forschung zu Digitalisierung und Informationstechnologien, Sicherheitsforschung	https://www.mkw.nrw/hochschule-und-forschung/foerderungen/foerderlinie-digitale-sicherheit
Geschäftsbereich des Ministers für Bundes- und Europaangelegenheiten sowie Internationales		https://www.mbei.nrw/

Glossar

Begriffe der Cybersicherheit, Cybersicherheitsakteure und Angebote auf Landesebene, Forschungseinrichtungen, Institute, Fachbereiche und sonstige wissenschaftliche Einrichtungen Nordrhein-Westfalens, die sich mit Cybersicherheit beschäftigen.
Alle Universitäten und Hochschulen für angewandte Wissenschaften in Nordrhein-Westfalen forschen zu verschiedenen Aspekten der IT- Sicherheit. Die folgende Auflistung ist darum nicht abschließend sondern stellt eine Auswahl spezialisierter Institute in NRW dar.

Botnetze
Unter einem „Bot“ versteht man ein Computerprogramm, das weitgehend automatisch sich wiederholende Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Nutzenden angewiesen zu sein. Damit ein Rechner Teil eines Botnetzes wird, muss er vorher mit Schadsoftware infiziert werden.

CERT-Bund
CERT-Bund, das Computer Emergency Response Team für Bundesbehörden, ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen.

CERT NRW
Das CERT NRW (CERT = Computer Emergency Response Team) ist zentrale Anlaufstelle in der Landesverwaltung für präventive und reaktive Maßnahmen in Bezug auf sicherheitsrelevante Vorfälle. Im Rahmen des ressortüber-greifenden ISMS unterstützt das CERT NRW die Arbeit der beziehungsweise des NRW CISO, beispielsweise als Ansprechpartner in Fragen der Informationssicherheit.

Chief Information Officer NRW (NRW CIO)
Die/Der NRW CIO koordiniert die Umsetzung der Sicherheitsstrategie und unterrichtet die Landesregierung über den aktuellen Stand der Informationssicherheit in der Landesverwaltung. Die/Der CIO benennt innerhalb der CIO-Stabsstelle die/den NRW CISO (CISO = Chief Information Security Officer). Die/Der CIO führt in Abstimmung mit den Ressorts Entscheidungen über ressortübergreifende Richtlinien und Regelungen zur Informationssicherheit in der Landesverwaltung herbei.

Chief Information Security Officer NRW (NRW CISO)
Nordrhein-Westfalens Chief Information Security Officer (NRW CISO) beziehungsweise Landesbeauftragte/r für Informationssicherheit unterstützt die/den CIO bei der Beratung und Aufklärung der Landesregierung zu Fragen hinsichtlich der IT-Sicherheit.

Cyber Campus Nordrhein-Westfalen

Neben innovativen Konzepten in der gemeinsamen Ausbildung und Qualifizierung für Doktorandinnen und Doktoranden gehen die Hochschulen in NRW auch neue gemeinsame Wege in der Konzeption von Studiengängen. Als Beispiel sei der „Cyber-Campus Nordrhein-Westfalen“ der Hochschule Bonn-Rhein-Sieg und der Hochschule Niederrhein genannt, die mit dem Wintersemester 2020/2021 erstmalig Studiengänge zu den Themen Cybersicherheit, Cyberkriminalität und Digitale Transformation anbieten.

Cyber-Cops

Die „Cyber Cops“ aus dem Kreis Minden-Lübbecke bilden eine Bildungsinitiative von Jugendlichen für Jugendliche zum Thema Cybersicherheit. Schülerinnen und Schüler werden zu Medienbetreuenden ausgebildet, die an Schulen Gleichaltrigen digitale Kenntnisse beibringen. Die Federführung des Projekts obliegt der Polizei, die die Fortbildung koordiniert.

