Freistaat
SACHSEN

Cybersicherheits-Strategie Sachsen

Gesellschaft und Wirtschaft

- Schützen
- Informieren
- Unterstützen

Inhaltsverzeichnis

1. Vorwort

Sehr geehrte Leserin, sehr geehrter Leser,

Cybersicherheit ist eine wesentliche Grundlage für eine moderne Informationsgesellschaft. Angesichts der unaufhaltsam voranschreitenden und alle Lebensbereiche gleichermaßen durchdringenden Digitalisierung ist sie notwendige Voraussetzung staatsbürgerlicher Teilhabe und wirtschaftlicher Betätigung. Ihre Gewährleistung ist daher ein Kernauftrag zukunftsgewandter Staatsverwaltung. Cybersicherheit ist hierbei weit mehr als eine rein technische Fragestellung. Störungen der Integrität und Funktionalität informationstechnischer Systeme können unser gesellschaftliches Leben in Anbetracht wachsender Interdependenz von digitalem und physischem Raum nachhaltig beeinträchtigen. Cybersicherheit ist daher ein zentrales Tätigkeitsfeld moderner Gefahrenabwehr. Entlang ihres verfassungsmäßigen Auftrags tragen die Länder besondere Verantwortung für deren Gewährleistung.

Ich freue mich, Ihnen die Cybersicherheitsstrategie Sachsen zu präsentieren. In dieser Strategie vereinen wir erstmals die strategischen Ziele und konkreten Maßnahmen der Sächsischen Staatsregierung in allen Handlungsfeldern der Cybersicherheit und legen diese für die nächsten Jahre fest.

Die Cybersicherheitsstrategie Sachsen ist das Ergebnis intensiver Zusammenarbeit zwischen den Ressorts und vielen Behörden der sächsischen Staatsverwaltung unter Einbeziehung des privaten Sektors wie z. B. Unternehmen, als auch Akteuren der Zivilgesellschaft. Sie reflektiert nicht nur die sich ständig weiterentwickelnde Bedrohungslandschaft, sondern auch unsere Entschlossenheit, innovative Lösungen zu entwickeln und eine widerstandsfähige digitale Zukunft zu gestalten. Denn um nichts Anderes geht es: Die digitale Transformation muss auf sicherem und vertrauenswürdigem Fundament stattfinden, um die damit einhergehenden Chancen vollumfänglich nutzen zu können.

Unsere Strategie beruht auf messbaren Zielen, die darauf ausgerichtet sind, die Effizienz unserer Cybersicherheitsmaßnahmen zu steigern, die Reaktionsfähigkeit zu verbessern und die digitale Souveränität zu stärken. Gleichzeitig setzen wir uns für eine transparente und rechenschaftspflichtige Vorgehensweise ein, um immer auch für das notwendige Vertrauen unserer Bürgerinnen und Bürger in unsere Maßnahmen zu sorgen.

Es ist unabdingbar, dass wir die Dynamik des Cyberraums verstehen und uns kontinuierlich anpassen. Daher wird unser Ansatz von Forschung und Innovation begleitet, um sicherzustellen, dass wir nicht nur auf aktuelle Bedrohungen reagieren, sondern auch proaktiv die nächste Generation von Cybersicherheitslösungen gestalten. Ich möchte allen danken, die an der Entwicklung dieser Strategie beteiligt waren - den Experten, Partnern und allen Interessengruppen, die ihre wertvollen Einblicke und Erfahrungen eingebracht haben. Die Cybersicherheitsstrategie Sachsen ist ein lebendiges Dokument, das sich weiterentwickeln wird, um den Herausforderungen der Zukunft gerecht zu werden.

Gemeinsam werden wir in Sachsen für Staat, Wirtschaft und Gesellschaft eine Cybersicherheitslandschaft schaffen, die nicht nur widerstandsfähig gegenüber Bedrohungen ist, sondern auch die Werte und Prinzipien unserer freiheitlich demokratischen Grundordnung schützt.

Dr. Daniela Dylakiewicz
Amtschefin der Sächsischen Staatskanzlei
Beauftragte für Informationstechnologie
des Freistaates Sachsen

2. Rechtliche und strategische Rahmenbedingungen

Die Cybersicherheitsstrategie Sachsen hat sowohl rechtliche Anforderungen zu erfüllen als auch sich in das bestehende System der Strategien der Staatsverwaltung zu integrieren. Die hierin beschriebenen Ziele und Maßnahmen müssen im Einklang stehen mit grundlegenden Prinzipien und Werten unseres Rechtsstaates. Zudem sind gesetzliche Vorgaben zu beachten und die konkreten Anforderungen aus der NIS-2-Richtlinie[1] der Europäischen Union (EU) zu berücksichtigen. Aber auch auf der strategischen Ebene bestehen Vorgaben, wie die von der Ständigen Konferenz der Innenminister und -senatoren der Länder – kurz Innenministerkonferenz (IMK) – beschlossene Leitlinie für föderale Cybersicherheitsstrategien. Überdies sind andere Strategien der Staatsverwaltung mit ihren Zielen und Umsetzungsmaßnahmen zu Handlungsfeldern dieser Strategie mit einzubeziehen.

1 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80; L, 2023/90206, 22.12.2023)

2.1. Grundlegende Prinzipien und Werte der Cybersicherheitsstrategie Sachsen

Maßnahmen zur Erhöhung der Cybersicherheit sind vielfältig. Für sie gelten dieselben Normen, Grundsätze und Werte, für die der Freistaat auch „offline" eintritt. Alle Maßnahmen zur Cybersicherheit müssen daher im Einklang mit den Grundrechten und der freiheitlich-demokratischen Grundordnung unseres Staates stehen. Unsere Grundrechte, Demokratie und Rechtsstaatlichkeit müssen durch Maßnahmen zur Erhöhung der Cybersicherheit gewährleistet und geschützt werden. Der Freistaat Sachsen fühlt sich bei seinen Cybersicherheitsmaßnahmen daher folgenden grundlegenden Prinzipien und Werten verpflichtet:

Grundrechte

Maßnahmen zur Cybersicherheit respektieren und schützen die Privatsphäre der Bürgerinnen und Bürger. Die Achtung der individuellen Grundrechte, wie z. B. das Recht auf Privatsphäre und Meinungsfreiheit, ist unerlässlich. Wesentliche Bedeutung bei Maßnahmen zur Cybersicherheit haben das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, die beide aus dem allgemeinen Persönlichkeitsrecht (Artikel 1 Absatz 1 i. V. m. Artikel 2 Absatz 1 des Grundgesetzes) abgeleitet werden, sowie das Telekommunikationsgeheimnis (Artikel 10 des Grundgesetzes). Das Recht auf informationelle Selbstbestimmung, welches das Recht eines jeden Einzelnen umfasst, gewährleistet dem Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Das Grundrecht schützt vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe von persönlichen Daten.[2] Unvereinbar ist danach eine Rechts- und Sachlage, bei der die „Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß".[3]

Auch aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen werden Schutzpflichten des Staates ableitbar.[4] Die grundrechtliche Schutzpflicht des Staates verlangt, dass der Staat Maßnahmen ergreift, um die Grundrechte der Bürgerinnen und Bürger vor Verletzungen durch Dritte zu schützen. Dies kann sowohl durch aktives Handeln als auch durch Unterlassungen geschehen. Konkret im Bereich der Cybersicherheit bedeutet dies, dass der Staat dazu verpflichtet ist, informations-

2 BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1-71 (43)
3 BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1-71 (42)
4 BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350

technische Systeme vor Angriffen durch Dritte zu bewahren. Der Freistaat schützt seine Behörden und Einrichtungen gegen Cyberangriffe und agiert mit seinen Gefahrenabwehr- und Strafverfolgungsbehörden zum Schutz von Wirtschaft und Gesellschaft. Dies beinhaltet den Schutz vor Cyberkriminalität, wie zum Beispiel Hackerangriffe, Phishing oder Verbreitung von Schadsoftware. Grundrechte werden jedoch nicht schrankenlos gewährleistet. Sie können aufgrund von gesetzlichen Ermächtigungsgrundlagen, etwa zur Gefahrenabwehr, eingeschränkt werden. Darüber hinaus ist der Staat nicht allumfassend zuständig für die Cybersicherheit in der Wirtschaft und bei Bürgerinnen und Bürgern. Eigenverantwortliches Handeln bleibt der Schlüssel für eine gelingende ganzheitliche Cybersicherheit.

Die Herausforderung bei der Gewährleistung der Cybersicherheit liegt somit darin, einen Ausgleich zwischen Sicherheit und Freiheit zu finden. Einerseits soll die Privatsphäre der Bürger geschützt werden, andererseits müssen Behörden in der Lage sein, auf Bedrohungen zu reagieren, was unter Umständen einen Eingriff in die Privatsphäre erfordern kann.

Demokratieprinzip

Das Demokratieprinzip ist Kernbestandteil der freiheitlich-demokratischen Grundordnung und im Grundgesetz in Artikel 20 verankert. Es besagt, dass alle Staatsgewalt vom Volke ausgeht. Dies wird durch die Existenz von Wahlen, von Parteien, der Volkssouveränität, dem Minderheitenschutz und den bürgerlichen Gleichheitsrechten sowie der freien Meinungs- und Willensbildung garantiert. Für Maßnahmen in der Cybersicherheit sind von Relevanz:

Demokratische Legitimation

Auch in der Cybersicherheit ist es wichtig, dass die Institutionen und Maßnahmen, die zum Schutz vor Cyberbedrohungen eingesetzt werden, eine klare demokratische Legitimation haben. Dies gewährleistet, dass die Bürgerinnen und Bürger Vertrauen in die Sicherheitsmaßnahmen haben und dass diese im Einklang mit den Grundrechten und demokratischen Prinzipien stehen.

Transparenz und Rechenschaftspflicht

Demokratie ist auf die Mitarbeit der Bürger angewiesen; sie braucht interessierte und informierte, d. h. mündige Bürger. Transparenz ist ein Schlüsselaspekt der Demokratie und ermöglicht es den Bürgern, Einblick in die Cybersicherheitspolitik und -praktiken zu erhalten. Dies fördert gerade das Vertrauen in staatliche Cybersicherheitsmaßnahmen und ermöglicht es den Bürgern, informierte Entscheidungen über ihre eigene Cybersicherheit zu treffen. Rechenschaftspflicht gewährleistet, dass staatliche Institutionen für ihre Handlungen im Bereich der Cybersicherheit verantwortlich sind. Dies schafft einen Rahmen, in dem Missbrauch und Fehlverhalten minimiert werden, während gleichzeitig das Vertrauen in und die Effektivität von Cybersicherheitsmaßnahmen verbessert wird. So informieren die zentralen staatlichen Akteure in der Cybersicherheit bezogen auf ihre jeweilige Zuständigkeit regelmäßig, z. B. in Jahresberichten, über ihre Tätigkeiten.

Bürgerbeteiligung

Bürgerbeteiligung ermöglicht, aktiv an der Gestaltung der Cybersicherheitspolitik teilzunehmen. Dies kann durch öffentliche Konsultationen, Bürgerforen oder die direkte Beteiligung an der Entwicklung von Cybersicherheitsstrategien erfolgen. Eine solche Beteiligung sorgt dafür, dass die Bedürfnisse und Bedenken der Bürgerinnen und Bürger berücksichtigt werden und dass die Cybersicherheitspolitik die Vielfalt der Gesellschaft widerspiegelt.

Zusammenfassend trägt das **Demokratieprinzip** wesentlich zur Stärkung der Cybersicherheit bei, indem es sicherstellt, dass die Politik und Praktiken im Bereich der Cybersicherheit transparent, rechenschaftspflichtig und beteiligend sind. Dies fördert nicht nur das Vertrauen der Bürger in die digitalen Systeme, sondern trägt auch dazu bei, eine sichere digitale Umgebung für alle zu schaffen.

Rechtsstaatsprinzip

Das Rechtsstaatsprinzip wird im Wesentlichen aus Artikel 20 Absatz 3 des Grundgesetzes abgeleitet, wonach das Parlament als gesetzgebende Gewalt (Legislative) an die Verfassung sowie die Verwaltung (Exekutive) und die Gerichte (Judikative) an Gesetz und Recht gebunden sind. Das Rechtsstaatsprinzip spielt eine entscheidende Rolle in der Cybersicherheit, indem es sicherstellt, dass Maßnahmen zur Erhöhung der Cybersicherheit im Einklang mit gesetzlichen Vorgaben und Grundrechten stehen. Für Maßnahmen in der Cybersicherheit sind daher folgende Prinzipien wichtig:

Gewaltenteilung

Ein Rechtsstaat basiert auf der Gewaltenteilung zwischen Exekutive, Legislative und Judikative. Auch in der Cybersicherheit gewährleistet sie eine klare Trennung und gegenseitige Kontrolle der verschiedenen staatlichen Gewalten. Die Verantwortlichkeiten und Befugnisse im Bereich Cybersicherheit sind zwischen den verschiedenen staatlichen Behörden und Einrichtungen klar aufgeteilt, um eine wirksame Kontrolle und Balance zu gewährleisten.

