Anhang II. Management Summary einer Best Practice Analyse der Cybersicherheitsarchitektur in Nordrhein-Westfahlen, Hessen und Sachsen

Durch die fortschreitende Digitalisierung sowie die aktuelle Bedrohungs- und Gefährdungslage im Cyberraum ist Cyber- und Informationssicherheit ein relevantes Thema für Bundes- und Landesregierungen, das zudem durch zahlreiche regulatorische Vorgaben u. a. aus der Europäischen Union in den Fokus gerückt wird. Dabei verfolgen die Länder oft unterschiedliche Ansätze, die ihren aktuellen Entwicklungsstand im Bereich Cybersicherheit sowie die Besonderheiten des jeweiligen Landes, beispielsweise hinsichtlich der Cybersicherheitsarchitektur, widerspiegeln. **Die im Rahmen der Erstellung der Cybersicherheitsstrategie für das Land Brandenburg durchgeführte Best-Practice-Analyse vergleicht in einem ersten Teil die Cybersicherheitsstrategien dreier ausgewählter Länder, Nordrhein-Westfalen (NRW), Hessen und Sachsen sowie in einem zweiten Teil politische, organisatorische und technische Maßnahmen, die in den drei Fallländern im Bereich Cybersicherheit angewendet werden, um Erkenntnisse für die Weiterentwicklung der Cybersicherheit in Brandenburg abzuleiten.**

Die Länder wurden ausgewählt, da sowohl Nordrhein-Westfalen als auch Hessen eine Vorreiterrolle in der Cybersicherheitspolitik auf Länderebene einnehmen. NRW war das erste Land, welches eine vollumfängliche Cybersicherheitsstrategie veröffentlicht hat. Hessen veröffentlichte ebenfalls eine Strategie und baute zudem in den letzten Jahren umfassende Kapazitäten in dem Bereich Cyber- und Informationssicherheit auf. So wurde beispielsweise mit dem Hessen CyberCompetenceCenter (Hessen3C)[1] eine zentrale Organisation gegründet, die die Cybersicherheitskapazitäten seither auf Landesebene bündelt.

Auch die sächsische Cybersicherheitsarchitektur ist weit vorangeschritten und wurde auch aufgrund seiner regionalen Beziehung zu Brandenburg ebenfalls analysiert. Das Land Sachsen kann eine Vielzahl staatlicher Akteure aufweisen, die im Bereich Cybersicherheit verortet und auf Bundes- und Landesebene stark vernetzt sind. Zudem hat Sachsen bereits ein IT-Sicherheitsgesetz beschlossen.

Konkret wurden deshalb im ersten Teil der hier vorliegenden Best Practice-Analyse die **Cybersicherheitsstrategien** von NRW und Hessen sowie das **Gesetz** zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (SächsISichG) untersucht. Ziel war es, Best-Practices für die Weiterentwicklung der Cybersicherheitsarchitektur im Land Brandenburg zu extrahieren.

Die Analyse der Strategiedokumente wurde anhand der folgenden sieben Kategorien durchgeführt:

- Bund-Länder Koordination;
- Horizontale Koordination auf Landesebene;
- Strukturen des Krisenmanagements und der Krisenkommunikation;
- Lagebild und Meldewege;
- Schulungen und Übungen;
- Wirtschaft, Wissenschaft und Gesellschaft als Partner;
- Gesetzgebung zur Bekämpfung von Cyber-Crime, -Spionage und -Sabotage.

[1] https://hessen3c.de/

Die sieben Kategorien basieren auf einer Studie zu nationalen Cybersicherheitsstrategien des Center for Security Studies der Eidgenössische Technische Hochschule Zürich[2] (CSS) und wurden für die Anwendung auf Länderebene in Deutschland angepasst. Eine achte Kategorie zur internationalen Kooperation wurde zudem aufgrund des ausschließlich internationalen Bezugs aus der Analyse herausgenommen. Alle sieben Kategorien konnten auf die Cybersicherheitsstrategien NRWs sowie Hessens angewendet werden. Da das sächsische Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen aufgrund seiner Natur als legislatives Dokument keine strategischen Ziele und entsprechende Maßnahmen listet, konnte Sachsen als Fallbeispiel in den Kategorien „Krisenmanagement", „Meldewesen" und „Wirtschaft, Wissenschaft und Gesellschaft als Partner" nicht berücksichtigt werden.

Im zweiten Teil der Best Practice-Analyse wurde eine Auswahl von weiteren politischen, organisatorischen und technischen Maßnahmen im Bereich Cybersicherheit unabhängig von den jeweiligen genannten Dokumenten der Länder identifiziert und kurz bewertet. Die zentralen Erkenntnisse aus beiden Teilen der Analyse stellen sich wie folgt dar:

Teil 1: Analyse strategischer und legislativer Dokumente im Bereich Cybersicherheit

Bund-Länder Koordination

Die erste Kategorie betrachtet die Bund-Länder-Zusammenarbeit. In ihren jeweiligen Strategien präsentieren sich sowohl NRW als auch Hessen als stark vernetzte Akteure auf der Bundesebene. Sachsen strebt ebenfalls eine verstärkte Vernetzung an.

Sowohl NRW als auch Hessen formulieren in ihren Cybersicherheitsstrategien das Ziel, die Interessen ihres Landes in den Gesetzgebungsverfahren des Bundes zu vertreten, um aktiv die Landesinteressen sowie die Interessen der im Land ansässigen Wirtschaftszweige einzubringen. Darüber hinaus streben alle drei Länder eine enge Zusammenarbeit mit dem Bund auf operativer Ebene an. Besondere Aufmerksamkeit gilt dabei dem BSI, das eine zentrale Rolle in den Bemühungen der untersuchten Länder spielt (z. B. in Bezug auf die allgemeine Zusammenarbeit, Unterstützung bei IT-Sicherheitsvorfällen, Sensibilisierung und gemeinsame Übungen). Die Zusammenarbeit wird durch Kooperationsvereinbarungen mit dem BSI auf Bundesebene und den zentralen Ansprechstellen auf Landesebene institutionalisiert (beispielsweise die Zentral- und Ansprechstelle Cybercrime in NRW und das Hessen3C). Die Teilnahme am zentralen deutschen Cyber-Abwehrzentrum zeigt ebenfalls die starke Vernetzung von Hessen und NRW auf Bundesebene.

