Die Landesregierung
Nordrhein-Westfalen

Bericht zur Cybersicherheit
in Nordrhein-Westfalen 2021

www.land.nrw

Vorwort

Die Freiheit des Cyberraums zu erhalten und dennoch eine möglichst große Sicherheit zu gewährleisten, gehört zu den wichtigsten Aufgaben unserer Zeit. Umso mehr, da die Vernetzung von digitaler und realer Welt immer mehr voranschreitet und die Grenzen zunehmend verschwimmen. Dies gilt für die Welt, Deutschland und besonders für Nordrhein-Westfalen. Für unsere moderne Industrie- und Dienstleistungslandschaft ist Cybersicherheit essentiell. Sie sichert den Wohlstand der Bürgerinnen und Bürger auch in einer digitalisierten Zukunft.

Im vorliegenden Cybersicherheitsbericht des Landes Nordrhein-Westfalen 2021 stehen daher zwei Themen besonders im Fokus: Zunächst die Vernetzung von Alltags-Objekten und dem World Wide Web, das sogenannte „Internet of Things“. Es vereinfacht das Leben der

HERBERT REUL
Minister des Innern
des Landes
Nordrhein-Westfalen

Menschen, bietet durch Sicherheitslücken aber gleichzeitig auch Cyberkriminellen neue Möglichkeiten und mehr Angriffsflächen. Ein zweites Phänomen ist „Ransomware“, also das Verschlüsseln oder Stehlen von Daten mit anschließender Lösegeldforderung. Diese Angriffe geschehen immer öfter - und es kann jeden treffen: Unternehmen jeder Größe, öffentliche und private Institutionen, einzelne Bürgerinnen und Bürger.

Gottlob sinken die allgemeinen Kriminalitätszahlen seit Jahrzehnten kontinuierlich. Cybercrime hingegen boomt. Die Zahl der Fälle in Nordrhein-Westfalen ist im vorliegenden Berichtszeitraum deutlich gestiegen und sie wird auch in Zukunft steigen, so die Prognose. Deshalb müssen wir Cyberkriminalität bekämpfen und gleichzeitig Präventionsmaßnahmen ausbauen. Die Landesregierung hat dies als eine wichtige Säule im Zukunftsvertrag für Nordrhein-Westfalen verankert.

Der Krieg in der Ukraine hat uns vor Augen geführt, dass wir auch bei Kritischen Infrastrukturen (KRITIS) bestmöglich auf Angriffe aus dem Cyberraum vorbereitet sein müssen. Es ist wichtig, dass in Nordrhein-Westfalen alle beteiligten Akteure an einem Strang ziehen und das Cybersicherheitsniveau für Bürgerinnen und Bürger sowie Unternehmen und Kritische Infrastrukturen kontinuierlich steigern.

Mit der Verabschiedung der Cybersicherheitsstrategie für Nordrhein-Westfalen im letzten Jahr haben wir einen großen Schritt in die richtige Richtung gemacht. Der diesjährige Bericht zeigt, dass wir uns auf dem richtigen Weg befinden, um Nordrhein-Westfalen auch im Cyberraum Stück für Stück sicherer zu machen.

Herbert Reul MdL

Management Summary

Der Bericht zur Cybersicherheit in Nordrhein-Westfalen 2021 beschäftigt sich neben den für die Zielgruppen Bürgerinnen und Bürger, Unternehmen und Kritische Infrastrukturen aufgearbeiteten Informationen, speziell mit den beiden Fokusthemen „IoT“ und „Ransomware“. Auch in diesem Jahr wurde der Bericht unter enger Einbindung aller Ressorts der Landesregierung erstellt.

Neben der Darstellung der auf die beschriebenen Zielgruppen heruntergebrochenen Gefährdungslage, wird ein Einblick in die Informationssicherheit der Landesregierung selbst gegeben. Nach der anschließenden Skizzierung der Entwicklung des Forschungs- und Innovationsstandortes NRW, wird die Cybersicherheitsstrategie für Nordrhein-Westfalen näher beleuchtet und der Umsetzungsstand dieser dargelegt.

Wie im Bericht des vergangenen Jahres, finden Sie zum Abschluss einem Ausblick in das Jahr 2022 und eine Auflistung mit aktualisierten Informations- und Hilfsangeboten. Ebenfalls ist ein aktualisiertes Glossar angefügt, in dem die wichtigsten Begriffe des Themenbereiches kurz und auf den Punkt erläutert werden.

Bereits im Jahr 2020 war ein Anstieg der Fallzahlen im Bereich Cybercrime zu beobachten, dieser Trend setzte sich auch im Jahr 2021 fort. Die zunehmende Vernetzung und die Verlagerung des Alltags in den digitalen Raum schaffen neue Einfallstore für Cyberkriminelle. Mit 30.115 erfassten Cybercrime-Fällen im Jahr 2021 (24.294 im Jahr 2020), was einer Zunahme von ca. 20% gegenüber dem Vorjahr entspricht, zeigt die Kurve dieser Fälle weiterhin stark nach oben. Damit einhergehend sind auch die durch Cybercrime verursachten und angezeigten Schadenssummen gestiegen und haben einen Höchstwert innerhalb der vergangenen fünf Jahre in Höhe von über 24 Mio. Euro erreicht. Hierbei ist zu beachten, dass in der Polizeilichen Kriminalstatistik ein hohes Dunkelfeld beispielsweise im Bereich der durch Erpressungsdelikte, wie Ransomware-Angriffen, entstandenen Schäden besteht.

Auch die Bedrohungslage durch ausländische Nachrichtendienste und sonstige geheimdienstlich oder sicherheitsgefährdend agierende Strukturen in Nordrhein-Westfalen ist so hoch wie seit Jahren nicht mehr. Verschiedenste Aktivitäten wie klassische Spionage, illegitime Einflussnahme, Streuung von Desinformationen und Cyberangriffe stellen eine dynamische und komplexe Bedrohung dar. Auch die Versuche der Beeinflussung der Politik auf allen Ebenen haben zugenommen. Dabei spielen auch Cyberangriffe vermehrt eine Rolle. Zur Mitigation dieser Bedrohungen setzt Nordrhein-Westfalen, in Form des Verfassungsschutzes Nordrhein-Westfalens, auf flächendeckende Sensibilisierungskonzepte und baut diese systematisch aus.

Mit dem Blick auf das kommende Jahr 2022 wird in diesem Bericht das Thema der Hybriden Bedrohungen adressiert. Insbesondere angesichts des Angriffskrieges Russlands auf die Ukraine ist dieser Themenbereich näher zu beleuchten. Dies wird im kommenden Bericht des Jahres 2022 wieder aufgegriffen und eingehender analysiert werden.

Inhaltsverzeichnis

Einleitung

1.0

Stetig zunehmende Vernetzung, Verlagerung von alltäglichen Aufgaben in den digitalen Raum, Distanzunterricht, Angriffe auf Satellitennetzwerke... Die Liste lässt sich beliebig weiterführen. Bei all diesen Szenarien, die aus den verschiedensten Themengebieten stammen, spielt Cybersicherheit eine entscheidende Rolle. Daher ist der Blick auf den Zustand und die Entwicklung des Cybersicherheitsniveaus in Nordrhein-Westfalen wichtig, um anhand dessen für die Zukunft vorbereitet zu sein.

Neben dem aktuellen Blick auf die Cybersicherheit in Nordrhein-Westfalen, wird das Augenmerk auf zwei wichtige Fokusthemen gelegt. „IoT (Internet of Things) - zunehmende Vernetzung im privaten Haushalt“ bildet das erste Fokusthema dieses Berichts. Verschiedene Statistiken belegen die wachsende Popularität der kleinen und großen Alltagshelfer, die zum großen Teil mit dem Internet verbunden sind. Gleichzeitig werden in diesem Bericht die Risiken der Nutzung von solchen Geräten geschildert, wenn diese mit einem nachlässigen Sicherheitsbewusstsein einhergehen.

Der zweite Fokusbereich widmet sich dem Thema Ransomware. Das komplexe Phänomen der Erpressungssoftwares stellt heutzutage für Privatpersonen sowie Unternehmen gleichermaßen eine ständige Bedrohung dar. Über verschiedenste Kanäle können die Angreifer in die Systeme der Opfer eindringen und dort Daten verschlüsseln und ggf. sogar ausschleusen. In diesem Teil des Berichts wird die Sensibilisierung für die Einfallstore wie verdächtige Anhänge in Emails oder suspekte Links im Internet prioritär in den Blick genommen.

Weitergehend werden neue Informations- und Hilfsangebote vorgestellt, die das Cybersicherheitsniveau in NRW anheben können. Hierbei sind für alle Zielgruppen des Berichts neue Angebote enthalten.

Außerdem wird, wie im letztjährigen Cybersicherheitsbericht für Nordrhein-Westfalen angekündigt, der Umsetzungsstand der Cybersicherheitsstrategie für Nordrhein-Westfalen dargelegt. Einzelne Projekte, die aus der Strategie entsprungen sind, werden vorgestellt und Initiativen, die aus den in der Strategie formulierten Zielen abgeleitet wurden, werden präsentiert.

Wie auch im letzten Jahr möchte die Landesregierung mit diesem Bericht dem Ziel „gemeinsam mit allen gesellschaftlichen Akteuren das Cybersicherheitsniveau in und für Nordrhein-Westfalen zu verbessern“ wieder ein Stück näherkommen.

1.1
Themenfokus 1: IoT zunehmende Vernetzung im privaten Haushalt

Die zunehmende Digitalisierung macht auch vor unseren vier Wänden nicht Halt. Das Update auf „intelligente Alltagsgegenstände“ erfreut sich wachsender Beliebtheit - in Nordrhein-Westfalen wie auch bundesweit. Dies belegte die Studie „Digitalbarometer 2021“, die von der polizeilichen Kriminalprävention der Länder und des Bundes sowie dem BSI erstellt wurde. Nach Aussage dieser Studie ist der Anteil vernetzter Heimgeräte vom Jahr 2020 von 8% im Jahr 2021 auf 29% gestiegen - rund acht von zehn Befragten besitzen zwischen drei und sechs internetfähige Geräte. Da mit der zunehmenden Vernetzung in privaten Haushalten auch mögliche Cybergefahren einhergehen, schenken wir im vorliegenden Bericht zur Cybersicherheit in Nordrhein-Westfalen der Thematik „IoT“ besondere Beachtung. IoT - das „Internet of Things“ - bezeichnet die Vernetzung von Alltagsgegenständen aller Art untereinander und mit dem Internet, wobei der Bereich Smart Home alle nutzbaren und vernetzten Geräte in Haushalten umfasst. Diese sind mit kleinen Computerchips, Sensoren, Datenspeicher- oder Softwaresystemen ausgestattet. Die IoT-Geräte ermöglichen den Datenaustausch untereinander, weshalb diese Geräte als „smart“ bezeichnet werden. Neben vernetzten Lautsprechern mit Sprachassistenten ist der weit verbreitete Smart TV wahrscheinlich das bekannteste Beispiel für Smart Home Produkte. Auch im Bereich Hausautomatisierungstechnik gibt es „smarte“ Möglichkeiten. Mithilfe eines intelligenten Heizungssystems ist es möglich Energie zu sparen, indem die Temperatur automatisch reguliert wird. Aber auch ganz alltägliche Haushaltsgeräte wie Wasch- oder Spülmaschinen, die Sie per Smartphone steuern können, gehören in den Bereich Smart Home.

Sehr populär und damit weit verbreitet, sind auch Smart Toys - intelligente Spielzeuge wie lernfähige Teddybären oder ein per Smartphone steuerbares Spielzeugauto. Ende 2021 hatte sich der

IMCO - Ausschuss für Binnenmarkt und Verbraucherschutz im EU-Parlament - für mehr Datenschutz und IT-Sicherheit von smartem Spielzeug ausgesprochen und eine entsprechende Entschließung zwecks Vorlage im EU-Parlament erarbeitet. Diese Entschließung fordert die EU-Kommission zur Nachschärfung der „Toy Safety Directive“ (TSD) - europäische Spielzeugrichtlinie - auf. Anlass der Richtlinie ist ein Jahresbericht der EU-Kommission 2020. Aus diesem geht hervor, dass es sich bei über einem Viertel der gefährlichen Non-Food-Produkte, die über das EU-Schnellwarnsystem „Safety Gate“ gemeldet werden, um Spielzeuge handelt.

So angenehm die Vereinfachungen im Alltag durch die smarten Helfer auch sind, so eröffnen sie gleichzeitig auch neue Angriffsflächen für Cyberangriffe. Aus der polizeilichen Kriminalstatistik ist zu entnehmen, dass die Computerkriminalität in Nordrhein-Westfalen im Jahr 2021 im Vergleich zum Vorjahr um 23,96 Prozent zugenommen hat. Darüber hinaus wird eine generelle Verschiebung von Straftaten in den digitalen Raum beobachtet - verstärkt durch die anhaltende Pandemie.