Grundsatz der Gesetzmäßigkeit der Verwaltung

Der Grundsatz der Gesetzmäßigkeit der Verwaltung stellt sicher, dass alle Maßnahmen und Aktivitäten der öffentlichen Verwaltung im Bereich der Cybersicherheit an Gesetz und Recht gebunden sind. Dies bedeutet, dass jedes Verwaltungshandeln im Kontext der Cybersicherheit auf einer gesetzlichen Grundlage basieren muss (sog. Vorbehalt des Gesetzes) und nicht gegen Gesetze verstoßen darf (sog. Vorrang des Gesetzes). Diese Prinzipien gewährleisten, dass die Verwaltung ihre Befugnisse nicht überschreitet und die Rechte der Bürgerinnen und Bürger sowie der Unternehmen auch bei eingreifenden Maßnahmen zur Erhöhung der Cybersicherheit beachtet werden.

Bestimmtheitsgebot

Das Bestimmtheitsgebot sorgt dafür, dass Regelungen für Bürgerinnen und Bürger klar und verständlich sind, so dass sie ihr Verhalten entsprechend ausrichten können. Im Kontext der Cybersicherheit bedeutet das Bestimmtheitsgebot, dass Gesetze und Vorschriften eindeutig formulieren müssen, welche Anforderungen z. B. an die Sicherheit von IT-Systemen gestellt werden. Dies ist entscheidend, um sicherzustellen, dass sowohl die Verantwortlichen für IT-Systeme als auch die Nutzer wissen, welche Maßnahmen zum Schutz vor Cyberangriffen ergriffen werden müssen, was für die effektive Prävention und Bekämpfung von Cyberbedrohungen unerlässlich ist. Grundsätzlich verfassungsrechtlich unbedenklich sind nach ständiger Rechtsprechung des Bundesverfassungsgerichts unbestimmte Rechtsbegriffe.[5] Unbestimmte Rechtsbegriffe sind solche, die vom Gesetzgeber bewusst offen gelassen werden, um Flexibilität in der Anwendung zu ermöglichen und auf unterschiedliche Sachverhalte anwendbar zu sein. Die Verwendung unbestimmter Rechtsbegriffe (z. B. Stand der Technik) ist im Bereich des Cybersicherheitsrechts wegen der raschen Entwicklung der Technologie, der zunehmenden Komplexität und der Bedrohungslage verbreitet, um auf neue Herausforderungen und Entwicklungen angemessen reagieren zu können.

Verhältnismäßigkeitsgrundsatz

Der Verhältnismäßigkeitsgrundsatz stellt sicher, dass staatliche Eingriffe in die Privatsphäre angemessen und gerechtfertigt sind. Der Verhältnismäßigkeitsgrundsatz spielt somit auch bei Maßnahmen zur Erhöhung der Cybersicherheit eine wichtige Rolle. Eine komplexe Herausforderung ist die Beachtung des Verhältnismäßigkeitsgrundsatzes bei der Abwägung zwischen Grundrechten und den ebenfalls verfassungsrechtlich geschützten Interessen im Bereich der Cybersicherheit, wie öffentliche Sicherheit und der Strafverfolgung. Dabei ist der Grundsatz der Verhältnismäßigkeit ein fundamentales Prinzip des Rechtsstaates und begrenzt staatliche Eingriffe in die Freiheitsrechte der Bürgerinnen und Bürger. Im Kontext der Cybersicherheit bedeutet dies, dass Eingriffe in die Grundrechte, wie beispielsweise das Recht auf informationelle Selbstbestimmung, nur dann gerechtfertigt sind, wenn sie zur Erreichung eines legitimen Ziels wie dem Schutz vor Cyberangriffen notwendig sind und keine weniger eingreifenden, gleich wirksamen Alternativen zur Verfügung stehen. Zudem müssen die Maßnahmen in einem angemessenen Verhältnis zu den damit verbundenen Einschränkungen stehen.

Zusammenfassend sorgt das **Rechtsstaatsprinzip** dafür, dass Cybersicherheitsmaßnahmen transparent, nachvollziehbar und rechtlich abgesichert sind, um die digitale Souveränität und die Grundrechte der Bürger zu schützen.

All die genannten Prinzipien tragen dazu bei, ein robustes und resilientes Cybersicherheitsumfeld zu schaffen, in dem die Rechte und Freiheiten der Bürger geschützt werden.

5 BVerfG, Beschluss vom 12. Januar 1967 – 1 BvR 169/63 –, BVerfGE 21, 73–87

2.2. Rechtsrahmen

Die Cybersicherheitsstrategie Sachsen hat ihre rechtliche Grundlage in der NIS-2-Richtlinie der Europäischen Union und bezieht sich inhaltlich auf die Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien der IMK. Zudem sollen die strategischen Ziele und Umsetzungsmaßnahmen dieser Strategie die landesgesetzlichen Regelungen beachten und mit weiteren Zielen und Maßnahmen neue Akzente für die Zukunft setzen.

2.2.1. Anforderung an eine Cybersicherheitsstrategie durch die NIS-2- Richtlinie

Am 16. Januar 2023 ist die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) in Kraft getreten. Nach Artikel 7 dieser Richtlinie hat jeder Mitgliedstaat eine nationale Cybersicherheitsstrategie zu erlassen, „die die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus enthält". Aufgrund seiner föderalen Struktur ist diese Anforderung für Deutschland so umzusetzen, dass auch die Länder Cybersicherheitsstrategien nach den in Artikel 7 beschriebenen Anforderungen einzuführen haben. Dabei ist kein einheitliches Dokument notwendig, sondern lediglich ein kohärenter Rahmen, der mit der in Kapitel 2.2.2. beschriebenen Leitlinie zur Entwicklung föderaler Cybersicherheitsrichtlinien der IMK inhaltlich untersetzt wird. Die in der NIS-2-Richtlinie geforderten Pläne bzw. Konzepte einer Cybersicherheitsstrategie umfassen zwar keine neuen Themengebiete, setzen jedoch einen klar umrissenen Fokus auf bestimmte Konzepte.

2.2.2. Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien

Im Jahr 2021 hat die Länderarbeitsgruppe Cybersicherheit der IMK eine Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien erarbeitet. Die Leitlinie nennt die wichtigsten Handlungsfelder und Zielgruppen, die bei der Erstellung einer Strategie in den Ländern beachtet werden sollten und stellt somit einen ganzheitlichen Ansatz dar, in dem sowohl etablierte Konzepte, z. B. zur Informationssicherheit in der Verwaltung, aufgegriffen werden, als

auch andere Themenfelder adressiert sind, wie Strafverfolgung und Arbeit der Sicherheitsbehörden im Cyberraum, Wissenschaft und Forschung sowie Einbindung der Zivilgesellschaft. Ziel der Leitlinie ist eine Standardisierung der Cybersicherheitsarchitektur in den Ländern, um durch größere Interoperabilität und fachlichen Austausch den nötigen Raum für Innovation und Weiterentwicklung zu eröffnen. Auf diesem Wege trägt die Leitlinie wesentlich zu einer Erhöhung des allgemeinen Cybersicherheitsniveaus bei. Als ein wesentliches konkretes Ziel wird die Fähigkeit der Länder angestrebt, ihr Cybersicherheitsniveau zu erhöhen und beispielsweise Sicherheitslagebilder über alle Bereiche (Verwaltung, Wirtschaft sowie Bürger) in jedem Land nach einheitlichen Kriterien erstellen zu können. Ausdrücklich versteht sie sich auch als Angebot und Anknüpfungspunkt für Kommunen und Landkreise. Sachsen orientiert sich mit der vorliegenden Cybersicherheitsstrategie an den Handlungsfeldern und Zielgruppen der Leitlinie.

2.2.3. Sächsisches Informationssicherheitsgesetz

Das einzige Landesgesetz mit inhaltlichen Bezügen zur Cybersicherheit in Sachsen ist das Sächsische Informationssicherheitsgesetz (SächsISichG), welches insbesondere für das Handlungsfeld 1 (s. Kapitel 4.1.) die regulatorische Basis bildet. Es regelt seit dem Jahr 2019 die wesentlichen Aspekte, wie sowohl die Staatsverwaltung als auch die Kommunen mit technisch-organisatorischen Maßnahmen ihre Systeme sicher betreiben und vor Cyberangriffen schützen sollen.

Für Fragen der Informationssicherheit der staatlichen Stellen auf der zentralen strategischen Ebene gibt es den Beauftragten für Informationssicherheit des Landes (BfIS Land). Seine Aufgaben sind in § 5 SächsISichG festgelegt. Beispielsweise fördert und unterstützt der BfIS Land die Erstellung von konkreten Handlungsempfehlungen und berät die staatlichen Stellen, insbesondere bei der Erstellung und Pflege eines Informationssicherheitsmanagementsystems (ISMS). Der BfIS Land erstellt verbindliche Mindeststandards zur Informationssicherheit für die staatlichen Stellen und kann auch bei der Umsetzung und Einhaltung der Mindeststandards beraten. Darüber hinaus initiiert und koordiniert er landesweite Sensibilisierungs- und Schulungsmaßnahmen und Projekte zur Informationssicherheit. Der BfIS Land hat ein direktes Vorspracherecht beim CIO des Freistaates Sachsen. Er berät ihn bei seiner Aufgabenwahrnehmung bezüglich der Informationssicherheit und unterstützt ihn bei der Umsetzung.

Ergänzend dazu ist auf der zentralen operativen Ebene das Sicherheitsnotfallteam (SAX. CERT) im Staatsbetrieb Sächsische Informatik Dienste (SID) angesiedelt, das der Fachaufsicht

des BfIS Land unterliegt. Das SAX.CERT fungiert als IT-Sicherheitszentrum, d. h. es analysiert die Lage der Informationssicherheit im Freistaat Sachsen und stellt interne Berichte dazu bereit und beobachtet Gefährdungen und deren Entwicklung. Hinzu kommen auf operativer und strategischer Ebene zugleich die Beauftragten für Informationssicherheit (BfIS) in den einzelnen Behörden der Staatsverwaltung wie auch in den Kommunen in Sachsen. Gemäß § 7 SächsISichG müssen zum Beispiel die obersten Behörden der Staatsverwaltung, die staatlichen IT-Dienstleister, das Landespolizeipräsidium, der Sächsische Rechnungshof und die Sächsische Datenschutz- und Transparenzbeauftragte einen hauptamtlichen BfIS einsetzen. Für alle anderen staatlichen Behörden und die Kommunen gilt die Pflicht, einen Informationssicherheitsbeauftragten zu ernennen.

2.3. Einordnung zu anderen Strategien

Für die Erstellung der Sächsischen Cybersicherheitsstrategie sind nicht nur die Anforderungen aus der NIS-2-Richtlinie relevant. In Ergänzung dazu ist es wesentlich, sich strukturell und mit Bezug auf die für die Cybersicherheit relevanten Handlungsfelder in die bestehenden Strategien der EU, des Bundes und einiger anderer Länder einzureihen. Darüber hinaus sind auch im Binnenverhältnis zu anderen Strategien der Staatsverwaltung die Inhalte mit Bezug zur Cybersicherheit einzubeziehen.

2.3.1. Cybersicherheitsstrategien auf Länderebene

Neben Sachsen gibt es weitere Bundesländer, die eine Cybersicherheitsstrategie erarbeitet haben. Niedersachsen war dabei das erste Land mit einer solchen Strategie. Die Ende 2012 von der dortigen Landesregierung verabschiedete Strategie konzentrierte sich dabei noch auf die Informationssicherheit der Verwaltung. Ein Jahr später wurde in Bayern eine Strategie vorgelegt, die vor allem die Vernetzung aller für die Cybersicherheit wichtigen Akteure beförderte. Beide Strategien wurden nicht veröffentlicht.

Die nächsten Cybersicherheitsstrategien auf Länderebene folgten dann mit einigem zeitlichen Abstand. Im Dezember 2021 legten zwei weitere Länder, Nordrhein-Westfalen[6] und Baden-Württemberg[7], ihre Cybersicherheitsstrategien öffentlich vor. Beide Strategien verfolgen einen ganzheitlichen Ansatz und berücksichtigen neben Strafverfolgung und Wirtschaftsschutz auch die staatliche und kommunale Cybersicherheit, die digitale Bildung der Bürger, Innovationsförderung sowie nationale wie internationale Vernetzung und Kooperation. Baden-

6 https://www.cybersicherheit.nrw/system/files/media/document/file/cybersicherheitsstrategie_nrw.pdf
7 https://digital-laend.de/wp-content/uploads/2023/01/Cybersicherheitsstrategie-BW---Perspektive-2026-Dezember-2021.pdf

Württemberg nimmt im Text dabei explizit Bezug auf die Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien der Länderarbeitsgruppe Cybersicherheit der IMK (s. Kapitel 2.2.2.)

