Die Landesregierung
Nordrhein-Westfalen

Bericht zur Cybersicherheit
in Nordrhein-Westfalen 2020

www.land.nrw

Vorwort

die Corona-Pandemie hat die Digitalisierung der Gesellschaft in rasanter Weise beschleunigt. Eilig wurden in vielen Behörden und Unternehmen Mitarbeiterinnen und Mitarbeiter mit Technik ausgestattet und schnell digitale Vertriebs- und Kommunikationswege gefunden. Auch im privaten Bereich erfuhr die digitale Kommunikation und die allgemeine Nutzung der vernetzten Welt in den Zeiten von Kontaktbeschränkungen einen rasanten Anstieg. So manchem wurde dabei erst in den vergangenen Monaten bewusst, wie sehr sich unsere Welt durch die Digitalisierung verändert hat.

Diese Entwicklung spiegelt sich auch im hier vorliegenden „Cybersicherheitsbericht des Landes Nordrhein-Westfalen 2020“ wider. Denn genau wie Unternehmen haben sich auch Kriminelle den Umständen angepasst und neue Betätigungsfelder gefunden. So ist die Anzahl der Cyberkriminalitätsdelikte um knapp 21 Prozent im Vergleich zum Vorjahr stark angestiegen. Inzwischen sind mehr als drei Viertel aller Unternehmen in Deutschland einmal Opfer von Cyberkriminellen geworden.

Der Bericht macht deutlich: Cybercrime ist eine der größten aktuellen Bedrohungen. Dies gilt nicht nur für unser aller Wohlstand, sondern auch für unsere Gesellschaft an sich. Die Gesamtschadenshöhe beläuft sich laut Statistik für ganz Nordrhein-Westfalen auf etwas über 18 Millionen Euro, allerdings ist das nur die Spitze des Eisbergs, denn viele – erfolgreiche – Cyberangriffe werden der Polizei nicht angezeigt, um z. B. einen Imageschaden für die Unternehmen zu vermeiden. Als Gesellschaft gilt es auch die Gefahren von digitalen Desinformationskampagnen zu erkennen und durch gezielte Maßnahmen eine Unterhöhlung der Demokratie zu vermeiden.

HERBERT REUL
Minister des Innern
des Landes
Nordrhein-Westfalen

Der Bericht möchte daher Bürgerinnen und Bürger, Unternehmen und Betreiber kritischer Infrastrukturen informieren und aufklären. Er soll helfen, Ansprechstellen und Hilfsangebote aufzuschlüsseln und für eine breitere und dauerhafte Wahrnehmung des Themas Cybersicherheit in Nordrhein-Westfalen sorgen. Darüber hinaus gilt es vorhandene Kompetenzen aufzuzeigen und den weiteren Ausbau zu unterstützen, wie zum Beispiel im Bereich der IT-Sicherheitsforschung. Die Landesregierung hat zur Unterstützung dieser Ziele die „Koordinierungsstelle Cybersicherheit NRW“ sowie einen „Interministeriellen Ausschuss Cybersicherheit“ unter Beteiligung aller Ressorts eingerichtet, die gemeinsam Vorhaben zur Steigerung des Cybersicherheitsniveaus anstoßen.

Mit dem Wirtschaftsschutz, der Spionageabwehr, der Koordinierungsstelle Cybersicherheit, dem Landeskriminalamt und der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) bei der Staatsanwaltschaft Köln sowie weiteren Stellen sagt das Land auf breiter Front den Cyberkriminellen den Kampf an.

Dieser Bericht, der jährlich erscheint, ist ein wichtiges Element in diesem Kampf. Denn nur, was wir gut kennen, können wir wirksam bekämpfen.

Herbert Reul

Management Summary

In der digitalisierten Welt nimmt die Cybersicherheit eine immer bedeutendere Rolle ein. Daher ist es notwendig, die Entwicklungen der Cybersicherheit in NRW in den Blick zu nehmen.

Der vorliegende **Bericht zur Cybersicherheit in Nordrhein-Westfalen 2020** informiert über wichtige Entwicklungen innerhalb der nordrhein-westfälischen Cybersicherheitslandschaft und die Lage der Cybersicherheit im Land im Jahr 2020. Der von der Landesregierung Nordrhein-Westfalen herausgegebene Bericht erscheint im Jahr 2021 zum ersten Mal und berichtet über den Vorjahreszeitraum, künftig erscheint er jährlich. Er enthält Hinweise zu Präventionsmaßnahmen sowie Hilfs- und Informationsangebote der Landesregierung.

Für das Jahr 2020 werden zwei wichtige Themen in den Fokus genommen. **Aktuelle Entwicklungen aus der Cybersicherheitsarchitektur in Nordrhein-Westfalen** bilden das erste Fokusthema dieses Berichts.

Die **Corona-Pandemie und ihr Einfluss auf die Cybersicherheit** des Landes ist das zweite Fokusthema. Pandemiebedingte Umstellungen wie die Verlagerung der Arbeits- und Lernorte ins Internet veränderten den Alltag der Menschen im Land maßgeblich und öffneten zugleich neue Einfallstore für Cyberkriminelle. Die intensivere und längere Nutzung digitaler Plattformen und Netzwerke steigerte das Risiko für Cyberangriffe zusätzlich. So stieg die Anzahl der Delikte im Bereich der Cyberkriminalität in Nordrhein-Westfalen im Jahr 2020 um knapp 21 Prozent im Vergleich zum Vorjahr an.

Dieser Bericht zur Cybersicherheit in Nordrhein-Westfalen betrachtet drei Zielgruppen, die unterschiedlichen Cybersicherheitsrisiken ausgesetzt sind: Bürgerinnen und Bürger, Unternehmen und kritische Infrastrukturen (KRITIS). Mit dem Kapitel Informationssicherheit für die Landesverwaltung werden auch die Beschäftigten der Landesverwaltung adressiert. Das Land Nordrhein-Westfalen bietet den Zielgruppen bereits eine Vielzahl an Präventions- und Hilfsangeboten, welche jedoch nicht immer bekannt sind. Ein **Ziel des Berichts** ist es, Ansprechstellen und Hilfsangebote zielgruppenspezifisch aufzuschlüsseln, wodurch eine breitere gesellschaftliche Wahrnehmung des Themas Cybersicherheit in Nordrhein-Westfalen geschaffen werden soll. Der Bericht wird zudem in den kommenden Jahren den Umsetzungsfortschritt der Cybersicherheitsstrategie 2021–2024 des Landes Nordrhein-Westfalen dokumentieren. Im Weiteren geht der Bericht auf die Rolle Nordrhein-Westfalens im Bereich der Cybersicherheitsforschung ein und stellt einige Initiativen, Institute und Forschungskooperationen vor.

Die in der Cybersicherheitsstrategie formulierte Ambition der Landesregierung „gemeinsam mit allen gesellschaftlichen Akteuren das Cybersicherheitsniveau in und für Nordrhein-Westfalen zu verbessern“ wird durch diesen Bericht unterstützt.

Inhaltsverzeichnis

Vorwort ... 2

Management Summary ... 4

Inhaltsverzeichnis ... 5

1.0 Einleitung ... 6

1.1 Themenfokus 1: Aktuelle Entwicklungen der Cybersicherheitslandschaft in Nordrhein-Westfalen ... 8

1.2 Themenfokus 2: Die Corona-Pandemie ... 10

2.0 Gefährdungslage in Nordrhein-Westfalen 2020 ... 12

3.0 Zielgruppenspezifische Informationen und Lösungsansätze ... 18

3.1 Bürgerinnen und Bürger ... 19

3.2 Unternehmen ... 26

3.3 Kritische Infrastrukturen (KRITIS) ... 30

4.0 Informationssicherheit innerhalb der Landesverwaltung ... 34

5.0 Forschung und Innovation in der Cybersicherheit in Nordrhein-Westfalen ... 38

6.0 Ausblick ... 43

Informationsangebote

– Informationsangebote für Bürgerinnen und Bürger ... 45

– Informationsangebote und Kontaktstellen für Unternehmen ... 46

– Informationsangebote für Betreibende kritischer Infrastruktur ... 47

Glossar ... 50

Impressum ... 54

Einleitung

1.0

Der vorliegende Bericht zur Cybersicherheit in Nordrhein-Westfalen 2020 informiert im Auftrag der Landesregierung über wichtige Entwicklungen innerhalb der nordrhein-westfälischen Cybersicherheitslandschaft und die Lage der Cybersicherheit im Land im Jahr 2020. Er richtet sich dabei insbesondere an die **Zielgruppen der Bürgerinnen und Bürger, der Unternehmen und der kritischen Infrastrukturen (KRITIS). Das Kapitel Informationssicherheit adressiert auch die Angehörigen der Landesverwaltung.** Der Bericht wird künftig jährlich herausgegeben und berichtet über den jeweiligen Vorjahreszeitraum. Dabei stehen für das Jahr 2020 zwei Themen im Fokus: Zum einen informiert der Bericht über aktuelle Entwicklungen der Cybersicherheitsarchitektur des Landes und zum anderen beleuchtet er die Auswirkungen, die die Corona-Pandemie auf die Cybersicherheitslage in Nordrhein-Westfalen im Jahr 2020 hatte.

Der Bericht ist das Resultat der Zusammenarbeit des **Interministeriellen Ausschusses Cybersicherheit Nordrhein-Westfalen**. Er wurde unter enger Einbindung aller Ressorts der Landesregierung von der 2020 neu gegründeten Koordinierungsstelle Cybersicherheit NRW erstellt. Darüber hinaus liefert der Bericht auch Hintergrundinformationen für die „Cybersicherheitsstrategie für Nordrhein-Westfalen“ und wird künftig die Cybersicherheitslage in Nordrhein-Westfalen und die Fortschritte bei der Umsetzung der neuen Cybersicherheitsstrategie des Landes darstellen.

Im Rahmen des Berichts wird die allgemeine Gefährdungslage des Landes Nordrhein-Westfalen im Jahr 2020 in Kapitel 2 zusammengefasst. Darauf aufbauend beschreibt Kapitel 3 detailliert die spezifische Gefährdungslage für die drei Zielgruppen. Zudem dient Kapitel 3 einer verbesserten Informationslage und erleichtert den Überblick über wichtige Ansprechstellen und Kontakte für Bürgerinnen und Bürger, Unternehmen und kritische Infrastrukturen. Dadurch soll den jeweiligen Zielgruppen eine Hilfestellung gegeben werden, Cyberangriffen präventiv vorzubeugen und im Falle eines Angriffs adäquat reagieren zu können. Weiterhin zeigt dieser Bericht auf, an welcher Stelle die Notwendigkeit einer verbesserten Datenlage besteht.

In Kapitel 4 bietet der Bericht einen Überblick über die Informationssicherheitsarchitektur der Landesverwaltung und stellt ausgewählte Institutionen und ihre Aufgaben vor. Darüber hinaus werden Zuständigkeiten und Schlüsselmaßnahmen der Landesregierung im Bereich der Informationssicherheit vorgestellt. Der Forschungs- und Innovationsstandort Nordrhein-Westfalen wird in Kapitel 5 beleuchtet. Kapitel 6 bietet schließlich einen Überblick über die Cybersicherheitslandschaft Nordrhein-Westfalens und befasst sich mit den Chancen und Risiken neuer Technologien.

1.1 Themenfokus 1: Aktuelle Entwicklungen der Cybersicherheitslandschaft in Nordrhein-Westfalen

Die Cybersicherheitslandschaft Nordrhein-Westfalens hat sich auch im Jahr 2020 tiefgreifend weiterentwickelt. Im Februar sicherte das Ministerium für Kultur und Wissenschaft dem **Projekt „Cyber-Campus Nordrhein-Westfalen“** sechs Millionen Euro für die Förderung neuer Studiengänge zur Cybersicherheit zu. Das Projekt ist eine Kooperation der Hochschule Bonn-Rhein-Sieg und der Hochschule Niederrhein und startete im Wintersemester 2020/21 in seine Pilotphase. Ziel ist es, Nachwuchsfachkräfte in der Erkennung von Cybercrime, IT-Forensik und Cyber-Security Management zu schulen, um dem Fachkräftemangel in der Wirtschaft und der öffentlichen Hand entgegenzuwirken. Nordrhein-Westfalen wird dadurch als Standort der Informationstechnologie gestärkt.

Weitere Aufmerksamkeit erhielt die Spitzenforschung am Standort Nordrhein-Westfalen durch die Verleihung des **Innovationspreises** von Minister Andreas Pinkwart in ihrem zehnten Jubiläumsjahr. Zukunftsfelder wie Blockchain, Cybersicherheit und Materialwissenschaften wurden mit dem hoch dotierten Preis ausgezeichnet.

Auf Vorschlag von Innenminister Reul und Wirtschafts- und Digitalminister Pinkwart hat das Kabinett im August 2020 beschlossen, die **Koordinierungsstelle Cybersicherheit NRW** einzurichten. Sie ist im Ministerium des Innern angesiedelt und eine der zentralen Maßnahmen für die im Koalitionsvertrag für Nordrhein-Westfalen (2017–2022) identifizierte Herausforderung einer Verbesserung der Cybersicherheit.
Mit der Koordinierungsstelle verfügt Nordrhein-Westfalen über eine wichtige Instanz, um die Beteiligten der Cybersicherheitsarchitektur im Land besser zu vernetzen. In ihrer Funktion als zentrale Servicestelle der Landesregierung arbeitet sie mit allen Ressorts zusammen und ist die erste Koordinierungsstelle auf Ebene einer Landesregierung bundesweit. Ihr Ziel ist es, das Schutzniveau der Cybersicherheit im Land zu erhöhen, die Informationsströme zwischen den nordrhein-westfälischen Institutionen der Cybersicherheit zu koordinieren und Synergieeffekte zu schaffen. Gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) agiert die Koordinierungsstelle als zentrale Kontaktstelle des Landes (ZKL). Sie erfüllt zudem drei wesentliche Aufgaben:

- **Transparenz** für alle relevanten Zielgruppen schaffen,
- **Kommunikation** innerhalb der Landesregierung sowie zwischen Land und Bund herstellen und
- **Vernetzung** ermöglichen, um ein effizienteres Arbeiten zu garantieren.