Im Vergleich zu Hessen oder NRW fehlt es in Brandenburg noch an einer vergleichbaren zentralen Stelle für Cybersicherheit mit ausreichenden Kapazitäten, die dann die Interessen des Landes auf Bundesebene noch effektiver vertreten und die Kommunikation in und aus dem Land steuern könnte.

Horizontale Koordination auf Landesebene

Die zweite untersuchte Kategorie analysiert die Koordinationsmuster innerhalb der Ministerial- oder Vollzugsverwaltung der Länder mit dem Ziel einer effektiven und effizienten Umsetzung von politischen Maßnahmen im Bereich der Cyber- und Informationssicherheit. Hier haben Hessen und NRW jeweils einen Interministeriellen Ausschuss Cybersicherheit gegründet, um so eine ressortübergreifende Abstimmung auf politisch-strategischer Ebene zu gewährleisten. Diese Ausschüsse werden in beiden Ländern von einer zentralen Steuerungsinstanz unterstützt.

[2] Baezner, Cordey: Nationale Cybersicherheitsstrategien im Vergleich – Herausforderungen für die Schweiz; Center for Security Studies (CSS), ETH Zürich. 2019.

In NRW bündelt die Koordinierungsstelle Cybersicherheit den Informationsfluss hinsichtlich cybersicherheitsrelevanter Themen, während in Hessen das Hessen3C auch operative Elemente wie das Landes-CERT oder die Erstellung des landesweiten Lagebilds aus einer Hand führt. NRW hat hierbei einen kooperativen Ansatz gewählt und spezifische Koordinationsplattformen (KoSt NRW; IMA) geschaffen, um die Vielzahl der Akteure im Bereich Cybersicherheit auf Landesebene zu koordinieren. Im Gegensatz dazu verfolgt Hessen einen eher zentralisierten Ansatz und hat mit dem Hessen3C eine Organisation etabliert, die zahlreiche staatliche Aufgaben im Bereich Cybersicherheit an einer Stelle bündelt.

Sachsen verfügt nach öffentlich zugänglichen Informationen weder über einen interministeriellen Ausschuss noch über eine zentrale Koordinationsinstanz, jedoch existiert eine Arbeitsgruppe Informationssicherheit, die dem Informationssicherheitsbeauftragten aus den Ressorts zuarbeitet und somit der aktuellen Cybersicherheitsarchitektur in Brandenburg ähnelt.

Für Brandenburg wurde daraus abgeleitet die Notwendigkeit erkannt, die Koordination und Kommunikation zwischen den Akteuren auf Landesebene hinsichtlich ihrer Effektivität und Effizienz zu verbessern. Die Einrichtung einer Koordinierungsstelle für Cybersicherheit stellt eine Praxis anderer Länder dar, an der sich Brandenburg nach entsprechender Prüfung orientieren kann. Durch die Schaffung einer Koordinierungsstelle könnte Brandenburg den Kommunikations- und Koordinationsaufwand für die im Bereich Cyber- und Informtionssicherheit beteiligten Akteure sowohl auf politisch-strategischer als auch auf operativer Ebene senken.

Strukturen des Krisenmanagements und der Krisenkommunikation

Die dritte Kategorie betrachtet den Aufbau klarer und effizienter Strukturen für die Krisenkommunikation und die Entwicklung ausreichender Kapazitäten für die Reaktion auf Cybervorfälle.

Die Cybersicherheitsstrategien von NRW und Hessen bieten nur wenige Details zum Krisenmanagement der jeweiligen Länder. NRW betrachtet Cybersicherheit als wichtige Voraussetzung einer zuverlässigen Krisenbewältigung und verweist auf das VIDAL-Projekt[3]. Das Projekt bildet Informationen von der kleinsten Kommune bis hin zum Krisenstab des Landes ab und stellt den Verantwortlichen sichere und zuverlässige Kommunikationskanäle bereit. Hessen strebt ein landesweites Business-Continuity-Management nach dem BSI Standard 200-4 an, welches auch den Ausfall von IT-Systemen abdeckt. Gegenwärtig wird das BCM durch das kommunale Dienstleistungszentrum (eKom21) und das Hessische Cyberabwehrausbildungszentrum Land/Kommune (HECAAZ L/K) auf kommunale Einrichtungen ausgeweitet. Dies schließt auch die Vorbereitung auf Ausfälle von kritischen Infrastrukturen ein, wobei perspektivisch auch der hessische Katastrophenschutz unterstützend tätig werden könnte.

Die Notwendigkeit, auf Cybersicherheitsvorfälle adäquat reagieren zu können und die Vorbereitung sowie Koordinierung von entsprechenden Schutzmaßnahmen für den Ernstfall wurde auch in Brandenburg als Handlungsbedarf identifiziert. Die Etablierung eines umfassenden Notfall- bzw. Business-Continuity-Managements ist auch für das Land Brandenburg eine realisierbare und wichtige Option. Ebenso sollte eine ständige Kooperationsplattform mit den Behörden des Katastrophenschutzes etabliert werden, um im Ernstfall auf belastbare Strukturen zurückgreifen zu können.

[3] Das Projekt VIDaL (Vernetzung von Informationen zur Darstellung der Landeslage) soll unterschiedliche Leitstellensysteme, Lagedarstellungssysteme und andere Anwendungen so vernetzen, dass die dort gehaltenen lagerelevanten Informationen zwischen allen Akteuren problemlos ausgetauscht werden können. Kernstück des Projekts ist die Entwicklung der dafür benötigten Schnittstelle und ihre Erprobung. Mehr Informationen unter https://pmev.de/themen/fachbereich-leitstellen/vidal/

Lagebild und Meldewege

Die vierte Kategorie fokussiert sich auf Strategien und Maßnahmen zur Aufrechterhaltung einer kontinuierlichen, ganzeinheitlichen und detaillierten Lageanalyse mit Risikobeurteilung für die eigenen IT-Systeme und Prozesse sowie die Sicherstellung effizienter und effektiver Informationsflüsse im Land.