Im Jahr 2023 folgten dann Bremen[8] und Hessen[9] mit ihren ersten Strategien, die sich ebenfalls an der Leitlinie der Länderarbeitsgruppe orientierten, sowie Bayern[10] mit einer überarbeiteten Cybersicherheitsstrategie 2.0. Auch Niedersachsen[11] legte im Jahr 2024 eine neue Cybersicherheitsstrategie vor. Im Rahmen der Notifizierung der NIS-2-Richtlinie zeigten die Länder Rheinland-Pfalz, Saarland und Thüringen die Erfüllung der in Artikel 7 der Richtlinie benannten Anforderungen durch bestehende oder neu geschaffene Strategien an. Diese sind bislang nicht veröffentlicht.

2.3.2. Cybersicherheitsstrategie der EU

Die Cybersicherheitsstrategie der EU für die digitale Dekade wurde im Dezember 2020 vorgelegt.[12] Die Strategie soll Europas kollektive Abwehrfähigkeit gegen Cyberbedrohungen stärken und dazu beitragen, dass alle Bürgerinnen und Bürger und Unternehmen die Vorzüge vertrauenswürdiger und zuverlässiger Dienste und digitaler Instrumente uneingeschränkt nutzen können. Sie soll einen globalen und offenen Cyberraum gewährleisten und zugleich Schutzvorkehrungen sowohl für die Sicherheit als auch für die europäischen Werte und Grundrechte bieten. So enthält die Strategie konkrete Vorschläge für Regulierungs-, Investitions- und Politikinstrumente zu den drei Themen „Widerstandsfähigkeit, technologische Unabhängigkeit und Führungsrolle" (hier u. a. die Einführung der NIS-2-Richtlinie), „Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion" sowie „Förderung eines globalen offenen Cyberraums durch verstärkte Zusammenarbeit". Die Umsetzung der Strategie wird dabei durch Investitionsprogramme in den digitalen Wandel flankiert, insbesondere durch die Programme „Digitales Europa" und „Horizont Europa" sowie den Europäischen Aufbauplan.

2.3.3. Cybersicherheitsstrategie des Bundes

Die „Cybersicherheitsstrategie für Deutschland 2021"[13] soll den strategischen Rahmen für das Handeln der Bundesregierung im Bereich der Cybersicherheit für einen Zeitraum von fünf Jahren bilden und gilt seit September 2021. Die Cybersicherheitsstrategie konzentriert sich auf die vier Handlungsfelder Gesellschaft, Wirtschaft, Staat und EU/Internationales. In den Handlungsfeldern werden 44 strategische Ziele beschrieben. Ein Schwerpunkt mit Auswirkung auf das Verhältnis zu den Ländern ist dabei das Ziel, das Bundesamt für Sicherheit

8 https://www.inneres.bremen.de/sixcms/media.php/13/Bremische%20Cybersicherheitsstrategie%202023_barrierefrei.pdf
9 https://hessen3c.de/sites/hessen3c.hessen.de/files/2023-10/hessische_cybersicherheitsstrategie_web.pdf
10 https://stmi.bayern.de/assets/stmi/sus/verfassungsschutz/stmi_cybersicherheitsstrategie_a5_web_bf.pdf
11 https://www.mi.niedersachsen.de/download/212851
12 https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2391
13 https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf

in der Informationstechnik (BSI) zu einer Zentralstelle auszubauen und somit – neben dem Bundeskriminalamt (BKA) im Polizeiwesen und dem Bundesamt für Verfassungsschutz im Verfassungsschutzverbund – zur dritten Säule einer föderal integrierten Cybersicherheitsarchitektur weiterzuentwickeln.

Die Strategie beschreibt die grundsätzliche, langfristige Ausrichtung der Cybersicherheitspolitik der Bundesregierung in Form von Leitlinien, Handlungsfeldern sowie strategischen Zielen. Sie hat einen aktiven gestaltenden Charakter und soll ein zielgerichtetes und abgestimmtes Zusammenwirken aller Akteure ermöglichen und fördern. Die Cybersicherheitsstrategie für Deutschland und die Cybersicherheitsstrategien der Länder sollen sich dabei gegenseitig ergänzen und damit die föderale Zusammenarbeit intensivieren. Eingebettet in die Europäische Cybersicherheitsstrategie trägt die Cybersicherheitsstrategie für Deutschland zudem auch zur Gestaltung der digitalen Zukunft Europas bei.

2.3.4. Verhältnis zu anderen Strategien der Staatsverwaltung

Neben der vorliegenden Cybersicherheitsstrategie Sachsen hat der Freistaat für weitere Themengebiete Strategien entwickelt, an denen sich seine Behörden orientieren. Diese sind teilweise auch mit Umsetzungsplänen zu konkreten Maßnahmen untersetzt. Die nachfolgend benannten Strategien beinhalten Themen bzw. Maßnahmen, die auch in Handlungsfeldern der Cybersicherheitsstrategie eine Rolle spielen, und daher in der hiesigen Strategie zu beachten sind.

Mit der **Digitalstrategie des Freistaates Sachsen** „sachsen digital 2030: besser, schneller, sicher“ [14] will die Sächsische Staatsregierung den digitalen Wandel in Sachsen erfolgreich gestalten. Die Strategie hat fünf Dimensionen: Gesellschaft, Staat, Wirtschaft und Arbeit, Digitale Infrastruktur sowie Bildung, Wissenschaft und Forschung. Bezug zur Cybersicherheitsstrategie haben dabei die hier genannten Maßnahmen „Evaluierung und Fortschreibung des Sächsischen Informationssicherheitsgesetzes“, die „Kontinuierliche Sicherstellung des Personalnachwuchses für die Verwaltung“ sowie die „Erarbeitung einer Cybersicherheitsstrategie Sachsen“ in der Dimension Staat. In der Dimension Wirtschaft und Arbeit werden die „Kontinuierliche Unterstützung von kleinen und mittleren Unternehmen beim Prozess der digitalen Transformation, inklusive des Themas der Informationssicherheit“ sowie die „Initiierung eines Firmennetzwerkes in Sachsen zur Unterstützung von kleinen und mittleren

14 https://publikationen.sachsen.de/bdb/artikel/41515/documents/63409
15 https://publikationen.sachsen.de/bdb/artikel/43191/documents/65495

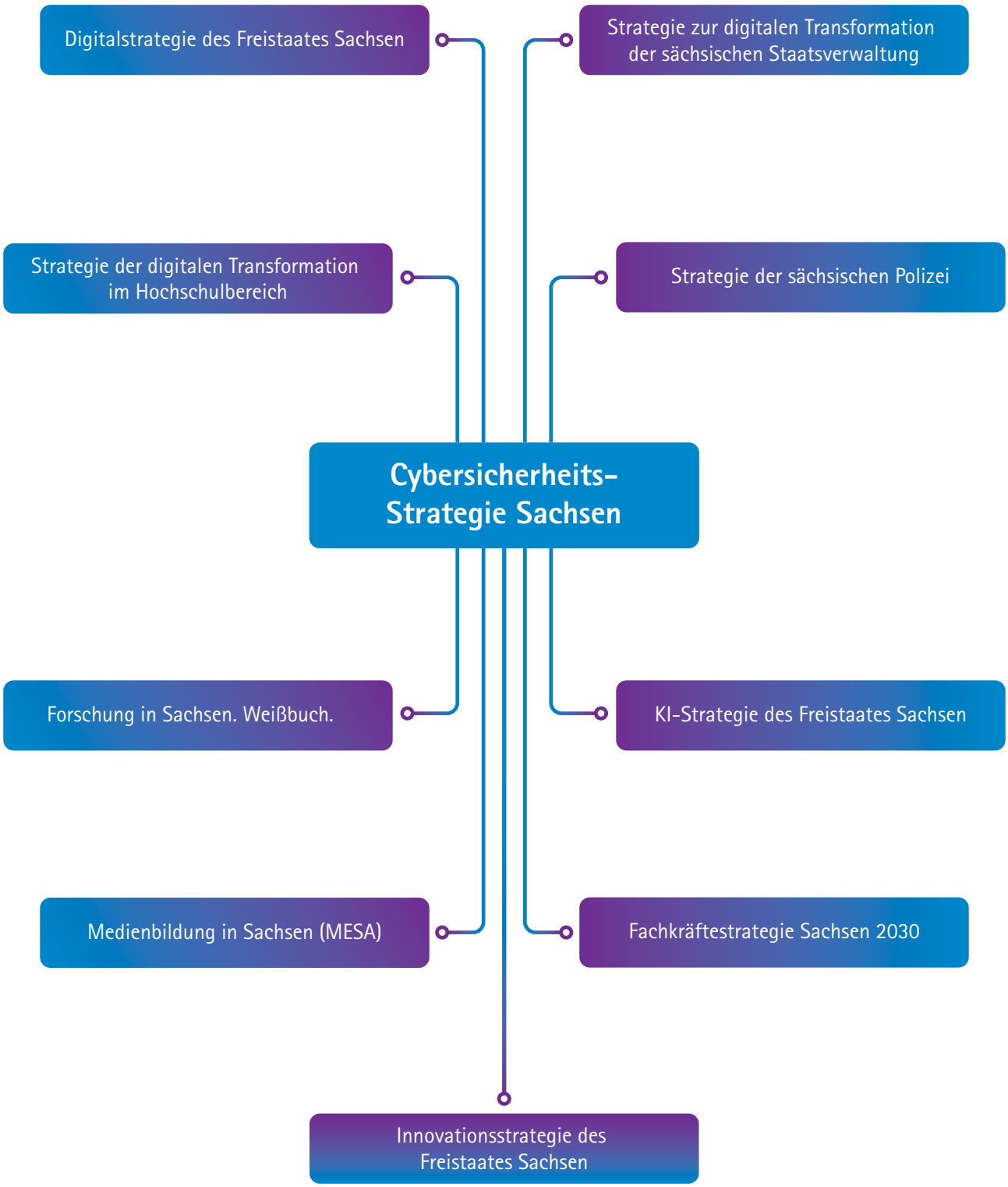
Unternehmen beim Thema Informationssicherheit durch die Digitalagentur Sachsen (DiAS)" als Maßnahmen genannt.

Mit der **Strategie zur digitalen Transformation der sächsischen Staatsverwaltung**[15] setzt sich der Freistaat das Ziel, auch langfristig angemessen auf die sich rasch entwickelnden Anforderungen aus Gesellschaft und Technik zu reagieren und als öffentliche Verwaltung ein effizienter und leistungsfähiger Dienstleister für die sächsischen Bürgerinnen und Bürger sowie Organisationen und Unternehmen im Freistaat zu sein und zu bleiben. Das Thema Informationssicherheit stellt hier eine zentrale Handlungsdimension der digitalen Verwaltung dar und wird als essenzielle Querschnittsaufgabe beschrieben, die in allen Handlungsfeldern mitzudenken ist. Ziele der Informationssicherheit werden u. a. in den Handlungsfeldern „Digitale Leistungserbringung" und „Digitale Infrastruktur und digitale Souveränität" benannt. Durch weitere Zentralisierung ressortübergreifender Infrastruktur und IT soll dafür gesorgt werden, dass normierte bzw. durch den zentralen IT-Dienstleister zertifizierte Hard- und Software verwendet wird und dadurch ein klar überschaubares Sicherheitslagebild für die verwendeten IT-Komponenten an zentraler Stelle existiert.

Der digitale Wandel erfasst und fordert auch die Hochschulen heraus. Er verändert die Art und Weise, wie sie in der Lehre Wissen und Kompetenzen vermitteln, in der Forschung neue Erkenntnisse generieren und transferieren und ihre administrativen Prozesse organisieren. Mit der **Strategie der digitalen Transformation im Hochschulbereich**[16] wollen Freistaat und Landesrektorenkonferenz die Zukunfts- und Wettbewerbsfähigkeit der sächsischen Hochschulen im nationalen und internationalen Kontext erhalten und die Attraktivität der Hochschulen für Studierende, Forschende sowie Bedienstete in den Verwaltungen und deren Arbeitserfolge gleichermaßen steigern. Im Handlungsfeld „Querschnittsaufgaben" soll die Informationssicherheit an den Hochschulen insb. durch kurzals auch mittelfristige kooperative Lösungen sowie durch die Etablierung dauerhafter Formen der Zusammenarbeit gestärkt werden.

Die **Strategie der sächsischen Polizei**[17] beschreibt sechs Handlungsfelder der Polizei in Sachsen. Die Strategie wurde im Jahr 2017 aktualisiert, 2021 fortgeschrieben, und bezieht sich auf die aktuellen und zukünftigen Entwicklungen, insbesondere auf die wachsenden Gefahren durch organisierte Kriminalität, Cybercrime sowie den Extremismus und Terrorismus. Die Strategie bezieht sich im Handlungsfeld Cybercrime auf ein wesentliches Handlungsfeld der vorliegenden Cybersicherheitsstrategie Sachsen und betont die Bedeutung von IT-Kompetenz und IT-Forensik bei der Bekämpfung von Cyberkriminalität. Die Polizei Sachsen hat auf diese Entwicklung unter anderem mit der Gründung des Cybercrime Competence Center Sachsen (SN4C) im Landeskriminalamt (LKA) sowie der Neuorganisation und einer angepassten Personalausstattung der Polizeidirektionen im Zusammenhang mit der Bekämpfung der Cybercrime-Delikte reagiert.