Das bedeutet: Jede und Jeder muss darauf achten, dass ihr oder sein smartes Zuhause sicher gestaltet wird. Smart Home Geräte, die keine Sicherheits-Updates erhalten oder bei denen beim ersten Start keine sicheren Passwörter vergeben werden, stellen ein Sicherheitsrisiko dar. Bestehende Sicherheitslücken sind Schwachstellen, die es Cyberkriminellen ermöglichen, sich Zugang zu diesen IoT-Geräten zu verschaffen und diese etwa fremdzusteuern. Kompromittierte Smart Home Geräte werden unter Umständen Teil eines Botnetzes, mit Hilfe dessen kriminelle Hacker beispielsweise DDoS-Angriffe auf Webseiten oder andere Internetdienste starten. Bei sogenannten DDoS(Distributed Denial of Service)-Angriffen nutzen Angreifende eine Vielzahl unterschiedlicher Systeme um Server mit einer koordinierten Flut von Anfragen, sodass seitens des Servers keine weiteren Anfragen mehr verarbeitet werden können, außer Betrieb zu setzen. Daneben können sie ebenfalls auch als trojanische Pferde benutzt werden und so das Eindringen in Netzwerke, einen Datenklau oder die Verankerung von Ransomware ermöglichen. Auch smarte Sicherheitstechnik wie Alarmanlagen und Videokameras mit Smartphone App oder intelligente Türschlösser können ein Sicherheitsrisiko darstellen, wenn diese zum Beispiel Sicherheitslücken aufweisen, keine Sicherheitsupdates erhalten, ein unsicheres Passwort gewählt wurde oder die Geräte falsch konfiguriert wurden. Nach Erkenntnis der Umfrage „Smart Locks / smarte Videoüberwachung“ des Bitkom e.V. überwachen drei von zehn Deutschen ihr Zuhause per Smartphone und ein Fünftel davon kann sich vorstellen zukünftig digitale Türschlösser zu nutzen - was eine enorme Vergrößerung der Angriffsfläche für Hacker bedeutet. Zwei Drittel derjenigen, die smarte Türschlösser nicht nutzen wollen, fürchten sich vor Hackern, die ihre Tür öffnen könnten. Solche Szenarien, bei dem Hacker in die tiefste Privatsphäre eindringen, sind alles andere als undenkbar. Dies verdeutlicht ein bekannter Fall aus den USA, bei dem ein Hacker sich Zugriff auf ein Babyphone verschaffte, die zugehörige Babyphone-Kamera aus der Ferne steuerte und anfing das Baby anzusprechen. Doch auch bestehende Sicherheitslücken wie beispielsweise ein für den Benutzer unsichtbarer Admin-Account mit gefähr-

lichem Vollzugriff in der Firmware einer Überwachungskamera, oder ein im Klartext aus dem Saugroboter auslesbarer WLAN-Schlüssel bieten Cyberkriminellen eine große Angriffsfläche.

Die Sicherheitsbedenken wie Furcht vor Hackerangriffen oder den Missbrauch persönlicher Daten, die laut der Studie „Das intelligente Zuhause: Smart Home 2021“ des Bitkom e.V. den Großteil der Bevölkerung umtrieben, sind also mehr als begründet. Gleichzeitig zeigte die Forsa Studie „TÜV Consumer IoT Zertifizierung - mehr Sicherheit für smarte Produkte“, die im Auftrag des TÜV-Verbands erstellt wurde, dass nicht einmal die Hälfte der Nutzenden smarter Geräte beim Kauf auf die Sicherheit des Produktes bzw. die Gewährleistung des Datenschutzes achteten. Um dieser Diskrepanz entgegenzuwirken, können unabhängige Prüfstellen und Sicherheitskennzeichen für mehr Orientierung beim Kauf von Smart Home Geräten sorgen.

Für die IT-Sicherheit von Produkten gab es bislang nur unzureichende gesetzliche Vorgaben. Auch im IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) ist eine herstellerunabhängige Prüfung und Zertifizierung nicht vorgesehen. Mit dem IT-SiG 2.0 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Auftrag erhalten ein freiwilliges IT-Sicherheitskennzeichen einzuführen. Über dieses Kennzeichen sollen grundlegende Sicherheitseigenschaften digitaler Geräte oder Dienste für die Verbraucherinnen und Verbraucher mit einem Blick erkennbar sein - genauer, ob sich der jeweilige Anbieter bzw. Hersteller dazu verpflichtet hat, bestimmte Sicherheitsanforderungen zu erfüllen wie beispielsweise regelmäßige Sicherheitsupdates. Somit gibt es neben dem TÜV-Prüfzeichen für vernetzte Geräte - dem CSC „Cybersecurity Certified“ - mit dem IT-Sicherheitskennzeichen vom BSI nunmehr zwei Kennzeichen, die Auskunft über die Sicherheit digitaler Produkte geben. Zum einen durch die vom BSI angestrebte Verwendung europäischer Normen wie der EN 303645 des Europäischen Instituts für Telekommunikationsnormen. Zum anderen trat im Juni 2019 der Cyber Security Act in Kraft, ein Zertifizierungswerk auf EU-Ebene, durch das sich die Möglichkeit einer europäischen Kennzeichnung ergibt. Somit steht ein starkes Werkzeug zur Regulierung des IoT für den gesamteuropäischen Binnenmarkt zur Verfügung. Eine verpflichtende Umsetzung zur Kennzeichnung auf EU-Ebene kann mithilfe des Cyber Resilience Acts, der im September 2021 angekündigt wurde, geschaffen werden.

Weitere Informationen zum Thema IoT „Internet of Things“ wie beispielsweise Hinweise zu dessen sicheren Nutzung sowie Links zur weiteren Vertiefung in die Thematik Smart Home finden Sie demnächst auf der Internetseite Cybersicherheit.nrw.

1.2
Themenfokus 2: Ransomware

Ransomware

Ransomware sind Schadprogramme, die dazu führen, dass entweder die auf dem infizierten Computer vorhandenen Daten an die Angreifer abfließen und auf dem System verschlüsselt werden oder der Computer gegen eine weitere Benutzung gesperrt wird. Eine Entschlüsselung oder Freigabe des Rechners kann ggfs. durch eine Zahlung von Lösegeld erreicht werden.

Daher kommt auch der Name der Schadprogramme: Das Wort „ransom“ kommt aus dem Englischen und heißt - ins Deutsche übersetzt - „Lösegeld“. Häufig werden diese Programme aber auch als Erpressersoftware oder Verschlüsselungstrojaner bezeichnet. Das Ziel ist immer gleich: Hinter diesen Angriffen stecken monetäre Ziele. Die Erpresser fordern Geld und nehmen dafür Dateien auf den infizierten Computern als „Geiseln“.

Wenn Ihnen morgens auf dem Arbeitsplatzrechner oder zuhause am heimischen PC statt der vertrauten Einwahlmaske nur „You have been hacked“ entgegen leuchtete, dann sind Sie damit dieses Jahr nicht die oder der Einzige gewesen. Auch im Jahr 2021 wurden wieder viele Bürgerinnen und Bürger sowie Arbeitnehmende Opfer sogenannter Ransomware. Die Art und Weise der Schadsoftware und wie diese agiert, ist übrigens nicht neu. Bereits 1989 wurde eine Ransomware - damals noch per Diskette - in Umlauf gebracht. Opfer waren Teilnehmende einer Konferenz der Weltgesundheitsorganisation. Um eine Entschlüsselung der Festplatte zu erreichen, mussten damals 189 US-Dollar per Post an eine Firma in Panama gesendet werden.

Eine Diskette - oder ein anderes Speichermedium - ist heute nicht mehr notwendig, um sich mit einer Ransomware zu infizieren. Oft reicht es, einen E-Mail-Anhang zu öffnen, in dem sich das Schadprogramm befindet. Auch der Klick auf eine kompromittierte Website oder zu einem anderen Online-Speicherplatz mit einer schadhaften Datei führt häufig dazu, dass man sich mit dieser infiziert. Dabei kann die Motivation, auf einen solchen Link zu klicken, beispielsweise von einer vermeintlich interessanten E-Mail, gefälschter Werbung oder verschiedener anderer Tricks, auf die man beim Surfen im Internet stoßen kann, ausgelöst werden. Die Schadsoftware wird anschließend im Hintergrund heruntergeladen und automatisch ausgeführt. Ab diesem Zeitpunkt ist das System infiziert. Die offensichtliche

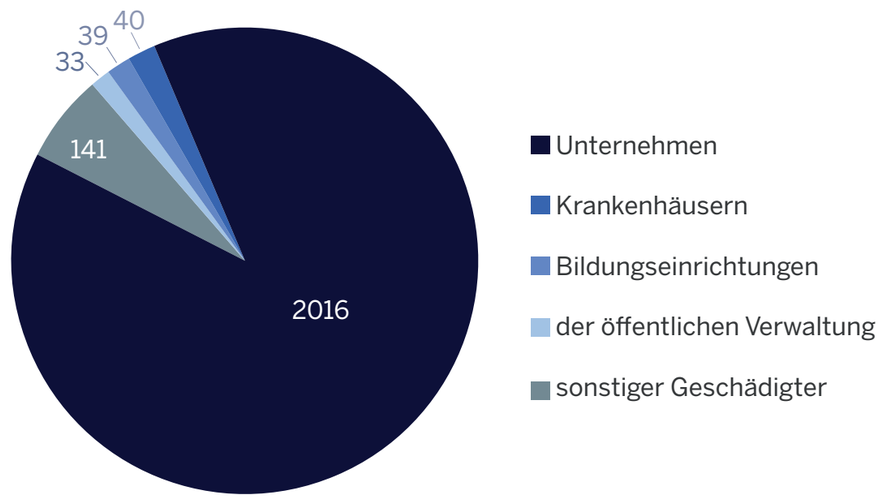
Verschlüsselung muss jedoch nicht sofort nach Infizierung des Systems beginnen. Häufig sind die Programme bereits „unsichtbar“ auf dem System aktiv, bis sie bemerkt werden oder ihre eigentliche Arbeit der Verschlüsselung und ggf. dem Diebstahl von Daten aufnehmen. Ab dem Zeitpunkt ist das System für den Anwendenden nun nicht mehr nutzbar. Durch den verzögerten Start der Computersabotage ist es oft nicht möglich nachzuvollziehen, wo und wann das System infiziert wurde. Es ist dann auch nur noch schwierig möglich, an die Schad-Quelle zu gelangen und das Einfallstor zu identifizieren. Häufig wird die Ursprungsdatei nach Beendigung der Verschlüsselung automatisch gelöscht. Nach Beendigung der Verschlüsselung erhält der Benutzende eine Mitteilung, in der das Lösegeld gefordert und die weitere Abwicklung - beispielsweise die Zahlung in Kryptowährung - beschrieben wird. Mit den eventuell zuvor abgezogenen Daten verleiht die Täterin oder der Täter, mit dem Hinweis auf eine ihm mögliche Veröffentlichung, seiner Forderung Nachdruck. Erst nach Zahlung des Lösegeldes würde eine Möglichkeit der Entschlüsselung des Systems durch die Kriminellen zur Verfügung gestellt werden.

Doch beim Umgang mit Kriminellen ist immer Vorsicht und Skepsis geboten. Die Richtlinien des BSI empfehlen, dass kein Lösegeld gezahlt wird. Im Falle einer erfolgreichen Erpressung werden die Angreifer motiviert, ihr Vorgehen fortzusetzen. Somit wird die Weiterentwicklung der Schadsoftware finanziert und die Verbreitung unterstützt. Gleichzeitig gibt es keine Garantie, dass die Entschlüsselung der Daten durch die Angreifer ermöglicht wird. Stattdessen sollte zum einen Strafanzeige bei der Polizei erstattet und zum anderen Spezialisten hinzugezogen werden. Es ist möglich, dass der betroffene Computer zum Zwecke der Spurensicherung von der Polizei untersucht wird. Daher ist es notwendig, dass dieser bis zur Freigabe durch die Behörden nicht verwendet wird. Das BSI hat zur Orientierung im Falle einer eigenen Betroffenheit auf der folgenden Seite Leitfäden bei einem IT-Sicherheitsvorfall erstellt: Erste Hilfe bei einem IT-Sicherheitsvorfall

Laut der Polizeilichen Kriminalstatistik sind die Fallzahlen in NRW im Deliktsbereich „Datenveränderung, Computersabotage §§ 303a, 303b StGB“ im Jahr 2021 (1653) im Vergleich zum Vorjahr (1258) um 31,40 Prozent gestiegen. Die Aufklärungsquote im Jahr 2021 betrug 16,27 Prozent (vorher 15,74 Prozent). Da unter die Deliktsbereiche „Datenveränderung, Computersabotage §§ 303a, 303b StGB“ neben Ransomware-Angriffen auch noch andere Delikte fallen, haben die Kreispolizeibehörden für das Jahr 2021 ihre jeweiligen Ransomware-Fälle gesondert erhoben und gemeldet, um so eine fokussierte Auswertung zu ermöglichen. Im Jahr 2021 kam es demnach zu insgesamt 2269 Ransomware-Fällen, der überwiegende Teil davon (88,85 Prozent) erfolgte zum Nachteil von Unternehmen.