Im Jahr 2020 wurde zudem der **Interministerielle Ausschuss Cybersicherheit (IMA Cybersicherheit)** gegründet, der von der Koordinierungsstelle Cybersicherheit NRW geleitet wird. Mitglieder des IMA Cybersicherheit sind alle Ressorts des Landes Nordrhein-Westfalen. Sie tauschen sich regelmäßig zu Themen der Cybersicherheit aus und stimmen Maßnahmen zur Erhöhung der Cybersicherheit ab. Der vorliegende Bericht sowie die Cybersicherheitsstrategie des Landes Nordrhein-Westfalen sind bereits erste konkrete Ergebnisse der Zusammenarbeit der Ressorts durch den IMA Cybersicherheit.

Das **Kompetenzzentrum für Cybersicherheit in der Wirtschaft „DIGITAL.SICHER.NRW“** des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie (MWIDE) wurde 2020 initiiert und dient zukünftig insbesondere der Unterstützung kleiner und mittlerer Unternehmen (KMU).

1.2 Themenfokus 2: Die Corona-Pandemie

Homeoffice, Homeschooling, Onlineshopping und Videokonferenzen prägten das Jahr 2020 in Nordrhein-Westfalen in digitaler Hinsicht. Die durch die **Corona-Pandemie** beschleunigte Digitalisierung und die damit verbundene Zunahme von zum Teil weitreichenden Cybersicherheitsvorfällen hat die Bedeutung des Themas Cybersicherheit auch für das Land Nordrhein-Westfalen erhöht. Die Pandemie führte zu einer Dezentralisierung der Arbeitsmittelpunkte vieler Menschen. Das Internet wurde zum Mittel der Wahl, um die alltägliche Lebensführung zu unterstützen. Laut Zahlen der OECD führte dies zu einem **Anstieg der Internetnutzung** von bis zu 60 Prozent in den Mitgliedsstaaten.

Die vielfältigen **Auswirkungen der Pandemie auf die Cybersicherheit** rückten erst nach und nach in den Blickpunkt. Die **intensivere Nutzung** des Internets steigerte das Risiko für Cyberangriffe sowohl auf Privatpersonen als auch auf Unternehmen. Beispielsweise legte der Onlinehandel in Deutschland im Vergleich zum Vorjahr um rund 15 Prozent zu und erwirtschaftete im Jahr 2020 über 80 Milliarden Euro. Gleichzeitig wurden Onlineshops auch ein immer beliebteres Ziel für Cyberangriffe. Sie werden insbe-

sondere durch Phishing-Angriffe und Social-Engineering-Angriffe bedroht, bei denen sich Cyberkriminelle als Kundinnen und Kunden ausgeben und Angestellte zum Download einer Datei mit Schadcode verleiten wollen, um auf diese Weise zum Beispiel Daten manipulieren oder abgreifen zu können.

Der rasche Umstieg auf digitale Lösungen war eine große Herausforderung sowohl für Unternehmen als auch für Arbeitnehmende. Ihr Cyberrisiko erhöhte sich, sobald die IT-Sicherheit zugunsten der ad hoc Funktionalität des Homeoffice zurückgestellt wurde, zudem ist der Internetzugang im Homeoffice meist weniger geschützt als am Arbeitsplatz. Wenn sich im Zuge dessen noch die Nutzung **privater Endgeräte im beruflichen Kontext** erhöht, beeinträchtigt dies zusätzlich das Cybersicherheitsrisiko von Unternehmen. Durch die erhöhte Nachfrage an mobilen Endgeräten, die in der Kürze der Zeit von Arbeitgeberseite oft nicht erfüllt werden konnte, verschärfte sich dieses Problem zunehmend.

Durch staatliche Konjunkturprogramme wie die Corona-Soforthilfen eröffneten sich zudem **neue Angriffsflächen für Cyberkriminelle**. Im Zuge sogenannter Social-Engineering-Angriffe gelang es Cyberkriminellen, vorübergehend Hilfsgelder abzugreifen, indem sie Internetseiten amtlicher Stellen täuschend echt nachbauten, so dass Antragsstellende auf den vermeintlich behördlichen Websiten ihre unternehmensbezogenen Daten preisgaben. Diese Daten konnten Cyberkriminelle sodann nutzen, um auf den echten Internetseiten Hilfsgelder zu beantragen und selbst davon zu profitieren.

Insgesamt veränderte die durch die Corona-Pandemie beschleunigte Digitalisierung die Alltags- und Arbeitswelt der Menschen in Nordrhein-Westfalen tiefgreifend, was zum einen zur Erhöhung der Frequenz und Art von Cyberangriffen führte, zum anderen jedoch auch die gesellschaftliche Wahrnehmung von Cybersicherheitsrisiken verstärkte.

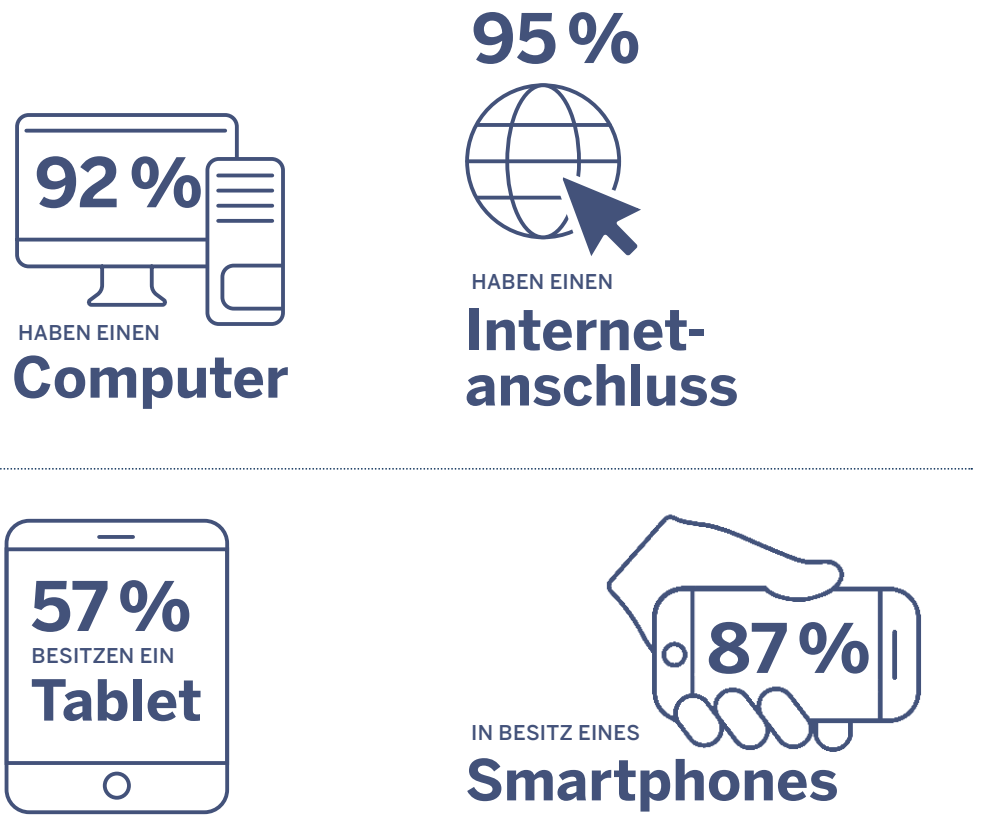
Gefährdungslage in Nordrhein-Westfalen 2020

2.0

Nordrhein-Westfalen ist mit knapp 18 Millionen Bürgerinnen und Bürgern das bevölkerungsreichste Bundesland in Deutschland. 95 Prozent der nordrhein-westfälischen privaten Haushalte verfügen über einen Internetanschluss und nutzen oft mehrere internetfähige Geräte wie PC's, Smartphones oder Tablets. Der Stellenwert der Cybersicherheit steigt daher auch für den privaten Bereich. Die Cyber-Bedrohungslage der Menschen in Nordrhein-Westfalen lässt sich aus den Entwicklungen auf Bundesebene ableiten: Rund ein Viertel der Bevölkerung der Bundesrepublik Deutschland ist bereits Opfer von Kriminalität im Internet geworden, 25 Prozent von ihnen sogar innerhalb der letzten zwölf Monate. Die aufgrund der Corona-Pandemie erhöhten Nutzungsfrequenzen schufen 2020 eine noch größere Angriffsfläche für Cyberkriminelle, ein Anstieg von Cyberangriffen ist bereits zu verzeichnen. Auch die politische Relevanz des Themas Cybersicherheit in Nordrhein-Westfalen wird durch vermehrte Anfragen aus dem politischen Raum, wie zum Beispiel Kleine Anfragen, deutlich.

ABBILDUNG 1

Ausstattungsgrad privater Haushalte mit ausgewählter Informations- und Kommunikationstechnik 2020



Laut dem Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit in Deutschland 2020 sind Bürgerinnen und Bürger beim **Onlineshopping dem größten Cyberrisiko** ausgesetzt. 44 Prozent der Befragten wurden im Zusammenhang mit Onlineshopping Opfer von Cyberattacken. Direkt danach folgte mit etwa 30 Prozent Betroffenen der Identitätsdiebstahl durch fremden Zugriff auf einen Online Account.

Dem **„Faktor Mensch“** gebührt besondere Aufmerksamkeit, da bis zu 50 Prozent der Cybersicherheitsvorfälle auf Unkenntnis oder Unachtsamkeit zurückzuführen sind. Cybersicherheit hängt stark vom Sicherheitsbewusstsein und den Fähigkeiten der Nutzenden, sich sicher im Cyberraum zu bewegen, ab. Aus diesem Grund sieht das BSI den gut geschulten Menschen als Abwehrschirm gegen Cyberangriffe. Auch immer mehr Unternehmen haben bereits erkannt, dass Cybersicherheit nicht allein durch technische Maßnahmen zu erreichen ist.

In Nordrhein-Westfalen waren im Jahr 2019 über 720.000 Unternehmen ansässig, die mehr als 1,6 Billionen Euro Umsatz erwirtschafteten. Davon sind ca. 700.000 kleine und mittlere Unternehmen (KMU), die 99,5 Prozent aller Unternehmen in Nordrhein-Westfalen ausmachen. Jedes fünfte Unternehmen in Deutschland hat seinen Sitz in Nordrhein-Westfalen. Eine sichere Internetnutzung ist für jede Branche zu einer Notwendigkeit geworden. Einkaufsprozesse und Kassen, die über das Internet verbunden sind, Kommunikation zu Auftraggebenden und Partnerunternehmen oder eine einfache Markterkundung sind in einer digitalisierten Umgebung zu einer Selbstverständlichkeit geworden. Für Unternehmen, die modern und konkurrenzfähig sein wollen, ist Cybersicherheit deshalb ein wichtiger Erfolgsfaktor.

Innerhalb der letzten zwei Jahre (2018/19) wurden 75 Prozent der deutschen Unternehmen Opfer von Cyberkriminellen. Die durch die Pandemie bedingte Verlegung der Arbeit ins Homeoffice machte viele Unternehmen in Nordrhein-Westfalen zusätzlich zum Ziel von Cyberangriffen. Je nach Schwere des Angriffs entstehen für die Unternehmen Kosten für Produktionsausfall, Überprüfung und Wiederherstellung der IT-Infrastruktur bis hin zu Verlusten durch den Abfluss von wichtigen Geschäftsdaten. Alleine in Nordrhein-Westfalen haben Cyberangriffe auf Unternehmen im Jahr 2020 18,1 Millionen Euro Schaden verursacht. Darin sind jedoch lediglich die angezeigten Schäden durch Computerbetrug und Softwarepiraterie abgebildet.

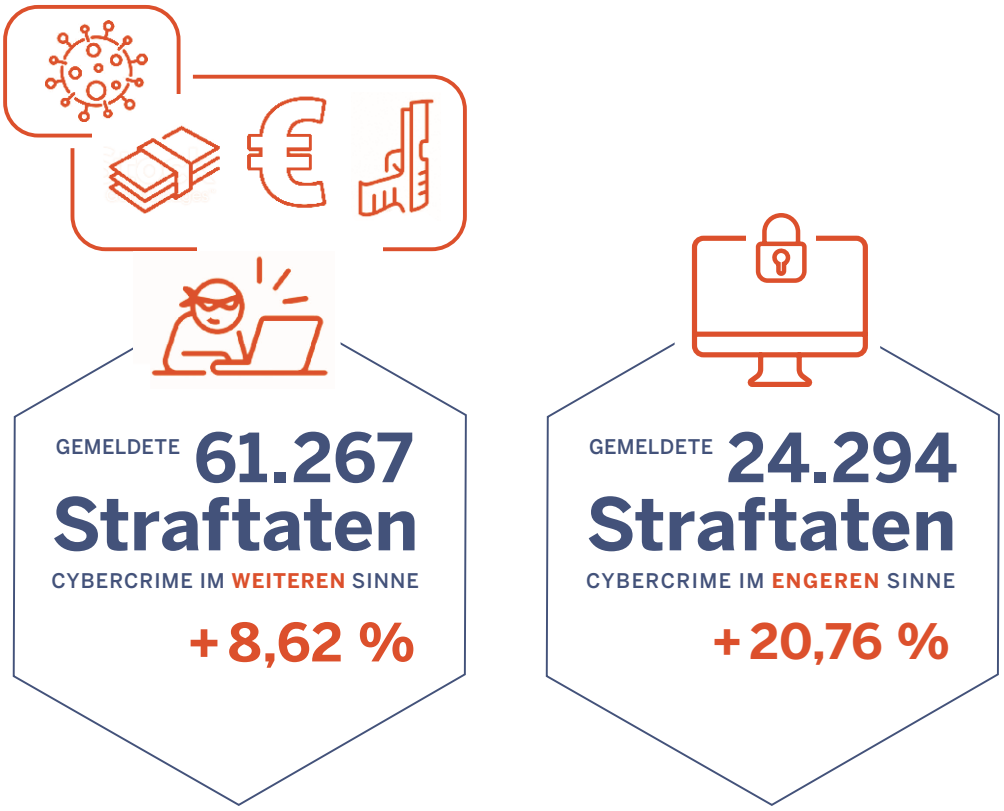


ABBILDUNG 2

Gemeldete Cybersicherheitsvorfälle in Nordrhein-Westfalen 2020

Im **Jahr 2020** sind in **Nordrhein-Westfalen 24.294 Straftaten** gemeldet worden, bei denen es sich um Fälle von **„Cybercrime im engeren Sinne“** handelt. Hiervon umfasst sind Straftaten, bei deren Begehung Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind. Dies entspricht einem **Anstieg von 20,76 Prozentpunkten** von 2019 auf 2020.