16 https://publikationen.sachsen.de/bdb/artikel/44462/documents/67342
17 https://www.polizei.sachsen.de/de/dokumente/Landesportal/Anlage3EndfassungStrategiebroschuere.pdf


Digitalstrategie des Freistaates Sachsen
Strategie zur digitalen Transformation der sächsischen Staatsverwaltung
Strategie der digitalen Transformation im Hochschulbereich
Strategie der sächsischen Polizei
Cybersicherheits-Strategie Sachsen
Forschung in Sachsen. Weißbuch.
KI-Strategie des Freistaates Sachsen
Medienbildung in Sachsen (MESA)
Fachkräftestrategie Sachsen 2030
Innovationsstrategie des Freistaates Sachsen

Die **KI-Strategie des Freistaates Sachsen**[18] zielt darauf ab, die Entwicklung von Künstlicher Intelligenz (KI) in Sachsen voranzutreiben. Sie basiert auf einer intensiven Stärken-Schwächen-Analyse der sächsischen Wirtschaft in Bezug auf KI und wurde von der Sächsischen Staatsregierung in einem ressortübergreifenden Prozess unter Federführung der Sächsischen Staatskanzlei entwickelt. Als eines von insgesamt neun strategischen Zielen wird darin festgelegt, dass KI in der Verwaltung verantwortungsvoll eingesetzt werden soll, um durch einen transparenten und nachvollziehbaren Einsatz von KI das Vertrauen der Bürgerinnen und Bürger in die KI-Technologie zu stärken. Um dies zu gewährleisten, will man im Bereich der Informations- und Cybersicherheit eine Vorbildfunktion für andere gesellschaftliche Bereiche einnehmen, wozu auch eine ausreichende Sensibilisierung der eigenen Mitarbeiterinnen und Mitarbeiter für das Thema gehört. Insgesamt wird angestrebt, die KIKompetenzen zu erhöhen und in diesem Zusammenhang auch die Cybersicherheit in der Aus- und Weiterbildung stärker zu berücksichtigen.

Die **Strategie „Forschung in Sachsen. Weißbuch."**[19] beschreibt die Grundsätze und Leitlinien für eine zukunftsorientierte Forschungspolitik in Sachsen und dokumentiert das Selbstverständnis der Forschung in Sachsen als freie, nutzerorientierte und innovative Säule der Wissenschaft. Wesentliche forschungspolitische Leitlinien des Weißbuches sind u. a., dass Forschung in Sachsen themenund technologieoffen ist, dass forschungspolitisches Handeln darauf abzielt, die leistungsfähigen Strukturen des gesamten sächsischen Forschungsökosystems bestmöglich zu unterstützen und dass das Forschungsgeschehen von Beginn an die spätere Anwendung in den Blick nehmen soll. Die Forschungsstrategie benennt als Themenfeld mit besonderer strategischer Bedeutung für Sachsen die Forschung in der Mobilkommunikation und bezeichnet hierbei die Sicherheit als eine wichtige Voraussetzung für die zukünftige Akzeptanz von Internet of Things (IoT)-Systemen.

Die Landesstrategie **„Medienbildung in Sachsen (MESA)"**[20] der Sächsischen Staatsregierung trägt der Digitalisierung aller Lebensbereiche und der damit verbundenen zunehmenden Relevanz von Medienbildung für die Bevölkerung Rechnung. Die Leitziele von MESA sind, die Aktivitäten zum Thema Medienbildung im Freistaat Sachsen zu koordinieren und sichtbarer zu machen und die Medienbildung in der frühkindlichen Bildung, der Kinder- und Jugendbildung, der Familien-, Erwachsenen- und Seniorenbildung weiterzuentwickeln. Diese Zielgruppen sollen lernen, mit Medien umzugehen, und sollen verstehen, wie Medien funktionieren und wie sie sich selbst an Medien beteiligen können. Im Handlungsfeld medienpädagogische Angebote werden u. a. Sensibilisierungsveranstaltungen zum Thema Cybersicherheit als Maßnahme genannt.

18 https://www.smartes.sachsen.de/download/KI_Strategiebroschuere_Auflage_2_Doppelseiten_neu.pdf
19 https://www.forschung.sachsen.de/download/Publikation_Weissbuch_barrierefrei.pdf
20 https://publikationen.sachsen.de/bdb/artikel/34222/documents/53001

Zentraler Orientierungsrahmen für alle Aktivitäten der Fachkräftesicherung und -gewinnung ist die **Fachkräftestrategie 2030 für den Freistaat Sachsen**[21], die von der Fachkräfteallianz Sachsen getragen wird, der alle relevanten Wirtschafts- und Arbeitsmarktakteure auf Landesebene sowie die regionalen Allianzen in allen Landkreisen und kreisfreien Städten angehören. Diese Strategie legt zwar keinen gesonderten Fokus auf IT- oder Cybersicherheits-Fachkräfte, jedoch sind in den vier Haupthandlungsfeldern der Strategie Ziele formuliert, die sich positiv auf das Fachkräfteangebot in der Cybersicherheit auswirken können. So zum Beispiel mittels Ausbau des Standortmarketings und der Schaffung besserer Rahmenbedingungen bei der Integration ausländischer Fachkräfte.

Die **Innovationsstrategie des Freistaates Sachsen**[22] steht als Landesstrategie im Mittelpunkt der Handlungen des Freistaats zur Stärkung der Innovationsfähigkeit und somit der Wettbewerbsfähigkeit und der Wachstumspotentiale der sächsischen Wirtschaft. Sie ist die Richtschnur für die sächsische Innovationspolitik insgesamt und stellt ein koordiniertes Ineinandergreifen aller innovationsrelevanten Politikdomänen und Instrumente sicher. Die Innovationsstrategie erkennt die herausragende Bedeutung von Digitalisierung und Daten nicht nur zur Steigerung der Produktivität, sondern auch für neue Geschäftschancen mit hohen Wachstumsprognosen auf globalen Märkten an. Dabei stellt sie fest, dass ein effektiver Schutz gegen IT-Abgriffen bzw. Cybersicherheit eine kritische Rolle bei den Entscheidungen der Unternehmen aus allen Wirtschaftsbereichen, in neue Technologien, Geschäftsmodelle und Innovation zu investieren, spielt.

21 https://publikationen.sachsen.de/bdb/artikel/33962/documents/52881
22 https://publikationen.sachsen.de/bdb/artikel/35302/documents/54808

3. Zielstellung der Cybersicherheitsstrategie Sachsen

Dieses Kapitel stellt die langfristigen Visionen und das daraus abgeleitete Leitbild der Cybersicherheitsstrategie Sachsen vor, um im weiteren Verlauf die sich daraus ergebenden strategischen Ziele zu erläutern. Damit fasst es die wesentlichen Zielstellungen zusammen, die in den kommenden Jahren handlungsleitend für alle staatlichen Behörden sein sollen. In den daran anschließenden Kapiteln wird gezeigt, inwiefern die strategischen Ziele und Maßnahmen in den neun staatlichen Handlungsfeldern der Cybersicherheit aufgegriffen werden.

3.1. Visionen und Leitbild der Cybersicherheit

Die Visionen von staatlichen Ebenen in Bezug auf Cybersicherheit können je nach den politischen, wirtschaftlichen und sicherheitspolitischen Gegebenheiten, Zuständigkeiten und der Wirkmacht der staatlichen Akteure variieren. Der Freistaat Sachsen verfolgt mit der vorliegenden Cybersicherheitsstrategie folgende Visionen:

Widerstandsfähigkeit

Präventive Maßnahmen allein gewährleisten keine Sicherheit. Mögliche erfolgreiche Cyberangriffe sind keine Frage des Ob, sondern des Wann. Daher schafft der Freistaat für seine Behörden eine widerstandsfähige digitale Infrastruktur, die gegen Cyberangriffe wehrhaft ist und sich schnell von Störungen erholen kann. Ausgehend von der Staatsverwaltung soll die Resilienz im Zusammenwirken mit den Kommunen über alle Verwaltungsebenen hinweg erhöht werden. Wirtschaft und Gesellschaft werden unterstützt, sich gegen Cyberangriffe robust aufzustellen.

Bewusstseinsbildung

Um Cybersicherheit als wichtiges Thema verstehen zu können, muss sowohl die eigene potenzielle Betroffenheit als auch Gestaltungsfähigkeit und Wirkmacht erkannt werden. Die Bewusstseinsbildung durch Sensibilisierungs- und Schulungsmaßnahmen auf allen Ebenen der Gesellschaft ist daher für die Entwicklung einer umfassenden Cybersicherheitskultur grundlegend.

Digitale Souveränität

Die Behörden des Freistaates Sachsen stärken ihre digitale Souveränität, um die Kontrolle über die eigenen digitalen Ressourcen und damit auch die Sicherheit der von Bürgerinnen und Bürgern und Unternehmen bereitgestellten Daten zu gewährleisten. Sie gestalten ihre IT selbst und können ihre Anforderungen und Bedarfe gegenüber Technologieanbietern formulieren und durchsetzen.[23]

Intensivierung der Zusammenarbeit

Sicherheit kann nur im Zusammenwirken erreicht werden. Daher arbeiten die Behörden des Freistaates Sachsen im Bereich Cybersicherheit eng zusammen, z. B. durch den Austausch von Informationen, bewährten Praktiken und die Verzahnung von Abwehrmaßnahmen. In diesen Austausch sollen auch die Kommunen und der private Sektor so eng wie möglich einbezogen werden.

Effektive Regulierung

Cybersicherheit ist ohne Regulierung nicht zu erreichen. Der Freistaat Sachsen reguliert die in seiner Zuständigkeit liegenden Ebenen durch die Verabschiedung und Durchsetzung von Gesetzen, Vorschriften und Mindeststandards, um in den Behörden in Sachsen ein möglichst gutes und aufeinander abgestimmtes Informationssicherheitsniveau zu erreichen.

Vor dem Hintergrund dieser Visionen wird folgendes Leitbild der Cybersicherheitsstrategie Sachsen formuliert:

Der Freistaat Sachsen schützt sich vor Cyberangriffen, unterstützt Wirtschaft und Gesellschaft bei Cybervorfällen durch Bildungs- und Sensibilisierungsangebote und informiert sie zu Lagebild, Präventionsmaßnahmen und Gefährdungen.

23 Strategie zur digitalen Transformation der Sächsischen Staatsverwaltung, S. 43: https://publikationen.sachsen.de/bdb/artikel/43191/documents/65495

3.2. Strategische Ziele und Maßnahmen der Cybersicherheit

Eine Cybersicherheitsstrategie hat das übergeordnete Ziel, eine sichere und widerstandsfähige digitale Umgebung zu schaffen, die vor Cyberbedrohungen schützt und die Risiken minimiert. Im föderalen System der Bundesrepublik Deutschland können die Ziele einer Landesstrategie immer nur im Verbund mit der nationalen Strategie und ggf. weiterer z. B. supranationaler Strategien, wie beispielsweise der Europäischen Union, gesehen werden. So sind bei allen im folgenden Kapitel genannten Zielen auch andere staatliche Ebenen in einer aktiven Rolle. Zudem gibt es Ziele, die eher oder ausschließlich auf nationaler Ebene oder darüber hinaus von den jeweiligen Akteuren verfolgt werden. Beispielsweise wird der Schutz kritischer Infrastrukturen gegen Cybersicherheitsvorfälle gesetzlich durch den Bund geregelt. Die Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit von Systemen, die für das Funktionieren kritischer Infrastrukturen wie Energie, Wasser, Verkehr und Gesundheitswesen entscheidend sind, liegt demnach v. a. in seiner Zuständigkeit. Aus dem im vorherigen Kapitel formulierten Leitbild werden folgende strategische Ziele und dazugehörige Maßnahmen festgelegt:

Ziel 1: Prävention von Cyberangriffen

Wir verhindern Cyberangriffe auf sächsische staatlichen und kommunale Behörden. Dazu ergreifen wir die folgenden Maßnahmen:,

Ausbau der Erkennungssysteme

Wir verbessern die Erkennung von Cyberangriffen durch Implementierung fortschrittlicher Überwachungstechnologien, um die Entdeckungszeit zu verkürzen. Die Sicherheitssysteme der Landesverwaltung werden permanent optimiert und neue Erkennungssysteme, z. B. zu Schwachstellen, in Software eingeführt. Auch die Anzahl durchgeführter Penetrationstests in den Behörden wird gesteigert.

Reduktion von ausnutzbaren Schwachstellen und Absicherung von Schnittstellen in den Behörden

Die staatlichen und kommunalen Behörden arbeiten daran, die Zahl ihrer Webseiten, die im Rahmen der regelmäßigen Webseitenscans eine schlechte Sicherheitsbewertung erhalten, kontinuierlich zu verringern. Ebenso werden mithilfe der Ergebnisse anderer Erkennungssysteme die Zahl von Schwachstellen abgebaut. Die Schnittstellen zwischen den Verwaltungsnetzen und dem Internet werden stärker abgesichert.