ABBILDUNG 1

Anzahl der Ransomware-Fälle auf bestimmte Zielgruppen in NRW 2021



Straftaten durch Ransomware betreffen jedoch auch Privatpersonen sowie Institutionen der öffentlichen Hand. Die Stadtverwaltung Witten und die Kreisverwaltung Wesel konnten aufgrund von Ransomware-Angriffen zeitweise nicht mehr auf ihre IT-Infrastruktur zugreifen, sodass der Betrieb nur stark eingeschränkt möglich war.

Insgesamt ist eine hohe Professionalisierung der Täter festzustellen, welche sich u. a. durch die Arbeitsteilung verschiedener krimineller Akteure auszeichnet. Unterschiedliche Handlungsfelder sind die Entwicklung und Vermarktung der Schadsoftware, die Einschleusung in die Fremdsysteme und die Korrespondenz mit den Betroffenen. Letztere findet in einigen Fällen im Stil eines IT-Support-Services statt, der durch den Prozess der Lösegeldzahlung und Wiederinbetriebnahme der IT-Systeme begleitet.

Unter der Überschrift „Cybercrime as a Service“ kann man im Internet auf diese kriminellen Dienstleister zugreifen, die gegen Bezahlung u. a. Schadsoftware zur Verfügung stellen oder DDoS-Angriffe als Auftragsleistung durchführen. Die Initiierung entsprechender Angriffe bedarf damit keiner fundierten Kenntnisse oder eigner technischer Infrastruktur.

Gefährdungslage in Nordrhein-Westfalen 2021

2.0

Die Fallzahlen im Bereich Cybercrime nehmen in den vergangenen Jahren stetig zu. Laut der Polizeilichen Kriminalstatistik (PKS) wurden in diesem Jahr 30115 Cybercrime Fälle erfasst. Dies entspricht einem Anstieg von 23,96 Prozent gegenüber dem Vorjahr (24294).

Die Anzahl der ermittelten Tatverdächtigen erhöhte sich um 17,23 Prozent auf 6056. Die am häufigsten vertretenen Delikte waren Computerbetrug gemäß § 263a StGB, Fälschung beweiserheblicher Daten gemäß § 269 StGB und Ausspähen von Daten gemäß § 202a StGB.

ABBILDUNG 2

Fallzahlen im Bereich Cybercrime in NRW lt. Polizeilicher Kriminalstatistik

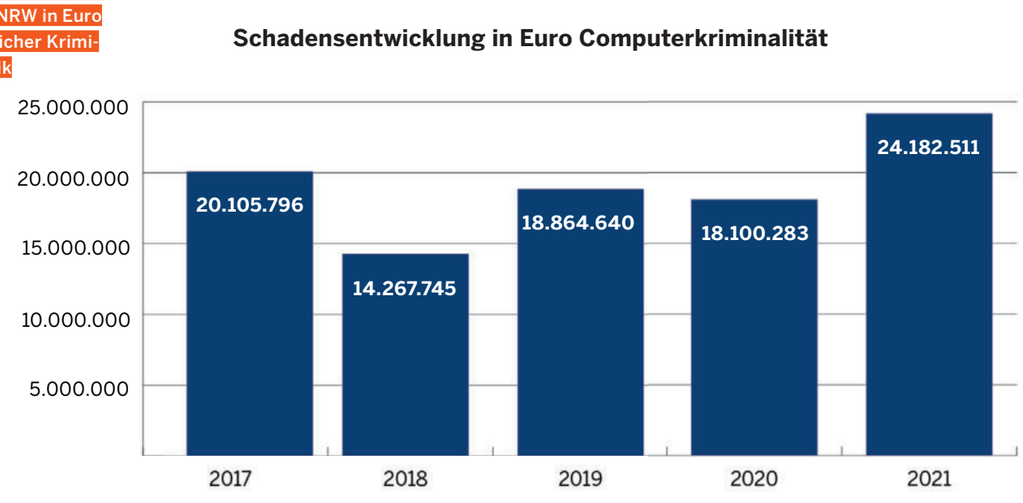
Jahr	Erfasste Fälle	Veränderung in %	aufgeklärte Fälle	Aufklärungsquote in %
2017	22 913	0,90	8 210	35,83
2018	19 693	-14,05	6 994	35,52
2019	20 118	2,16	5 911	29,38
2020	24 294	20,76	6 963	28,66
2021	30 115	23,96	8 020	26,63

Neben den zunehmenden Fallzahlen ist ebenso die Schadensentwicklung stark steigend. Schäden von Cybercrime werden in der Polizeilichen Kriminalstatistik ausschließlich für Computerbetrug und Softwarepiraterie abgebildet. 2021 erhöhte sich der Gesamtschaden der Computerkriminalität um 6.082.228 Euro auf 24.182.511 Euro und erreicht somit einen neuen Höchstwert innerhalb der vergangenen fünf Jahre.

Ein hohes Dunkelfeld kann bei Schäden, die durch Erpressungsdelikte, wie Ransomware zum Nachteil von Firmen, unterstellt werden. Die Polizeiliche Kriminalstatistik weist lediglich Schadensummen für Erpressungen allgemein aus. Eine separate statistische Erfassung von Cybercrime-Erpressungsdelikten gibt es nicht. Zudem werden erfolgreiche Erpressungen nur selten zur Anzeige gebracht.

ABBILDUNG 3

Schadensentwicklung durch Computerkriminalität in NRW in Euro lt. Polizeilicher Kriminalstatistik



Während die polizeilichen Auswertungen steigende Cybercrime-Fallzahlen darlegen berichtet der Verfassungsschutz NRW, dass auch die Bedrohungslage durch ausländische Nachrichtendienste und sonstige geheimdienstlich oder sicherheitsgefährdend agierende Strukturen in Nordrhein-Westfalen so hoch wie seit Jahren nicht mehr ist. Die Aktivitäten reichen von illegitimer Einflussnahme über klassische Spionage und Cyberangriffe bis hin zu staatsterroristischen Aktivitäten. Die Bedrohungslage ist komplex und dynamisch. Die Angreifer nutzen unter anderem das Internet und insbesondere soziale Medien.

Die Versuche illegitimer Einflussnahmen ausländischer Staaten auf Politik und Verwaltung auf Landes und Kommunalebene in Nordrhein-Westfalen – häufig flankiert durch Cyberangriffe – haben zugenommen. Sie sind in den letzten Jahren zu einem wesentlichen Mittel im Kampf um Einfluss und Vorherrschaft im globalen Gefüge geworden. Übergeordnete Ziele solcher Aktivitäten sind die Destabilisierung des jeweiligen Zielstaats und seiner demokratischen und rechtsstaatlichen Institutionen sowie die Schaffung günstiger Voraussetzungen für die Umsetzung der eigenen politischen Ziele. Daneben betreiben einige Staaten eine gezielte und oftmals desintegrative Diasporapolitik mit deren Hilfe die jeweilige Auslandscommunity kontrolliert, beeinflusst und für die eigenen politischen Zwecke instrumentalisiert werden soll. Die Spionageabwehr hat im Berichtsjahr umfassende Einflussnahmeversuche diverser Staaten auf unterschiedlichsten Feldern in Nordrhein-Westfalen festgestellt. So nutzten beispielsweise russische Stellen erneut intensiv soziale Netzwerke sowie den Cyberraum zur Verbreitung eigener Narrative beziehungsweise zur Unterstützung und Durchführung von Einflussnahme-Operationen.

Im Bereich der Spionage interessieren sich ausländische Nachrichtendienste für Haltungen, Verhandlungspositionen und Zielsetzungen politischer Akteure auf

Landes- und Kommunalebene. Aber auch Behördenmitarbeiter, ihre Zuständigkeiten und ihr Agieren werden in NRW durch nachrichtendienstliche Strukturen in den Blick genommen. Solche Aktivitäten folgen stets dem Interesse, Personen oder Organisationen für die eigene politische Agenda zu vereinnahmen, sie zu beeinflussen oder gar nachrichtendienstlich nutzbare Zugänge zu schaffen.

Zu den Bereichen, die im Berichtsjahr am häufigsten Gegenstand ausländischer Einflussnahmeversuche wurden, zählte neben der Corona-Pandemie, der Hochwasserkatastrophe, von der Nordrhein-Westfalen besonders stark betroffen war, vor allem die Bundestagswahl im September 2021.

Im Vorfeld der Bundestagswahl lagen dem Verfassungsschutz Hinweise vor, dass Personen im politischen Raum Deutschlands verstärkt durch Phishing-E-Mails bedroht wurden. Die Empfänger wurden unter einem Vorwand gedrängt, auf einer gefälschten Internetseite ihre Zugangsdaten zu meist privaten E-Mail-Konten einzugeben. Ein solcher Zugang zu E-Mail-Konten eröffnet Angreifern die Möglichkeit von sogenannten „Hack and Leak“ Operationen. Entsprechende Operationen können schon seit einigen Jahren im internationalen Raum beobachtet werden. Bei den in vielen Fällen unbemerkten Angriffen werden von den Angreifern vertrauliche Daten abgezogen, um sie zu einem späteren Zeitpunkt und gegebenenfalls modifiziert zu veröffentlichen. Angreifer versuchen, mit der Veröffentlichung in eine bestimmte Richtung auf die Wahlentscheidungen einzuwirken. Sofern es Angreifern gelingt, Zugangsdaten zu einem E-Mail-Konto zu erhalten, ergeben sich neben „Hack and Leak“ Operationen weitere Gefahren: Zum einen könnten mit der Funktion zum Zurücksetzen des Passworts verknüpfte Konten in den sozialen Medien übernommen werden. Zum anderen lassen sich im kompromittierten E-Mail-Konto gespeicherte Kontakte für Phishing-Angriffe auf die entsprechenden Personen missbrauchen. In beiden Fällen könnte ein Angreifer die Zugänge beispielsweise für die Verbreitung von Falschmeldungen oder Verleumdungen nutzen.

Die Vorgehensweise der Angreifer im Vorfeld der deutschen Bundestagswahl ähnelte der einer Gruppierung, die in Osteuropa mit Falschmeldungen in Zusammenhang gebracht wird. Aufgrund des Versendens von Nachrichten unter falschem Namen wird die Gruppierung als „Ghostwriter“ bezeichnet. Die Cyberangriffe auf Bundestags- und Landtagsabgeordnete wurden in einer Regierungspressekonferenz am 6. September 2021 durch die Bundesregierung verurteilt. In der Pressekonferenz ordnete die Bundesregierung die Aktivitäten Cyberakteuren des russischen Staates und konkret dem russischen Militärgeheimdienst GRU zu. Von den Phishing-Versuchen waren 15 politisch aktive Personen in Nordrhein-Westfalen betroffen. Hierzu zählten neun Mitglieder des Landtages, vier Lokalpolitiker, ein ehemaliges Mitglied des Landtages sowie ein früherer Lokalpolitiker.

Der nordrhein-westfälische Verfassungsschutz hat seine Sensibilisierungsmaßnahmen intensiviert. Er ist unmittelbar auf die betroffenen Personen zugegangen und hat auf die besondere Gefahr aufmerksam gemacht. Darüber hinaus wurden der Präsident des nordrhein-westfälischen Landtags informiert und Beschäftigte des Landtages mit einem Informationsschreiben sensibilisiert. Die Fraktionen des Landtags wurden im Vorfeld der Bundestagswahl durch den

Leiter des Verfassungsschutzes Nordrhein-Westfalen umfassend über die drohenden Gefahren der Einflussnahme ausländischer Nachrichtendienste informiert. Daneben wurden und werden in Politik und Verwaltung auf kommunaler und Landesebene Vorträge gehalten sowie Beratungen und Hintergrundgespräche durchgeführt. Der Bedarf in diesem Bereich ist groß und die Anzahl potentiell betroffener Stellen hoch. Vor diesem Hintergrund werden derzeit Konzepte erstellt, auf deren Basis eine systematische und langfristig flächendeckende Sensibilisierung für die nächsten Jahre sichergestellt werden soll.

Trotz der beschriebenen Sensibilisierungs- und Präventionsarbeit des Verfassungsschutzes sieht sich die nordrhein-westfälische Wirtschaft und Wissenschaft weiterhin einem erheblichen Spionagerisiko ausgesetzt. Die fortschreitende Digitalisierung sowie die zunehmende Vernetzung eröffnen ausländischen Nachrichtendiensten die Möglichkeit, ihre Operationsziele auch über Cyberangriffe zu erreichen. Entsprechende Angriffe von mutmaßlich staatlich gesteuerten Hackergruppierungen auf Unternehmen und Institutionen in Nordrhein-Westfalen bewegen sich weiterhin auf einem hohen Niveau.