Unter **„Cybercrime im weiteren Sinne“** sind Straftaten zusammengefasst, die mit Hilfe von Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung durchgeführt werden. Dem LKA NRW wurden **im Jahr 2020 61.267 Fälle** gemeldet, was einem **Anstieg von 8,62 Prozentpunkten** entspricht. Hiervon wurden im gleichen Zeitraum 1000 Strafanzeigen zu Betrugsdelikten im Zusammenhang mit Corona Soforthilfen erfasst. In 20 Fällen kam es tatsächlich zu einer Auszahlung auf Konten der Kriminellen. Da die Datenlage lediglich das „Hellfeld“ der zur Anzeige gebrachten Straftaten abbildet, muss an dieser Stelle darauf hingewiesen werden, dass die Dunkelziffer der erfolgten Angriffe aller Wahrscheinlichkeit nach um ein Vielfaches höher liegt.

Weiter ist anzumerken, dass diese Angriffe ihren Ursprung oft nicht in Nordrhein-Westfalen hatten, sondern aus ganz Deutschland und überwiegend aus dem Ausland stammten. Sie richteten sich sowohl gegen Politik, Verwaltung, Privat-

personen als auch Unternehmen und kritische Infrastrukturen. Auch Angriffe fremder Nachrichtendienste zählten dazu. So konnte die Cyberabwehr des **Landesverfassungsschutzes** im Jahr 2020 in 110 Fällen Unternehmen und Institutionen in Nordrhein-Westfalen vor Angriffsversuchen warnen.

Dem BSI wurde in den Jahren 2019–2020 deutschlandweit **419 Cybersicherheitsvorfälle** von Betreibenden **kritischer Infrastrukturen** (KRITIS) gemeldet, auf die detaillierter im Kapitel 3.3 eingegangen wird. Insgesamt gestaltet es sich jedoch schwierig, eine aussagekräftige, quantifizierte Einschätzung der Gefährdungslage von KRITIS-Unternehmen in Nordrhein-Westfalen zu treffen, da der Landesregierung nur vereinzelt Daten aus dem Berichtszeitraum vorliegen und die Gefährdungslage aus bundesdeutschen Daten abgeleitet werden muss. Zukünftig wird das Land Nordrhein-Westfalen durch eigene Maßnahmen landesspezifische Daten erheben.

Die Datengrundlage für die Gefährdungslage von Bürgerinnen und Bürgern sowie Unternehmen in Nordrhein-Westfalen basiert zu einem hohen Anteil ebenfalls auf bundesdeutschen Daten. Hinsichtlich der Bürgerinnen und Bürger ist die Datengrundlage für die Gefährdungslage jedoch aufgrund der Bevölkerungsstruktur auch für Nordrhein-Westfalen repräsentativ. Die Verbesserung der Datenlage zählt zu den wichtigen strategischen Zielen der Landesregierung zur weiteren Erhöhung der Cybersicherheit im Land und ermöglicht es, künftig noch passgenauere Maßnahmen für die Erhöhung der Cybersicherheit im Land zur Verfügung zu stellen.

Zusammenfassend ist festzustellen, dass die Bedrohungen aus dem Cyberraum im Jahr 2020 für Bürgerinnen und Bürger sowie Unternehmen erheblich zugenommen haben. Zwei Ursachen trugen dazu bei: Das gesamte Land Nordrhein-Westfalen war in 2020 noch mehr auf das Internet angewiesen als jemals zuvor und die Cyberangriffe wurden häufiger und ausgefeilter. Die Corona-Pandemie wird im Berichtszeitraum als potentieller Katalysator beider Entwicklungen erkannt. Als Antwort auf diese Entwicklung hat die Landesregierung 2020 mehr Stellen zur Bekämpfung von Cybercrime geschaffen. Generell wird die Bedeutung der Cybersicherheit zunehmend von Verwaltung, Unternehmen sowie Bürgerinnen und Bürgern wegen der Verschiebung von Arbeit und Leben in den Cyberraum erkannt.

Im Jahr 2020 konnte ein starker Anstieg an Cybersicherheitsvorfällen beobachtet werden. Die Bedrohungslage verstärkte sich tendenziell durch die zunehmende Nutzung des Internets und einer Ausweitung der Cyberkriminalität. Die Landesregierung hat diese zunehmende Gefährdungslage im Blick und verstärkt die Maßnahmen zur Bekämpfung von Cybercrime.

Zielgruppenspezifische Informationen und Lösungsansätze

3.0

In diesem Kapitel wird die vorangestellte Gefährdungslage in Nordrhein-Westfalen speziell für die Zielgruppen **Bürgerinnen und Bürger, Unternehmen** und **kritische Infrastrukturen** (KRITIS) detailliert und aufgearbeitet. Jede Zielgruppe sieht sich verschiedenen Herausforderungen und Gefahren im Cyberraum ausgesetzt.

Um die vorangestellte Gefährdungslage zu entschärfen und Cyberangriffen vorzubeugen, werden im Folgenden Präventionsmaßnahmen und Hilfsangebote der Landesregierung zielgruppenspezifisch aufgezeigt. Daran anschließend werden im Anhang Ansprechstellen kompakt aufgeschlüsselt.

Cybersicherheit ist ein Querschnittsthema. So verfügt Nordrhein-Westfalen über eine Vielzahl staatlicher Institutionen und Akteure, die sich mit ihrem Informations- und Maßnahmenangebot an Bürgerinnen und Bürger oder (KRITIS-)Unternehmen und teilweise auch an die Landesverwaltung selbst richten. Diese Anlaufstellen und Institutionen werden im Folgenden selektiv vorgestellt (für eine ausführlichere Auflistung, siehe Anhang).

3.1 Bürgerinnen und Bürger

Bürgerinnen und Bürger begegnen Gefahren durch Kriminelle heute nicht mehr nur in der analogen Welt, sondern auch im Cyberraum. Vor diesen Gefahren gilt es sie zu schützen und ihr Risiko, Opfer einer Straftat zu werden, zu minimieren. Je nachdem in welcher Rolle oder mit welchem Anliegen Menschen das Internet nutzen, setzen sie sich häufig unbewusst unterschiedlichsten Cyberrisiken aus.

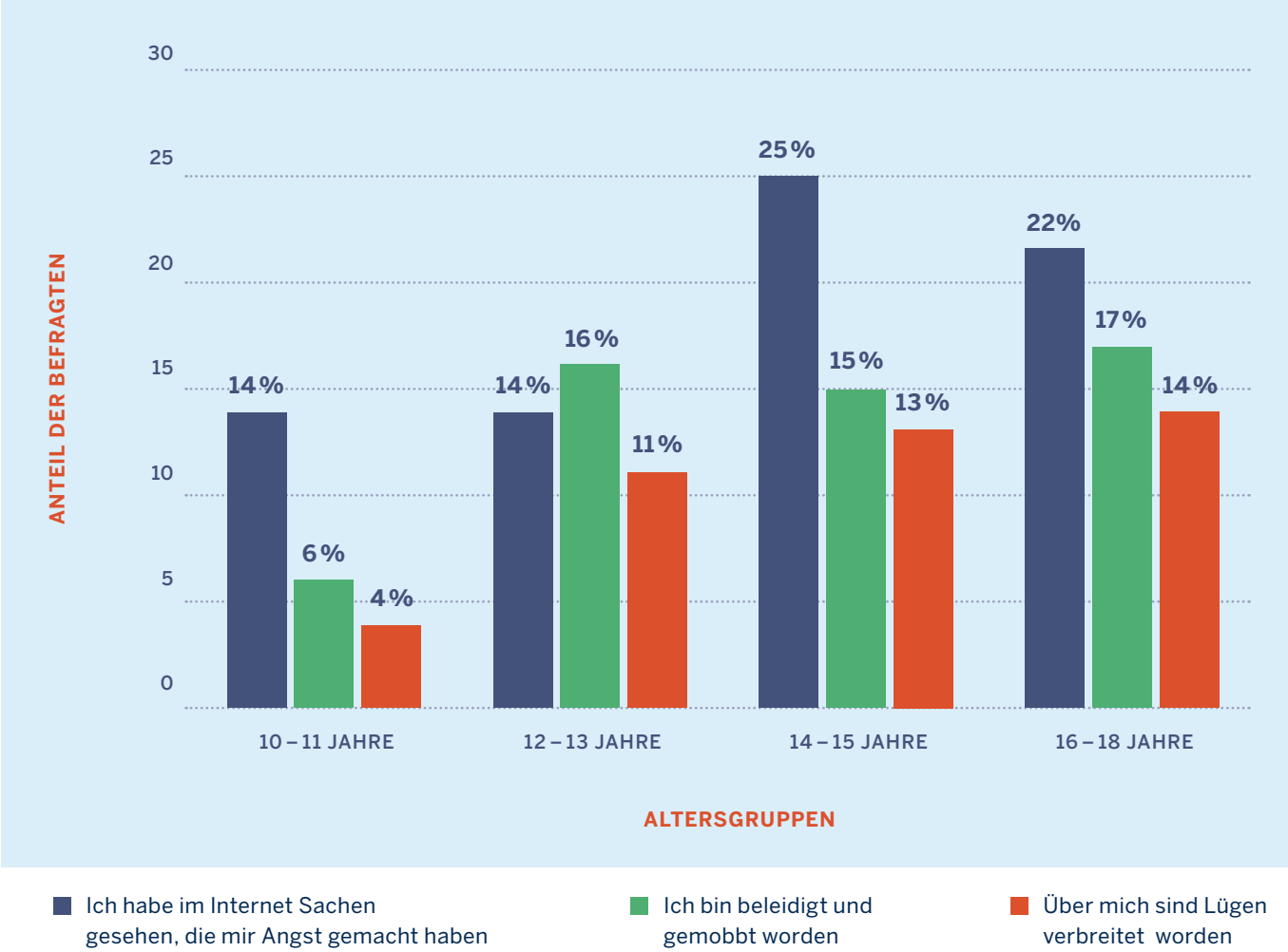
Zu den Risiken der Nutzung des Internets zählt auch die digitale Gewalt. Darunter werden verschiedene Formen der Belästigung, Beleidigung und Nötigung verstanden, die u.a. über Soziale Medien oder Messenger-Dienste verbreitet werden.

Cybergewalt kann sich besonders schwerwiegend auswirken, da sie durch die räumliche und zeitliche Entgrenzung des Internets allgegenwärtig ist. Zudem können sich diffamierende Inhalte (zum Beispiel Cybermobbing) schnell verbreiten und nur schwer wieder gelöscht werden. Mädchen und Frauen sind in besonderem Maße von digitaler Gewalt betroffen. Äußern sie sich online, riskieren sie sexistische oder beleidigende Reaktionen, pornografische Belästigungen bis hin zu Morddrohungen.

Kinder und Jugendliche erfahren im Cyberraum noch weitere Bedrohungen beispielsweise durch frei verfügbare, nicht jugendfreie und jugendgefährdende Inhalte.

ABBILDUNG 3

Negative Erfahrungen von Kindern und Jugendlichen im Internet 2011



Bedrohungen aus dem Cyberraum betreffen somit nicht nur die technische Sicherheit, sondern umfassen auch Gefährdungen der psychischen Gesundheit der Betroffenen.

Die Landesregierung bietet unterschiedliche Hilfestellungen und Präventionsangebote an. Betroffene von digitaler Gewalt finden Unterstützung bei den örtlichen Schutz- und Beratungsangeboten z. B. für von Gewalt betroffene Frauen oder auf dem Opferschutzportal (www.opferschutzportal.nrw) der Landesregierung. Hilfesuchende werden auf den Seiten des Portals zielgerichtet zu Hilfs- und Unterstützungsangeboten bei digitaler Gewalt und Cybercrime geführt. Präventionsprogramme wie das Projekt Medienscouts NRW unterstützen Schulen, Probleme wie Cybermobbing, Hassrede, Cybergrooming aktiv anzugehen. Projekte wie „Klicksafe“ und „Verfolgen statt Löschen“ richten sich gegen Hassrede im Internet.