Regelmäßige Sicherheitsüberprüfungen und Zertifizierungen

Wir führen in der Staatsverwaltung regelmäßig Sicherheitsüberprüfungen durch, um zu ge-

währleisten, dass staatliche Systeme und Netzwerke den aktuellen Informationssicherheitsstandards entsprechen. Pro Jahr sollen mindestens zehn Sicherheitsüberprüfungen bei staatlichen Behörden vorgenommen werden.

Ziel 2: Stärkung der Cyberabwehrfähigkeiten

Wir minimieren die Auswirkungen von Cyberangriffen. Dazu ergreifen wir die folgenden Maßnahmen:

Stärkung der Resilienz von Behörden

Wir entwickeln das IT-Notfallmanagement der Staatsverwaltung kontinuierlich weiter, um die Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen. Mindestens zwei staatliche Behörden üben pro Jahr selbstgewählte IT-Notfallszenarien. Alle zwei Jahre wird eine landesweite Übung mit Einbindung von Kommunen durchgeführt.

Ziel 3: Bereitstellung von Ressourcen für Cybersicherheit

Wir ermöglichen eine effektive Umsetzung von Cybersicherheitsmaßnahmen. Dazu ergreifen wir die folgenden Maßnahmen:

Ausbau der Erkennungssysteme

Wir verbessern die Erkennung von Cyberangriffen durch Implementierung fortschrittlicher Überwachungstechnologien, um die Entdeckungszeit zu verkürzen. Die Sicherheitssysteme der Landesverwaltung werden permanent optimiert und neue Erkennungssysteme, z. B. zu Schwachstellen in Software eingeführt. Auch die Anzahl durchgeführter Penetrationstests in den Behörden wird gesteigert.

Stärkung des Informationssicherheitsmanagements

Auf allen Verwaltungsebenen im Freistaat Sachsen ist das Niveau der Informationssicherheitsmanagementsysteme zu verbessern. Die Zahl der Kommunen in Sachsen, die ein ISMS auf Grundlage des IT-Grundschutzprofils Kommunalverwaltung betreiben, steigt jährlich um mindestens fünf Kommunen an. Darüber hinaus wird das BSIModell „Wege in die Basis-Absicherung" jährlich in mindestens 20 Kommunen durchgeführt. Die Beratungs- sowie Hilfsangebote des Freistaates sollen ausgebaut werden.

Stärkung von Gefahrenabwehr, Strafverfolgung und Verfassungsschutz

Das SN4C im LKA wird kontinuierlich als Zentralstelle organisatorisch, materiell-technisch und personell weiterentwickelt, um im nationalen und internationalen Vergleich angemessen agieren zu können. Die in den Polizeidirektionen mit der Bekämpfung von Cybercrime befassten ermittlungsunterstützenden und ermittlungsführenden Organisationseinheiten werden den Erfordernissen entsprechend fortentwickelt.

Ziel 4: Schaffung einer Cybersicherheitskultur

Wir schaffen eine Cybersicherheitskultur, die Angriffe erschwert. Dazu ergreifen wir die folgenden Maßnahmen:

Förderung von Cybersicherheitsbewusstsein

Wir steigern das Bewusstsein für Cybersicherheit durch umfassende Bildungsprogramme, Schulungen und Kampagnen. So sollen staatliche Einrichtungen Sensibilisierungsmaßnahmen für 5.000 Bürgerinnen und Bürger pro Jahr durchführen bzw. unterstützen. Für ihre eigenen Bediensteten führen die Behörden des Freistaates Sachsen und der Kommunen jährlich Veranstaltungen oder E-Learning-Angebote zum Thema Informationssicherheit durch, die insgesamt mindestens 10.000 Bedienstete erreichen.

Fortbildungsangebote für Fachkräfte in den Behörden

Die Fortbildung von jährlich 60 ausgebildeten Fachkräften in den Verwaltungen von Land und Kommunen im IT-Grundschutz des BSI bzw. in vertiefenden Cybersicherheitsthemen wird aus einem zentralen Budget finanziert.

Stärkung der Cybersicherheit in kleinen und mittleren Unternehmen (KMU)

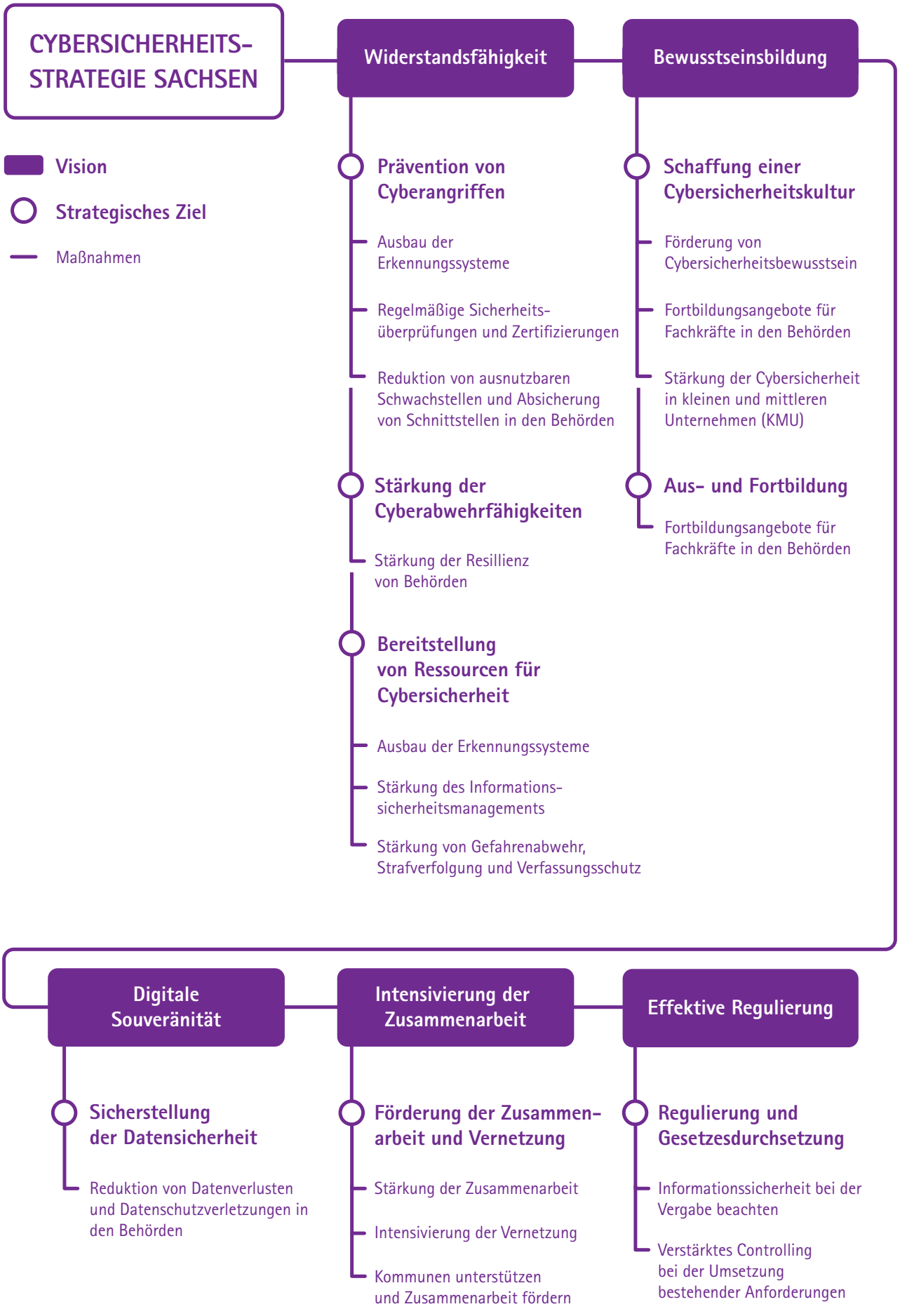
Wir unterstützen Sicherheitsmaßnahmen und Schulungen für KMU, um deren Anfälligkeit für Angriffe zu verringern. So soll die Zahl der im „Cyber-Sicherheitsnetzwerk Sachsen" aktiven Akteure (Digitale Ersthelfer, Vorfall-Praktiker und -Experten sowie IT-Dienstleister) kontinuierlich zulegen.

Ziel 5: Stärkung der Aus- und Fortbildung

Wir fördern die Aus- und Fortbildung unterschiedlicher gesellschaftlicher Zielgruppen im Bereich Cybersicherheit, um sicherzustellen, dass Gesellschaft, Unternehmen und staatliche Institutionen über das erforderliche Know-how verfügen, um kompetent und souverän Cybersicherheitsrisiken zu erkennen und ihnen wirkungsvoll zu begegnen.

Fortbildungsangebote für Fachkräfte in den Behörden

Die Fortbildung von jährlich 60 ausgebildeten Fachkräften in den Verwaltungen von Land und Kommunen im IT-Grundschutz des BSI bzw. in vertiefenden Cybersicherheitsthemen wird aus einem zentralen Budget finanziert.


CYBERSICHERHEITS-
STRATEGIE SACHSEN
Vision
Strategisches Ziel
Maßnahmen
Widerstandsfähigkeit
Prävention von Cyberangriffen
Ausbau der Erkennungssysteme
Regelmäßige Sicherheits-überprüfungen und Zertifizierungen
Reduktion von ausnutzbaren Schwachstellen und Absicherung von Schnittstellen in den Behörden
Stärkung der Cyberabwehrfähigkeiten
Stärkung der Resillienz von Behörden
Bereitstellung von Ressourcen für Cybersicherheit
Ausbau der Erkennungssysteme
Stärkung des Informations-sicherheitsmanagements
Stärkung von Gefahrenabwehr, Strafverfolgung und Verfassungsschutz
Bewusstseinsbildung
Schaffung einer Cybersicherheitskultur
Förderung von Cybersicherheitsbewusstsein
Fortbildungsangebote für Fachkräfte in den Behörden
Stärkung der Cybersicherheit in kleinen und mittleren Unternehmen (KMU)
Aus- und Fortbildung
Fortbildungsangebote für Fachkräfte in den Behörden
Digitale Souveränität
Sicherstellung der Datensicherheit
Reduktion von Datenverlusten und Datenschutzverletzungen in den Behörden
Intensivierung der Zusammenarbeit
Förderung der Zusammen-arbeit und Vernetzung
Stärkung der Zusammenarbeit
Intensivierung der Vernetzung
Kommunen unterstützen und Zusammenarbeit fördern
Effektive Regulierung
Regulierung und Gesetzesdurchsetzung
Informationssicherheit bei der Vergabe beachten
Verstärktes Controlling bei der Umsetzung bestehender Anforderungen

Ziel 6: Sicherstellung der Datensicherheit und des Datenschutzes

Wir gewährleisten die Sicherheit und den Schutz der von Wirtschaft und Gesellschaft den Behörden anvertrauten sensiblen Daten. Dazu ergreifen wir folgende Maßnahme:

Reduktion von Datenverlusten und Datenschutzverletzungen in den Behörden

Wir senken die Anzahl von Datenverlusten und Datenschutzverletzungen durch Implementierung verschärfter Sicherheitsmaßnahmen und Sensibilisierung der Bediensteten, um einen durchschnittlichen Rückgang um mindestens 25 Prozent gemeldeter Fälle von Datenschutzverstößen in den Behörden innerhalb der nächsten fünf Jahre zu erreichen.

Ziel 7: Förderung der Zusammenarbeit und Vernetzung

Wir gehen innerhalb der Staatsverwaltung und gemeinsam mit Bund und Ländern gegen Cyberangriffe und -kriminalität vor. Dazu ergreifen wir die folgenden Maßnahmen:

Stärkung der Zusammenarbeit

Wir setzen uns für den Ausbau der Zusammenarbeit mit Partnern in Bund und Ländern sowie mit Unternehmen bei Maßnahmen zur Erhöhung der Cybersicherheit und zum Austausch von Bedrohungsinformationen ein. In allen acht Themenfeldern der Kooperationsvereinbarung des Freistaates Sachsen mit dem BSI sollen in den nächsten zwei Jahren konkrete Ergebnisse erreicht werden.

Intensivierung der Vernetzung

Ein Lagebild zur Cybersicherheit im Freistaat Sachsen wird regelmäßig erstellt und an alle Behörden mit Cybersicherheitsbezug verteilt. Mittelfristig sollen die Daten in einem besonders gesicherten Portal zusammenlaufen. Perspektivisch soll dieses Lagebild mit Informationen weiterer Partner auch außerhalb der Verwaltung ergänzt und zur gegenseitigen Information verwendet werden. Innerhalb der Staatsverwaltung soll durch eine neue Meldepflichtenverordnung erreicht werden, dass die Meldeintensität zunimmt und von möglichst vielen Behörden automatisierte Sicherheitskennzahlen in das Informationssicherheits-Lagebild der Staatsverwaltung einfließen.