Die detektierten Cyberangriffe ausländischer Dienste lassen die immensen technischen Fähigkeiten erahnen. In Nordrhein-Westfalen konnten insbesondere Aktivitäten von Hackergruppierungen beobachtet werden, die mutmaßlich den Ländern Russland, China, Nordkorea und dem Iran zugeordnet werden. Dabei gibt es vielfältige Möglichkeiten, den Ursprung von Cyberangriffen zu verschleiern und sie zu leugnen. Beispielsweise lassen sich Systeme unbeteiligter Dritter hacken, um über diese Angriffe gegen die eigentlichen Ziele durchzuführen. Cyberangriffe können im Land des Angreifenden geplant, vorbereitet und ausgeführt werden. Aufwändige und riskante Auslandseinsätze entfallen ganz oder lassen sich auf ein Minimum reduzieren. Große und interdisziplinäre Teams können auftragsspezifisch gebildet und geführt werden. Die Zusammenarbeit zwischen Hackern und Wissenschaftlern staatlicher Hochschulen oder anderen Spezialisten kann angeordnet werden. Die Tarnung der Angriffe führt dazu, dass sie sehr oft technisch nicht eindeutig einem bestimmten Land zugeordnet werden können. Die verwendeten Werkzeuge sowie die Vorgehensweise der Angreifer in Verbindung mit den Operationszielen erlauben jedoch Rückschlüsse auf bestimmte Staaten.

Die Ziele der Cyberangriffe decken sich mit Zielen klassischer nachrichtendienstlicher Operationen: Durch Spionage sollen Wirtschaftsunternehmen des angreifenden Staates unterstützt, Wissen über politische Entscheidungsprozesse des Auslands erlangt und militärische Geheimnisse des Gegners offengelegt werden. Durch das Veröffentlichen vermeintlicher Leaks oder Falschmeldungen kann das Ansehen von Personen im Zielland beschädigt werden, Stimmungen und Einstellungen geprägt oder Personen gezielt eingeschüchtert werden. Im Konfliktfall können Cyberangriffe als Teil einer hybriden Strategie über Sabotage oder die Stilllegung von Unternehmen der Kritischen Infrastrukturen (KRITIS) einen Gegner schwächen oder von innen heraus destabilisieren. Mit zahlreichen politischen Institutionen, erfolgreichen Wirtschafts- und Energieunternehmen sowie einer Vielzahl überregional politisch aktiver Personen steht insbesondere Nordrhein-Westfalen im besonderen Fokus ausländischer Nachrichtendienste.

KRITIS und hybride Bedrohungen

Im Jahr 2021 waren Kommunen und Behörden in Nordrhein-Westfalen durch mehrere Cyberangriffe mutmaßlicher Cyber-Krimineller betroffen. Die damit verbundenen Systemausfälle machten deutlich, welche Auswirkungen Cyberangriffe auf kritische Infrastrukturen (KRITIS) auch in Deutschland haben können. Nachhaltig wirkende Versorgungsengpässe und andere Folgen von Cyberangriffen können zu einer erheblichen Störung der inneren Sicherheit führen. Daher gewinnt die IT-Sicherheit mit Blick auf die zahlreichen globalen Konflikte als Schutzmaßnahme zunehmend an Bedeutung. Hierauf hat der Verfassungsschutz im Jahr 2021 verstärkt hingewiesen.

Cyberangriffe auf KRITIS-Einrichtungen und -Unternehmen können ähnlich gravierende Folgen haben wie klassische Angriffen mit konventionellen Waffen. Daher gilt in der NATO und der Bundeswehr der Cyberraum neben Land, Luft, See und Weltraum als eigenes Gefechtsfeld. Militärexperten gehen davon aus, dass gewalttätige Konflikte zwischen Staaten in Zukunft von Cyberangriffen, insbesondere auf KRITIS, begleitet werden. Militärisch wird die Wirksamkeit eines Cyberangriffs, der mit gezielten militärischen Schlägen und begleitenden Maßnahmen zur Einflussnahme und Desinformation in den sozialen Medien verbunden ist, von vielen Strategen inzwischen als kostengünstiger und effizienter als konventionelle Angriffe bewertet.

Cyberangriffe mit dem Ziel der Sabotage erfordern eine umfangreiche Vorbereitung. Um im Konfliktfall Cyberangriffe als Waffe einsetzten zu können, müssen sie bereits in Friedenszeiten vorbereitet werden. Zunächst werden Informationen über die eingesetzten Systeme gesammelt. Mit ihrem staatlichen Hintergrund haben die Akteure häufig die Möglichkeit, Spezialisten oder Forschende für ihre Operationen zu verpflichten. Von der Ausforschung von Produkten für den Sabotageeinsatz sind auch Unternehmen in Nordrhein-Westfalen betroffen. So wurde bekannt, dass eine mutmaßlich den Iranischen Revolutionsgarden zugeordnete Hackergruppierung unter falscher Identität den Kontakt zum Produkt-Support eines Unternehmens in Nordrhein-Westfalen suchte. Mutmaßliches Ziel war, detaillierte Informationen zur Funktionsweise zu erhalten und diese für mögliche Sabotage-Angriffe in der Zukunft zu nutzen.

Die Bedeutung von Cyberangriffen auf kritische Infrastrukturen hat sich bereits im Konflikt um die Ukraine gezeigt. Seit Beginn des russisch-ukrainischen Konfliktes im Jahr 2014 sprechen Indizien dafür, dass Russland Cyberangriffe als Teil einer hybriden Kriegsführung nutzt. Cyberangriffe führten in der Ukraine beispielsweise in den Jahren 2015 und 2016 zu Stromausfällen. Ein Cyberangriff mit der Schadsoftware „NotPetya“, die über Updates der ukrainischen Buchhaltungssoftware MeDoc verteilt wurde, führte im Jahr 2017 sogar zu weltweiten Produktionsausfällen. Die Schadsoftware erweckte zunächst den Eindruck einer gewöhnlichen Erpressungssoftware. Analysen offenbarten aber, dass eine Wiederherstellung der verschlüsselten Daten technisch nicht möglich war. Daher wird der Angriff inzwischen als Sabotage bewertet. Es liegt die Vermutung nahe, dass die Angreifer primär das ukrainische Finanzsystem schädigen wollten. Der Schaden für die Weltwirtschaft war jedoch beträchtlich.

Hybride Bedrohungen

Hybride Bedrohungen sind kein neues Phänomen, jedoch neu in ihrer Wirksamkeit. Bei Hybriden Bedrohungen handelt es sich um die illegitime Einflussnahme fremder Staaten auf Zielstaaten mit dem Ziel von deren Destabilisierung. Diese Angriffe fallen oft in einen gesetzlichen Graubereich und werden über verschiedene Bereiche gespielt (Medien, politisches System, Wirtschaft etc.). Hybride Bedrohungen beschreiben z.B. die Kombination aus militärischen und nicht-militärischen Angriffsmethoden. Angreifer setzen vermehrt verschiedene Angriffsarten gegen ein Ziel ein, wie der Einsatz von Bodentruppen im urbanen Umfeld kombiniert mit Cyberangriffen auf Computersysteme und die Manipulation der öffentlichen Meinung durch Desinformation in sozialen Medien.

Ein vorausschauender Blick in das Frühjahr 2022 bekräftigt einmal mehr, dass Cyberangriffe, die Auswirkungen auf das alltägliche Leben haben können, immer mehr zur Realität werden. Aufgrund des Angriffskrieges Russlands gegen die Ukraine besteht die Gefahr, dass fortlaufende, mutmaßlich staatlich gesteuerte Cyberangriffe in der Ukraine als Kollateralschaden auch zu Auswirkungen in westlichen Staaten führen können. Ebenso könnte der Aggressor die Cyberangriffe auf westliche Staaten ausweiten. Die Ereignisse des Angriffskriegs Russlands gegen die Ukraine zeigen auch, dass hybride Bedrohungen enorm an Bedeutung gewonnen haben. Diese Thematik wird im Cybersicherheitsbericht des nächsten Jahres als Fokusthema näher beleuchtet.

Geänderte Strategie der Angreifer

Im vergangen Jahr konnte laut des Verfassungsschutzberichts NRW erneut eine bereits im Vorjahr aufgefallene veränderte Strategie der Angreifer beobachtet werden. Angriffsmethoden werden nicht mehr nur gegen einzelne, gezielt ausgewählte Opfer eingesetzt, sondern großflächig und zeitgleich gegen eine Vielzahl von Organisationen angewendet. Das Ziel der Angriffe scheint hier zunächst die Installation verdeckter Fernzugriffe zu sein. Erweckt eine bestimmte Organisation ein tiefergehendes Interesse der Angreifer, kann die dann bereits vorhandene Hintertür für weiterreichende Angriffe genutzt werden. In anderen Fällen kann über den vorbereiteten Zugang die Infrastruktur eines Opfers für Cyberangriffe gegen andere Opfer missbraucht werden. Verschiedene Angriffe über Zero-Day-Exploits und Angriffe über kompromittierte Software-Updates ließen 2021 diese Entwicklung beispielhaft erkennen. in Beispiel für die Ausnutzung von Zero-Day-Exploits sind

Exploits

Die technische Beschreibung, wie in einem System eine Sicherheitslücke ausgenutzt werden kann, wird als Exploit bezeichnet. Angreifer nutzen Exploits, um in fremde Systeme einzudringen. Um dies zu verhindern, veröffentlichen Hersteller Updates, die das zugrundeliegende Fehlverhalten des Systems korrigieren. Solange nur der Angreifer Kenntnis von einem Exploit hat, kann der Hersteller keine Updates zur Verfügung stellen. Um hervorzuheben, dass der Hersteller die Schwachstelle noch nicht (oder bildlich gesprochen für 0-Tage) kennt, hat sich der Begriff Zero-Day-Exploit etabliert. Bis zu ihrer Veröffentlichung gewähren Zero-Day-Exploits einen nahezu sicheren Zugang zu jedem System eines Herstellers. Nach der Veröffentlichung können die Exploits solange weiter genutzt werden, bis die Sicherheitsupdates in allen Systemen verteilt sind.

die Anfang März 2021 bekannt gewordenen Angriffe auf die auch in Nordrhein-Westfalen weit verbreiteten Installationen des Microsoft Exchange Servers. Microsoft Security hatte auf mehrere Zero-Day-Exploits aufmerksam gemacht, die zunächst für gezielte Angriffe, zumeist gegen Systeme in Nordamerika, missbraucht worden waren. Für die Angriffe machte Microsoft eine mutmaßlich aus China gesteuerte Hackergruppierung verantwortlich, die Microsoft als HAFNIUM bezeichnete. Obwohl der Software-Hersteller zeitnah Sicherheitsupdates zur Verfügung stellte, konnte weltweit eine starke Verbreitung der Angriffe unter Ausnutzung der Sicherheitslücken beobachtet werden. Sowohl Cyberkriminelle als auch vermutlich staatlich gesteuerte Akteure nutzten die Angriffsmethode für erfolgreiche Cyberangriffe. Indizien deuteten darauf hin, dass sich ausländische Nachrichtendienste systematisch Informationen über Zero-Day-Exploits beschafft haben. Die Cyberabwehr des nordrhein-westfälischen Verfassungsschutzes sensibilisierte in diesem Zusammenhang zahlreiche Opfer, bei denen es Hinweise auf staatlich gesteuerte Cyberangriffe gab.

Mit zunehmender Komplexität technischer Systeme steigt die Wahrscheinlichkeit, dass sich bei der Entwicklung Fehler einschleichen. Im späteren Betrieb der Systeme kann dann unter bestimmten, zumeist selten auftretenden Rahmenbedingungen ein undefiniertes Verhalten des Systems provoziert werden. In einigen Fällen kann das Verhalten dazu führen, dass ein Anwender unbeabsichtigt weitgehende Zugriffsrechte erhält und eigenen Programm-Code ausführen kann. In diesem Fall wird der Fehler zu einer Sicherheitslücke.

Angriffe über die Software-Lieferkette

Gelingt es Angreifern, einen Software-Hersteller zu kompromittieren, sind alle Nutzer der Software ebenso gefährdet. Die Schadsoftware kann in einem solchen Fall in Software-Updates des Herstellers versteckt werden. In der Regel vertrauen Nutzer ihren Software-Lieferanten und installieren regelmäßig die bereitgestellten Aktualisierungen, die dann mit Schadcode versehen sind.

Opfer eines solchen Angriffes ist auch die texanische Firma SolarWind geworden, bei dem Angreifer kompromittierte Updates in die von dem Unternehmen zur Verfügung gestellte Netzwerkmanagement-Software Orion eingeschleust hatten. Von dem Cyberangriff waren rund 18.000 Institutionen und Unternehmen weltweit betroffen, darunter verschiedene US-Behörden sowie rund 300 Stellen in Deutschland. Der Angriff wurde von einer selbst betroffenen Sicherheitsfirma publik gemacht, die die Entdeckung nach eigenen Angaben einem aufmerksamen Mitarbeiter verdankte. Als Reaktion auf den Angriff veröffentlichte das Weiße Haus am 15. April 2021 eine Verlautbarung, in der der russische Auslands-Geheimdienst SWR und die ihm zugeordnete Hackergruppierung APT29 als Urheber der Angriffe genannt werden. Beobachtungen verschiedener Sicherheitsfirmen deuten darauf hin, dass auch andere staatlich gesteuerte Hackergruppierungen die beschriebene Vorgehensweise weltweit adaptiert haben und adaptieren.