Cybercrime Kompetenzzentrum

Das im Landeskriminalamt angesiedelte Cybercrime Kompetenzzentrum wurde 2011 eingerichtet, um den wachsenden Herausforderungen der Cybercrime zu begegnen. Das Cybercrime Kompetenzzentrum zielt auf die Steigerung des Gefahrenbewusstseins und die Vermittlung wirkungsvoller Maßnahmen zur Minimierung von Cybercrime ab, so werden beispielsweise einheitliche Präventionskonzepte für die Kreispolizeibehörden entwickelt. Das Zentrum bietet rund um die Uhr fachkompetente Sofortmaßnahmen für Unternehmen, Behörden und Institutionen der Forschung und Wissenschaft an.

Cybersicherheit nach BSI

Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Digitale.Verwaltung.NRW

Das Programm Digitale.Verwaltung.NRW wird von dem Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie gefördert. Es hilft unter anderem durch Schulungsangebote für alle Beschäftigten der öffentlichen Verwaltung, unterstützt die Digitalisierung der Landesverwaltung und auch fördert die digitalen Kompetenzen unter dem Sicherheitsaspekt.

DIGITAL.SICHER.NRW – Kompetenzzentrum für Cybersicherheit in der Wirtschaft

DIGITAL.SICHER.NRW – Kompetenzzentrum für Cybersicherheit in der Wirtschaft wurde 2021 zur Unterstützung kleiner und mittelständischer Unternehmen geschaffen. Zum Aufgabenspektrum gehören das Aufbereiten von Informationen zur Prävention, das Anbieten von Hilfestellung bei der Bedarfsermittlung für grundlegenden IT-Schutz sowie das zielgruppenspezifische Aufbereiten von Cybersicherheitsthemen. Zudem ist das Kompetenzzentrum Erstanlaufstelle bei Cyberfragen für kleine und mittelständische Unternehmen und strebt den Aufbau eines Netzwerks für Cybersicherheitsverantwortliche an.

Graduiertenkolleg NERD – North Rhine Westphalian Experts in Research on Digitalization

Das Ziel des Graduiertenkollegs ist es, die Nachwuchsförderung in der IT-Sicherheit an Universitäten und Hochschulen in ganz Nordrhein-Westfalen zu stärken und das Forschungsprofil im Forschungsbereich Human Centered Systems Security nachhaltig zu schärfen. Standortübergreifend werden seit 2016 die Nachwuchswissenschaftlerinnen und -wissenschaftler sowie die beteiligten Professorinnen und Professoren zusammengeführt und die Vernetzung der Wissenschaftlerinnen und Wissenschaftler gestärkt. Aktuell läuft das Auswahlverfahren für die zweite Programmausschreibung.

Graduiertenkolleg SecHuman

Das Forschungskolleg SecHuman, kurz für „Schöne neue Welt: Sicherheit für Menschen im Cyberspace“, ist am Horst-Görtz-Institut für IT-Sicherheit angesiedelt und auch eingebunden in das Exzellenzcluster CASA – Cybersicherheit im Zeitalter großskaliger Angreifer. In der ersten Förderperiode stand die Interaktion zwischen Mensch und IT-Sicherheit im Fokus. In der aktuellen Förderphase fokussieren die Arbeiten die IT-Sicherheit als weitergefasstes gesellschaftliches Phänomen inter- und transdisziplinär.

Horst-Görtz-Institut für Sicherheit in der Informationstechnik

Das HGI beheimatet den Exzellenzcluster „CASA: Cyber Security in the Age of Large-Scale Adversaries“. Gegenstand der Forschung ist die Aufklärung von Cyberattacken. Durch sein Bildungs- und Vernetzungsangebot strebt das HGI die Ausbildung der nächsten Generation der Führungskräfte in der Sicherheitsberatung an.

Heinz-Nixdorf-Institut der Universität Paderborn

Forschungsschwerpunkt des Instituts ist Safety und Security. Hierbei liegt die Betrachtung auf Safety Eigenschaften, die eine Kernfragestellung im Entwurf Intelligenter Technischer Systeme sind und Bestandteil heutiger Entwicklungsmethoden sind. Ziel ist es, diese Methodik so zu erweitern, dass die entworfenen Systeme „Secure by Design” sind, also aufgrund ihres Entwurfs auch aktiven Angriffen möglichst gut standhalten können.