CASE STUDY **Medienscouts**

Die Möglichkeiten, Schülerinnen und Schüler als Medienscouts in den Alltag der Schulen NRWs einzubeziehen, sind vielfältig. Als Beispiel dient eine Dortmunder Realschule, in dem Medienscouts neben regelmäßig stattfindenden Sprechstunden auch bei Veranstaltungen und Aktionstagen mit einem Informationsstand eingebunden sind, auf denen sie ihren Informationsflyer „Im Netz unterwegs“ präsentieren. Sie veranstalten in den fünften Klassen der Schule eine Unterrichtsstunde zu dem Thema „Cybermobbing, Klassenchats und WhatsApp“, zusätzlich sind die Medienscouts in die Anti-Mobbing-AG der Schule integriert. Hauptanliegen der AG ist es, Schülerinnen und Schüler über das Thema „Mobbing“ bzw. „Cyber-Mobbing“ aufzuklären. Damit sind die Medienscouts ein wichtiger Baustein, präventiv Probleme wie Cybermobbing, Sexting, Datenmissbrauch und exzessive Mediennutzung im schulischen Alltag aufzugreifen und zu bearbeiten. Mit Hilfe des Projektes lernen und vermitteln Schülerinnen und Schüler durch den Ansatz der „Peer-Education“ die Kompetenzen, die Voraussetzungen für einen sicheren, fairen und selbstbestimmten Umgang mit digitalen Medien sind.

ABBILDUNG 4

Wie in der Gefährdungslage beschrieben, verbrachten Bürgerinnen und Bürger 2020 mehr Zeit im Cyberraum als in den Vorjahren. Ob beim Arbeiten im Homeoffice oder beim Onlineshopping: Bürgerinnen und Bürger sind den wachsenden Bedrohungen im Cyberraum inzwischen deutlich häufiger ausgesetzt. Cyberkriminelle fanden 2020 schnell einen Weg, die vermehrte Nutzung von digitalen Angeboten für ihren Zweck auszunutzen. In Nordrhein-Westfalen ist der Betrug mit Corona-Soforthilfen ein prominentes Beispiel, bei dem sensible Daten von Bürgerinnen und Bürgern über gefälschte Internetseiten abgegriffen worden sind. Ziel dieser Phishing-E-Mails und Phishing-Webseiten ist das unberechtigte Erlangen von personenbezogenen Daten, wie z. B. von Bankdaten. Pro Tag wurden allein von Google ca. 240 Millionen Spam-E-Mails und rund 2,5 Millionen Phishing E-Mails mit Corona Narrativen abgewehrt.

ABBILDUNG 5

Bedrohungslage in Deutschland 2020 lt. BKA-Lagebild „Cybercrime“

Doch Spam und Phishing E-Mails sind nicht die einzigen Gefahren für Bürgerinnen und Bürger. Auch 2020 war „123456“ das meist benutzte Passwort der Welt. Solche Schwachstellen können die Cybersicherheit von Bürgerinnen und Bürgern massiv beeinträchtigen.

Die besondere Aufmerksamkeit der Landesregierung liegt daher auch auf dem „Faktor Mensch“ als Einfallstor für Cyberkriminelle. Durch die **Sensibilisierung der Bürgerinnen und Bürger** für Themen der Cybersicherheit kann das Risiko von Cyberattacken gemindert werden.

Für ein sicheres Passwort gilt:

1. Es ist gut merkbar
2. Ein längeres Passwort ist sicherer als ein kurzes
3. Alle möglichen Kategorien werden verwendet (z. B. Zahlen und Sonderzeichen)
4. Keine Namen /Geburtsdaten werden verwendet
5. Das Passwort sollte nicht im Wörterbuch stehen

ABBILDUNG 6

Häufige Merkmale von Spam und Phishing E-Mails:

1. Grammatik- und Rechtschreibfehler
2. Fehlende persönliche Anrede sowie persönliche Abschiedsformel
3. Vorgetäuschter, dringender Handlungsbdarf
4. Nachrichten mit z. B. Gewinnversprechen, die zu schön sind, um wahr zu sein
5. Unprofessionelle Aufmachung
6. Aus dem Kontext gegriffene Nachrichten
7. Aufforderung zur Eingabe von sensiblen oder persönlichen Daten
8. Aufforderung einen Dateianhang, eine Webseite oder ein Formular zu öffnen

ABBILDUNG 7

Zur Erhöhung der Cybersicherheit der Bürgerinnen und Bürger Nordrhein-Westfalens greifen unterschiedliche Maßnahmen ineinander.

Die **Website des LKA NRW** (https://lka.polizei.nrw/) bietet Bürgerinnen und Bürgern umfassende Informationen rund um das Thema Cybercrime. Die Präventions- und Öffentlichkeitskampagne **„Mach dein Passwort stark“** (https://www.mach-dein-passwort-stark.de/) des LKA NRW gibt Tipps zur Wahl eines sicheren Passworts.

Das Onlineportal der **Koordinierungsstelle Cybersicherheit NRW** (https://www.cybersicherheit.nrw) dient der Übersicht und Information der Bürgerinnen und Bürger, Unternehmen und KRITIS-Einrichtungen Nordrhein-Westfalens zu Cybersicherheitsthemen.

Der **#DigitalCheckNRW** ermöglicht es Bürgerinnen und Bürgern mithilfe eines Selbsttests herauszufinden, wie stark ihre Medienkompetenz ist und schlägt passgenau Fortbildungsangebote vor. Weiterbildungsanbietenden zeigt er zudem, wo noch Bildungsangebote fehlen und entwickelt werden müssen. Dieses Angebot ist unter https://www.digitalcheck.nrw ohne Registrierung und kostenfrei abrufbar.

Die Landesanstalt für Medien NRW bietet unter der Schirmherrschaft der Deutschen UNESCO-Kommission die neue **Beratungsplattform ZEBRA** (https://www.fragzebra.de/) an. Hier bekommen Bürgerinnen und Bürger individuelle Antworten auf ihre Fragen zum Thema digitale Medien und der Sicherheit im Netz. Außerdem wird dort benutzerorientiert Hilfe bei Sorgen, Unsicherheiten und Notlagen im Umgang mit digitalen Medien angeboten.

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**

Ergänzend dazu stellt das Land Nordrhein-Westfalen als erstes Bundesland den Schulträgern Mittel für die Ausstattung der Lehrkräfte mit dienstlichen Endgeräten in Höhe von 103 Millionen Euro bereit.

Darüber hinaus unterstützt das Angebot **Eltern und Medien** der Landesanstalt für Medien NRW (https://www.elternundmedien.de/) Kitas, Schulen und andere Einrichtungen aus Nordrhein-Westfalen bei der Planung, Organisation und Durchführung von Vor-Ort- oder Online-Elternabenden zur Medienerziehung und stellt hierfür kostenfrei Referierende zur Verfügung. Seit Projektstart wurden bereits über 240.000 Eltern aus ganz Nordrhein-Westfalen erreicht.

Der 25. Deutsche Präventionstag des Landes Nordrhein-Westfalen und der Stadt Köln, der über Risiken und Kriminalprävention im Cyberraum für diverse Zielgruppen aufklärt, wurde ebenso in 2020 durchgeführt, wie auch der internationale Safer Internet Day, der lokal durch viele Behörden in Nordrhein-Westfalen umgesetzt wurde.

Die Cybercops sind eine Bildungsinitiative von Jugendlichen für Jugendliche aus dem Kreis Minden-Lübbecke. 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.

Die Medienscouts (https://www.medienscouts-nrw.de/) stellen ein weiteres Präventionsprojekt für Schülerinnen und Schüler dar. Hierbei erarbeiten Schülerinnen und Schüler in gemeinsamen Workshops mit ihren Lehrkräften Grundlagen der sicheren Internetnutzung, um die Qualifikation „Medienscout“ zu erlangen. Soziale Netzwerke, Smartphones und Computerspiele sind ebenfalls Teil des Curriculums. Auch wird verstärkt auf das Themenfeld Cybermobbing eingegangen. Anschließend können die Schülerinnen und Schüler ihre Kompetenzen an Gleichaltrige in ihren Schulen weitergeben.

Generelle Präventionsmaßnahmen

- Hegen eines gesunden Misstrauens gegenüber Links und Anlagen in E-Mails unbekannter Absendenden,
- Verwendung eines starken Passworts oder Anmeldung per Zwei-Faktor-Authentifizierung,
- Softwarenutzung nur von seriösen Anbietenden oder App-Stores; Betriebssysteme, Antivirenprogramme und weitere Softwareprodukte sollten immer auf dem neuesten Stand sein,
- Nutzung von E-Mail-Anbietenden mit gutem Spamfilter und Kontrolle der E-Mail-Adressen von Absendenen.

ABBILDUNG 8

3.2 Unternehmen

Cybersicherheit ist eine wichtige Voraussetzung für eine **erfolgreiche Digitalisierung**, welche wiederum den Grundstein für ein erfolgreiches und wirtschaftliches Handeln im 21. Jahrhundert legt. In Nordrhein-Westfalen gibt es über 700.000 Unternehmen. Für viele dieser Unternehmen ist Cybersicherheit ein wichtiger Baustein für den wirtschaftlichen Erfolg. Deutlich wird dies besonders dadurch, dass laut des Branchenverbands Bitkom e. V. 75 Prozent aller Unternehmen in Deutschland in den Jahren 2018/19 von Cyberangriffen betroffen waren. Dabei entstand ein **Gesamtschaden von 205,7 Milliarden Euro**.

Allein im Jahr 2019 wurden **drei von vier Unternehmen in Deutschland Opfer von Cybercrime**. Jedes fünfte Unternehmen in Deutschland hat seinen Sitz in Nordrhein-Westfalen, die Bedrohung durch Cyberangriffe betrifft somit auch in besonderem Maße die Unternehmen und die Wirtschaft des Landes. Die Landesregierung sieht daher den Schutz der Unternehmen vor Cyberangriffen als wichtige Aufgabe an.

Kleine und mittlere Unternehmen (KMU) stellen mit 99,5 Prozent der Unternehmen des Landes das **Rückgrat der nordrhein-westfälischen Wirtschaft dar**. Sie beschäftigten 2017 rund 3,69 Millionen sozialversicherungspflichtig Arbeitnehmende und damit 53,5 Prozent aller sozialversicherungspflichtig Arbeitnehmenden in Nordrhein-Westfalen.

Als Industrieland sind in Nordrhein-Westfalen viele Unternehmen ansässig, die genehmigungsbedürftige Anlagen nach dem Bundesimmissionschutzgesetz betreiben. Von den insgesamt 20.316 Anlagen fallen 3.410 Anlagen unter die Industrieemissionsrichtlinie, von 611 Betriebsbereichen im Sinne der Störfallverordnung (12.BImSchV) gehören 301 Betriebsbereiche der oberen Klasse an. Die Zahlen verdeutlichen, dass Cyberattacken auf digitale Steuerungsstrukturen dieser Anlagen erhebliche Auswirkungen auf den Produktionsprozess, auf die Menschen und die Umwelt haben können.

Im Lagebild zum Wirtschaftsschutz wurde für das Jahr 2019 ermittelt, dass KMU in Nordrhein-Westfalen ihre **Unternehmenssicherheit im Bereich Cybersicherheit** branchenübergreifend als **nicht ausreichend** einschätzten. Diese ohnehin geringe Selbsteinschätzung der Unternehmenssicherheit überschätzt jedoch noch das tatsächlich vorhandene, gemessene Schutzniveau – insbesondere fehlt es an Krisen- und Notfallkonzepten. Hinzu kommt, dass bei 42 Prozent aller

Unternehmen in Nordrhein-Westfalen ein Sicherheitskonzept zur Dokumentation von Aufgabenverteilungen und -bereichen im Falle eines Cyberangriffs „eher nicht“ oder „gar nicht“ existiert. Für den Fall eines Cyberangriffs ist der Großteil der Unternehmen somit nicht ausreichend vorbereitet.

Die Dynamik der Digitalisierung in den Unternehmen kann eine der Ursachen sein, dass die notwendigen Überlegungen für eine ganzheitliche Cybersicherheitsstruktur mit dieser Entwicklung nicht Schritt halten können. Zum Beispiel werden Anlagen, die bisher unabhängig von einander betrieben wurden, im Zuge der Digitalisierung miteinander vernetzt, ohne dass ein angepasstes Sicherheitskonzept erstellt wird. Dies kann zu Schwachstellen führen, die ein hohes Risiko für die Betriebe darstellen.

Obwohl 71 Prozent der KMU ihren Betrieb selbst als zu klein einstufen, um in den Fokus von Cyberkriminellen zu geraten und verhältnismäßig wenig Wert auf Schulungs- und Sensibilisierungsprogramme für ihre Mitarbeitenden legen, sind gerade auch **kleine und mittlere Unternehmen Angriffsziel von Cyberkriminellen**. Denn sie sind meist höchst spezialisiert, besitzen enormes Fachwissen und arbeiten häufig eng mit großen Unternehmen zusammen.

Digitale Angriffe auf Unternehmen erfolgten insbesondere in Form von Passwortdiebstahl, unbemerktes Einschleusen von Schadsoftware oder Phishing-Attacken. Laut einer BSI-Befragung würde jeder sechste Mitarbeitende auf eine gefälschte E-Mail der Chefetage antworten und sensible Unternehmensinformationen preisgeben. Phishing-E-Mails wie diese bilden eine der größten Gefahren für Unternehmen. Im Jahr 2020 waren Onlineshops weltweit das am häufigsten getroffene Ziel von Phishing-Angriffen, was sowohl für Verbraucherinnen und Verbraucher, als auch für Betreibende von Onlineshops zu einem erheblichen finanziellen Schaden führen kann.

Zur Erhöhung der Cybersicherheit für Unternehmen in Nordrhein-Westfalen wird von der Landesregierung auf Be-

Wodurch kann ich die Gefahr am Arbeitsplatz abmindern?

- **Wählen Sie ein sicheres Passwort oder die Zwei-Faktor-Authentifizierung**
- **Öffnen Sie Links und Anhänge nur von vertrauenswürdigen Absendenden**
- **Lassen Sie Ihre Hardware an öffentlichen Orten nicht unbeaufsichtigt**
- **Downloaden Sie neue Software nur von vertrauenswürdigen Anbietenden**

ABBILDUNG 9

ratungs- und Präventionsmaßnahmen gesetzt. Diese betreffen zum einen Informationsveranstaltungen und kompetenzbildende Maßnahmen für Mitarbeitende, zum anderen die Unternehmenskultur und IT-Sicherheitsausstattung.