Ausnutzen des menschlichen Faktors - Social Engineering

Nach wie vor führen ausländische Nachrichtendienste gezielte Cyberoperationen durch. Das Ziel der Angriffe sind Institutionen, Unternehmen oder Einzelpersonen, die in das Visier der Angreifer geraten sind. Die Angriffe folgen hierbei stets einem bestimmten Schema. Zunächst wählen die Angreifer gezielt Beschäftigte der Ziel-Organisation aus. Offene Datenquellen wie Websites oder Berufsportale stellen hierbei eine wertvolle Datenquelle dar. Im nächsten Schritt wird unter falschem Vorwand Kontakt aufgenommen. Durch eine möglichst perfekte Täuschung sollen die Personen dazu verleitet werden, eine bestimmte Webseite aufzurufen oder ein Dokument mit Schadsoftware zu öffnen. Ein mutmaßlich nordkoreanischer Akteur nutzt hierfür beispielsweise fiktive Stellenangebote und setzt sogar Schauspieler als vermeintliche Headhunter ein. In anderen Fällen versenden Angreifer Phishing-E-Mails an Firmenangehörige, die dazu auffordern, die Zugangsdaten zum Unternehmensnetz auf einer gefälschten Webseite einzugeben.

Im Frühjahr und Herbst des Jahres 2021 sensibilisierte der nordrhein-westfälische Verfassungsschutz erneut Hochschulen vor einer langjährigen APT-Kampagne, die unter dem Namen Silent Librarian bekannt ist und mutmaßlich aus dem Iran heraus gesteuert wird. Mit Hilfe von Phishing-E-Mails sollten Hochschulangehörige dazu verleitet werden, auf einer gefälschten Webseite ihre Zugangsdaten für die eigene Hochschulbibliothek einzugeben. Die Angreifer haben es dabei auf Forschungsarbeiten und wissenschaftliche Abhandlungen abgesehen.

Advanced Persistent Threat (APT)

Verschiedene ausländische Staaten haben seit Jahren schlagkräftige Hackergruppierungen aufgebaut, die über exzellente technische Fähigkeiten verfügen und deren Cyberangriffe bewusst im Verborgenen durchgeführt werden. Im Gegensatz zu Cyber-Kriminellen verfolgen Angreifer im staatlichen Auftrag in der Regel keine finanziellen Interessen. Eine hohe Priorität besteht vielmehr darin, möglichst lange unentdeckt im Netz des Opfers zu verbleiben. Der Ablauf solcher Angriffe deutet auf eine gute Organisation der Angreifer hin. Behördliche Organisationsstrukturen sind immer wieder erkennbar. Die einzelnen Schritte eines Angriffs werden oft in Arbeitsteilung von verschiedenen, spezialisierten Teams ausgeführt. Als Kategorie für Angriffe solcher Hackergruppierungen hat sich die Bezeichnung Advanced Persistent Threat (APT) – „Fortgeschrittene andauernde Bedrohung“ – etabliert.

Ab März 2021 sensibilisierte die nordrhein-westfälische Cyberabwehr politisch aktive Personen gegenüber Phishing-E-Mails einer als Ghostwriter bezeichneten Gruppierung. In einer bundesweiten Kampagne drohten die Angreifer in gefälschten E-Mails damit, dass die E-Mail-Konten der betroffenen Personen gesperrt würden. Die Sperrung könne nur verhindert werden, wenn auf einer gefälschten Seite die Zugangsdaten für das eigene Postfach eingegeben würden. Über die Kenntnis dieser Daten kann es Angreifern gelingen, Passwörter für Konten in den sozialen Medien zurückzusetzen.

Wie schon zuvor in anderen Ländern beobachtet, drohte somit die Gefahr, dass die Angreifer die erschlichenen Zugangsdaten im Vorfeld der Bundestagswahl für Desinformation und Einflussnahme nutzen würden.

Zielgruppenspezifische Informationen und Lösungsansätze

In diesem Kapitel wird die vorangestellte Gefährdungslage in Nordrhein-Westfalen speziell für die Zielgruppen Bürgerinnen und Bürger, Unternehmen und kritische Infrastrukturen (KRITIS) detailliert dargestellt und aufgearbeitet. Ob Phishing, Wirtschaftsspionage oder Online Fake Shops, jede Zielgruppe sieht sich verschiedenen Herausforderungen und Gefahren im Cyberraum ausgesetzt. Im weiteren Verlauf des Kapitels werden einige dieser Gefahren näher beleuchtet, Hinweise zur Minimierung der daraus entstehenden Risiken gegeben und neue Unterstützungsangebote in Nordrhein-Westfalen vorgestellt.

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 dargestellt und aufgearbeitet. Ob Phishing, Wirtschaftsspionage oder Online Fake Shops, jede Zielgruppe sieht sich verschiedenen Herausforderungen und Gefahren im Cyberraum ausgesetzt. Im weiteren Verlauf des Kapitels werden einige dieser Gefahren näher beleuchtet, Hinweise zur Minimierung der daraus entstehenden Risiken gegeben und neue Unterstützungsangebote in Nordrhein-Westfalen vorgestellt.

3.1 Bürgerinnen und Bürger

Die Bevölkerung NRWs sensibilisieren

Bürgerinnen und Bürger gerieten im Jahr 2021 immer mehr ins Visier der Cyberkriminellen und standen dabei auch neuen Sicherheitsrisiken gegenüber. Nahezu alle Risiken aus dem Jahr 2020 ließen sich ebenfalls im Jahr 2021 beobachten - mit weiterhin rasant steigenden Fallzahlen. Die Studie „Digitalbarometer 2021“ kam zu dem Ergebnis, dass knapp 4/5 der Befragten durch Cyberangriffe einen Schaden erlitten. Die drei häufigsten Straftaten waren Fremdzugriff auf einen Online-Account 31%, Download von Schadsoftware 28% und Phishing 25%. Jeder Fünfte stand Cyberkriminalität im Zusammenhang mit der Coronapandemie bzw. Covid-19-Bezug gegenüber bspw. in Form einer Phishing-E-Mail mit Covid-19-Thematik. Die Betroffenen halfen sich nach Aussage der Studie zu 36% selbst, erstatteten zu 29% Anzeige bei der Polizei oder baten in jedem fünften Fall Familie oder Freunde um Hilfe - nur eine Minderheit von 3% wusste nicht, wie in so einem Fall gehandelt werden sollte.

Die bekannten, gefälschten Paketbenachrichtigungen per SMS beispielsweise haben im Rahmen der pandemischen Lage einen weiteren Mitspieler hervorgebracht. Cyberkriminelle nutzen bei den steigenden Onlineshoppingzahlen die Herausforderungen bei Versand- wie Zustellprozessen aus. Sie geben sich unter anderem als Zollbeamte oder Zustelldienst aus, um die Kosten für die Zustellung der Produkte über anonyme Zahlungsdienste zu erlangen. Die Studie „Digitalbarometer 2021“ resümierte, dass der Accountschutz beim Onlineshopping unterschätzt wird, da bei etwa jedem Viertem von Cyberkriminellen Login- bzw. Accountdaten ebenso wie Kredit- oder Kontodaten entwendet wurden. Wie bereits ausgeführt, wurden neue Trends im Bereich Cyberattacken festgestellt. Parallel zum Smishing - das Phishing über SMS, beispielsweise wie die oben erwähnte gefälschte Paketbenachrichtigung - werden zunehmend Vishingkampagnen beobachtet. Bei Vishing handelt es sich um Voice-Phishing-Anrufe, wobei sich Cyberkriminelle am Telefon beispielsweise als vermeintlicher IT-Support ausgeben.

Sie werden gephisht...

...Ein vermeintlicher IT-Support spricht am anderen Ende der Leitung und möchte ein nicht vorhandenes Computerproblem lösen. Bei dieser Betrugsmasche zielen die Betrügerinnen und Betrüger darauf ab, per Fernzugriff Schadprogramme auf Geräten zu installieren, um sich im Anschluss an sensiblen Daten zu bereichern. Speziell in 2014 warnte Microsoft vor genau diesen Anrufen. Im Jahr 2021 wird ein erneuter, sichtbarer Anstieg derartig betrügerischer Anrufe beim BSI sowie den Verbraucherschutzvereinen registriert. Dabei werden die Namen verschiedener Unternehmen für das Vishing missbraucht.

Weiterhin zugenommen hat auch die Verbreitung von Online Fake Shops. Insbesondere in umsatzstarken Monaten, beispielsweise um die Weihnachtszeit. Aber auch bei Produkten, die aufgrund der Saison oder einer Mangellage einer erhöhte Nachfrage aufweisen, war der Einsatz solcher Fake Shops zu beobachten. Über Indikatoren für Fake Shops klärt das BSI Bürgerinnen und Bürger auf seiner Website www.bsi.bund.de auf.

Indikatoren für Fake Shops

1. Kein eindeutiger Bestellbutton. Unklare Begriffe wie „Anmelden“ oder „Abschließen“.
2. Keine verschlüsselte Verbindung zu Webseiten (kein „Vorhängeschloss“ in der Browserzeile) sowie auffällige Domain-Endungen - beispielsweise „.de.com“ - oder zum Produkt unpassender Domainname.
3. Ausschließliches Kontaktformular, kostenpflichtige Rufnummern (Ausland) oder Postfächer als Kontakt.
4. Bei Fake Shops sind die Adressen im Impressum zwar korrekt, aber die vermeintliche Firma unter dieser - nach Internetrecherche - nicht zu finden.
5. Realitätsferne und fehlende Transparenz. Der Produktpreis ist ungewöhnlich niedrig, Gebühren für Porto oder andere Zusatzkosten werden nicht aufgeführt oder es sind keine Allgemeinen Geschäftsbedingungen sind einsehbar.
6. Der Shop nutzt ein frei erfundenes Gütesiegel. Ein Indikator für ein echtes Gütesiegel (z.B. „Trusted Shop“) ist, dass mit ihnen interagiert werden kann und sie beispielsweise auf die Webseite des Gütesiegels weitergeleitet werden.
7. Zunächst stehen vermeintlich verschiedenste Zahlungsmöglichkeiten zur Verfügung. Beim tatsächlichen Bestellvorgang ist allerdings nur noch die Zahlung per Vorkasse möglich.
8. Ausschließlich positive Bewertungen, die sich zum Großteil wie schlechte Übersetzungen lesen lassen.

Ein Ziel der 2021 veröffentlichten Cybersicherheitsstrategie des Landes Nordrhein-Westfalen ist es die Kompetenzen im Bereich Cybersicherheit von Bürgerinnen und Bürgern sowie Unternehmen auszubauen, um das bewusste Handeln jeder einzelnen Person zu stärken. Die meisten Cybersicherheitsvorfälle resultieren durch den Faktor „Mensch“ als Urheber. Genau an diesem Punkt ist anzusetzen, um durch den Ausbau des Wissens im Bereich der Cybersicherheit das Verhalten in Bezug auf technische Systeme sicherer zu machen. Oftmals sind es schon relativ niedrigschwellige Maßnahmen, die dabei helfen können die Risiken eines Cyberangriffs zu senken - wie ein sicheres Passwort oder die Nutzung einer möglichen Zwei-Faktor-Authentifizierung. Hier kam die Studie „Digitalbarometer 2021“ zu dem Ergebnis, dass die Zwei Faktor-Authentifizierung nur 40% der Befragten nutzen, wohingegen sichere Passwörter von drei Fünftel der Befragten genutzt werden - ein aktuelles Virenschutzprogramm sowie Firewall wurden von 62% bzw. 53% der Befragten als Sicherungsmaßnahme eingesetzt. Unterstützende Informationen zu Cybersicherheit wünschen sich die Befragten laut dieser Studie hinsichtlich der Thematik wie sie Kriminalität erkennen können (57%), Hinweise zum Schutz sensibler Daten (48%), Empfehlungen geeigneter Sicherheitssoftware (48%) oder auch Informationen zur Reaktion auf Cyberangriffe (45%). Die jüngeren Altersklassen von 14-29 Jahren bevorzugen dabei Informationen über soziale Medien. Die Stärkung der Kompetenzen der Bürgerinnen und Bürger im Bereich Cybersicherheit in Nordrhein-Westfalen sowie das Schaffen eines Gefährdungsbewusstseins, ist ein zentraler Pfeiler im Kampf gegen die rasant steigenden Zahlen der Cybersicherheitsvorfälle. Hierzu läuft ein Kooperationsprojekt der Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen zusammen mit der Staatskanzlei Nordrhein-Westfalen und der Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK).

Der von der Staatskanzlei Nordrhein-Westfalen initiierte und von der GMK entwickelte #DigitalCheckNRW wird demnächst um das Angebot des #CyberCheckNRW erweitert. Mithilfe des #DigitalCheckNRW können Bürgerinnen wie auch Bürger ihre Medienkompetenz testen und Vorschläge für personalisierte Weiterbildungsmaßnahmen erhalten. Der #CyberCheckNRW erweitert den Wissensrahmen des #DigitalCheckNRW um die Thematik „Cybersicherheit“. Der Selbsttest zielt auf die Lebenswirklichkeit der Bürgerinnen und Bürger ab, um das Bewusstsein für Cyberrisiken wie Phishing, Social Engeneering oder Malware auszubauen sowie handlungsorientierte Problemlösungskompetenz zu fördern. Ergeben sich nach der Durchführung des #CyberCheckNRW Wissenslücken, können diese von den Bürgerinnen und Bürgern durch personalisierte Vorschläge zu Informations- und Weiterbildungsmaßnahmen geschlossen werden.