Kommunen unterstützen und Zusammenarbeit fördern

Die Zusammenarbeit der Kommunen untereinander soll weiter intensiviert werden. So ermöglicht es das SächsISichG bereits jetzt, dass mehrere Kommunen gemeinsam einen BfIS benennen können. Die Nutzung dieser Möglichkeit soll stärker forciert werden, damit sich die Zahl der Kommunen mit einem BfIS jährlich um 10 Prozent erhöht. Auch der Aufbau einer kommunalen Plattform für Richtlinien und Best-Practices in der Informationssicherheit ist eine weitere Maßnahme.

Ziel 8: Regulierung und Gesetzesdurchsetzung

Wir entwickeln Gesetze und Vorschriften, die sich mit Cybersicherheit befassen, regelmäßig weiter und bringen neue Vorschriften und Mindeststandards zur Anwendung. Dazu ergreifen wir folgende Maßnahmen:

Informationssicherheit bei der Vergabe beachten

Die Cybersicherheit in Lieferketten von IT-Produkten oder IT-Diensten wird zunehmend betrachtet werden müssen, insbesondere wenn IT-Services nicht mehr allein auf Servern im Verwaltungsnetz betrieben, sondern als Cloud-Lösungen genutzt werden. In der Vergabe und Beschaffung von IT-Produkten und IT-Diensten soll die Sicherheit von vornherein in die Bewertung mit einfließen. Sicherheitsgütesiegel, wie das des BSI, sollen hier als Entscheidungshilfe dienen.

Verstärktes Controlling bei der Umsetzung bestehender Anforderungen

Die Umsetzung der im SächsISichG verankerten Pflichten ist zu verstärken und zu kontrollieren. Das gilt auch für weitere verbindliche Anforderungen, z. B. aus der Leitlinie Informationssicherheit des IT-Planungsrats oder aus für die Staatsverwaltung beschlossenen Leit- und Richtlinien zur Informationssicherheit.

Die im Rahmen der Maßnahmen festgelegten Kennzahlen bieten eine Orientierung für die staatlichen Akteure im Bereich Cybersicherheit, um ihre Wirksamkeit zu bewerten und die Cybersicherheitsstrategie entsprechend anzupassen. Im Kapitel 4 wird dargestellt, in welchen Handlungsfeldern die hier benannten strategischen Ziele und Maßnahmen eine Rolle spielen werden.

4. Handlungsfelder der Cybersicherheitsstrategie Sachsen

Die im Folgenden dargestellten Handlungsfelder bilden die Grundbausteine der Cybersicherheitsstrategie Sachsen und orientieren sich zum einen an den Vorgaben der Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien der IMK und zum anderen an den Anforderungen der NIS-2- Richtlinie. Die Leitlinie der IMK sieht vor, dass ausgehend von einer themenbezogenen Bestandsaufnahme eine maßgeschneiderte Cybersicherheitsstrategie entlang der bestehenden fachlichen Anforderungen entwickelt und mit größtmöglicher Effizienz umgesetzt werden soll. Der erarbeitete Katalog der Leitlinie bietet eine belastbare Grundlage für die Erarbeitung der Sächsischen Cybersicherheitsstrategie und gewährleistet zugleich die länderübergreifende Vergleichbarkeit, Interoperabilität und fachliche Austauschfähigkeit der beteiligten Akteure. Ergänzend setzen die Anforderungen an eine Cybersicherheitsstrategie gemäß Artikel 7 NIS-2-Richtlinie einen klaren Fokus auf Konzepte in bestimmten Themenbereichen, die einem Handlungsfeld zugeordnet werden können.

Die Handlungsfelder selbst sind dabei nicht als voneinander klar zu trennende Silos zu verstehen, sondern stehen in einer Wechselwirkung zueinander. So gibt es in Bezug auf das Thema Kompetenzvermittlung enge Verknüpfungen der Inhalte der Handlungsfelder 4 „Digitalisierungsbezogene Kompetenz" und 5 „Verbraucherschutz" untereinander wie auch zu den Handlungsfeldern 1 „Staat liche Verwaltung und Kommunen", 6 „Fachkräfte" und 7 „Forschung/Hochschulen". Das letztgenannte Handlungsfeld hat wiederum Auswirkungen auf das Handlungsfeld 3 „Wirtschaft und KRITIS" bezogen auf Unternehmensgründungen und Technologieentwicklungen.

Alle in der Cybersicherheitsstrategie Sachsen genannten Handlungsfelder und die darin agierenden Akteure sind in ihren unterschiedlichen Rollen gleichzeitig voneinander abhängig und beeinflussen sich gegenseitig. Neue technologische Entwicklungen und daraus resultierende Veränderungen im Cyberraum führen zu Wechselwirkungen zwischen den Handlungsfeldern und treiben deren Entwicklung voran. Die in den Handlungsfeldern agierenden Akteure bilden die Cybersicherheitsarchitektur in Sachsen und tragen zur Gewährleistung eines hohen Sicherheitsniveaus bei.

4.1. Informationssicherheit in der Staatsverwaltung und in den Kommunen

Die rasant fortschreitende Digitalisierung aller Lebensbereiche erfordert eine zeitgemäße digitalisierte Verwaltung auf staatlicher und kommunaler Ebene. Sie muss dabei moderne, leistungsfähige und sichere Infrastrukturen aufbieten. Die daraus resultierenden Prozesse, ob verwaltungsintern oder im Kontakt der Bürgerinnen und Bürger mit dem Staat, müssen von Beginn an informationstechnisch sicher gestaltet werden. Insbesondere bei personenbezogenen Daten und anderen vertraulichen Informationen muss die Verwaltung sicherstellen, diese vor unbefugten Zugriff zu schützen, da viele der Daten von Bürgerinnen und Bürgern, Unternehmen und anderen Institutionen aufgrund gesetzlicher Pflichten übermittelt worden sind. Verstöße gegen die Schutzziele der Informationssicherheit in der Verwaltung können schwerwiegende Folgen für das Grundvertrauen in die Digitalisierung und das Funktionieren des Staates generell haben.

Wie unter 2.2.3. beschrieben, hat dieses Handlungsfeld mit dem Sächsischen Informationssicherheitsgesetz eine starke rechtliche Basis, die nicht nur die staatlichen Behörden, sondern auch die Kommunen reguliert: So wird die organisatorische Verortung von Beauftragten für Informationssicherheit ebenso festgelegt, wie die Einsetzung angemessener organisatorischer und technischer Vorkehrungen sowie sonstiger Maßnahmen zur Gewährleistung der Informationssicherheit. Auch die Kommunen sind gesetzlich verpflichtet, zum Beispiel ein ISMS aufzubauen und technische Systeme zur Abwehr von Cyberangriffen zu betreiben bzw. betreiben zu lassen. Für Letzteres steht den Kommunen in Sachsen bereits eine etablierte IT-Infrastruktur zur Verfügung. So bietet der Verbund aus Sächsischem Verwaltungsnetz (SVN) und Kommunalem Datennetz (KDN) mit seinen technischen Schutzmaßnahmen eine gute Basis für ein auskömmliches Informationssicherheitsniveau. Fast alle Kommunen sind zumindest in Teilen ihrer IT-Infrastruktur mit dem KDN verbunden.

Bezogen auf die Informationssicherheitsorganisation konnten durch das SächsISichG seit seinem Inkrafttreten im Jahr 2019 enorme Verbesserungen erreicht werden: So wurden in allen obersten Staatsbehörden und weiteren, im Gesetz benannten besonderen Behörden, hauptamtliche Beauftragte für Informationssicherheit eingesetzt. Durch das Hauptamt in den Ressorts hat sich die Professionalisierung spürbar erhöht. So haben sich die Meldung von IT-Sicherheitsereignissen bzw. - Vorfällen intensiviert, wodurch sich der damit einhergehende Informationsfluss zum Schutze aller erhöht hat. Während auf der staatlichen Ebene bis auf wenige Ausnahmen alle Behörden die Rolle eines BfIS besetzt haben, liegt die Quote in den Kommunen bei ca. 60 Prozent. Hier ist jedoch ergänzend festzustellen, dass alle Land-

kreise und kreisfreien Städte die Rolle eines BfIS besetzt haben. Bei den Gemeinden sind vor allem in allen größeren Gebietskörperschaften die Rollen besetzt, sodass hier immerhin rund 80 Prozent der Bevölkerung abgedeckt werden.

Flankierend zu den gesetzlichen Pflichten in der Informationssicherheit unterstützt der Freistaat Sachsen seine Kommunen jedoch auch mit einigen Unterstützungsangeboten. So bietet das SAX.CERT, welches in Sachsen nicht nur für die Staatsverwaltung, sondern auch für die Kommunen zuständig ist, kostenlose Sicherheitsservices wie einen Warn- und Informationsdienst, digitale Sensoren zur Überwachung des Netzwerkverkehrs oder auch einen Webseitenscan an. Daneben finanziert der BfIS Land regelmäßig Schulungsangebote für die Weiterbildung der Beauftragten für Informationssicherheit und bietet monatliche Sprechstunden an. Zudem sind die Vertreter der kommunalen Spitzenverbände stimmberechtigte Mitglieder der Arbeitsgruppe Informationssicherheit (AG IS) auf Landesebene. Damit besteht in Sachsen für die Kommunen ein Dreiklang aus Regulierung, sicherer Basis-Infrastruktur und freiwilligen Unterstützungsangeboten.

Ergänzend wird mit der vorliegenden Cybersicherheitsstrategie Sachsen auf die nachstehenden Themen ein verstärkter Fokus gelegt:

4.1.1. Informationssicherheitsmanagement

Auch nach der Implementierung und Weiterentwicklung von ISMS in den Behörden der Staatsverwaltung und der Kommunen in den letzten Jahren sollen weitere Maßnahmen geprüft werden, um das Niveau der Informationssicherheit zu erhöhen. Bei den Staatsbehörden sollen jährlich zehn Sicherheitsprüfungen und Revisionen durchgeführt werden, um sicherzustellen, dass staatliche ITInfrastruktur und Organisationen den aktuellen Informationssicherheitsstandards entsprechen.

Bei den Behörden auf kommunaler Ebene wird angestrebt, deren Reifegrad der Informationssicherheit systematisch zu erfassen und auszuwerten, um gezielt Maßnahmen zur Verbesserung einleiten zu können. Dazu gehört als möglicher Einstieg insbesondere die Förderung der Umsetzung des vom BSI konzipierten Modells „Weg in die Basis-Absicherung" (WiBA). In mindestens 20 Kommunen soll dieser Einstieg in den IT-Grundschutz jährlich initiiert werden. Die Zahl der Kommunen, die ein ISMS auf Grundlage des deutlich höheren Niveaus des IT-Grundschutzprofils Kommunalverwaltung betreiben, soll in jedem Jahr um mindestens fünf anwachsen. Die Beratungs- sowie Hilfsangebote des Freistaates für die Kommunen, v.a. vom SAX.CERT, sollen ausgebaut werden.

Parallel dazu soll auch die Zusammenarbeit der Kommunen untereinander weiter intensiviert werden. So ermöglicht es das SächsISichG bereits jetzt, dass mehrere Kommunen gemeinsam einen BfIS benennen können. Die Nutzung dieser Möglichkeit soll stärker forciert werden, damit sich die Zahl der Kommunen mit einem BfIS jährlich um zehn Prozent erhöht. Auch der Aufbau einer kommunalen Plattform für Richtlinien und Best-Practices in der Informationssicherheit ist eine weitere Maßnahme. Schließlich ist es unser Anliegen, die erforderlichen Voraussetzungen dafür zu schaffen, dass das KDN intensiver als bislang durch die Kommunen genutzt wird, da erst durch eine breite Anbindung an das KDN alle in diesem Netz eingesetzten technischen Sicherheitsmaßnahmen zur vollen Wirkung kommen.

All diese Bemühungen sollen auch dazu führen, die Anzahl an Datenverlusten und Datenschutzverletzungen in den Behörden zu minimieren. So weist der Tätigkeitsbericht Datenschutz für das Jahr 2023 ca. 950 Meldungen der Verletzung des Schutzes personenbezogener Daten aus, wovon nach Angaben der Sächsischen Datenschutz- und Transparenzbeauftragten rund ein Viertel öffentlichen Stellen zuzurechnen sind. Durch Implementierung verschärfter Sicherheitsmaßnahmen soll ein durchschnittlicher Rückgang um mindestens 25 Prozent der gemeldeten Fälle von Datenschutzverstößen aus den Behörden innerhalb der nächsten fünf Jahre erreicht werden.