Institut für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen

Das if(is) fokussiert Innovationen im Bereich der anwendungsorientierten Internet-Sicherheitsforschung. Erklärtes Ziel des Instituts für Internet-Sicherheit ist es, einen Mehrwert an Vertrauenswürdigkeit und Sicherheit im Internet herzustellen. Das if(is) bietet neben Forschung und Lehre auch einen kostenlosen Service zur Zertifizierung von OpenPGP-Schlüsseln sowie eine Jobbörse für IT-Sicherheit an.

Informationssicherheit nach BSI

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein.

Internet der Dinge (Internet of Things, IoT)

Internet der Dinge bezeichnet die zunehmende Vernetzung von globalen technologischen Infrastrukturen der Informationsgesellschaften. Verschiedene Objekte, Alltagsgegenstände oder Maschinen werden mit Prozessoren und Sensoren ausgestattet, sodass sie miteinander kommunizieren können.

Interministerieller Ausschusses Cybersicherheit NRW (IMA Cybersicherheit NRW)

Das Landeskabinett hat 2020 die Einrichtung eines Interministeriellen Ausschusses Cybersicherheit NRW (IMA Cybersicherheit NRW) beschlossen, der von der Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen geleitet wird. Durch die Gründung des IMA Cybersicherheit NRW wurde eine wichtige Institution zur besseren ressortübergreifenden Zusammenarbeit geschaffen.

Im IMA Cybersicherheit NRW kommen in regelmäßigen Abständen Kontaktpersonen aller Ressorts der Landesregierung Nordrhein-Westfalen zusammen, um über neueste Entwicklungen im Bereich der Cybersicherheit zu sprechen. Dadurch werden nun auch Bereiche abgedeckt, die bisher nicht in den Austausch eingebunden waren.

IT-Sicherheit nach BSI

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

Kleine und mittlere Unternehmen (KMU)

Unter den Sammelbegriff KMU fallen Kleinst-, Kleinunternehmen und mittlere Unternehmen.

Große Unternehmen hingegen zählen meist mehr als 250 Mitarbeitende, haben einen Umsatz von über 50 Millionen Euro und eine Bilanzsumme von mehr als 43 Millionen Euro.

Koordinierungsstelle für Cybersicherheit in Nordrhein-Westfalen

Die Koordinierungsstelle für Cybersicherheit in Nordrhein-Westfalen wurde im August 2020 gegründet, um die Akteure der Cybersicherheit zu koordinieren und Synergieeffekte zu schaffen. Die Koordinierungsstelle hat zum Ziel, das Schutzniveau der Cybersicherheit im Land zu erhöhen und erfüllt dabei drei wesentliche Aufgaben:

— Transparenz für alle relevanten Zielgruppen schaffen,

— die Kommunikation innerhalb Nordrhein-Westfalens sowie zwischen Land und Bund herzustellen und

— die Vernetzung ermöglichen, um ein effizienteres Arbeiten zu garantieren.

Durch den jährlich zu veröffentlichenden Bericht zur Cybersicherheit in Nordrhein-Westfalen fördert die Koordinierungsstelle neben der Informationsaufbereitung auch das Erkennen potenzieller Lücken im Cybersicherheitsangebot. Die Koordinierungsstelle stellt zudem nicht nur den Austausch innerhalb des Landes Nordrhein-Westfalen sicher, sondern agiert auch als zentrale Kontaktstelle des Landes (ZKL) gegenüber dem BSI. Nordrhein-Westfalen ist das erste Bundesland, das eine Koordinierungsstelle dieser Art eingerichtet hat.

KRITIS
KRITIS steht kurz für Kritische Infrastruktur. Dies sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen.

Malware
Bösartige Programme, die dazu entwickelt wurden, Nutzenden von elektronischen Endgeräten zu schaden, werden unter dem Begriff „Malware“ zusammengefasst. Viren, Trojaner, Botnetze, Ransomware, Adware und Spyware sind solche bösartigen Programme.

Max-Planck-Institut für Sicherheit und Privatsphäre
Das Institut erforscht und entwickelt die technischen Grundlagen und interdisziplinären Aspekte der IT-Sicherheit und des Datenschutzes.