Zur fachlich-inhaltlichen Konzeption der zentralen Frage des Projektes: „Welche Kompetenzen brauchen erwachsene Menschen – NRW-Bürger/innen – in einer vernetzten digitalen Welt über die Medienkompetenzen hinaus, um souverän mit den Anforderungen von Cybersicherheit umzugehen? Wie kann der #DigitalCheckNRW diese Cybersicherheits-Kompetenzbildung unterstützen?“

wurden zunächst weitereichende Webrecherchen durchgeführt und im Anschluss daran Fragen für Expertinnen und Experten mit unterschiedlichen Steakholderperspektiven abgeleitet. Die so identifizierten Kompetenzen wurden danach den sechs Dimensionen des Medienkompetenzrahmens NRW zugewiesen:

1. Bedienen und Anwenden
2. Informieren und Recherchieren
3. Kommunizieren und Kooperieren
4. Produzieren und Präsentieren
5. Analysieren und Reflektieren
6. Problemlösen und Modellieren

Bei den Interviews zu den Kompetenzen von Cybersicherheit, wiesen die interviewten Experten auf einige grundsätzliche Aspekte hin:

• Die eigene Betroffenheit der Bürgerinnen und Bürger muss verdeutlicht werden, um die Aufmerksamkeit für das Thema Cybersicherheit zu erhöhen.

• Die Auseinandersetzung mit dem Thema Cybersicherheit ist aufwendig. Es muss veranschaulicht werden, dass die Investition von Zeit und Geld in die eigene Sicherheit einen Mehrwert für alle Bürgerinnen und Bürger erzeugt.

• Der Abstand zwischen dem eigentlichen Wissen über Cybersicherheit in der Bevölkerung und dem was tatsächlich umgesetzt wird, kann noch weiter verringert werden.

• Cyberkriminellen stehen viele und einfach nutzbare Einfallstore zur Verfügung um Personen zu hacken.

• Die Gruppe der Kinder und Jugendlichen Bedarf einer besonderen Aufklärung und Schutz. Es handelt sich um eine Generation, in der schon früh persönliche Daten im Web auftauchen. Eltern sollten ihre Kinder und Jugendlichen beim Umgang mit dem Netz begleiten.

• Die Vielzahl an Regeln für den sicheren Umgang mit Daten und IT müssen verständlich erklärt und deren Konsequenzen aufgezeigt werden.

• Die Kompetenzen der Bürgerinnen und Bürger im Bereich Cybersicherheit müssen weiter ausgebaut werden.

• Das Angebot des #CyberCheckNRW befindet sich noch im Aufbau. Dieser wird ohne Registrierung frei zugänglich sein.

Zur Verbesserung der Cybersicherheit von Bürgerinnen und Bürger in Nordrhein-Westfalen gibt es auch aktuell schon ein vielfältiges Angebot an Maßnahmen, die miteinander verknüpft sind.

Die Wahrnehmung von Kontakt- und Hilfsangeboten für Hinweise auf Betrugsmaschen und Phisingmails muss bei Bürgerinnen und Bürgern erhöht werden.

Unter anderem z.B. das Phishing-Radar (https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059). Ein Informations- und Warndienst, der von der Verbraucherzentrale NRW in Kooperation mit dem BSI entwickelt wurde. Das Phishing-Radar soll zu einem besseren Schutz der Bürgerinnen und Bürger in NRW vor unseriösen Angeboten beitragen.

Oder die durch das LKA NRW entwickelte, breit angelegte Kampagne zum Passwortschutz „www.mach-dein-passwort-stark.de“. Die Kooperationspartner Verbraucherzentrale NRW, eco-Verband der Internetwirtschaft e. V. und Bundesverband Verbraucherinitiative e. V. sind konzeptionell eingebunden. Die crossmediale Kampagne hat die Aufgabe, Präventionshinweise zu vermitteln, die auf Grundlage einer umfassenden Analyse der Schwachstellen bei den digitalen Endgeräten erstellt wurden. Ende 2020 hat der Minister des Innern des Landes Nordrhein-Westfalen, Herbert Reul, die Präventionskampagne www.mach-dein-passwort-stark.de der Öffentlichkeit vorgestellt und den Startschuss gesetzt. In diesem Jahr lief die Kampagne durchgehend und wird fortgeschrieben.

3.2 Unternehmen

Sensibilisierung durch die Cyberabwehr des Verfassungsschutzes

Aufgrund der Fähigkeiten der Angreifer werden viele Angriffe von den Nutzenden nicht erkannt. Herkömmliche Schutzmechanismen der IT-Systeme, wie z.B. Virenscanner, können versagen. Häufig ist die Entdeckung von Fremdzugriffen einer besonderen Aufmerksamkeit eines Systemadministrators zu verdanken. In anderen Fällen können entsprechende Angriffe nur durch nachrichtendienstliche Hinweise abgewehrt werden.

Die Cyberabwehr des Verfassungsschutzes NRW informiert und sensibilisiert potentielle Opfer. Die Sensibilisierung der betroffenen Personen gegenüber dieser besonderen und nicht alltäglichen Gefahr kann helfen, Angriffe abzuwehren. Die Bereitstellung technischer Erkennungsmerkmale der Angreifer hilft Systemadministratoren, Angriffe zu erkennen und zu mitigieren. Im Jahr 2021 hat sich die Anzahl der vom Verfassungsschutz sensibilisierten Unternehmen und Institutionen gegenüber dem Vorjahr mehr als verdoppelt. Die Entwicklung spiegelt die höhere Reichweite einzelner Kampagnen wider, deren Anzahl sich gegenüber dem Vorjahr nicht wesentlich verändert hat.

Landeskriminalamt NRW (LKA NRW)

Bei der Prävention von Cybercrime wird zwischen Cybercrime im weiteren Sinn und Cybercrime im engeren Sinn unterschieden. Während die Prävention von Cybercrime im weiteren Sinn (Tatmittel Internet) vollständig in der Hand der Kreispolizeibehörde liegt, deckt das LKA NRW mit dem Cybercrime-Kompetenzzentrum den Bereich der Cybercrime-Prävention im engeren Sinn ab. Adressaten sind insbesondere Unternehmen, aber auch Behörden und vergleichbare Institutionen. Die Prävention von Cybercrime im weiteren Sinne ist vor dem Hintergrund der vielfältigen Deliktsbereiche durch intensive Kooperationen geprägt. Dabei wird das LKA NRW koordinierend tätig und setzt die

Entwicklungen in diesem Deliktsbereich in Empfehlungen und Standards um.

Im Bereich Cybercrime im engeren Sinn wird ein bewährtes Netzwerk unterschiedlichster Kooperationspartner wie dem Bitkom, dem Voice - Bundesverband der IT-Anwender und der Sicherheitspartnerschaft mit der Allianz für Sicherheit in der Wirtschaft West NRW bedient. Seit 2017 besteht eine gleichgelagerte Kooperationsvereinbarung mit dem eco - Verband der Internetwirtschaft e. V. und dem Networker NRW e. V. Dieses Netzwerk wurde im Zusammenhang mit den Herausforderungen der aktuellen Pandemie genutzt, um auf die Gefahren der sprunghaft angestiegenen Digitalisierung und die damit verbundenen Risiken aufmerksam zu machen. Insbesondere der Bereich Homeoffice und Sicherheit unternehmenskritischer Daten wurden vorangestellt.

Zudem wird durch die enge Zusammenarbeit erreicht, dass das LKA NRW unterschiedlichste Akteure als Multiplikatoren innerhalb der Wirtschaft für den Bereich Prävention von Cybercrime sensibilisiert. Durch die Beteiligung an „Round Tables“ und die Zusammenarbeit in Regionalgruppen verbessert das LKA NRW die vertrauensvolle Zusammenarbeit zwischen Wirtschaft und Polizei und steigert so die Anzeigebereitschaft und das Bewusstsein für die durch Cybercrime bestehenden Gefahren (Awareness). Die Informations- und Wissensvermittlung umfasst neben den Möglichkeiten zum Schutz vor Angriffen auch die Sensibilisierung zur Notwendigkeit der Vorbereitung auf den „Ernstfall“. Potentiell Betroffene, die sich mit geplanten Reaktionsmustern und Notfallplänen wappnen, können Angriffe deutlich besser abwehren, so dass geringere Schäden entstehen oder ganz vermieden werden können.

Durch die vorherrschenden Distanzregeln im 2. Corona Jahr wurden auch 2021 nahezu alle Kontakte via Video-Konferenztechnik realisiert. Dieser Technikeinsatz ermöglicht eine noch höhere Kontaktdichte und Reichweite und wird dauerhaft ein wichtiger Kommunikationskanal der polizeilichen Präventionsarbeit. Dabei gab es beinahe wöchentliche Veranstaltungen mit einer Teilnehmerzahl im dreistelligen Bereich.

Durch die Pandemiebedingten Kontaktreduzierungen wurde in vielen Bereichen der Arbeitsplatz in das Homeoffice verlegt. Dies hat zu einer erhöhten Risikobewertung der IT-Sicherheit geführt. Das LKA NRW hat hier bereits im Sommer 2021 reagiert und eine Handlungsempfehlung für eine Netzwerktrennung des häuslichen WLAN erstellt. Ebenso wurden die Beratungsempfehlungen in dem Kontext von Ransomware-Angriffen angepasst.

Die Bekämpfung von Cybercrime ist eine gesamtgesellschaftliche Aufgabe, bei der die Maßnahmen der polizeilichen Präventionsarbeit einen wesentlichen Beitrag leisten.

Sicherheitspartnerschaft NRW

In diesem Jahr konnte die Sicherheitspartnerschaft gegen Wirtschaftsspionage und Wirtschaftskriminalität Nordrhein-Westfalen einen runden Geburtstag „feiern“. Im Dezember 2001 gegründet, steht die Partnerschaft seit zwei Jahrzehnten für den Dialog von Sicherheitsbehörden (LKA NRW, Polizeiabteilung und Verfassungsschutz im Innenministerium) mit Vertretern der Wirtschaft (IHK NRW, Allianz für Sicherheit in der Wirtschaft West e.V. und Verband der Wirtschaftsförderungs- und Entwicklungsgesellschaften NRW) sowie dem Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie NRW. Der Wirtschaftsschutz im nordrhein-westfälischen Verfassungsschutz übernimmt dabei weiterhin die Aufgabe der Geschäftsführung.

Die Partnerschaft verfolgt insbesondere die Ziele, Schäden durch Wirtschaftsspionage, Wirtschaftskriminalität und Konkurrenzausspähung insbesondere durch Cyberangriffe zu vermeiden beziehungsweise zu reduzieren, die gegenseitige Kooperationsbereitschaft und den Informationsaustausch zu diesem Thema zu fördern und die Sensibilität der Wirtschaft hinsichtlich des entsprechenden Gefahrenpotentials zu erhöhen. Dies soll durch eine vernetzte Zusammenarbeit zwischen Wirtschaft und Staat erreicht werden. Die Partner setzen dabei auf den kontinuierlichen Austausch von Informationen, die Beratung und Unterstützung von Unternehmen, aber auch auf gemeinsame Projekte und öffentlichkeitswirksame Aktivitäten. Die Sicherheitspartnerschaft profitiert dabei von der Expertise der einzelnen Partner.

Als ein wichtiges Projekt wurde im Jahr 2021 die Fortschreibung des Lagebilds Wirtschaftsschutz in Angriff genommen. Das Lagebild wurde im Jahr 2019 erstmals erhoben und veröffentlicht. Wissenschaftlicher Partner der nordrhein-westfälischen Sicherheitspartnerschaft ist, wie schon vor zwei Jahren, die Fachhochschule des Mittelstands (FHM) mit Sitz in Bielefeld.

Präventiver Wirtschaftsschutz

Aufgrund der fortbestehenden pandemischen Situation und der damit einhergehenden Beschränkungen mussten die Mitarbeiterinnen und Mitarbeiter des Wirtschaftsschutzes 2021 weiter neue Wege beschreiten. Sie boten verschiedene Sensibilisierungsformate auch als Webinare beziehungsweise Online-Vorträge an. Auf diesem Wege konnten bis zu 280 Teilnehmerinnen und Teilnehmer gleichzeitig über die aktuelle Gefahrenlage unter anderem aufgrund von Bedrohungen aus dem Cyberraum informiert werden. Das Referat Wirtschaftsschutz beabsichtigt auch zukünftig, als Ergänzung des bisherigen Angebots, Online-Formate für Unternehmen anzubieten. Dies kann insbesondere bei dezentral organisierten Institutionen oder Unternehmen mit mehreren Firmensitzen eine vorteilhafte Variante sein. Insgesamt konnten 2021 durch Sensibilisierungsvorträge in Online- und Präsenzformaten mehr als 1.700 Personen bei rund 35 Veranstaltungen informiert und sensibilisiert werden.