Die Landesverwaltung in NRW strebt danach, die allgemeine Informationslage zu Cyberbedrohungen zu verbessern und forciert dabei die Einbindung wissenschaftlicher Akteure sowie eine stärkere Vernetzung von Unternehmen und Sicherheitsbehörden. Außerdem strebt NRW an, möglichst viele (öffentlich nicht näher definierte) Datenquellen innerhalb und außerhalb der Verwaltung für das Cybersicherheitslagebild nutzbar zu machen. Federführend ist hierbei die Koordinierungsstelle Cybersicherheit NRW. In Hessen ist das Hessen3C als zentrale Koordinierungsstelle für Cyber- und Informationssicherheit verantwortlich für die Erstellung und Kommunikation von anlassbezogenen und regelmäßigen Lageberichten mit Einrichtungen der Landesverwaltung, Kommunen sowie hessischen Unternehmen. Alle gewonnenen Erkenntnisse und Entwicklungen fließen in Beratungs- und Awareness-Veranstaltungen des Hessen3C ein. Mit wenigen Ausnahmen sind in Hessen alle öffentlichen und nichtöffentlichen Stellen, die hoheitliche Aufgaben wahrnehmen, dazu verpflichtet, IT-Sicherheitsvorfälle an das Hessen3C zu melden. Perspektivisch möchte Hessen das Lagebild zu einem vollautomatisierten, landesweiten Lagebild weiterentwickeln und hierfür ggf. auch rechtliche Rahmenbedingungen anpassen.

Die CERTs aller drei untersuchten Länder, NRW, Hessen und Sachsen, geben regelmäßige Warnungen an die Landesverwaltung heraus. Sowohl in NRW als auch in Hessen sind die Kommunen bereits an das System angeschlossen, wobei NRW noch daran arbeitet, einen Kommunikationsweg von den Kommunen zum CERT hin aufzubauen (Kenntnisstand zum Zeitpunkt der Veröffentlichung der Strategie im Dezember 2021). Zudem prüfen beide Länder die Möglichkeit, kritische Infrastruktur-Betreiber in ihr Warnsystem einzubeziehen.

Eine Erfassung, Bewertung und Zusammenführung von Informationen im Rahmen eines landesweiten Lagebilds wird gegenwärtig in Brandenburg noch nicht vollumfänglich vorgenommen. Ähnlich wie in NRW und Hessen könnte die Etablierung einer gut vernetzten, zentralen koordinierenden Stelle für Cyber- und Informationssicherheit dazu beitragen, die Effektivität und Effizienz der Lageanalyse, die Klarheit der Meldewege sowie der Informationsflüsse im Land zu verbessern.

Schulungen und Übungen

Die fünfte Kategorie betrachtet den Aufbau von personellen Kapazitäten und die Bereitstellung relevanter Bildungsangebote und Informationen im Kontext von Cyber- und Informationssicherheit, um die eigenen Mitarbeiter und Mitarbeiterinnen sowie relevante Zielgruppen wie Unternehmen und Bürger des betreffenden Landes auf die Bedeutung von Cybersicherheit aufmerksam zu machen sowie sie zur Umsetzung von Cybersicherheitsmaßnahmen zu schulen.

Zur Förderung der Awareness für Cybersicherheit bieten Hessen, Nordrhein-Westfalen und Sachsen landesweite Schulungsangebote für alle Beschäftigten der Landesverwaltung an. In Hessen sind IT-Sicherheitsschulungen verpflichtend. Hessen und NRW haben kommunale Beschäftigte in Schulungsangebote aufgenommen und planen außerdem, Mitarbeiterinnen und Mitarbeitern von kritischen Infrastrukturen (KRITIS) ebenfalls aufzunehmen. Im Gegensatz dazu ist das E-Learning-Angebot in Sachsen ausschließlich für Landesbedienstete zugänglich. Hessen plant darüber hinaus, die Beteiligung an der LÜKEX zu intensivieren und eine eigene Cybersicherheitsübung zu etablieren. NRW und Sachsen nehmen ebenfalls an der LÜKEX teil.

Auch in Brandenburg ist die Information und Sensibilisierung relevanter Zielgruppen sowie die Weitergabe konkreter Handlungsempfehlungen im Bereich Cybersicherheit eine Aufgabe, die ausgeweitet werden muss, um das Cybersicherheitsniveau des Landes weiter zu erhöhen. Brandenburg könnte so beispielsweise ein umfassendes landesweites Schulungssystem einführen, um bei Mitarbeiterinnen und Mitarbeitern der Landesverwaltung fundierte Expertise und Bewusstsein für das Thema Cybersicherheit zu entwickeln und zu fördern. Zusätzlich wurde der Handlungsbedarf identifiziert, behördenübergreifende Zusammenarbeit zwischen mit Cyber- und Informationssicherheit betrauten Stellen auf Landes- und Kommunalebene im Fall eines IT-Sicherheitsvorfalls praktisch zu üben. Hier können insbesondere NRW und Hessen als positive Beispiele herangezogen werden.

Wirtschaft, Wissenschaft und Gesellschaft als Partner

Diese Kategorie umfasst Maßnahmen, die die Zusammenarbeit der Verwaltung mit der Wirtschaft, der Gesellschaft und der Wissenschaft betreffen. Dies ist wichtig, da ein wesentlicher Teil der Umsetzungslast von Cybersicherheitsvorschriften im privaten Sektor liegt, beispielsweise bei der Umsetzung der NIS-2-Richtlinie. Verwaltungen können außerdem von Expertise aus dem privaten Sektor, der Wissenschaft und der Gesellschaft profitieren.

NRW hat mit der DIGITAL.SICHER.NRW ein gesondertes Kompetenzzentrum zur Unterstützung und Kooperation mit der Wirtschaft gegründet. Diese bietet kostenlose Beratungs- und Unterstützungsleistungen für kleine und mittlere Unternehmen (KMU) an und unterstützt diese bei der Netzwerkarbeit zu Akteuren der NRW Cybersicherheitsarchitektur als auch Akteuren auf der Bundesebene. Außerdem setzt NRW einen Fokus auf die ansässigen Hochschulen und Forschungseinrichtungen, vor allem zur Ausbildung von IT-Fachkräften.