4.1.2. Sensibilisierung und Fortbildung

Bereits seit vielen Jahren bieten die Behörden im Freistaat für ihre Bediensteten diverse Sensibilisierungs- und Schulungsmaßnahmen an. Zuvorderst stehen hier die Angebote des BfIS Land, zu denen seit vielen Jahren ein E-Learning-Angebot zur „Informationssicherheit am Arbeitsplatz" zählt, an dem bereits über 30.000 Nutzerinnen und Nutzer teilgenommen haben. Ähnlich hohe Teilnehmerzahlen konnten beim so genannten Live-Hacking, einem Format für Sensibilisierungs-Veranstaltungen, erzielt werden: So nahmen allein an der zentral organsierten landesweiten Reihe „Die Hacker kommen!" seit dem Jahr 2012 – und trotz einiger Jahre Ausfall aufgrund der Corona-Pandemie – über 15.000 Bedienstete aller Behördenebenen in Sachsen teil. Wir wollen das Bewusstsein für Cybersicherheit weiterhin durch umfassende Bildungsprogramme und Kampagnen auf einem guten Niveau halten. Daher werden jedes Jahr E-Learning-Formate, Sensibilisierungsmaßnahmen wie das Live-Hacking oder Präsenzschulungen zu Informationssicherheitsthemen durchgeführt, die mindestens 10.000 Bedienstete von staatlichen und nicht-staatlichen Stellen erreichen. Dabei wird zunehmend auch eine adressatengerechte Fortbildung eine Rolle spielen, z. B. spezielle Angebote für Führungskräfte, Stellen mit IT-Bezug oder andere Stellen, die speziellen Gefährdungen aus dem Cyberraum ausgesetzt sind.

4.1.3. Ausbau der Analyse- und Reaktionskompetenz im Sicherheitsnotfallteam SAX.CERT

Das Sicherheitsnotfallteam SAX.CERT ist zentraler operativer IT-Sicherheitsakteur innerhalb der sächsischen Staatsverwaltung mit Zuständigkeit auch für die kommunale Ebene. Es hat die Aufgabe, zusammen mit dem Netzdienstleister Cyberangriffe durch fortschrittliche Überwachungstechnologien zu erkennen und abzuwehren. Um die Cyberabwehr auf einem hohen Niveau zu halten, müssen sowohl die Sicherheitssysteme des Verwaltungsnetz-Verbunds SVN/KDN als auch die der Behörden permanent optimiert und aufeinander abgestimmt werden sowie Erkennungssysteme ausgebaut bzw. neu eingeführt werden. So gilt es, die Schnittstellen zwischen den Verwaltungsnetzen und dem Internet weiter abzusichern und Schwachstellen zu beseitigen. Die Zahl von Webseiten staatlicher und kommunaler Behörden, die im Rahmen der regelmäßigen Webseitenscans eine schlechte Sicherheitsbewertung erhalten, soll kontinuierlich zurückgehen.

Zu den bestehenden Analyse- und Reaktionskompetenzen im SAX.CERT sollen neue hinzukommen: Die bestehenden Dienste des Security Operations Center in Verbindung mit dem Security Information and Event Management sollen ausgebaut und optimiert werden. Eine als Malware Information Sharing Platform bezeichnete Austauschplattform von Sicherheitsereignissen und Schwachstellen soll zur Verbesserung der Informationsaustausch- und Analysefähigkeiten im SAX.CERT eingeführt werden. Schließlich soll durch gezielte technische und organisatorische Maßnahmen ein Mobile Incident Response Team aufgebaut werden, das von Cyberangriffen betroffene Behörden vor Ort unterstützen kann.

4.1.4. IT-Notfallmanagement zwischen Land und Kommunen verzahnen

Cyberangriffe können zu einem länger dauernden Ausfall von IT-Infrastruktur oder zumindest ITVerfahren führen, unter dem dann Bürgerinnen und Bürger sowie Unternehmen oder andere Institutionen als Kunden der öffentlichen Verwaltung leiden. Auch wenn ein absoluter Schutz nicht existiert, sollten sich die Behörden auf Schadenereignisse aufgrund von IT-Ausfällen vorbereiten, die sich kritisch auf den Geschäftsbetrieb auswirken. Seit Anfang des Jahres 2022 gilt für die Staatsverwaltung die Leitlinie IT-Notfallmanagement des Freistaates

Sachsen. Ausgehend von dieser Leitlinie wurden vom BfIS Land in seiner zusätzlichen Rolle als strategischer IT-Notfallbeauftragten des Landes im Zusammenwirken mit dem operativen IT-Notfallbeauftragten des Landes im SID und den von den Ressorts benannten IT-Notfallbeauftragten Aktivitäten rund um das IT-Notfallmanagement begonnen, z. B. wurden Risikoanalysen durchgeführt und ein übergreifendes IT-Notfallkonzept erstellt inklusive eines IT-Notfallvorsorgekonzepts, das die Aufbauorganisation im IT-Notfallmanagement gestaltet, bis hin zu einem IT-Notfallhandbuch. Das IT-Notfallmanagement der Staatsverwaltung wird in den kommenden Jahren kontinuierlich weiterentwickelt. Mindestens zwei Behörden pro Jahr üben IT-Notfallszenarien.

Zusätzlich zu diesen Arbeiten ist es Ziel der Staatsverwaltung, die kommunale Ebene ausgehend von den Landkreisen und kreisfreien Städten in ein landesweites, ebenenübergreifendes IT-Notfallmanagement einzubeziehen. Hierzu soll als erstes ein regelmäßiger Austausch zwischen den Akteuren zur Förderung der Vernetzung im Bereich des IT-Notfallmanagements etabliert werden, um die Resilienz bei Ausfällen von IT-Systemen oder -Verfahren zu erhöhen. So sollen gemeinsame Schulungen und Übungen für die effektive Bewältigung spezifischer Szenarien sowie übergreifender IT-Sicherheitsvorfälle im Rahmen des IT-Notfallmanagements anvisiert werden: Alle zwei Jahre wird eine landesweite Übung mit Einbindung von Kommunen durchgeführt. Hierzu zählt auch die Unterstützung der Kommunen bei individuellen IT-Notfallübungen durch die Möglichkeit der kostenfreien Nachnutzung bereits erprobter Übungsszenarien und verwendeter Trainingswerkzeuge. Schlussendlich steht die Bewertung der Möglichkeiten zur zentralen Unterstützung betroffener staatlicher Stellen, Landkreise und Kommunen bei IT-Vorfällen zur Wiederherstellung der Leistungsfähigkeit der IT-Infrastruktur im Rahmen des IT-Notfallmanagements an. So sollte die Maßnahme geprüft werden, dass sich Behörden aus Kommunen und Freistaat bei IT-Ausfällen gegenseitig aushelfen können, z. B. indem sie IT-Infrastruktur oder auch Büroarbeitsplätze zur Nutzung anbieten.

4.1.5. Rechtlichen Rahmen erneuern

Die Informationssicherheit von Staat und Kommunen unterliegt zunehmend Regulierungsakten. Mit dem SächsISichG hat der Sächsische Landtag der Staatsverwaltung und den nicht-staatlichen Stellen zwar bereits im Jahr 2019 ein in seiner Zuständigkeit liegendes Gesetz in Kraft treten lassen. Jedoch hat die NIS-2-Richtlinie der EU nicht nur Anforderungen an eine Cybersicherheitsstrategie in Sachsen gesetzt, sondern auch Änderungen am SächsISichG notwendig gemacht, die ebenfalls bis zum 17. Oktober 2024 umgesetzt sein mussten. Da zudem nicht alle Anforderungen der NIS-2- Richtlinie Eingang ins Gesetz finden

können, wird zusätzlich noch eine gesonderte Meldepflichtenverordnung notwendig, die das Melden und Erfassen von IT-Sicherheitsereignissen und IT-Vorfällen genauer reguliert. Diese Rechtsverordnung soll auch regeln, dass die staatlichen Behörden automatisierte Sicherheitskennzahlen in das IT-Sicherheitszentrum des SAX.CERT einfließen lassen. Neben der NIS-2-Richtlinie gibt es weitere europarechtliche Regelungen, die einen Einfluss auf die Cybersicherheit in den Ländern haben, so z. B. die EU-Verordnung zur Cyberresilienz, welche sicherere Hard- und Software gewährleisten soll.

Für den Freistaat ergibt sich daraus insgesamt die Aufgabe, seine Gesetze, Verordnungen und Strategien fortlaufend zu überprüfen, zu evaluieren und zu überarbeiten. Nicht nur das SächsISichG wird nach der NIS-2-bedingten Anpassung auch wieder zu evaluieren und fortzuschreiben sein. Auch die bereits bestehenden Leit- und Richtlinien, die nach SächsISichG in der AG IS erarbeitet und durch den Lenkungsausschuss IT- und E-Government (LA ITEG) verbindlich für die Staatsverwaltung beschlossen werden, müssen regelmäßig überprüft und angepasst werden. Hinzu kommen neue Richtlinien und Strategien nebst integrierter Konzepte, wie z. B. die Open Source Strategie des Freistaates, die ggf. Konzepte für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IT-Produkte und IT-Dienste bei der Vergabe öffentlicher Aufträge erforderlich macht. Auch die Cybersicherheit in Lieferketten von IT-Produkten oder IT-Diensten ist zu betrachten, insbesondere, wenn IT-Services nicht mehr allein auf Servern im Verwaltungsnetz betrieben, sondern als Cloud-Lösungen genutzt werden. In der Vergabe und Beschaffung von IT-Produkten und IT-Diensten soll die Sicherheit von vornherein in die Bewertung miteinfließen. Sicherheitsgütesiegel, wie das des BSI, sollen hier als Entscheidungshilfe dienen.

4.2. Gefahrenabwehr, Strafverfolgung und Verfassungsschutz

Kriminelle nutzen das Internet, um Geld zu erbeuten, Identitäten zu stehlen, Betrug zu begehen und andere illegale Aktivitäten durchzuführen. Dies kann erhebliche wirtschaftliche Schäden verursachen und das Vertrauen der Menschen in digitale Systeme beeinträchtigen. Nach Definition des BKA werden Delikte, die lediglich unter Nutzung von Informationstechnik begangen werden und bei denen das Internet vorwiegend Tatmittel ist, als Cybercrime im weiteren Sinne bezeichnet. Delikte, die sich gegen das Internet und informationstechnische Systeme richten, werden hingegen als sogenannte Cybercrime im engeren Sinne bezeichnet. Als Straftat Cybercrime wurden im Jahr 2023 bezogen auf Sachsen knapp 4.500 Fälle erfasst, und damit gut 28 Prozent mehr als im Vorjahr.[24] Bei den Staatsanwaltschaften im Freistaat liefen im Jahr 2022 Ermittlungen zu rund 13.700 Cybercrime- Fällen.[25] Das Dunkelfeld ist jedoch deutlich höher. So geben über ein Viertel der befragten Bürgerinnen und Bürger in Deutschland im Rahmen der Erhebung zum Cybersicherheitsmonitor 2023 an, bereits persönlich Erfahrung mit Cyberkriminalität gemacht zu haben.[26] Aufgrund dieser erheblichen Gefahren für die Cybersicherheit ist die Arbeit von Gefahrenabwehr, Strafverfolgung und Verfassungsschutz wesentlich, um digitale Delikte zu bekämpfen und Täter zur Rechenschaft zu ziehen.

Effektive Strafverfolgung wirkt abschreckend auf potenzielle Cyberkriminelle. Die Aussicht auf rechtliche Konsequenzen kann dazu beitragen, dass Personen von illegalen Aktivitäten im digitalen Raum absehen. Die Bestrafung von Cyberkriminellen durch konsequente Strafverfolgung trägt zur Sicherheit im digitalen Raum bei. Dies ist entscheidend, um die Integrität von Netzwerken, Systemen und persönlichen Daten zu wahren. Mit effizienter Gefahrenabwehr und konsequenter Strafverfolgung wird das Vertrauen gestärkt, dass es keine rechtsfreien Räume – auch nicht im Digitalen – gibt.

Wichtige Akteure auf Seiten der Staatsverwaltung im Bereich Cybercrime sind spezialisierte polizeiliche Organisationseinheiten, die für die Untersuchung und Verfolgung von Cybercrime zuständig sind. In Sachsen sind das die Polizeidirektionen und das LKA, hier insbesondere das SN4C. Zudem spielen Gerichte und Staatsanwaltschaften eine entscheidende Rolle bei der strafrechtlichen Verfolgung von Cyberkriminalität. In Sachsen gibt es hierfür bei der Generalstaatsanwaltschaft Dresden die Sächsische Zentralstelle zur Bekämpfung von Cybercrime. Daneben ist das Landesamt für Verfassungsschutz (LfV) bei Auswirkungen von Cyberspionage und staatlich unterstützten Angriffen im Cyberraum auf die Sicherheit der verfassungsrechtlichen Ordnung zuständig.

24 https://www.polizei.sachsen.de/de/dokumente/Landesportal/XPKSXJahresXberblickX2023.pdf
25 https://www.mdr.de/nachrichten/sachsen/justiz-kriminalitaet-internet-cybercrime-100.html
26 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/CyMon-ProPK-BSI_2023_Kurzbericht.pdf

4.2.1. Polizei Sachsen

Die Polizei Sachsen sieht die Bekämpfung von Cybercrime als einen strategischen Schwerpunkt sowie gesamtpolizeiliche Aufgabe in der Kriminalitätsbekämpfung. Für diesen Phänomenbereich ist die jeweils geltende „Polizeiliche Bund-Länder-Strategie zur Bekämpfung der Cybercrime" grundsätzliche Maßgabe. Das LKA verfügt mit dem SN4C über ein zentrales Organisationselement zur Bekämpfung von Cybercrime und der Ermittlungsunterstützung im IT-Bereich. Hier sind Expertinnen und Experten in den Bereichen Ermittlung, Massendaten, Telekommunikationsüberwachung und ITForensik vereint. Dadurch werden Methoden für die Ermittlungsunterstützung und Bearbeitung von Verfahren im Bereich Cybercrime weiterentwickelt. Das SN4C im LKA wird kontinuierlich als Zentralstelle organisatorisch, materiell-technisch und personell weiterentwickelt, um im nationalen und internationalen Vergleich angemessen agieren zu können.