Dem **„Faktor Mensch“** gilt eine besondere Aufmerksamkeit. Aus aktuellen Studien zu Cyberangriffen gegen Unternehmen geht hervor, dass bis zu 50 Prozent der Cybersicherheitsvorfälle auf die Unkenntnis oder die Unachtsamkeit von Mitarbeitenden zurückzuführen sind.

Daher ist es für Unternehmen besonders bedeutend, dass **alle Mitarbeitenden** fortlaufend für die **Risiken** von Cybervorfällen **sensibilisiert und geschult werden**. Nur durch ausreichende Kompetenz im Umgang mit dem Internet können Vorfälle vermieden oder leichter abgewehrt werden.

Neben den Präventions- und Sensibilisierungsmaßnahmen für Mitarbeitende ist es für Unternehmen besonders wichtig, eine ausreichende **IT-Ausstattung** zur Abwehr, Vermeidung und Minimierung von Gefahren durch Cyberbedrohungen einzurichten. In Deutschland, vergleichbare Zahlen werden für Nordrhein-Westfalen angenommen, verfügen zwar fast 100 Prozent der Unternehmen über einen **technischen Basisschutz**, deutlich weniger sind dagegen jedoch mit erweiterten Sicherheitsmaßnamen wie abhörsicherer Sprachkommunikation (56 Prozent), Datenverschlüsselung auf Datenträgern (52 Prozent), Verschlüsselung des E-Mail-Verkehrs (39 Prozent) oder der Absicherung gegen den Datenabfluss von innen (36 Prozent) ausgestattet. Insgesamt umfasst die Prävention von Cyberangriffen eine Bandbreite an Handlungsfeldern, die sowohl Mitarbeitende als auch die Sicherheitsinfrastruktur betreffen.

In Nordrhein-Westfalen gibt es bereits eine **Vielzahl von Angeboten**, um Unternehmen über Cybersicherheit zu informieren und sie in ihrem Schutz zu unterstützen. So bieten z. B. das **Cybercrime Kompetenzzentrum des LKA NRW** (https://lka.polizei.nrw/artikel/abteilung-4), die bei der Justiz eingerichtete Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen **– ZAC NRW –** (https://www.justiz.nrw.de/JM/schwerpunkte/zac/index.php) und der **Verfassungsschutz** (https://www.im.nrw/themen/verfassungsschutz) Beratung und Präventionsmaßnahmen zur Verbesserung der Cybersicherheit an. Diese Angebote werden rege wahrgenommen und weiter ausgebaut.

Die **Initiative Wirtschaftsschutz** (https://www.wirtschaftsschutz.info/DE/Home/home_node.html) ist ein Zusammenschluss von vier Sicherheitsbehörden: Bundesamt für Verfassungsschutz, Bundeskriminalamt, Bundesnachrichtendienst und dem Bundesamt für Informationssicherheit. Die Initiative bietet ausführliche Informationen zum Thema Cybercrime genauso wie zur Wirtschafts- und Wissenschaftsspionage oder zum Thema IT-Sicherheit. In Nordrhein-Westfalen können die Informationen über www.wirtschaftsschutz.info kostenfrei abgerufen werden. Darüber hinaus war die Initiative Wirtschaftsschutz einer der Impulsgeber für die Entstehung der Sicherheitspartnerschaft.

Die **Sicherheitspartnerschaft Nordrhein-Westfalen gegen Wirtschaftsspionage und Wirtschaftskriminalität (Sicherheitspartnerschaft NRW)** (https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/sicherheitspartnerschaft-nord-

rhein) dient der Sensibilisierung und Fortbildung von Wirtschaftsakteuren. Die Sicherheitspartnerschaft NRW setzt sich aus dem Ministerium des Innern, dem Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, der Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e. V., der Industrie- und Handelskammer in Nordrhein-Westfalen e. V. und dem Verband der Wirtschaftsförderungs- und Entwicklungsgesellschaften in NRW e. V. zusammen.

Die Cyberabwehr und der **Wirtschaftsschutz** (https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/wirtschaftsschutz) gehören zum Aufgabenspektrum der Spionageabwehr des Verfassungsschutzes des Landes Nordrhein-Westfalen. Die beiden Bereiche bieten insbesondere Unternehmen und Forschungseinrichtungen Präventions- und Zusammenarbeit zu Bedrohungen ausgehend von fremden Nachrichtendiensten an. Dies umfasst die Informationsvermittlung im Fall von Cyberattacken durch ausländische Nachrichtendienste sowie kostenfreie Sensibilisierungsprogramme zum Schutz vor Cyberattacken.

Die **Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)** (https://www.justiz.nrw.de/JM/schwerpunkte/zac/index.php), angesiedelt bei der Staatsanwaltschaft Köln, ist zentrale Ansprechstelle für Cybercrime im Rahmen der Strafverfolgung und steht Unternehmen präventiv und reaktiv bei Cyberangriffen zur Verfügung. Sie führt die Ermittlungen in Fällen der herausgehobenen Cybercrime, zudem wirkt sie bei regionalen und überregionalen Aus- und Fortbildungsmaßnahmen im Bereich der Cybercrime mit. Im April 2016 eingerichtet, ist sie die bundesweit größte Cybercrime-Einheit der Justiz. Ihr Angebot richtet sich neben Unternehmen auch an Staatsanwaltschaften und Polizeibehörden in Nordrhein-Westfalen.

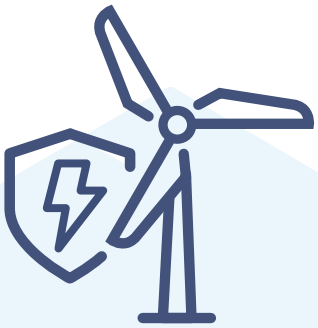
Das Cybercrime-Kompetenzzentrum LKA NRW (CCCC) (https://lka.polizei.nrw/artikel/abteilung-4) wurde 2011 eingerichtet, um den wachsenden Herausforderungen der Cybercrime zu begegnen. Das Kompetenzzentrum zielt auf die Steigerung des Gefahrenbewusstseins und der Vermittlung wirkungsvoller Maßnahmen zur Minimierung von Cybercrime ab. So werden unter anderem einheitliche Präventionsmaßnahmen für die Kreispolizeibehörden angeboten. Im Sinne eines ganzheitlichen Ansatzes kooperiert das CCCC mit dem bitkom Branchenverband der IT, dem Bundesverband der IT-Anwender-Unternehmen VOICE, dem eco-Verband der Internetwirtschaft, networker NRW und ist zudem Teil der Sicherheitspartnerschaft NRW. Neben dem LKA NRW bieten auch die **Polizeibehörden in Nordrhein-Westfalen** den hier angesiedelten Unternehmen zum Schutz vor Cyberangriffen kostenfreie Informationen in Form von Vorträgen oder Veranstaltungen und bieten telefonische Beratung, wie beispielsweise die Polizei Münster.

Die **Koordinierungsstelle Cybersicherheit NRW** (https://www.cybersicherheit.nrw/de/unternehmen) hat im Jahr 2020 den Auftrag erhalten, ein Onlineportal zu entwickeln, um unter anderem auch Unternehmen eine Bandbreite von Informationsangeboten und Handlungsempfehlungen zur Erhöhung der Unternehmenssicherheit bereitzustellen.

Nach aktuellen Umfragen gaben 84 Prozent aller deutschen Unternehmen an, von staatlichen Stellen nicht ausreichend über das Gefahrenpotenzial von Cyberangriffen und angemessenen Präventionsmaßnahmen aufgeklärt worden zu

sein. Es liegt grundsätzlich im **Eigeninteresse und in der Eigenverantwortung** eines jeden Unternehmens, sich bestmöglich vor Cyberangriffen zu schützen. Das Land unterstützt sie in diesem Bemühen durch die zuvor genannten Angebote. Damit diese Angebote auch bei den Unternehmen ankommen, ist es wichtig, die Reichweite der Angebote zu erhöhen, vorhandene Kontaktpunkte zu bündeln und Notfall-Kontaktdaten besser zu kommunizieren. Diese Handlungsbedarfe werden in der Cybersicherheitsstrategie des Landes Nordrhein-Westfalen aufgegriffen und mit passgenauen Maßnahmen flankiert.

Unternehmen in Nordrhein-Westfalen können sich außerdem an das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/unternehmen-und-organisationen_node.html) wenden. Es bietet auf seiner Webseite eine Vielzahl von themenspezifischen Informationsangeboten aus dem Bereich der Cybersicherheit. Das Angebot beinhaltet unter anderem Sicherheitsempfehlungen speziell für Unternehmen als Angriffsziel. Zudem bietet das BSI für konkret von Informationssicherheitsvorfällen betroffenen Unternehmen unterschiedliche Checklisten (Organisatorisches; Technisches) und Erste-Hilfe-Pakete an, damit Unternehmen einem Vorfall vorbeugen, ggf. melden und bewältigen, können.



3.3 Kritische Infrastrukturen (KRITIS)

Kritische Infrastrukturen (KRITIS) werden als Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen definiert, deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, Störungen der öffentlichen Sicherheit oder andere dramatische Folgen hätte. Durch ihre Abhängigkeit von der Informationstechnologie sind sie ins Visier Cyberkrimineller geraten. In Anbetracht ihrer großen Angriffsfläche und des hohen Schadpotentials, haben sie erhöhten Schutzbedarf und bilden eine wichtige Zielgruppe dieses Berichts. Im Rahmen der Gefahrenvorsorge ist Cybersicherheit auch ein Teilbereich des Schutzes von KRITIS.

2020 wurden deutschlandweit insgesamt 419 Cybersicherheitsvorfälle bei KRITIS-Unternehmen an das BSI gemeldet. Diese verteilten sich deutschlandweit auf unterschiedliche KRITIS Sektoren. Die am stärksten betroffenen waren:

- Der Gesundheitssektor mit 134 Fällen,
- Der IT und TK Sektor mit 75 Fällen,
- Im Energiesektor wurden im Berichtszeitraum 73 Fälle gemeldet.

Für Nordrhein-Westfalen ist der Gesundheitssektor von großer wirtschaftlicher Bedeutung. Daher ist davon auszugehen, dass diese Einrichtungen im Land ein relevantes Angriffsziel für Cyberkriminelle sind. Die Landesregierung fördert mit dem Projekt **MITSicherheit.NRW** (https://mits.nrw/) die Datensicherheit in Krankhäusern auch zum Schutz besonders sensibler Gesundheitsdaten. In dem Projekt werden innovative Sicherheitsinstrumente entwickelt, die erstmalig medizinische Standardprotokolle in ihre Schwachstellenanlyse einbeziehen und so einen wichtigen Grundstein für eine erfolgreiche Digitalisierung der Gesundheitswirtschaft in Nordrhein-Westfalen legen.

Nordrhein-Westfalen ist Deutschlands größtes Energieland. Rund 30 Prozent des bundesweit genutzten Stroms wird hier produziert. Der Blick auf die bundesdeutschen Gesamtzahlen zu Angriffen auf die einzelnen Sektoren lässt den Schluss zu, dass auch nordrhein-westfälische Unternehmen des Energiesektors in nicht unerheblichem Maße Angriffsziel aus dem Cyberraum sind.

Die Gefährdungslage für KRITIS ist besonders durch die vier folgenden **Bedrohungsarten** geprägt:

- **Spionageangriffe** auf den KRITIS-Sektor Staat und Verwaltung nehmen seit 2005 zu. Ziel der Täterinnen und Täter ist es, meist Behörden und Politikerinnen und Politiker auszuspionieren oder zu sabotieren.
- **Cyberterrorismus**, der sich gegen jegliche KRITIS-Sektoren richten kann, zielt darauf ab, der Bevölkerung sowie Wirtschaft und Politik den größtmöglichen Schaden zuzufügen.
- **Schadsoftware** ist mittlerweile so ausgeklügelt, dass sie nicht sofort von aktuellen Virenschutzprogrammen erkannt wird. Durch sie können betriebsrelevante Anwendungen erheblich gestört werden.
- **Ransomware-Angriffe** auf Versorgungsdienstleistende können zum Beispiel Krankenhäuser stilllegen und die lebenswichtige Versorgung von Patientinnen und Patienten beeinträchtigen.

CASE STUDY

Ransomware-Angriff auf die IT-Systeme des Universitätsklinikums Düsseldorfs

Am 10.09.2020 wurde das IT-System der Universitätsklinik Düsseldorf durch einen Ransomware-Angriff folgenschwer gestört. Der Cyberangriff erfolgte über einen Citrix-VPN-Server, über den typischerweise externe Mitarbeitende Zugriff auf das Universitätsnetz bekommen. Die Angreifenden nutzten eine Sicherheitslücke in der Citrix-Software aus, welche bereits seit dem Jahreswechsel 2019/2020 durch das BSI bekannt gemacht wurde. Es wird davon ausgegangen, dass sich die Angreifenden bereits einen dauerhaften Zugang zum System verschafft hatten, bevor die Installation des Citrix-Sicherheitsupdates zur Behebung der Schwachstelle im Januar 2020 erfolgte.

Durch die Verschlüsselung zentraler Server, die für den Klinikbetrieb elementar waren, musste sich das Klinikum bis zum Wiederanlauf der wichtigsten Systeme vom 10.09.2020 bis zum 23.09.2020 für 13 Tage von der Notfallversorgung im Großraum Düsseldorf abmelden.

Die Erpressung galt laut Angaben der Ermittelnden eigentlich der Heinrich-Heine-Universität Düsseldorf. An diese hatten die Cyberkriminellen auch ein digitales Erpresserschreiben adressiert. Nachdem die Polizei Kontakt zu den Tätern aufgenommen hatte und diese darüber in Kenntnis gesetzt wurden, dass durch den Hackerangriff ein Krankenhaus mit einer erheblichen Gefährdung der Patientinnen und Patienten betroffen sei, nahmen die Täterinnen oder Täter von dem Erpressungsversuch Abstand und händigten einen digitalen Schlüssel zur Wiederherstellung der betroffenen Daten aus.