In Hessen nimmt das Hessen3C eine ähnliche Rolle ein und unterstützt sowohl KMU als auch Sektor spezifische Vorhaben, um das Cybersicherheitsniveau der hessischen Wirtschaft zu erhöhen. Außerdem besteht eine Kooperation mit der Koordinierungsstelle KRITIS (KoSt KRITIS). Hessen hat ferner eine Förderrichtlinie zur Cybersicherheitsforschung in Hessen[4] verabschiedet, mithilfe derer Forschungsergebnisse aus dem Bereich Cybersicherheit generiert und allgemein verfügbar und nutzbar gemacht werden sollen.

Im Bereich KRITIS betonen sowohl NRW als auch Hessen die hohe Bedeutung, die die kritischen Infrastrukturen und deren Schutz haben. Beide Länder gehen dabei über die Definition des Bundes nach der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) hinaus und erfassen und unterstützen auch Betreiber, die nach EU- bzw. Bundesgesetzgebung unterhalb der Schwellenwerte angesiedelt sind, aber trotzdem eine wichtige Rolle für die lokale Daseinsvorsorge spielen. NRW und Hessen betonen die Zusammenarbeit zwischen ihren Zentralstellen für Cybersicherheit und den Kontaktstellen für KRITIS und formulieren das Ziel, die allgemeine Netzwerkarbeit mit und zwischen den KRITIS-Betreibern zu unterstützen und zu fördern. In diesem Kontext erwähnen sie beispielsweise die Netzwerkarbeit im UP-KRITIS. Hessen will sich dabei explizit nicht auf den Schutz der IT-Systeme von KRITIS beschränken, sondern auch physische Sicherheit betrachten und einen holistischen „All-Gefahren-Ansatz“ verfolgen.

Auch in Brandenburg kann die Effektivität und Effizienz der Kommunikation und Zusammenarbeit der Cybersicherheitsakteure im Land Brandenburg weiter verbessert werden. Die beschriebenen Maßnahmen NRWs und Hessens zur Verbesserung des Austausches zwischen der Landesverwaltung und privaten sowie wissenschaftlichen Akteuren können als *Good Practice* dienen, um flächendeckend Anreize für die Verbes-

[4] Microsoft Word - 2020_Förderrichtlinie Cybersicherheitsforschung_final.docx (hessen.de)

serung der Cybersicherheit bei privaten Akteuren zu setzen. Ferner könnte die Etablierung und Zusammenarbeit einer für Cybersicherheit zuständigen zentralen Stelle auf Landesebene sowie einer zentralen Organisationseinheit für kritische Infrastrukturen von der Landesverwaltung Brandenburgs geprüft werden, um einen entsprechenden Informations- und Erfahrungsaustausch zu fördern. Zudem könnte die Verwaltung Brandenburgs die Netzwerkarbeit der ansässigen KRITIS-Betreiber untereinander und mit Betreibern anderer Länder im UP-KRTIS durch entsprechende Maßnahmen weiter verbessern.

Gesetzgebung zur Bekämpfung von Cyber-Crime, -Spionage und -Sabotage

Die siebte und letzte Kategorie zielt darauf ab, den Bedarf eines Landes zu erfassen, die landesspezifische Gesetzgebung zu harmonisieren und etwaige Rechtslücken zu schließen. Ein spezielles Augenmerk liegt dabei auf den rechtlichen Rahmenbedingungen für die Tätigkeit traditioneller Sicherheitsbehörden, die mit der Prävention, Aufklärung und Verfolgung von Cyberspionage, -sabotage und -kriminalität betraut sind.

Die Abwehr von Cyberkriminalität, -sabotage und -spionage ist von einem ausgeprägten Netzwerkcharakter geprägt, der eine enge Koordination zwischen den Landesverfassungsschutzbehörden, Polizeibehörden, CERTs und dem Chief Information Security Officer (CISO) erfordert. Diese Koordination erfolgt über verschiedene Kooperationsplattformen. Hessen hat in seinem IT-Sicherheitsgesetz klare Richtlinien festgelegt, welche Daten von Sicherheitsbehörden mit dem Hessen3C-System geteilt werden dürfen und zu welchen Zwecken. Ebenso hat Sachsen in seinem IT-Sicherheitsgesetz die Erhebung und den Austausch von Daten geregelt.

In Brandenburg fehlt es aktuell noch an einer umfassenden landesrechtlichen Grundlage für Cyber- und Informationssicherheit in Form eines Landes IT-Sicherheitsgesetzes. Dieses könnte dazu beitragen, gesetzlich die Cybersicherheitsarchitektur in Brandenburg weiter zu stärken. Teil eines solchen Gesetzes sollte es auch in Brandenburg sein, Aufgaben und Befugnisse zentraler staatlicher Akteure im Bereich Cyber- und Informationssicherheit festzulegen. So kann die Rechtssicherheit für alle Mitarbeiter und Mitarbeiterinnen des Landes gestärkt werden. Ein besonderes Augenmerk sollte auf dem Datenaustausch zwischen der geplanten Koordinationsstelle für Cyber- und Informationssicherheit, dem Landes-CERT sowie den Polizei-, Verfassungsschutz- und Katastrophenschutzbehörden liegen. Eine solche gesetzliche Verankerung würde die Effektivität und Effizienz der Zusammenarbeit dieser Organisationen erhöhen und damit die Resilienz des Landes gegenüber Cyberbedrohungen stärken.

Teil 2: Analyse technischer, organisatorischer und politischer Maßnahmen

Im zweiten Teil der Best Practice Analyse wurden weitere politische, organisatorische und technische Maßnahmen der ausgewählten Länder untersucht, die zum Ziel haben, das allgemeine Cybersicherheitsniveau des betreffenden Landes zu verbessern, nicht aber in den jeweiligen Cybersicherheitsstrategien enthalten sind. Dieser zweite Analyse-Teil flankiert die Analyse der Dokumente im ersten Teil und soll ergänzende Informationen als Grundlage zur Erstellung der Cybersicherheitsstrategie Brandenburgs bieten.