Unternehmen und andere Institutionen, die an den Sensibilisierungsangeboten des Verfassungsschutzes interessiert oder Opfer von Spionage- oder Sabotageattacken geworden sind, können unter wirtschaftsschutz@im1.nrw.de Kontakt zum Wirtschaftsschutz aufnehmen. Als Inlandsnachrichtendienst obliegt der Verfassungsschutz Nordrhein-Westfalen dem Opportunitätsprinzip und kann ein Maximum an Vertraulichkeit zusichern.

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

Die Leitung der im April 2016 bei der Staatsanwaltschaft Köln eingerichteten Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) (https://www.justiz.nrw.de/JM/schwerpunkte/zac/index.php) ist nunmehr bei der Generalstaatsanwaltschaft Köln angesiedelt. Die bundesweit größte Cybercrime-Einheit der Justiz wurde nochmals personell verstärkt. Darüber hinaus wurde ihre Zuständigkeit im Jahr 2021 erweitert. Sie führt weiterhin die Ermittlungen in Fällen der herausgehobenen Cybercrime und wirkt bei regionalen und überregionalen Aus- und Fortbildungsmaßnahmen im Bereich der Cybercrime mit. Außerdem ist sie auch für Verfahren wegen besonderer Kriminalitätsphänomene im Cyberraum zuständig. Hierzu zählen insbesondere Straftaten der politisch motivierten Hasskriminalität im Internet mit besonderer Bedeutung sowie Internet-konnexe Straftaten gegen die sexuelle Selbstbestimmung von Kindern und Jugendlichen gegen noch unbekannte Täter, wenn deren Identifizierung die Auswertung einer Vielzahl gebündelter digitaler Spuren erfordert. Ihr Angebot richtet sich neben Unternehmen auch an Staatsanwaltschaften und Polizeibehörden in Nordrhein-Westfalen.

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

Das Kompetenzzentrum für Cybersicherheit in der Wirtschaft in Nordrhein-Westfalen – DIGITAL.SICHER.NRW – steht insbesonders kleinen und mittleren Unternehmen (KMU) seit 2021 mit Rat und Tat zur Seite. Ziel und Auftrag ist es, die KMU in NRW dabei zu unterstützen, die Sicherheit der eigenen digitalen Infrastruktur effizient zu erhöhen und eine gute Orientierung im Bereich der Cybersicherheit zu erlangen. Denn gerade in Zeiten rasant steigender Cyberangriffszahlen – auch auf nordrhein-westfälische KMU – und einer volatilen allgemeinen IT-Sicherheitslage ist digitale Selbstverteidigung systemrelevant für die Wirtschaft.

Nach der europaweiten Ausschreibung des Projektes durch das Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie (MWIDE) des Landes Nordrhein-Westfalen erhielt die vom eurobits e.V. Bochum und dem Cyber Security Cluster Bonn e.V. gegründete CYBERSEC-NRW gGmbH im Januar 2021 den Zuschlag für den Auftrag. Das gemeinnützige Unternehmen ist Träger von DIGITAL.SICHER.NRW. Nach der Startphase ab März 2021 wurden die beiden Standorte des Kompetenzzentrums – Bochum und Bonn – im August 2021 offiziell eröffnet.

Seitdem hat DIGITAL.SICHER.NRW verschiedene kostenlose und praxisnahe Angebote aufgebaut, die speziell auf die Bedarfe von KMU zugeschnitten sind. Dazu zählen individuelle Erstberatungen, offene digitale Sprechstunden, Webinare zu Themen rund um Fragen der digitalen Sicherheit sowie auch virtuelle Stammtische, die zum Austausch der KMU untereinander einladen. Auf der Website des Zentrums werden Informationsmaterialien, Artikel und Berichte bereitgestellt. Ziel des Zentrums ist darüber hinaus die Stärkung des Ökosystems der digitalen Sicherheit in Nordrhein-Westfalen. Unterstützt wird der Austausch und die Zusammenarbeit unterschiedlicher Stakeholder aus NRW mit verschiedenen Vernetzungsangeboten, die das Kompetenzzentrum anbietet.

DIGITAL.SICHER.NRW entwickelt einen IT-Sicherheitskompass, der einen Überblick über alle für KMU relevante Themen der IT-Sicherheit gibt und diese umsetzungsorientiert strukturiert. Ziel des Kompasses ist es, Unternehmen notwendige Maßnahmen aufzuzeigen, die durch Webinare und andere Informationsangebote vertieft werden können. Zu den einzelnen Themenbereichen erstellt das Kompetenzzentrum sukzessive Handlungsanleitungen, Flyer und Checklisten, die auch eine eigenständige Vertiefung der Themen ermöglichen. Das Modell wird zukünftig in Zusammenarbeit mit verschiedenen Expertinnen und Experten aus der Forschung und der IT-Sicherheitsbranche stetig weiterentwickelt.

Abgerundet wird das Tätigkeitsspektrum von DIGITAL.SICHER.NRW durch Kooperationen und dem Austausch mit der Wissenschaft. So wird u.a. ein KMU Cybersicherheit-Panel aufgebaut, um den laufenden Status quo sowie die Entwicklung von Bedarfen nach Cybersicherheitslösungen der KMU in NRW zu erheben und auf dieser Datenbasis effektive Maßnahmen abzuleiten.

Über aktuelle Angebote, Veranstaltungen und Neuigkeiten von DIGITAL.SICHER.NRW informiert das Kompetenzzentrum über die Website https://www.digital-sicher.nrw, einen eigenen Newsletter und über Social Media.

3.3 Kritische Infrastruktur (KRITIS)

Kritische Infrastrukturen im Visier

Das Risiko eines Angriffs wächst für die Wirtschaft, für Hochschulen und Forschungseinrichtungen sowie für die Verwaltung. Wegen der hohen Bedeutung für das gesellschaftliche Funktionieren des Gemeinwesens stellen die sogenannten Kritischen Infrastrukturen (KRITIS) eine besondere Zielkategorie für Cyberkriminelle und ausländische Nachrichtendienste dar. Unter die KRITIS-Kategorie, im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), fallen insbesondere Unternehmen und Betriebe aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Siedlungsabfallentsorgung sowie dem Finanz- und Versicherungswesen. Ein besonderes Augenmerk wird ebenfalls auf die Sektoren Staat und Verwaltung sowie Medien und Kultur gelegt. Hochindustrieländer wie die Bundesrepublik Deutschland und damit auch das einwohnerstärkste Bundesland Nordrhein-Westfalen sind im hohen Maße von der digitalen Anbindung an die übrige Welt abhängig und auf stabile Strom- und Wasserversorgungsnetze angewiesen. Für klassische Industriesparten wie beispielsweise die Stahlbranche ist dies essentiell.

Ein Übergriff auf entsprechende Netzwerke und Computeranlagen von KRITIS-Unternehmen kann neben dem wirtschaftlichen Erfolg des jeweiligen Unternehmens auch die öffentliche Sicherheit des Landes Nordrhein-Westfalen gefährden. Erfolgreiche Cyberangriffe auf Energieversorgungssysteme europäischer Länder hat es bereits gegeben und auch in Deutschland waren entsprechende Angriffe zu verzeichnen. Neben der Energiebranche ist auch mit einer Gefährdung der Wasserversorgung, der hygienischen und umweltverträglichen Ableitung von Abwasser, der Talsperrensteuerung, medizinischer Einrichtungen (wie unter anderem die Universitätskliniken des Landes) und der Telekommunikationsverbindungen zu rechnen. Ein mehrtägiger Ausfall solcher Systeme hätte schwere wirtschaftliche Schäden zur Folge, was die Sicherheit und Handlungsfähigkeit des Landes insgesamt beeinträchtigen würde.

Um die Risiken für die Wasserwirtschaft und die damit verbundene Daseinsvorsorge zu vermindern, wurde der Branchenstandard „IT-Sicherheit Wasser/Abwasser“ (B3S) zur operativen Hinterlegung der KRITIS-Anforderungen entwickelt. Ein weiteres wichtiges Präventionselement ist der unternehmensübergreifende, branchenspezifische Austausch zwischen den Unternehmen. Der Austausch richtet sich nicht nur an die KRITIS-Unternehmen, sondern ausdrücklich auch an die mehreren Tausend weiteren Wasserwirtschaftsunternehmen im Land, die im Auftrag der Kommunen rund um die Uhr leistungsfähig sein müssen. Das vom Land NRW und einigen Wasserwirtschaftsunternehmen getragene Kompetenzzentrum Digitale Wasserwirtschaft (KDW) unterstützt diesen Austausch durch zielgerichtete Veranstaltungen, die Bereitstellung von Informationsmaterial und von Konzepten, mit denen sich Präventionsangebote, Patchmanagement und nicht zuletzt auch die Kompetenzbündelung im Krisenfall unter Ausnutzung der gemeinsamen Stärke der Branche unternehmensübergreifend organisieren lassen.

Zur Verhütung größerer Störfälle stand der Verfassungsschutz auch 2021 in Kontakt mit verschiedenen KRITIS-Unternehmen und führte zusammen mit diesen Gefahrenanalysen und Sensibilisierungsveranstaltungen durch. Daneben arbeitet der Verfassungsschutz an Konzepten, mit denen sich seine Präventionsangebote maßgeschneidert für Organisationen, große Unternehmen und Konzerne planen und umsetzen lassen.

Auch die Koordinierungsstelle Cybersicherheit NRW hat Ihre Aufgaben erweitert und zum 01.04.2021 ihre Funktion als Zentrale Kontaktstelle des Landes gegenüber dem BSI (ZKL) eingenommen. In dieser Funktion verbindet sie das BSI, die KRITIS-Unternehmen, die politisch-zuständigen Aufsichten der Ressorts sowie die Strafverfolgungsbehörden des Landes miteinander, um einen schnellen und zielgerichteten Informationsaustausch zu gewährleisten. Bereits in diesem Jahr konnte die ZKL Meldungen für spezifische Sektoren oder die gesamte Landesverwaltung verteilen. Der stete Kontakt zwischen den für KRITIS zuständigen Verwaltungseinheiten wurde intensiviert und in bilateralen Workshops mit der ZKL vertieft.

Informationssicherheit innerhalb der Landesverwaltung

4.0

Die Informationssicherheit in der Landesverwaltung ist von der Cybersicherheit der Bürgerinnen und Bürger, Unternehmen und KRITIS in Nordrhein-Westfalen grundsätzlich zu unterscheiden. Unter Cybersicherheit versteht man alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik, die im Cyberraum stattfinden. Informationssicherheit hingegen 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-Abteilung 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 informationssicherheitsrelevante Vorfälle. Im Rahmen des ressortübergreifenden ISMS unterstützt das CERT NRW die Arbeit der bzw. des NRW-CISO, z. B. als Ansprechpartner in Fragen der operativen 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-CISOs der Landesverwaltung Nordrhein-Westfalens.

Weitere Teilnehmende können beratend hinzugezogen werden. Die KG InfoSic hat sich eine Geschäftsordnung gegeben, 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 2021 gingen 8763 Warn- und Informationsmeldungen vom CERT NRW an die Landesverwaltung. Es kam zu keinem erfolgreichen Ransomware-Angriff in diesem Zeitraum. Knapp 34,7 Mio. Spam-Mails wurden abgewiesen. Es wurden 7955 bekannte Schadsoftware-Systeme im Internet zentral für die Nutzer innerhalb der Landesverwaltung gesperrt. Der NRW-CISO hat 2021 zudem 68 Penetrationstest beauftragt und abgeschlossen. 2021 gab es 4 erkannte dezidierte Angriffsversuche auf die Landesverwaltung sowie 32 sonstige 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.

ABBILDUNG 4

Informationssicherheit der Landesverwaltung NRW

34,7 Mio. Spam-Mails
WURDEN ABGEWIESEN

7965
GESPERRTE SCHAD-SOFTWARE-SYSTEME

68
PENETRATIONSTESTS

4
ERKANNTE DEZIDIERTE ANGRIFFSVERSUCHE

32
SONSTIGE INFORMATIONSSICHERHEITSVORFÄLLE

Forschung und Innovation in der Cybersicherheit in Nordrhein-Westfalen

5.0

Auch im Jahr 2021 hat sich die Forschungslandschaft in Nordrhein-Westfalen rasant weiterentwickelt und im Bereich Cybersicherheit und IT-Sicherheitsforschung einige spannende Projekte sowie Studiengänge hinzugewonnen.

So hat die Hochschule Niederrhein zum Wintersemester 2020/21 am Standort Mönchengladbach den Bachelor-Studiengang „Cyber Security Management“ ins Leben gerufen. Seit dem Sommersemester 2021 wird auch ein Masterstudiengang angeboten, der den Schwerpunkt in der IT Sicherheit auf Managementaufgaben legt. Die enge Vernetzung mit dem inter- und transdisziplinären Forschungsinstitut für Informationssicherheit der Hochschule Niederrhein (Clavis) und Organisationen der IT-Sicherheit sowie problem-based Learning und anwendungsorientierte Projektarbeiten sind Kernelemente des Studienangebots.