ABBILDUNG 10

Um den Gefährdungen bundesweit besser begegnen zu können, erfolgt bereits **eine Vernetzung und Kommunikation** zwischen den KRITIS-Betreibenden und dem BSI zu Sicherheitsvorfällen und Schwachstellen. Zum einen müssen KRITIS-Betreibende dem BSI unverzüglich einen Vorfall mit Einfluss auf die Anlagensicherheit melden. Zum anderen warnt das BSI auf Grundlage dieser Informationen die weiteren KRITIS-Unternehmen vor aktuellen Cybergefahren und stellt dazu Informationen auf seiner Webseite zur Verfügung. Zusätzlich hält das BSI KRITIS-Unternehmen dazu an, regelmäßig nach Lücken in ihrer IT-Sicherheit zu suchen.

Das Land Nordrhein-Westfalen nutzt die Chancen der gesteigerten Digitalisierung unter Einbeziehung von Cybersicherheit für KRITIS-Unternehmen. Ein Beispiel dafür ist das **Kompetenzzentrumm Digitale Wasserwirtschaft** (https://www.kompetenzzentrum-digitale-wasserwirtschaft.de/). Das Zentrum wurde gemeinsam mit mehreren Wasserwirtschaftsunternehmen geschaffen, um die Kompetenzen zur agilen Gestaltung der Digitalisierung der Wasserwirtschaft, insbesondere in Nordrhein-Westfalen, weiterzuentwickeln und dabei Aspekte der Cybersicherheit von vornherein mitzudenken.

Unternehmen, die dem KRITIS-Sektor zuzuordnen sind, jedoch nicht die Schwellenwerte der KRITIS-Verordnung erreichen und damit keiner Meldepflicht unterliegen, können sich dennoch auf freiwilliger Basis beim BSI registrieren lassen. Damit profitieren sie von regelmäßigen Informationen des BSI über Sicherheitsvorfälle sowie bekanntgewordene Schwachstellen und können auch ihrerseits Sicherheitsvorfälle dem BSI melden.

Die Koordinierungsstelle Cybersicherheit NRW fördert in ihrer Doppelfunktion als **Zentrale Kontaktstelle des Landes (ZKL)** (https://www.cybersicherheit.nrw/de/kritische-infrastrukturen) den intensiven Austausch zwischen BSI, KRITIS-Unternehmen, Fach- und Rechtsaufsichten der Ressorts sowie Strafverfolgungsbehörden (z.B. Polizei). Insbesondere der KRITIS-Sektorübergreifende Austausch zwischen den verschiedenen Ressorts der Landesverwaltung ermöglicht eine branchenübergreifende Betrachtung von Gefährdungen für alle KRITIS-Unternehmen. Ein besonderes Augenmerk gilt den KRITIS-Unternehmen, die die Schwellenwerte der KRITIS-Verordnung nicht erreichen, aber für Nordrhein-Westfalen als lokale Versorgungs- oder Zuliefererunternehmen von Bedeutung sind.

Das **Bereitstellen von Informationen** stellt für die Zielgruppe KRITIS eine wichtige Präventionsmaßnahme dar. Jedoch gibt die Mehrzahl der deutschen KRITIS-Unternehmen (53 Prozent) an, nicht oder nur unzureichend von staatlichen Stellen über Cybervorfälle informiert worden zu sein. Nicht vorhandenes Wissen verschärft die Gefährdungslage für KRITIS-Unternehmen ähnlich wie für andere Zielgruppen, doch die Folgen können weitaus schwerwiegender sein. Daher hat die Koordinierungsstelle Cybersicherheit NRW im Jahr 2020 damit begonnen, die Vernetzung und Kommunikation zwischen den Behörden und den KRITIS-Betreibern auf Landesebene fortlaufend zu optimieren. Durch diese Bündelung der Informationen und dem ganzheitlichen Ansatz der Cybersicherheit in Nordrhein-Westfalen können die aktuellen und zukünftigen Herausforderungen, Bedrohungs- und Gefährdungslagen besser bewältigt werden.

Die Landesregierung sieht weiteren Bedarf für Beratungs-und Präventionsmaßnahmen und wird diesen im Rahmen der Cybersicherheitsstrategie, mit zielgerichteten Maßnahmen für KRITIS, aufgreifen. Um die Wirksamkeit der Präventionsmaßnahmen für KRITIS-Unternehmen messen und steigern zu können, ist eine Verbesserung der Datenlage notwendig. Deshalb werden Instrumente entwickelt werden müssen, damit Maßnahmen noch besser auf Zielgruppen angepasst werden können.

Bürgerinnen und Bürger, Unternehmen und Betreibende kritischer Infrastrukturen sind unterschiedlichen Gefahren im Cyberraum ausgesetzt. Aus diesem Grund werden zielgruppenspezifische Beratungs- und Präventionsmaßnahmen sowie Hilfsangebote von verschiedenen staatlichen Institutionen und Akteuren des Landes angeboten.

Informationssicherheit innerhalb der Landesverwaltung

4.0

Die **Informationssicherheit** in der Landesverwaltung ist von der **Cybersicherheit** der Bürgerinnen und Bürger, Unternehmen und KRITIS in Nordrhein-Westfalens grundsätzlich zu unterscheiden. Unter Cybersicherheit versteht man alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik, die im Cyberraum stattfinden. **Informationssicherheit** hingegen spezifiziert diese Definition und betrachtet die Sicherheit von Informationen in der Verwaltung sowohl technisch als auch organisatorisch. Im Kontrast zur Cybersicherheit bezieht sich die Informationssicherheit ausdrücklich auch auf nicht digitale Informationen einschließlich Papierakten und das gesprochene Wort.

Bezogen auf die Informationssicherheit innerhalb der Landesverwaltung gibt es fünf wichtige Institutionen, deren Informations- und Maßnahmenangebote sich konkret und ressortübergreifend an die Behörden und Institutionen der öffentlichen Verwaltung richten:

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

- **Die/der Informationssicherheitsbeauftragte der Landesverwaltung (NRW-CISO)**: Die bzw. der NRW-CISO plant und koordiniert in Abstimmung mit den Ressort-CISOs das ressortübergreifende Informationssicherheitsmanagementsystem (ISMS). Dazu initiiert und koordiniert sie bzw. er die Erstellung und Fortschreibung ressortübergreifender Richtlinien und Regelungen zur Informationssicherheit in der Landesverwaltung und überprüft diese regelmäßig mit dem Ziel, Defizite zu erkennen und zu beheben. Sie bzw. er leitet die Koordinationsgruppe Informationssicherheit. Unter Berücksichtigung der Erkenntnisse und Vorschläge der Ressort-CISO unterrichtet sie bzw. er die/den CIO über den aktuellen Stand der Informationssicherheit in der Landesverwaltung.

- **Computer Emergency Response Team (CERT NRW)**: Das CERT NRW ist zentrale Anlaufstelle in der Landesverwaltung für präventive und reaktive Maßnahmen in Bezug auf sicherheitsrelevante Vorfälle. Im Rahmen des ressortübergreifenden ISMS unterstützt das CERT NRW die Arbeit der bzw. des NRW-CISO, z. B. als Ansprechpartner in Fragen der Informationssicherheit.

- **Die Koordinierungsgruppe Informationssicherheit (KG InfoSic)**: Die KG InfoSic als Informationssicherheitsmanagement-Team unterstützt und berät die bzw. den NRW-CISO in Fragen der Informationssicherheit. Sie wirkt bei der Entwicklung der ressortübergreifenden Regelungen für die Informationssicherheit sowie IT-Sicherheitsstandards mit. Sie besteht aus der bzw. dem NRW-CISO als Vorsitzenden und den Ressort-CISO der Landesverwaltung Nordrhein-Westfalen. Weitere Teilnehmer können beratend hinzugezogen werden. Die KG InfoSic gibt sich eine Geschäftsordnung, in der die Grundlagen für die Zusammenarbeit innerhalb der KG InfoSic geregelt werden.

– **Die/der Ressort-Informationssicherheitsbeauftragte (Ressort-CISO)**: Die bzw. der Ressort-CISO koordiniert den Informationssicherheitsprozess im jeweiligen Geschäftsbereich. Sie oder er unterstützt die bzw. den NRW-CISO in allen Fragen der Informationssicherheit, insbesondere bei der Erstellung von Berichten zur Informationssicherheit. Die Aufgaben und Befugnisse der bzw. des Ressort-CISO regelt das Ressort.

Die Landesverwaltung deckt zwei Aspekte der Informationssicherheit ab: Zum einen wird mit dem bzw. der CIO, dem bzw. der NRW-CISO und dem CERT NRW die Erhaltung der Handlungsfähigkeit der Verwaltung angestrebt und eigene Systeme und Infrastrukturen abgesichert. Zum anderen setzt sich die Landesverwaltung für die Erhöhung der Cybersicherheit in Nordrhein-Westfalen ein, indem sie Anwendungen für die Bürgerinnen und Bürger sowie Unternehmen im Kontakt mit den Behörden sicher gestaltet.

Im Jahr 2020 gingen **5761 Warn- und Informationsmeldungen** vom NRW-CISO an die Landesverwaltung. Es kam zu keinem erfolgreichen Ransomware-Angriff in diesem Zeitraum. 8450 SPAM-Funde machten ein Nachschärfen der SPAM-Abwehr erforderlich und es wurden 2601 bekannte Schadsoftware-Systeme im Internet zentral für die Nutzer innerhalb der Landesverwaltung gesperrt. Der NRW-CISO hat 2020 zudem 55 Penetrationstest durchgeführt.

2019 gab es 26 durch das CERT NRW bearbeitete Schwachstellen innerhalb der Landesverwaltung. 2020 stieg diese Zahl auf 38 Informationssicherheitsvorfälle. Die Datengrundlage basiert auf den dem CERT NRW gemäß der Meldeverpflichtung übermittelten und einzelnen Behörden oder Einrichtungen der Landesverwaltung zuzuordnenden Informationssicherheitsvorfällen.

Weiterhin bildet das Cybercrime-Kompetenzzentrum beim LKA NRW ein wichtiges Element der Informationssicherheit innerhalb Nordrhein-Westfalens. Das Cybercrime-Kompetenzzentrum bietet nicht nur für Unternehmen und Forschungseinrichtungen, sondern auch für Behörden eine zentrale Ansprechstelle für fachkompetente Sofortmaßnahmen.

Informationssicherheit bezieht sich auf die Sicherheit aller Informationen, auch in nicht digitalen Formaten wie beispielsweise in Papierakten oder dem gesprochenen Wort. Sie ist daher von Cybersicherheit abzugrenzen, die ausschließlich die Gefährdungen aus dem Cyberraum betrachtet. Innerhalb der Landesverwaltung gibt es zuständige Institutionen, deren Angebote sich konkret an die Behörden und Institutionen der öffentlichen Verwaltung des Landes richten und diese vor Gefahren aus dem Cyberraum schützen.

Forschung und Innovation in der Cybersicherheit in Nordrhein-Westfalen

5.0

Nordrhein-Westfalen ist seit Jahren **führend im Bereich der IT-Sicherheitsforschung**. Insgesamt gibt es mehr als 700 Forscherinnen und Forscher im Bereich der IT-Sicherheit, verteilt auf 30 Hochschulinstitute und außeruniversitäre Forschungseinrichtungen, zu welchen unter anderem das Horst-Görtz-Institut für IT-Sicherheit (HGI) in Bochum, das Heinz-Nixdorf-Institut in Paderborn und das Institut für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen zählen, sowie über 400 in Nordrhein-Westfalen ansässige IT-Sicherheitsunternehmen – Tendenz steigend.

Unter dem Dach des Promotionskolleg NRW hat sich die Abteilung Informatik und Data Science thematisch zur wissenschaftlichen Vernetzung und Forschung organisiert und bietet Promotionsprogramme an. Zudem bietet die Region Bonn Rhein-Sieg mit der Hochschule Bonn-Rhein-Sieg, der Universität Bonn, den Fraunhofer-Instituten in St. Augustin, Wachtberg und Bonn Bad Godesberg sowie dem BSI, dem Kommando für Cyber- und Informationsraum der Bundeswehr und der Deutsche Telekom AG einen innovativen Nährboden der IT-Sicherheitsforschung. Im Mai 2019 wurde das Max-Planck-Institut für Sicherheit und Privatsphäre mit der Unterstützung des Landes Nordrhein-Westfalen am Standort Bochum gegründet und dient als Kompetenzzentrum für Grundlagenforschung und stärkt die Ausbildung der nächsten Generation wissenschaftlicher Führungskräfte im Bereich IT-Sicherheit und Datenschutz im Land.

Inhaltlich fokussiert sich die IT-Sicherheitsforschung in Nordrhein-Westfalen auf das Gebiet der **Human-Centered System Security**. Dies bedeutet, dass der Mensch bei allen Entwicklungs- und Anwendungsstufen in den Mittelpunkt gestellt wird. Ziel dabei ist es, die Sicherheitsmechanismen auf allen Ebenen der Wertschöpfungskette so zu gestalten, dass sie für betroffene Personenkreise auch effektiv anwendbar sind. Die übergeordnete Fragestellung, mit der sich die Forschung rund um Human-Centered System Security beschäftigt, ist, wie die Akzeptanz der Nutzenden erhöht werden kann.