Die betreffenden Maßnahmen wurden durch eine offene Internetrecherche identifiziert. Zur besseren Übersicht wurden die Maßnahmen in 12 Kategorien unterteilt, die aus einer Studie der Stiftung Neue Verantwortung und der Konrad-Adenauer-Stiftung abgeleitet wurden[5]. Diese Kategorien umfassen: Vorfallsbearbeitung, Bewertung/Evaluation, Warn- und Informationsdienst, Orientierungshilfen, Veranstaltungen; Zertifizierung, regelmäßiger Austausch; Beratung (IT-Sicherheit und Resilienz), Schulungen (Kompetenzen); Tools zur Gefahrendetektion, finanzielle Förderung sowie Übungen/Spiele. Zusätzlich zur Kategorisierung

[5] https://www.stiftung-nv.de/sites/default/files/kas_informationssicherheit_kurzstudie_web_final.pdf

wurde eine Kurzbeschreibung jeder Maßnahme für das betreffende Land vorgenommen und eine allgemeine Bewertung erstellt.

Für Hessen und Sachsen umfassen die identifizierten Maßnahmen hauptsächlich niedrigschwellige technische Lösungen oder Informationsdienste, die durch das jeweilige Computer Emergency Response Team (CERT) bereitgestellt werden. Maßnahmen wie eine rund um die Uhr erreichbare 24/7 Hotline, ein Leak Checker, HoneySens oder regelmäßige Schwachstellenberichte erfordern vergleichsweise geringe finanzielle Mittel und können auch in Brandenburg eingeführt werden, um das Cybersicherheitsniveau weiter zu verbessern.

Weitere identifizierte Maßnahmen umfassen die finanzielle Förderung von Akteuren außerhalb der Verwaltung. Hier ist beispielsweise die Förderrichtlinie zur Cybersicherheitsforschung in Hessen zu erwähnen, die auch für Brandenburg mit Blick auf eine engere Zusammenarbeit mit dem in Brandenburg ansässigen wissenschaftlichen Einrichtungen und insbesondere auch mit dem Hasso-Plattner-Institut interessant sein könnte. Der Nutzen für die Verwaltung ist bei einer solchen Maßnahme als eher langfristig anzusehen.

Insbesondere Nordrhein-Westfalen hat mit der Initiative "Wirtschaft.Digital. Sicher NRW" einen klaren Schwerpunkt auf die Förderung der Wirtschaft gelegt. Dabei zielen die Maßnahmen oft nicht direkt darauf ab, einen unmittelbaren Mehrwert für die Verwaltung zu generieren, sondern haben das übergeordnete Ziel, das durchschnittliche Cybersicherheitsniveau aller Organisationen in NRW ganzheitlich zu erhöhen. Ein Beispiel hierfür sind die verschiedenen Versionen der Orientierungshilfen und Beratungsangebote, die das Land NRW KMU kostenlos zur Verfügung stellt. Diese dienen als Multiplikator und sollen den Einstieg in den Aufbau von Cybersicherheit für KMU erleichtern. Besonders hervorzuheben ist diese Maßnahme im Kontext der komplexen NIS-2 Regelungen, die im Rahmen des zugehörigen Umsetzungsgesetzes auf Unternehmen zukommen. Sie kann dahingehende Unterstützung bieten, auch wenn die NIS-2 Richtlinie per se nicht durch das Land zu regulieren ist.

Des Weiteren fallen bei der Analyse der Maßnahmen verschiedene Netzwerkformate der untersuchten Länder auf. Die eurobits women academy des Landes NRW zielt darauf ab, Frauen zu unterstützen, den Einstieg in das Gebiet der Cybersicherheit zu finden, wodurch der Fachkräftemangel abgemildert werden soll. Das CISO-Netzwerk in Nordrhein-Westfalen (NRW) strebt ferner danach, Chief Information Security Officers (CISOs) aus verschiedenen Sektoren wie Wirtschaft, Wissenschaft und Gesellschaft mit Sicherheitsbehörden zu vernetzen, um einen vertraulichen Austausch zu ermöglichen und die Sektor übergreifende Zusammenarbeit zu verbessern. Ebenso sind Veranstaltungsreihen zu identifizieren, die dazu beitragen sollen, das Bewusstsein für Cybersicherheit in der Gesellschaft zu fördern. Gesondert hervorzuheben ist das Projekt der „CYBERWEHR NRW“, welches sich noch in der Pilotphase befindet und letztlich Unternehmen in ganz Nordrhein-Westfalen abdecken soll. Im Kern fungiert die „CYBERWEHR NRW“ als Vermittlungsplattform zwischen betroffenen Unternehmen und IT-(Notfall-)Dienstleistern, wodurch die Vorfallsbearbeitung beschleunigt und somit auch Ressourcen in der Verwaltung freigesetzt werden sollen.

Im Folgenden werden noch einmal alle identifizierten organisatorischen, politischen und technischen Maßnahmen aus dem zweiten Teil der Analyse mit Zuordnung zu den jeweiligen Kategorien, Kurzbeschreibung sowie der kurzen allgemeinen Bewertung tabellarisch aufgelistet.