Safer Internet Day
Der jährlich stattfindende Safer Internet Day ist ein Beispiel für eine internationale Initiative, die lokal in Nordrhein-Westfalen umgesetzt wird. Der Aktionstag für mehr Onlinesicherheit wird von der EU-Initiative „klicksafe“ koordiniert. Viele nordrhein-westfälische Behörden nehmen jährlich daran teil. Neben der Informationsverbreitung über Social-Media-Kanäle wird am Safer Internet Day auch eine Telefon-Hotline zur Verbraucherzentrale eingerichtet, unter der sich Menschen persönlich beraten lassen können.

Sicherheitspartnerschaft NRW
Ressortübergreifend wirkt die Landesregierung mit der „Sicherheitspartnerschaft NRW“ der Wirtschaftsspionage und Wirtschaftskriminalität entgegen. Mit dem Ziel, die Sicherheit des Wirtschaftsstandorts Nordrhein-Westfalen zu verbessern, arbeiten Beteiligte aus der Wirtschaft, den Verbänden und staatlichen Institutionen eng zusammen. Sie stehen in kontinuierlichem Austausch zu wichtigen Themen der Wirtschaftssicherheit und erstellen ein jährliches Lagebild zur Unternehmenssicherheit von kleinen und mittelständischen Unternehmen in Nordrhein-Westfalen. Die Geschäftsführung der Sicherheitspartnerschaft hat das Ministerium des Innern, wodurch die Expertise des Verfassungsschutzes und der Polizei in das Gremium direkt einfließt. Über die Zusammenarbeit mit dem MWIDE wird die Perspektive der Wirtschaft eingebracht.

Spam-Mails
Als Spam bezeichnet man unerwünschte Nachrichten, die über das Internet übermittelt werden. Spam tritt in verschiedenen Formen auf: als E-Mail, Werbebanner auf Webseiten und in Foren, wo Links geteilt werden.

Wirtschaftsschutz

Der Wirtschaftsschutz gehört zum Aufgabenspektrum des Verfassungsschutzes des Landes Nordrhein-Westfalen. Der Bereich bietet Unternehmen und Forschungseinrichtungen Präventions- und Zusammenarbeit zu Bedrohungen ausgehend von fremden Mächten, etwa durch Wirtschaftsspionage oder Cyberangriffen, an. Zum einen durch die Sensibilisierung der Mitarbeiter hinsichtlich der aufgezeigten Bedrohungen durch Vorträge, aber auch durch Initialberatungen zwecks Erstellung/Überarbeitung von Sicherheits- und Notfallkonzepten.

Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)

Die ZAC NRW, angesiedelt bei der Staatsanwaltschaft Köln, hat sich bundesweit als größte Cybercrime-Einheit etabliert. Ihr obliegt u.a. die Verfahrensführung bei Ermittlungen im Bereich der herausgehobenen Cybercrime. Zudem wirkt sie bei regionalen und überregionalen Aus- und Fortbildungsmaßnahmen im Bereich der Cybercrime mit.

Impressum

Herausgeber:
Ministerium des Innern
des Landes Nordrhein-Westfalen
Friedrichstr. 62 – 80
40217 Düsseldorf
Tel.: +49 (0) 211/871-01
Internet: www.im.nrw.de

Redaktion:
Ministerium des Innern
des Landes Nordrhein-Westfalen
Referat 73
Koordinierungsstelle Cybersicherheit NRW
E-Mail: cybersicherheit@im.nrw.de

Bildnachweise:
Cover: Luftbild © Hans Blossey
Seite 3: beide © Ralph Sondermann
Seite 6, 21, 25, 34: © greenbutterfly – stock.adobe.com
Seite 11, 63: © monsitj – stock.adobe.com

Mediengestaltung:
Rohloff Design
www.rohloff-design.de

Die Publikation ist auf der Homepage des Ministeriums des Innern des Landes Nordrhein-Westfalen unter https://www.cybersicherheit.nrw als PDF-Dokument abrufbar.


lected mirror modifier object
ob
ier ob is the active ob

Die Landesregierung
Nordrhein-Westfalen

Horionplatz 1, 40213 Düsseldorf
Telefon 0211 83 7- 1001
nrwdirekt@stk.nrw.de
land.nrw