An der Hochschule Bonn-Rhein-Sieg startete zum Wintersemester 2021/22 am Standort Sankt Augustin der Bache-lor-Studiengang „Cyber Security & Privacy“, der aus dem bereits bestehen-den Schwerpunkt IT-Sicherheit im Studiengang Informatik hervorging. Er vermittelt ein solides Wissen zu Grundlagen der Informatik und bietet ein breitgefächertes Angebot an Fachthemen aus den Bereichen Cyber Security und Schutz privater Daten. Dabei werden praxisnahe Inhalte von Professoren der Hochschule Bonn-Rhein-Sieg, Experten des BSI und dem Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) vermittelt.

Um die Führungsstellung des Forschungsstandortes NRW im Bereich IT-Sicherheit beizubehalten und auszubauen, ist die Förderung von jungen Forschenden eine essentielle Aufgabe, der sich das Land NRW gerne annimmt. So ist zum Beispiel das bereits letztes Jahr beschriebene Graduiertenkolleg NERD - North Rhine Westphalian Experts in Research on Digitalization eine Institution, die eine aktive Nachwuchsförderung an Universitäten und Hochschulen in diesem Bereich fördert. Beispielhaft ist hier zu nennen, dass im März des kommenden Jahres die zweite Kohorte mit weiteren 10 standortübergreifenden Promotionen starten wird. Die Doktorandinnen und Doktoranden werden etwa zur Sicherheit von Videokonferenzsystemen und E-Mail-Programmen, zur digitalen Sicherheit in Krankenhäusern oder an der Entwicklung von interaktiven Lernangeboten zur Sensibilisierung und Förderung sicheren Onlineverhaltens von Schülerinnen und Schülern forschen.

Umsetzungsstand der Cybersicherheitsstrategie

6.0

Parallel zum letztjährigen Bericht wurde ebenfalls die Cybersicherheitsstrategie des Landes Nordrhein-Westfalen veröffentlicht. Um das Ziel „gemeinsam mit allen gesellschaftlichen Akteuren das Cybersicherheitsniveau in und für Nordrhein-Westfalen zu verbessern“ zu erfüllen, hat die Landesregierung eine umfassende Strategie erarbeitet, die für 3 Jahre die Richtung der cybersicherheitstechnischen Entwicklungen des Landes vorgibt. Um über den Umsetzungsstand der Strategie und den darin beschriebenen Maßnahmen zu informieren, wird in diesem und den folgenden Berichten zur Cybersicherheit in Nordrhein-Westfalen über den Fortschritt dieser berichtet.

Im Jahre 2021 wurde der Grundstein für den zukünftigen #CyberCheckNRW gesetzt. Durch die Koordinierungsstelle Cybersicherheit NRW wurde eine Expertise in Auftrag gegeben, mit der die Cybersicherheits-Basiskompetenzen zu ermitteln sind, die erwachsene Menschen in einer vernetzten, digitalen Welt benötigen, um souverän mit den Anforderungen von Cybersicherheit umgehen zu können. Die Ergebnisse aus dieser Expertise werden verwendet, um den #CyberCheckNRW zu entwickeln.

Als weiterer Erfolg der Cybersicherheitsstrategie ist die Initiierung von Interministeriellen Austauschgremien im Bereich der Cybersicherheit zu nennen. So wurden der Strategische sowie der Operative Austausch Cybersicherheit (SAC/OAC) initiiert. Bestehend aus Vertretern des LKA, der Zentralen Ansprechstelle Cybercrime der Staatanwaltschaft Köln (ZAC), des Wirtschaftsschutzes und der Cyberabwehr des Verfassungsschutzes NRW, der Abteilung Polizei des Innenministeriums NRW, der Koordinierungsstelle Cybersicherheit sowie dem NRW CISO, tagt der OAC alle zwei Wochen, um aktuelle und konkret fallbezogene Themen im Bereich Cybersicherheit zu besprechen. Der SAC, bei dem neben den Teilnehmern des OAC auch Vertreter des Wirtschaftsministeriums sowie von DIGITAL.SICHER.NRW teilnehmen, beschäftigt sich quartalsmäßig mit übergreifenden Themen der Cybersicherheit. Die so gewährte, engmaschige Vernetzung der wesentlichen Akteure der Landesverwaltung stellt sicher, dass Doppelstrukturen vermieden, noch effizientere Kommunikationskanäle etabliert und die interministerielle Zusammenarbeit erleichtert werden kann.

Um die Kapazitäten der vorhandenen Referenten des LKA NRW, des Wirtschaftsschutzes, ZAC NRW, des CERT und weiterer Institutionen effektiver nutzen zu können, wurde der in der Strategie angekündigte Referenten-Pool ins Leben gerufen. Die Koordinierungsstelle Cybersicherheit hat die verfügbaren Referenten der verschiedenen Institutionen sowie die von ihnen abgedeckten Themen in einer dynamischen Liste gesammelt und verwaltet diese zentral. So können Anfragen bei Bedarf dynamisch und zielgruppenspezifisch, über die Koordinierungsstelle, an einen adäquaten Ersatz weitervermittelt werden. Durch den Referenten-Pool kann die Expertise, die in der Landesverwaltung vorhanden ist, effizienter und einfacher an die Unternehmen in NRW transportiert werden.Wie bereits im Kapitel 3.3 beschrieben, konnte die Koordinierungsstelle um die Zentrale Kontaktstelle des Landes gegenüber dem BSI verstetigt werden. Die ZKL hat in einem ersten Schritt die Kommunikation zum Bund weiter ausgebaut und den Informationsfluss auf der Bund-Länder-Ebene verbessert. Weitergehend wird nun das Augenmerk auf der Arbeit mit den einzelnen Ministerien liegen.

Ausblick

7.0

Das Jahr 2021 war aus dem Blickwinkel der Cybersicherheit eines, in dem das Land Nordrhein-Westfalen gefordert war, sich agil an aktuelle Entwicklungen anzupassen. Die anhaltende Pandemie führte zu einer vermehrten Verschiebung des Alltags in den digitalen Raum. Die damit einhergehende Verlagerung von Straftaten in die virtuelle Welt sowie technologische Innovationen haben viele Menschen in puncto Cybersicherheit in Atem gehalten. Wieder einmal zeigt es sich, dass dieses Themengebiet ein sich rapide veränderndes ist, bei dem Errungenschaften aus einem Jahr, im nächsten bereits wieder überholt sein können. Aus diesem Grund wird auch die Landesverwaltung sich nicht auf dem in diesem Jahr erreichten ausruhen, sondern auch im Jahr 2022 den Kampf für mehr Cybersicherheit in Nordrhein-Westfalen weiterführen.

So wird zum Beispiel das Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie im Jahr 2022, gemeinsam mit dem Kompetenzzentrum DIGITAL. SICHER.NRW, Spitzenvertreterinnen und -vertreter maßgeblicher Wirtschaftsverbände, Wirtschaftsförderungen und anderen Multiplikatoren aus NRW halbjährlich zu einem Gespräch einladen. Ziel ist es, den Austausch der Stakeholder untereinander zu fördern und die Weiterentwicklung des Ökosystems der digitalen Sicherheit in NRW zu unterstützen.

Der Austausch mit Kooperationspartnern und anderen Initiativen erfolgt ebenfalls durch die Teilnahme an Fachmessen wie der it-sa in Nürnberg, Industriemessen wie der Hannover-Messe sowie auch regionalen Messen in NRW. Um weniger digital-affine Unternehmen auch in der Fläche NRWs zu erreichen, werden mit den Multiplikatoren regionale Kooperationsveranstaltungen angeboten.

Außerdem wird die Koordinierungsstelle Cybersicherheit weitere Informationsangebote für die verschiedenen Zielgruppen erstellen. Ebenso wird die Teilnahme an verschiedenen Präsenzveranstaltungen wie Messen und Vorträgen geplant. Die Website der Koordinierungsstelle Cybersicherheit „Cybersicherheit.nrw“ wird darüber hinaus ausgebaut und weiterentwickelt. Der Onlineauftritt wird um zusätzliche Informationen ergänzt.

Die mit dem Angriffskrieg Russlands auf die Ukraine einhergehenden Auswirkungen auf die Cybersicherheit im globalen Sinne wie auch speziell auf Nordrhein-Westfalen werden im kommenden Bericht für das Jahr 2022 aufgearbeitet.

Der Themenbereich der Hybriden Bedrohungen wurde im vorliegenden Bericht bereits aufgegriffen. Diese Art der Bedrohung ist kein neues Phänomen. Speziell im Angriffskrieg Russlands auf die Ukraine lässt es sich jedoch vermehrt beobachten. Da anzunehmen ist, dass Hybride Bedrohungen aufgrund der im Bericht beschriebenen technologischen Entwicklungen und der zunehmenden

digitalen Vernetzung der Welt in Zukunft weiterhin für Angriffe genutzt werden, wird der kommende Bericht das Thema vertieft behandeln.

Insgesamt wird die Cybersicherheitslandschaft - auch in NRW - zunehmend komplexer auf den verschiedensten Ebenen: Es existiert eine Vielzahl an Informationsangeboten zum Thema Cybersicherheit, die Auswahl an Softwareunternehmen und deren Produkte zum Thema Sicherheit ist kaum zu überblicken und auch in Wissenschaft und Forschung zeigt sich das Thema Cybersicherheit in den verschiedensten Facetten. Dabei geht jegliche Nutzung von Technologie einher mit der Verantwortung Sicherheit mitzudenken. Vor dem Hintergrund der Informationsflut bei zunehmender Verantwortung jedes Einzelnen wird es in Zukunft notwendig, Sicherheit benutzerfreundlich zu gestalten - Usable Security oder auch Human-Centered Security beschreiben wissenschaftliche Disziplinen, die sich damit befassen, z.B. dem Nutzer zu erleichtern, Software sicher zu nutzen - sei es durch benutzerfreundliche Softwaregestaltung oder durch die Verbesserung der digitalen Kompetenzen der Nutzer.

Auch auf europäischer Ebene ist Cybersicherheit ein viel diskutiertes Thema. Insbesondere mit dem zurzeit verhandelten Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2), die die derzeitige Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) ersetzen soll. Diese zielt darauf ab, einen gemeinsamen Standard für das Cybersicherheitsniveau aller EU-Mitgliedsstaaten zu etablieren. Nach Beschluss durch das Europäische Parlament und den Europäischen Rat, ist es an den Ländern, die in der Richtlinie erarbeiteten Vorgaben in nationales Recht umzusetzen. Die sich aus diesem Prozess ergebenden, neuen Sicherheitsstandards und Vorschriften werden in den kommenden Berichten zur Cybersicherheit in Nordrhein-Westfalen aufgegriffen werden.

Die in diesem Bericht aggregierten Informationsangebote und ihre zielgruppenspezifische Aufbereitung tragen dazu bei, das Cybersicherheitsniveau in Nordrhein-Westfalen zu erhöhen. Eine vollständige Sicherheit ist gerade im Bereich der Cybersicherheit nicht zu gewährleisten. Daher wird die Landesregierung, im Zusammenspiel mit allen gesellschaftlichen Akteuren, auch in den kommenden Jahren weiter daran arbeiten, den digitalen Raum Stück für Stück sicherer zu machen.

Informationsangebote

Informationsangebote **für Bürgerinnen und Bürger**

Allgemeine Informationsangebote	Kontakt
Beratungsplattform ZEBRA	https://www.fragzebra.de/ E-Mail: info@medienanstalt-nrw.de Telefon: 0211 77007-0
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
#DigitalCheck NRW	https://www.digitalcheck.nrw/ E-Mail: digitalcheck@medienpaed.de
Digital in NRW	https://www.digital-in-nrw.de/de/ E-Mail: info@digital-in-nrw.de Telefon: 0231 9743611
#einfachaBSIchern	https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/kampagne_node.html
Eltern und Medien	https://www.elternundmedien.de/ E-Mail: elternundmedien@medienanstalt-nrw.de Telefon: 0211 77007-140
Fakeshop-Finder	https://www.verbraucherzentrale.de/fakeshopfinder-71560
Informationsportal Ransomware	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe.html
Koordinierungsstelle Cybersicherheit NRW	https://www.cybersicherheit.nrw
Landeskriminalamt Nordrhein-Westfalen (LKA NRW)	https://lka.polizei.nrw/
Medienscouts	https://www.medienscouts-nrw.de/ E-Mail: imedienscouts@medienscouts-nrw.de Telefon: 0211 77007-164
Phishing-Radar	https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnu
Polizei-Beratung	https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/

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
Informationsportal Ransomware	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe.html
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
Informationsportal Ransomware	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe.html
IT-Sicherheitsgesetz	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=7
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
KRITIS Verordnung	https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf
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/

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 Informations-logistik (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 Sicherheits-beratung an.

Cyber Campus Nordrhein-Westfalen

Neben innovativen Konzepten in der gemeinsamen Ausbildung und Qualifizie-rung 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 Nord-rhein-Westfalen“ der Hochschule Bonn-Rhein-Sieg und der Hochschule Niederrhein genannt, die mit dem Wintersemester 2020/2021 erstmalig Studiengänge zu den Themen Cyber-sicherheit, 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 Entwicklungs-methoden sind. Ziel ist es, diese Metho-dik 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

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 35, 39, 47: © greenbutterfly – stock.adobe.com
Seite 59: © monsitj – stock.adobe.com

Layout:
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.

Die Landesregierung
Nordrhein-Westfalen

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