Maßnahme	Land	Kurzbeschreibung	Art	Kategorie	Bewertung	Quelle
24/7 Hotline	Hessen	Eine Rund-um-die-Uhr Hotline für die Landesverwaltung, Kommunen und kommunale Eigenbetriebe, KRITIS-Einrichtungen sowie hessische Unternehmen	Organisatorisch	Vorfallsbearbeitung	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	https://hessen3c.de/unsere-leistungen
Hessen Leak Checker	Hessen	Tool um gestohlene Datensätze nach dienstlichen Daten zu durchsuchen	Technisch	Tools zur Gefahrendetektion	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	https://hessen3c.de/unsere-leistungen/hessen-leak-checker
Werktäglicher Schwachstellenbericht	Hessen	Werktäglicher Bericht über aktuelle Schwachstellen in Soft- und Hardware	Organisatorisch	Warn- und Informationsdienst	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	https://hessen3c.de/unsere-leistungen/schwachstellenbericht
Digitaler Warnmeldungsdienst	Hessen	Warndienst für Schwachstellen in Soft- und Hardware, die in Hessen benutzt wird	Technisch	Warn- und Informationsdienst	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	https://hessen3c.de/unsere-leistungen/warnmeldungsdienst
IT-Sicherheitsarchitektur- und Prozess-Beratung	Hessen	Beratung für Landesverwaltung, Kommunen, KRITIS, KMU bzgl. Implementierung von ISO 27xxx und BSI-IT-Grundschutz	Organisatorisch	Beratung (IT-Sicherheit und Resilienz)	Sinnvoll um Lücken in Expertise kleinerer Organisationen auszugleichen. Bindet allerdings umfangreiche personelle Ressourcen.	https://hessen3c.de/unsere-leistungen/prozess-und-architekturberatung
Distr@l	Hessen	Förderung für innovative Cybersicherheitsanwendungen von KMUs	Politisch	Finanzielle Förderung	Langfristige Maßnahme, um Innovationen durch KMUs zu fördern. Auch wenn durch die Maßnahme kein direkter Vorteil für Verwaltungen entsteht, trägt diese zur Erhöhung des Cybersicherheitsniveaus des Landes bei	https://digitales.hessen.de/Foerderprogramme/Distrl/
Digitale Erstberatung	NRW	Kostenfreie Erstberatung für ISMS für Unternehmen aus NRW	Organisatorisch	Beratung (IT-Sicherheit und Resilienz)	Dieses Programm gibt Organisationen erste Anreize für die Verbesserung des Cybersicherheitsniveaus. Es bindet wenig (personelle) Ressourcen.	https://www.digital-sicher.nrw/sprechstunde/erstberatung

Maßnahme	Land	Kurzbeschreibung	Art	Kategorie	Bewertung	Quelle
Förderrichtlinie „Cybersicherheitsforschung in Hessen“	Hessen	Zuwendungen für Projektförderungen an Hochschulen des Landes Hessen sowie an außeruniversitäre Forschungseinrichtungen mit Sitz im Land Hessen zur Förderung von Forschungsvorhaben im Bereich Cybersicherheit.	Politisch	Finanzielle Förderung	Sinnvolles Programm, um Cybersicherheitsforschung im eigenen Land zu unterstützen und zu steuern. Der Nutzen ist abhängig von der Qualität der Forschungsinstitute im Land. Die individuellen Förderaufrufe bewegen sich im mittleren sechsstelligen Bereich (~350.000€). Geringer unmittelbarer Nutzen für die Verwaltung.	https://innen.hessen.de/Sicherheit/Cyber-und-IT-Sicherheit/Innovationsmanagement-Cybersicherheit/Forschungsfoerderung
Förderprogramm MID Digitale Sicherheit	NRW	Mit dem Teilprogramm können kleine und mittlere Unternehmen eine Forderung beantragen, um den Ist-Zustand ihrer IT-Sicherheitssysteme zu analysieren, etwaige Sicherheitslücken zu beheben und Mitarbeiterinnen und Mitarbeiter in entsprechenden Schulungen und Fortbildungen für das Thema zu sensibilisieren. Außerdem werden Unternehmen dabei unterstützt, Soft- und Hardware für den IT-Basisschutz anzuschaffen.	Politisch	Finanzielle Förderung	Sinnvoll, um die Kosten für den Aufbau eines ISMS bei KMU zu senken. Auch wenn durch die Maßnahme kein direkter Vorteil für Verwaltungen entsteht, trägt diese zur Erhöhung des Cybersicherheitsniveaus des Landes bei	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
Eurobits Woman Academy (ewa)	NRW	Mit dem Projekt soll eine Plattform geschaffen werden, die Frauen insbesondere den Quereinstieg in das Themenfeld erleichtert. Dabei soll ihnen geholfen werden, passende Aus- und Weiterbildungsangebote oder Umschulungen wahrzunehmen, die einen starken praxisorientierten Ansatz vertreten. Interessierten Frauen steht ein großes Netzwerk und Kontaktmöglichkeiten im Bereich Cybersicherheit zur Verfügung, die ihnen bei der beruflichen Orientierung helfen sollen.	Politisch	Schulungen (Kompetenzen)	Geeignete Maßnahme, um gegen den Fachkräftemangel vorzugehen, wovon auch die Verwaltung profitieren kann.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)

Maßnahme	Land	Kurzbeschreibung	Art	Kategorie	Bewertung	Quelle
Digitale Sicherheit für Gründer:innen	NRW	Im Rahmen einer Kooperation zwischen DIGITAL.SICHER.NRW und den zentralen Start-up-Einrichtungen in NRW werden Start-ups in einem möglichst frühen Stadium ihrer Entwicklung an Cybersicherheit herangeführt, sodass das Thema frühzeitig in den eigenen Unternehmensstrukturen und Produkten einfließen kann.	Organisatorisch	Beratung (IT-Sicherheit und Resilienz)	Maßnahme, um Innovationen zu fördern und KMU schon in sehr frühem Stadium abzusichern. Nutzen für die Verwaltung eher mittelbar.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
Landesweite Sicherheitskampagne „Tür zu im Netz!“	NRW	Die Aktion “Tür zu im Netz” ist eine groß und längerfristig angelegte Sichtbarkeitskampagne unter Federführung von DIGITAL.SICHER.NRW, um mehr Bewusstsein zum Thema IT-Sicherheit insbesondere bei kleinen und mittleren Unternehmen (KMU) zu schaffen.	Politisch	Veranstaltungen	Großangelegte Awareness-Veranstaltungsreihe. Auch hier ist eher die Wirtschaft der Adressat mit indirektem Nutzen für die Verwaltung, aber einem Beitrag zur Verbesserung des Cybersicherheitsniveaus des Landes.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
Roadshow zur digitalen Sicherheit	NRW	Die NRW Roadshow zur digitalen Sicherheit präsentiert Antworten auf ganz praktische Fragen der IT-Sicherheit von Unternehmen und Einrichtungen – persönlich und direkt vor Ort. Die kooperativ ausgelegten Veranstaltungen von regionalen Partnerinnen und Partnern und DIGITAL.SICHER.NRW informiert und sensibilisiert Unternehmen und setzt zugleich Anknüpfungspunkte für eine Verstetigung des Themas digitale Sicherheit in den Regionen.	Organisatorisch	Veranstaltungen	Großangelegte Awareness-Veranstaltungsreihe. Auch hier ist eher die Wirtschaft der Adressat mit indirektem Nutzen für die Verwaltung, aber einem Beitrag zur Verbesserung des Cybersicherheitsniveaus des Landes.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
CISO Netzwerk NRW	NRW	Workshops mit CISOs, Austauschformate z.B. zwischen Sicherheitsbehör-	Politisch	Regelmäßiger Austausch	Der durch die Initiative verbesserte Austausch zwischen Sicherheitsbehörden und den CISOs von Unternehmen	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)