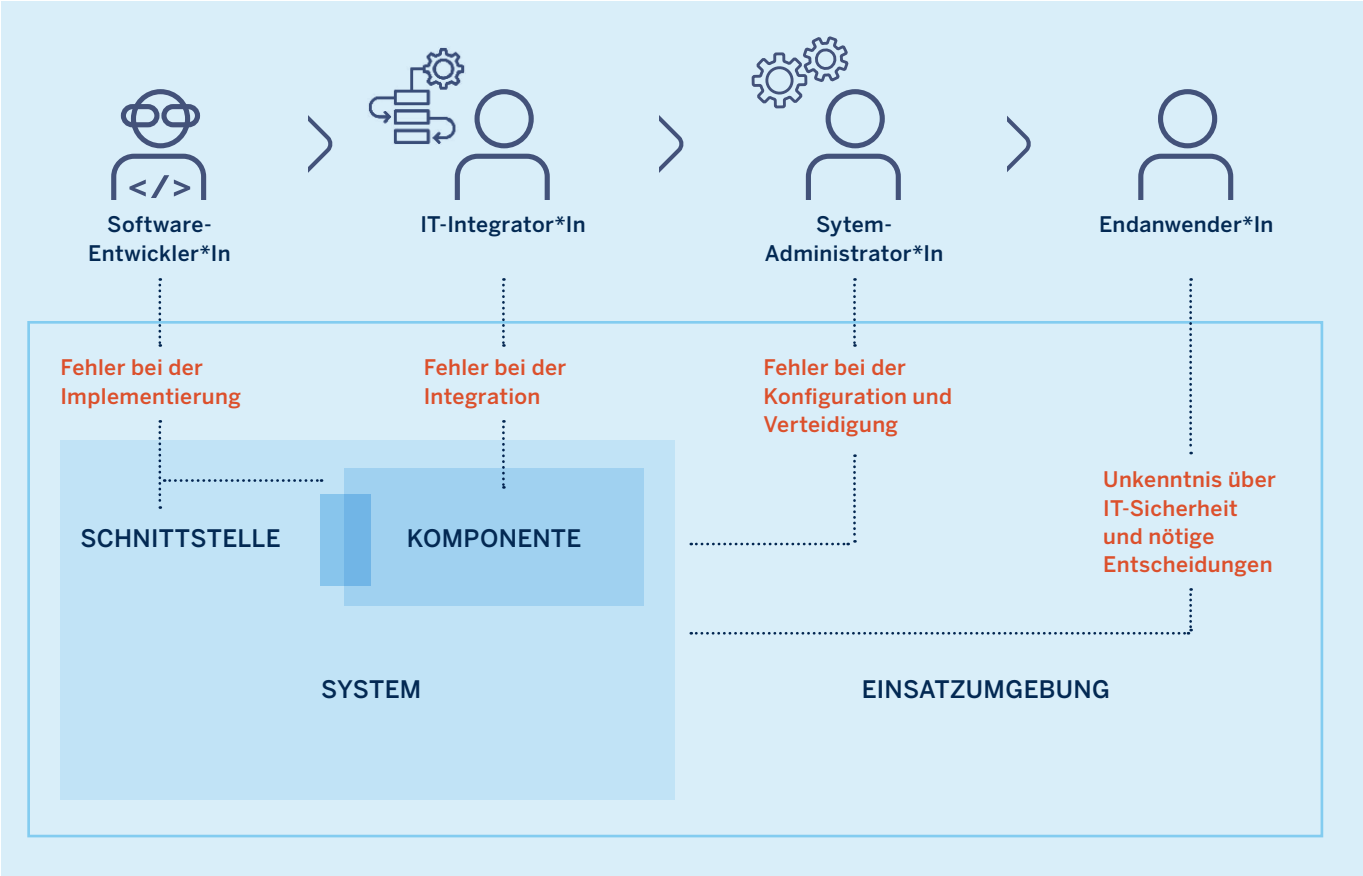


ABBILDUNG 11

Human-Centered System Security, Zusammenspiel der Parteien und potenzielle Sicherheitsprobleme

Kontinuierlich entstehen neue Angriffsflächen im Cyberraum. Am Forschungs- und Innovationsstandort Nordrhein-Westfalen wird intensiv daran geforscht, wie diesen Herausforderungen der Zukunft begegnet werden kann und der Einsatz innovativer Technologien sowie Methoden die Cybersicherheit erhöhen können.

Viele IT-Angriffe kommen heutzutage von groß skalierten Angreifern, insbesondere von staatlichen oder halbstaatlichen Organisationen. Diese Widersacher sind besonders besorgniserregend, da sie langfristig agieren und über erhebliche technische Fähigkeiten und Ressourcen verfügen.

Gegenmaßnahmen gegen diese mächtigsten Angreifer liegen im Fokus des **Exzellenzclusters Cyber-Sicherheit im Zeitalter großskaliger Angreifer**, kurz **CASA**. Die Forschung verfolgt einen interdisziplinären Ansatz, bei dem führende Wissenschaftlerinnen und Wissenschaftler aus der Informatik, aus der Mathematik und aus den Ingenieurwissenschaften mit Expertinnen und Experten aus der Psychologie kooperieren, die das Zusammenspiel von menschlichem Verhalten und IT-Sicherheit untersuchen. Diese Konstellation ist europaweit inzigartig.

Das Cluster CASA ist am Horst Görtz Institut für IT-Sicherheit (HGI) der RUB beheimatet. Es gilt international als eine der führenden Forschungsstätten in dem Feld, hat Europas größtes Ausbildungsprogramm für IT-Sicherheit und verfügt über umfangreiche akademische und industrielle Netzwerke.

Zusätzlich zu den bereits etablierten exzellenten Wissenschaftlerinnen und Wissenschaftlern fördert das Land Nordrhein-Westfalen auch junge Forschende in ihren wissenschaftlichen Karrieren. Die hervorragend qualifizierten jungen Forschenden bilden das Fundament für Spitzenforschung und die weitere zukunftsorientierte Entwicklung der IT-Sicherheit.

Eine dieser Initiativen ist das **Graduiertenkolleg NERD – North Rhine Westphalian Experts in Research on Digitalization**. Ziel des Graduiertenkollegs ist es, die Nachwuchsförderung in der IT-Sicherheit an Universitäten und Hochschulen zu stärken und das Forschungsprofil im Forschungsbereich Human-Centered Systems Security nachhaltig zu schärfen. Seit 2016 werden hier die Nachwuchswissenschaftlerinnen und -wissenschaftler sowie die beteiligten Professorinnen und Professoren zusammengeführt und ihre Vernetzung gestärkt. Aktuell befindet sich die zweite Kohorte im Begutachtungsverfahren.

Eingebunden in das Exzellenzcluster CASA ist das **Forschungskolleg SecHuman**, kurz für „Schöne neue Welt: Sicherheit für Menschen im Cyberspace“. In der ersten Förderperiode stand die Interaktion zwischen Mensch und IT-Sicherheit im Fokus. Die aktuelle Förderphase fokussiert sich auf inter- und transdisziplinäre Arbeiten, die IT-Sicherheit als weitergefasstes gesellschaftliches Phänomen betrachten.

Neben innovativen Konzepten in der gemeinsamen Ausbildung und Qualifizierung für Doktorandinnen und Doktoranden gehen die Hochschulen in Nordrhein-Westfalen auch neue gemeinsame Wege in der Konzeption von Studiengängen. So sichert der **Cyber-Campus Nordrhein-Westfalen**, eine Kooperation zwischen der Hochschule Niederrhein und der Hochschule Bonn-Rhein-Sieg, die Ausbildung der Sicherheitsexpertinnen und -experten von morgen. Im Rahmen des Cyber-Campus werden unter anderem gemeinsam neue Studiengänge konzipiert. Erstmalig wurden zum Wintersemester 2020/2021 Studiengänge zu den Themen Cybersicherheit, Cybercrime und Digitale Transformation angeboten.

Das Land Nordrhein-Westfalen nutzt Kooperationen von Wissenschaft und Forschung, Wirtschaft und Verwaltung um innovative Lösungen zur Verbesserung der Cybersicherheit zu entwickeln. Im Blickpunkt steht der Einsatz neuer Technologien wie z. B. KI für die Praxis.

Das **Thema KI-Forschung und -Anwendung** spielt auch für die Justiz in Nordrhein-Westfalen eine große Rolle. In Zusammenarbeit mit der Microsoft Deutschland GmbH, Wissenschaftlerinnen und Wissenschaftlern unter anderem der Universität des Saarlandes und dem Deutschen EDV-Gerichtstag e. V. hat die ZAC NRW ein Grundlagenprojekt im Themenfeld „Bekämpfung der digitalen Kinderpornographie“ initiiert. Da Straftaten im Bereich der Kinderpornographie heutzutage fast ausschließlich unter Verwendung des Internets bzw. digital erfolgen und regelmäßig ein sehr hohes Datenvolumen nach erfolgter Durchsuchung und Beschlagnahme von Datenträgern zeitkritisch gesichtet und ausgewertet werden muss, besteht das Bedürfnis nach einer effizienten Unterscheidung von kinder- und jugendpornographischem Material zu unbelasteten Dateiinhalten. Der hohe Anteil manueller Auswertearbeit erfordert bislang einen intensiven Personal- und Zeiteinsatz für diese Sichtung.

Gegenstand der vorbeschriebenen interdisziplinären Forschungsarbeit war strategisch die Entwicklung einer hybriden Cloudinfrastruktur, die durch ausschließlich auf Rechnern der Justiz aufbereitetes

und dekonstruiertes Datenmaterial das Training einer künstlichen Intelligenz in der Public Cloud ermöglicht. Der Einsatz der trainierten künstlichen Intelligenz wird die **Strafverfolgung maßgeblich effektiver gestalten**. Das mit Blick auf den Forschungsansatz einer hybriden Cloudinfrastruktur bundesweit – soweit ersichtlich – einzigartige Projekt erarbeitete die technische Perspektive, unter Berücksichtigung der datenschutzrechtlichen und strafprozessualen Vorgaben wesentlich schneller große Mengen an Datenmaterial auf dessen strafrechtliche Relevanz hin im Bereich der Kinderpornographie vorab zu filtern. Auf diese Weise werden die Strafverfolgungsbehörden in die Lage versetzt, nur als strafrechtlich relevant eingestuftes Bildmaterial anschließend auswerten zu müssen. Zudem dient der Einsatz einer künstlichen Intelligenz dem Gebot der zeitnahen Auswertung beschlagnahmter Beweismittel, wodurch die Gefahr der Verpflichtung zur Herausgabe des Datenträgers vor vollständiger Feststellung des Dateninhalts aufgrund einer unverhältnismäßig langen Beschlagnahmedauer minimiert wird.

Das Forschungsprojekt erbrachte zuletzt den Nachweis, dass ein hybrides Cloudszenario, in dem Bildmaterial zunächst auf behördeneigenen Rechnern technisch dekonstruiert wird, um die vollständig abstrahierten Komponenten sodann zum Training einer künstlichen Intelligenz in einer Cloudumgebung zu nutzen, grundsätzlich geeignet ist, ein entsprechend angelegtes neuronales Netzwerk auszubilden. Die entwickelte KI-Infrastruktur hat den Projektnamen **„AIRA“ (Alenabled Rapid Assessment)** erhalten. Ein funktionsfähiger Prototyp ist bei der ZAC NRW implementiert. Auf Basis der Forschungsergebnisse soll eine KI-taugliche Infrastruktur, die den Leistungsmerkmalen des Prototypen „AIRA“ entspricht, im Praxisbetrieb zunächst bei der ZAC NRW eingerichtet werden. Dabei ist die Infrastruktur bewusst offen gestaltet, so dass weitere computerforensische Services von Wirtschafts- oder Forschungspartnern im Sinne einer im Nutzerinteresse gelegenen Ausweitung der Verwendbarkeit in die Gesamtarchitektur integriert werden können. Die im Anschluss an die Forschungsphase erforderliche Beauftragung geeigneter Unternehmen mit der Umsetzung wird derzeit vorbereitet.

Nordrhein-Westfalen verfügt über eine ausgezeichnete Forschungslandschaft und ist führend im Bereich der IT-Sicherheitsforschung. Die Forschungsergebnisse fließen in Projekte mit neuen Technologien ein und fördern den Innovationsstandort Nordrhein-Westfalen.

Ausblick

6.0

Als bevölkerungsreichstes Bundesland sowie bedeutender Wirtschafts- und Wissenschaftsstandort ist Nordrhein-Westfalen besonders schützenswert – auch im Cyberraum. Viele verwaltungsinterne und verwaltungsnahe Institutionen arbeiten bereits daran, das **Cybersicherheitsniveau nachhaltig zu erhöhen** und die **Kommunikation** zwischen allen Beteiligten effizienter und effektiver zu gestalten.

Durch die **Corona-Pandemie** hat sich im Jahr 2020 einiges für die Menschen in Nordrhein-Westfalen verändert. Um die Potentiale des raschen Digitalisierungsschubs sicher und nachhaltig nutzen zu können, muss Cybersicherheit als eine wichtige Voraussetzung sicherer digitaler Lebens- und Arbeitsbereiche betrachtet werden. Es ist zu erwarten, dass dem mobilen Arbeiten, Onlineshopping, digitalen Lernen und dem Homeoffice auch in Zukunft ein großer Stellenwert zukommen wird.

Der Bericht zur Cybersicherheit in Nordrhein-Westfalen für das Jahr 2020 lässt folgende drei Schlussfolgerungen zu:

1. Der **„Faktor Mensch“** ist wesentlich für die Sicherheit bei der Internetnutzung. Die Landesregierung hat das Handlungsfeld für Präventions- und Hilfsangebote früh erkannt und wird entsprechende Angebote noch weiter in den Mittelpunkt stellen.
2. Die Landesregierung hat die Wichtigkeit der Cybersicherheit im Kontext technologischer Fortschritte erkannt und den Handlungsbedarf der verschiedenen Felder in der Cybersicherheitsstrategie definiert.
3. Das Land Nordrhein-Westfalen verfügt bereits über **starke Cybersicherheitsakteure**. Die Landesregierung fördert die Vernetzung zwischen den Akteuren, damit neue Kooperationen entstehen und Synergien gehoben werden.