Maßnahme	Land	Kurzbeschreibung	Art	Kategorie	Bewertung	Quelle
		den und CISOs, Verknüpfung bestehender Formate miteinander unter Federführung von DIGITAL.SICHER.NRW, Formate zur Offenlegung von Herausforderungen und dem Umgang damit.			sollte einen unmittelbaren Vorteil für beide Akteursgruppen darstellen, insbesondere, wenn das Netzwerk durch eine Zentralstelle koordiniert wird. Dazu entstehen durch die Initiative nur geringe Kosten für die Verwaltung.	
Vorlagen für Notfallplanung und Notfallkarten	NRW	Die Notfallkarte besteht aus einer Anleitung für die Einleitung von Notfallmaßnahmen sowie Notfallnummern. Hinzu kommen allgemeine Hinweise zu Maßnahmen, jedoch auch individuell auf das Unternehmen zugeschnittene Informationen (IT- Dienstleister, Hotline Cyberversicherung, Ansprechpartner: innen für das Einspielen von Backups usw.).	Organisatorisch	Orientierungshilfen; Beratung (IT-Sicherheit und Resilienz)	Die Erstellung von Orientierungshilfen kann einen Multiplikator-Effekt haben und hat ein gutes Kosten-Nutzen Verhältnis, insbesondere durch die Möglichkeit einer langen Weiterbenutzung der Orientierungshilfen.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
Erarbeitung eines Frameworks für ein "NRW Basispaket Digitale Sicherheit für KMU"	NRW	Vereinfachung des Zugangs und Einsatz des Cybersecurity-Marktangebots für Kleinstunternehmen (KKMU) sowie kleine und mittlere Unternehmen (KMU), gemeinsame Erarbeitung von Cybersicherheits-Paketen, die (MID) Förderprogramme vereinfachen können, Bewerbung als Teil von der Aktion „Tür zu im Netz!“ möglich.	Organisatorisch	Orientierungshilfen	Die Erstellung von Orientierungshilfen kann einen Multiplikator-Effekt haben und hat ein gutes Kosten-Nutzen Verhältnis, insbesondere durch die Möglichkeit einer langen Weiterbenutzung der Orientierungshilfen.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
Regionale Cybersicherheitsberatung & Anlaufstellen/Multiplikatorenschulungen	NRW	Mit einer regionalen Cybersicherheitsberatung, Anlaufstellen vor Ort sowie Multiplikatorenschulungen soll der Aufbau von flächendeckendem Grundwissen in allen Regionen Nordrhein-Westfalens zur digitalen Sicherheit verstärkt werden.	Organisatorisch	Regelmäßiger Austausch	Der durch die Initiative verbesserte Austausch zwischen Sicherheitsbehörden und den CISOs von Unternehmen kann einen unmittelbaren Vorteil für beide Akteursgruppen darstellen, insbesondere wenn das Netzwerk durch eine Zentralstelle koordiniert wird. Der Koordinationsaufwand ist vermutlich aber vergleichsweise hoch.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)

Maßnahme	Land	Kurzbeschreibung	Art	Kategorie	Bewertung	Quelle
Informationsoffensive zur NIS2-Richtlinie	NRW	Analyse der Gesetzgebung, Identifikation der Anzahl an betroffenen Unternehmen und Branchen, Erarbeitung einer geeigneten Kommunikationsstrategie, Analyse und Vereinfachung der Gesetzgebung. Zu prüfen wäre ggf. die Etablierung einer NIS2-Anlaufstelle in NRW.	Organisatorisch	Orientierungshilfen; Beratung	Diese Initiative hat einen hohen Nutzen aufgrund der Relevanz von NIS-2 für hunderte von Organisationen und der Komplexität der Gesetzgebung, insbesondere nachdem NIS-2 auf Landesebene umgesetzt wurde.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
CYBERWEHR NRW	NRW	Im Rahmen eines öffentlich geförderten Projektes hat der Verband eurobits e.V. eine Cyberwehr als Piloten für das Ruhrgebiet aufgebaut. Die Cyberwehr orientiert sich in ihrer Wirkungsweise und in ihrem Aufbau an den (Freiwilligen) Feuerwehren. Sie soll als erste Anlaufstelle und Notruf für Cyber-Notfälle bei kleinen und mittleren Unternehmen platziert und etabliert werden. Im Ernstfall soll sie schnell und effizient die Gefahren abwehren und Schäden für die Betriebe und letztlich Wirtschaft begrenzen. Zu diesem Zweck vermittelt die Cyberwehr im Notfall qualifizierte Dienstleister:innen, die unterstützen. Nach erfolgreicher Etablierung im Ruhrgebiet soll das Pilotprojekt Cyberwehr in eine zweite Phase überführt werden, in der es als Angebot an alle Unternehmen in NRW ausgerollt wird und somit seine Wirkungsweise vergrößert.	Organisatorisch	Vorfallsbearbeitung; Regelmäßiger Austausch; Übungen und Spiele	Der Nutzen der Cyberwehr NRW lässt sich zum Stand der Erstellung der Strategie nur schwer beurteilen, da sie sich noch in der Pilot-Phase befindet.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)

Maßnahme	Land	Kurzbeschreibung	Art	Kategorie	Bewertung	Quelle
Checkliste "Digitale Sicherheit für Chefinnen und Chefs"	NRW	Erstellung einer Art Mappe mit Checkliste(n) für die Inhaber:innen und Geschäftsführer:innen von Unternehmen. Die Mappe soll neben der Notfallkarte für IT-Maßnahmen und Ansprechpartner: innen bei Notfallmaßnahmen eine Übersicht über die interne IT-Struktur sowie über noch erforderliche Maßnahmen geben. Die Streuung der Inhalte in Richtung der Unternehmen erfolgt mit Hilfe unterstützender Verbände und Institutionen.	Organisatorisch	Orientierungshilfen; Beratung (IT-Sicherheit und Resilienz	Die Erstellung von Orientierungshilfen kann einen Multiplikator-Effekt haben und hat ein gutes Kosten-Nutzen Verhältnis, insbesondere durch die Möglichkeit einer langen Weiterbenutzung der Orientierungshilfen.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
Risiko-Folgenabschätzung "Cyberangriff" für KMU	NRW	Es soll ein allgemein zugängliches Werkzeug geschaffen werden, mit dem sich ein Unternehmen selbst einschätzen und bewerten kann. Dazu zählt auch eine Auswahl an richtigen Fragen und der Einordnung möglicher Antworten im jeweiligen Unternehmenskontext und Ausprägung des Cyberangriffs.	Organisatorisch	Orientierungshilfen	Bietet ein vorteilhaftes Kosten-Nutzen-Verhältnis, da es von jeder Organisation ohne zusätzlichen Koordinationsaufwand genutzt werden kann und im Falle eines Cyberangriffs als erste Anlaufstelle für die Vorfallbearbeitung dienen könnte.	Initiative "Wirtschaft.Digital.Sicher NRW" (digital-sicher.nrw)
HoneySens	Sachsen	HoneySens ist eine Sicherheitslösung zur Erkennung von Hacker-Angriffen in internen Netzwerken, bestehend aus Sensoren /Clients zur Überwachung des Netzwerks sowie einer zentralen Serverinstanz, an die die Clients verdächtige Zugriffsversuche melden. Interessierte können beim SAX.CERT kostenlos Sensoren beantragen, die anschließend im eigenen Netzwerk betrieben werden können.	Technisch	Tools zur Gefahrendetektion	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	Jahresbericht Informationssicherheit 2023 (sachsen.de)

Maßnahme	Land	Kurzbeschreibung	Art	Kategorie	Bewertung	Quelle
Schwachstellen-warndienst	Sachsen	Mit dem Schwachstellenwarndienst (Vulnerability Advisory Service „dCERT“) stellt das SAX.CERT in Zusammenarbeit mit einem technischen Dienstleister tagesaktuelle Informationen zu Schwachstellen und Sicherheitslücken in IT-Systemen zur Verfügung. Über das SAX.CERT kann kostenfrei ein eigenes Nutzerkonto angelegt werden, mit dem sich der Kunde aus aktuell mehr als 2.000 Hard- und Softwareprodukten eine individuelle Zusammenstellung auswählen kann. Wird für eines der ausgewählten Produkte eine neue Sicherheitslücke bekannt, versendet das Portal automatisch eine Warn-E-Mail mit ausführlichen Details und Maßnahmenempfehlungen zu dieser Schwachstelle an den betreffenden Nutzer.	Technisch	Warn- und Informationsdienst	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	Jahresbericht Informationssicherheit 2023 (sachsen.de)
Identity Leak Checker	Sachsen	Mit dem Identity Leak Checker bietet das SAX.CERT in Zusammenarbeit mit dem Hasso-Plattner-Institut einen individuellen Dienst zur Überprüfung von E-Mail-Adressen des Freistaates Sachsen auf die Betroffenheit derartiger Leaks an, mit dem alle Maildomains der Staatsverwaltung ständig überwacht werden.	Technisch	Tools zur Gefahrendetektion	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	Jahresbericht Informationssicherheit 2023 (sachsen.de)
Passwort-Checker	Sachsen	Als Sensibilisierung für die Mitarbeiterinnen und Mitarbeiter der Staatsverwaltung bietet das SAX.CERT einen Passwort-Checker auf seiner Internetseite	Technisch	Tools zur Gefahrendetektion	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	Jahresbericht Informationssicherheit 2023 (sachsen.de)

Maßnahme	Land	Kurzbeschreibung	Art	Kategorie	Bewertung	Quelle
		https://apps.sachsen.de/cert/passwortcheck an. Er soll Mitarbeiterinnen und Mitarbeitern dabei helfen, zu überprüfen, ob ihr Passwort eine Mindestsicherheit aufweist.				
Sicherheitsprüfung Webseiten	Sachsen	Auf Grundlage des AK ITEG Beschlusses „Automatische Scandienste und Erhöhung der Webseitensicherheit“ werden bereits seit 2017 regelmäßig 7.400 Internetseiten der Staats- und Kommunalverwaltung durch das SAX.CERT auf veraltete Software und bekannte Schwachstellen getestet (Vorjahreszeitraum: 7.200). Bei schwerwiegenden Sicherheitslücken werden die Betroffenen informiert. Bei den Kommunen erfolgt dies in der Regel über die KDN GmbH.	Technisch	Tools zur Gefahrendetektion	Maßnahme mit besonders gutem Kosten-Nutzen-Verhältnis, kann eventuell technisch von anderen Ländern übernommen werden	Jahresbericht Informationssicherheit 2023 (sachsen.de)
Roadshow Kommunen		Nach der „Roadshow Kommunen“ des BSI in Zusammenarbeit mit der SK wird seit Oktober 2022 monatlich eine Online-Sprechstunde des SAX.CERT zu Themen der IT-Sicherheit für die Kommunen angeboten.	Organisatorisch	Veranstaltungen	Großangelegte Awareness-Veranstaltungsreihe, die Expertise für die Kommunen nutzbar macht.	Jahresbericht Informationssicherheit 2023 (sachsen.de)