Die im Bericht vorgestellten Maßnahmen der Landesregierung, wie beispielsweise die Bereitstellung von Präventionsangeboten für spezifische Zielgruppen und die Institutionalisierung des Themas Cybersicherheit, z. B. durch die Einrichtung der Koordinierungsstelle Cybersicherheit, leisten schon jetzt einen qualifizierten Beitrag zur Erhöhung des Schutzniveaus und zur Erreichung der in der Cybersicherheitsstrategie des Landes Nordrhein-Westfalen angestrebten Ziele.

Die Erstellung einer landesspezifischen Datenlage wird dazu beitragen, die Maßnahmen und Präventionsangebote weiterzuentwickeln. Die Förderung von Wissenschaft und Forschung wird weiterhin vorangetrieben, denn die Entwicklung neuer Ansätze und **innovativer Methoden leistet** einen wichtigen Beitrag zur Erhöhung der Cybersicherheit in Nordrhein-Westfalen.

Informationsangebote

Informationsangebote **für Bürgerinnen und Bürger**

Allgemeine Informationsangebote	Kontakt
Koordinierungsstelle Cybersicherheit NRW	https://www.cybersicherheit.nrw
BSI für Bürgerinnen und Bürger	https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Buergerinnen-und-Buerger/buergerinnen-und-buerger_node.html E-Mail: service-center@bsi.bund.de Telefon: 0800 274-1000
Landeskriminalamt Nordrhein-Westfalen (LKA NRW)	https://lka.polizei.nrw/
#DigitalCheck NRW	https://www.digitalcheck.nrw/ E-Mail: digitalcheck@medienpaed.de
Beratungsplattform ZEBRA	https://www.fragzebra.de/ E-Mail: info@medienanstalt-nrw.de Telefon: 0211 77007-0
Eltern und Medien	https://www.elternundmedien.de/ E-Mail: elternundmedien@medienanstalt-nrw.de Telefon: 0211 77007-140
Digital in NRW	https://www.digital-in-nrw.de/de/ E-Mail: info@digital-in-nrw.de Telefon: 0231 9743611
Medienscouts	https://www.medienscouts-nrw.de/ E-Mail: imedienscouts@medienscouts-nrw.de Telefon: 0211 77007-164

Informationsangebote und Kontaktstellen **für Unternehmen**

Informationsangebote	Kontakt
Allianz für Cybersicherheit des Bundes	https://www.allianz-fuer-cybersicherheit.de E-Mail: info@cyber-allianz.de Telefon: 0800 274-1000
Bundesamt für Sicherheit in der Informationstechnik	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/unternehmen-und-organisationen_node.html E-Mail: bsi@bsi.bund.de
Cybercrime-Kompetenzzentrum LKA NRW	https://polizei.nrw/artikel/das-cybercrime-kompetenzzentrum-beim-lka-nrw E-Mail: cybercrime.lka@polizei.nrw.de Telefon: 0211 939-4040
Deutschland sicher im Netz	https://www.sicher-im-netz.de/ E-Mail: info@sicher-im-netz.de Telefon: 030 767581-500
DIHK | Deutscher Industrie- und Handelskammertag e. V.	https://www.ihk.de/daten-und-informationssicherheit
Initiative Wirtschaftsschutz	https://www.wirtschaftsschutz.info/DE/Home/home_node.html E-Mail: wirtschaftsschutz@bfv.bund.de Telefon: 0211 792-0
IT-Sicherheit@Mittelstand	https://www.it-sicherheit-mittelstand.org/ E-Mail: info@sicher-im-netz.de Telefon: 030 767581-500
Koordinierungsstelle Cybersicherheit NRW	https://www.cybersicherheit.nrw
Kompetenzzentrum Cybersicherheit für die Wirtschaft des MWIDE	https://www.wirtschaft.nrw/cybersicherheit https://www.digital-sicher.nrw/ E-Mail: info@digital-sicher.nrw Telefon: 0234 5200-7334
Wirtschaftsschutz im Verfassungsschutz	https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/wirtschaftsschutz E-Mail: wirtschaftsschutz@im1.nrw.de Telefon: 0211 871-2821
Sicherheitspartnerschaft NRW	https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/sicherheitspartnerschaft-nordrhein E-Mail: wirtschaftsschutz@im1.nrw.de
Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)	https://www.justiz.nrw.de/JM/schwerpunkte/zac/index.php E-Mail: zac@sta-koeln.nrw.de Telefon: 0211 477-4922

Informationsangebote **für Betreibende kritischer Infrastruktur**

Informationsangebote	Kontakt
Bundesamt für Sicherheit in der Informationstechnik	https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/kritis-und-regulierte-unternehmen_node.html E-Mail: bsi@bsi.bund.de
Computer Emergency Response Team NRW (CERT NRW)	https://www.it.nrw/cert-nrw-91640 E-Mail: cert@it.nrw.de Telefon: 0211 9449-2124
Koordinierungsstelle Cybersicherheit NRW	https://www.cybersicherheit.nrw E-Mail: cybersicherheit@im.nrw.de Telefon: 0211 871-01
Kompetenzzentrum digitale Wasserwirtschaft	https://www.kompetenzzentrum–digitale-wasserwirtschaft.de E-Mail: nfo@kdw-nrw.de Telefon: 0201 47589020
Ministerium des Innern des Landes Nordrhein-Westfalen	https://www.cybersicherheit.nrw/de/kritis-nordrhein-westfalen E-Mail: cybersicherheit@im.nrw.de Telefon: 0211 871-01
MITSicherheit.NRW	https://mits.nrw/
IT-Sicherheit@Mittelstand	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=7
KRITIS Verordnung	https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf

Meldestelle für KRITIS

Meldestelle	Kontakt
Bundesamt für Sicherheit in der Informationstechnik	https://mip.bsi.bund.de/ E-Mail: Kritische.Infrastrukturen@bsi.bund.de

Auswahl von Forschungsinstituten mit Schwerpunkt Cybersicherheit und Nachwuchsförderung in diesem Bereich in Nordrhein-Westfalen

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.

Fraunhofer-Institut für Software und Systemtechnik ISST

Forschungsschwerpunkte liegen in den Bereichen verteilter und vernetzter Anwendungen sowie der Informationslogistik (Optimierung komplexer IT-Infrastrukturen). Weiterer Fokus ist Cloud Computing.

Max-Planck-Institut für Sicherheit und Privatsphäre

Das Institut erforscht und entwickelt die technischen Grundlagen und inter disziplinären Aspekte der IT-Sicherheit und des Datenschutzes.

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.

Cyber Campus Nordrhein-Westfalen

Neben innovativen Konzepten in der gemeinsamen Ausbildung und Qualifizierung für Doktorandinnen und Doktor anden 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.

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.

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.

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 her-zustellen. Das if(is) bietet neben Forschung und Lehre auch einen kostenlosen Service zur Zertifizierung von OpenPGP-Schlüsseln sowie eine Jobbörse für IT-Sicherheit 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.

Glossar

Begriffe der Cybersicherheit, Cybersicherheitsakteure und Angebote auf Landesebene, Forschungs-einrichtungen, Institute, Fachbereiche und sonstige wissenschaftliche Einrichtungen Nordrhein-Westfalens, die sich mit Cybersicherheit beschäftigen.

Blockchain
Eine kontinuierlich erweiterbare Liste von Datensätzen, die mittels kryptographischer Verfahren miteinander verkettet sind, nennt man Blockchain. Jeder Block enthält dabei typischerweise einen kryptographisch sicheren Hash (Streuwert) des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten.

BSI-Gesetz
Das BSI-Gesetz für Betreibende kritischer Infrastrukturen regelt organisatorische und technische Vorkehrungen zur Vermeidung von Störfällen.

BSI-KRITIS-Verordnung
Die BSI-KRITIS-Verordnung definiert Schwellenwerte, die manchen KRITIS-Unternehmen einen bedeutenderen Versorgungsgrad zuschreibt. So gelten für KRITIS-Betreibende über diesem Schwellenwert besondere Meldepflichten bei Cybersicherheitsvorfällen gegenüber dem BSI.

CERT – Verbund
Der CERT (Computer Emergency Response Team) -Verbund ist die Allianz deutscher Sicherheits- und Computer-Notfallteams mit heute über 40 Mitgliedern. Die einzelnen Teams sind für ihre jeweilige Zielgruppe verantwortlich. Traditionell gibt es eine enge Kooperation zwischen den verschiedenen Teams, um die Informationen zu sammeln und aufzubereiten, die für die eigene Arbeit notwendig sind. Durch den Zusammenschluss zum CERT-Verbund wird diese Kooperation auf eine einheitliche Basis gestellt.

Cybercrime oder Computerkriminalität
Cybercrime oder Computerkriminalität meint „das Verbrechen im Internet“. Darunter sind alle Straftaten zu verstehen, die unter Nutzung von Informations- und Kommunikationstechnik oder gegen diese begangen werden. Eine allgemein gültige Definition des Begriffs gibt es jedoch noch nicht. Unter Cybercrime versteht man alle Straftaten, die unter Nutzung von Informations- und Kommunikationstechnik oder gegen diese begangen werden.

Cybermobbing
Cybermobbing ist das bewusste Beleidigen, Bedrohen, Bloßstellen oder Belästigen von Personen mithilfe von Kommunikationsmedien, wie Smartphones, E-Mails, Webseiten und Sozialen Medien.

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.

Identitätsdiebstahl
Cyberkriminelle verschaffen sich beim Identitätsdiebstahl Zugang zu fremden Accounts und nutzen diese für ihre kriminellen Machenschaften. So werden bei diesem Vorgang Bekannte und Freunde des Opfers getäuscht, um an ihr Geld zu gelangen. Die Täter geben sich dabei in gefälschten E Mails als das Opfer aus, das seine nahestehenden Personen um Geld bittet. Oft erfährt die Person, deren Identität gestohlen wurde, erst sehr viel später, was ohne ihr Wissen von ihrem Account autorisiert wurde.

Information Security Management System (ISMS)
Um Unternehmen vor Cyber-Angriffen zu bewahren, ist die Einführung eines Information Security Management System (ISMS) als Präventionsmaßnahme besonders bedeutsam. Insgesamt werden mittels eines Unternehmens-ISMS Zuständigkeiten und Verantwortung für die Unternehmenssicherheit ermittelt, übergeordnete Leitlinien zur Informationssicherheit verabschiedet und der Posten eines/einer Informationssicherheitsbeauftragten eingeführt.

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.

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.

IT-Sicherheitsgesetz 2.0
Zur Erhöhung der Sicherheit in den informationstechnischer Systeme wurde das IT-Sicherheitsgesetz 2.0 beschlossen.

KRITIS
KRITIS steht kurz für Kritische Infrastruktur. Dies sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Die nationale KRITIS-Strategie 2009 definiert neun Sektoren und 29 Branchen der Kritischen Infrastrukturen: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur. Die Sektoren sind teilweise divers aufgestellt, wie z. B. der Sektor Transport und Verkehr mit seinen Branchen Luftfahrt, See- und Binnenschifffahrt, Schienenverkehr, Straßenverkehr, ÖPNV und Logistik.

Künstliche Intelligenz (KI)
Auch die Nutzung von KI bietet das Potenzial, das Cybersicherheitsniveau zu erhöhen. KI umfasst Systeme, die basierend auf verschiedenen Methoden wie Deep Learning, konstant durch ihr Handeln eigenständig dazulernen und sich permanent verbessern. Dies birgt einen zentralen Vorteil im Kontext von Cybersicherheit, da KI das Nutzungsverhalten überwachen und Unregelmäßigkeiten melden kann. Konkret bietet KI Möglichkeiten, Anti-Viren Programme oder Spam-Prognose für E-Mail Programme zu verbessern.

Phishing
Phishing ist der Versuch, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdige Person auszugeben, um so an vertrauenswürdige, persönliche Informationen zu gelangen.

Ransomware
Ransomware ist bösartige Schadsoftware, die internetfähige Endgeräte sperrt oder wichtige Dateien verschlüsselt. Erst nach Zahlung eines Lösegeldes bekommt man von den Cyberkriminellen ein Pass-wort, um das Endgerät oder die Dateien wieder zu entsperren.

Social Engineering
Beim Social Engineering werden verschiedene Eigenschaften des Menschen ausgenutzt, z.B. Hilfsbereitschaft, Angst, Respekt, Vertrauen oder Unwissenheit über bestimmte Unternehmensprozesse. Social Engineering wird durch immer raffiniertere Technik leider auch immer schwieriger aufzudecken. Durch eine realistisch wirkende E-Mail, einen Anruf oder einem Video (sog. Deepfakes) welche mit Hilfe künstlicher Intelligenz abgewandelt und verfälscht wurden können Cyberkriminelle auf immer realistischere Methoden zurückgreifen, um an ihr Ziel zu gelangen.

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.

RAUM FÜR NOTIZEN

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:
Seite 3: © Ralph Sondermann
Seite 17, 37: © greenbutterfly – stock.adobe.com
Seite 55: © 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.

HINWEIS
Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Landesregierung Nordrhein-Westfalen herausgegeben. Sie darf weder von Parteien noch von Wahlbewerberinnen und -bewerbern oder Wahlhelferinnen und -helfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden.

Dies gilt auch für Landtags-, Bundestags- und Kommunalwahlen sowie für die Wahl der Mitglieder des Europäischen Parlaments.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung.

Eine Verwendung dieser Druckschrift durch Parteien oder sie unterstützende Organisationen ausschließlich zur Unterrichtung ihrer eigenen Mitglieder bleibt hiervon unberührt. Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Schrift der Empfängerin oder dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte.

© Dezember 2021 / Ministerium des Innern NRW


selected mirror modifier object
r_ob
ifier ob is the active ob

Die Landesregierung
Nordrhein-Westfalen

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