Neben dem SN4C des LKA verfügen die Polizeidirektionen über Fachkommissariate mit Cyberermittlungskompetenz. Die in den Polizeidirektionen mit der Bekämpfung von Cybercrime befassten ermittlungsunterstützenden und ermittlungsführenden Organisationseinheiten werden den Erfordernissen entsprechend fortentwickelt. Ziel ist es, der dynamischen technologischen Entwicklung mit steigender materiell-technischer Ausstattung sowie spezialisiertem Personal zu entsprechen. Methoden der Ermittlungs- und Beweisführung sind dieser Entwicklung stetig anzupassen. Die für die Zusammenarbeit der Organisationseinheiten erforderliche moderne IT-Infrastruktur wird fortlaufend ausgebaut.

Neben den repressiven Bekämpfungsmöglichkeiten setzt das LKA beim Thema Cybercrime auch auf Prävention. Das SN4C klärt mit seiner Zentralen Ansprechstelle Cybercrime (ZAC) für Unternehmen, Behörden und Verbände des Freistaates Sachsen zu den Gefahren von Angriffen auf IT-Systeme auf (s. Kapitel 4.3.). Die Cybercrime-spezifische polizeiliche Prävention ist zielgruppenentsprechend und orientiert sich an bundesweiten Bestrebungen.

4.2.2. Landesamt für Verfassungsschutz

Kernaufgaben der nachrichtendienstlichen Cyberabwehr sind die Detektion (Erkennung), die Attribution (Zuordnung) und sowie die Prävention von nachrichtendienstlich gesteuerten Cyberangriffen. Das LfV sammelt Informationen zum Thema Cybersicherheit im Rahmen seiner Zuständigkeit gemäß § 2 Abs.1 Nr. 2 SächsVSG über „sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht" und informiert die zuständigen Sicherheits- und Gefahrenabwehrbehörden. Insbesondere

durch sein Zusammenwirken im Verfassungsschutzverbund erhält das LfV wertvolle Hinweise zu aktuellen Cyberkampagnen und Sabotage- Operationen und gibt vor allem Informationen zu Indicators of Compromise (IoC) in die Staatsverwaltung.

Die Anforderungen an die Cyberabwehr im Verfassungsschutzverbund sind durch die Zunahme von Cyberspionage und -sabotage in den letzten Jahren und insbesondere seit dem russischen Angriff auf die Ukraine deutlich angestiegen. Cyberattacken als Element hybrider Bedrohungen werden perspektivisch weiter zunehmen. Sie bedrohen insbesondere die freiheitliche demokratische Grundordnung und die Sicherheit Deutschlands. Vor diesem Hintergrund wurde im Verfassungsschutzverbund ein gemeinsames Maßnahmenpapier mit Vorschlägen zur Weiterentwicklung und Optimierung der Cyberabwehr erarbeitet und abgestimmt. Die Vorschläge zielen insbesondere auf eine weitere Optimierung des Informationsflusses sowie der Aufgabenverteilung zwischen Bund und Ländern und eine Verbesserung der allgemeingültigen Prozesse und Workflows im Bereich der Cyberabwehr ab.

Ziele des LfV sind die Stärkung der eigenen Resilienz der Sicherheitsbehörden gegen Cyberbedrohungen und die Unterstützung bei der Beratung von Verwaltung und Wirtschaft zur Resilienzbildung und Abwehr von Cyberangriffen ausländischer staatlicher Akteure. Die dazu erforderlichen technischen und personellen Kapazitäten im Bereich der Spionageabwehr/ Cybersicherheit müssen dafür grundlegend ausgebaut und die bereits bestehenden Kooperationen mit dem BSI intensiviert werden.

4.2.3. Justiz

Zur Bekämpfung von Cybercrime wurde 2016 bei der Generalstaatsanwaltschaft Dresden die Sächsische Zentralstelle zur Bekämpfung von Cybercrime (ZCS) eingerichtet, die für den gesamten Freistaat Sachsen zuständig ist. Sie nimmt die Aufgaben einer zentralen Ansprechstelle für Cyberkriminalität, die Organisation und Mitwirkung bei regionalen und überregionalen Aus- und Fortbildungsmaßnahmen in diesem Bereich sowie die Bearbeitung von Cybercrime-Ermittlungsverfahren mit besonderer Bedeutung wahr.

Auch aufgrund der stark steigenden Anzahl von Cybercrime-Ermittlungsverfahren und der zunehmenden Bedeutung dieses Kriminalitätsbereichs wurden mit Wirkung zum 1. September 2023 die Staatsanwaltschaften Dresden und Leipzig zu Schwerpunktstaatsanwaltschaften für Cybercrime ausgestaltet. Diese sind - soweit nicht die ZCS diese Verfahren führt - zur Verfolgung von Straftaten von besonderer Bedeutung im Bereich der Cyberkriminalität zuständig, auch soweit diese Straftaten in den Zuständigkeitsbereich der Staatsanwaltschaften

Görlitz (Schwerpunktstaatsanwaltschaft Dresden), Chemnitz oder Zwickau (Schwerpunktstaatsanwaltschaft Leipzig) fallen.

Darüber hinaus besteht ein enger Austausch mit den am Nationalen Cyberabwehr-Zentrum (NCAZ) direkt beteiligten Generalstaatsanwaltschaften Bamberg und Köln, um über die aktuelle Bedrohungslage und frühzeitig über relevante IT-Sicherheitsvorfälle im Bundesgebiet informiert zu sein. Ziel ist es, darüber je nach Fall relevante sächsische Ermittlungskomplexe zur Darstellung im wöchentlichen Lagebericht und Erörterung mit den Beteiligten im NCAZ einzubringen.

4.3. Wirtschaft und KRITIS

Cyberangriffe, die zu einem Ausfall von IT-Systemen führen, stellen eine enorme Bedrohung für die sächsische Wirtschaft dar. Sind sogar kritische Infrastrukturen (KRITIS) als Träger der Daseinsvorsorge betroffen, kann sich die Bedrohung auf die Versorgungssicherheit der Bevölkerung und das Funktionieren der öffentlichen Verwaltung auswirken. Eine Studie des Verbandes der deutschen Informations- und Telekommunikationsbranche Bitkom e. V. weist aus, dass der jährliche Schaden für die deutsche Wirtschaft aufgrund von Cyberattacken bei rund 150 Milliarden Euro liegt.[27] Insofern ist es nachvollziehbar, dass die deutschen Unternehmen Cybervorfälle und damit einhergehende IT-Ausfälle als das größte Geschäftsrisiko bezeichnen.[28] Cybersicherheit muss daher integraler Bestandteil des Managements von Unternehmen sein, da sie nicht nur durch Cyberbedrohungen verursachte Risiken reduziert, sondern auch die Grundlage für ein vertrauenswürdiges und resilienteres Geschäftsumfeld bildet. Da Unternehmen durch den zunehmenden Digitalisierungsgrad eine enorme Menge an sensiblen Daten verarbeiten und speichern, kann ein Cybervorfall zu erheblichen Datenverlusten führen, was das Vertrauen der Kunden beeinträchtigen kann. Zudem müssen Unternehmen in diesem Zusammenhang auch sicherstellen, dass sie die gesetzlichen Bestimmungen einhalten, um rechtliche Konsequenzen zu vermeiden. Cyberangriffe können zudem die Verfügbarkeit von IT-Systemen und geschäftskritischen Anwendungen beeinträchtigen. Eine robuste Cybersicherheitsinfrastruktur ist entscheidend, um die Geschäftskontinuität sicherzustellen und Ausfallzeiten zu minimieren. Der durch Cyberangriffe ausgelöste Ausfall von IT-Systemen kann zu erheblichen finanziellen Verlusten führen, sei es durch Datenverlust, Erpressung (Ransomware), Betrug oder Betriebsunterbrechungen. Investitionen in Cybersicherheit sind daher eine notwendige präventive Maßnahme. Da manche Unternehmen erhebliche Ressourcen in Forschung, Entwicklung und Innovation investieren, helfen Maßnahmen zur Erhöhung der Cybersicherheit zudem, geistiges Eigentum vor Diebstahl und unbefugtem Zugriff zu schützen.

27 https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf
28 https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024-Appendix.pdf

Die Verantwortung für den Schutz der IT-Infrastrukturen liegt in erster Linie bei den Unternehmen selbst. Die konkreten Maßnahmen, um Cybersicherheit von Unternehmen zu gewährleisten, unterscheiden sich prinzipiell nicht von denen von Behörden oder anderen Institutionen. Insofern gelten die im Kapitel 3.2. benannten strategischen Ziele auch für Unternehmen. Größere Unternehmen sind hier in der Regel bereits gut aufgestellt und vernetzt. Staatliche Angebote zur Stärkung der Resilienz von Wirtschaft und Versorgung konzentrieren sich daher auf den Bereich der KMU mit Fokus auf kritische und wichtige Einrichtungen. Die Cybersicherheitsstrategie Sachsen zeigt deshalb auf, mit welchen Maßnahmen staatliche Behörden Unternehmen in der Cybersicherheit unterstützen und welche Ziele erreicht werden sollen.

Im Bereich der Regulierung ist festzustellen, dass das IT-Sicherheitsgesetz des Bundes seit dem Jahr 2015 die Cybersicherheit der Wirtschaft im Gebiet der Versorgung durch kritische Infrastrukturen regelt. Das Ziel des IT-Sicherheitsgesetzes ist die Verbesserung der IT-Sicherheit durch Vorgabe von Sicherheitsstandards bei Unternehmen, die Betreiber kritischer Anlagen nach der BSIKRITIS- Verordnung sind. Es reguliert also Unternehmen in Sektoren wie Ernährung, Energie, Gesundheit, Transport und Verkehr sowie Wasser. Durch die NIS-2-Richtlinie der EU wird sich der Anwendungsbereich erheblich ausweiten, sodass künftig deutlich mehr Unternehmen dadurch reguliert werden. Um die Einheitlichkeit des Wirtschaftsraums bezogen auf die Regulierung der Cybersicherheit nicht zu unterlaufen, reguliert der Freistaat Sachsen die Cybersicherheit von Unternehmen nicht eigenständig, solange und soweit der Bund von seiner Zuständigkeit Gebrauch macht.

Um die Wirtschaft zu unterstützen, stellt der Freistaat Sachsen gezielt finanzielle Mittel zur Verfügung oder entlastet die Wirtschaft in anderer Weise finanziell. Somit werden Investitionen in Cybersicherheitsmaßnahmen erleichtert. In der aktuellen EU-Förderperiode 2021 bis 2027 unterstützt der Freistaat über das Sächsische Staatsministerium für Wirtschaft, Arbeit und Verkehr (SMWA) Digitalisierungs- und Markteinführungsvorhaben kleiner und mittlerer Unternehmen sowie junger, innovativer Firmen (Start-ups) mit Mitteln aus dem Europäischen Fonds für regionale Entwicklung (EFRE). Demnach werden Transformationsprojekte gefördert, wenn mit Hilfe moderner Informations- und Kommunikationstechnologien komplexe Geschäftsprozesse digitalisiert, neue Geschäftsmodelle eingeführt oder bestehende Geschäftsmodelle verbessert werden. Förderfähige Projekte können hierbei auch solche sein, die der Verbesserung der IT-Sicherheit und des Informationsschutzes dienen. Mittel- und langfristiges Ziel ist es, die Erfahrungen aus der aktuellen Förderperiode zu nutzen und somit konkrete Bedarfe der Unternehmen noch besser zu erfassen, damit diese bei der Ausgestaltung etwaiger zukünftiger Fördermittelprogramme berücksichtigt werden können.

Neben der finanziellen Förderung ist die Stärkung von Zusammenarbeit eine weitere zentrale Säule der Unterstützungsleistungen des Freistaates Sachsen: Die Schaffung von Plattformen und Foren, um den Austausch bewährter Praktiken und die Zusammenarbeit zwischen Unternehmen zu fördern, kann einen enormen Mehrwert bieten. Mit der Initiative „Cyber-Sicherheitsnetzwerk Sachsen", die sich am Konzept des gleichnamigen Netzwerks des BSI orientiert, befördern die DiAS aus dem Geschäftsbereich des SMWA, die sächsischen Handwerkskammern, die Industrie- und Handelskammern (IHK) sowie das LKA Sachsen den Aufbau eines Netzwerks für Unternehmen in den zentralen Bereichen Prävention und Reaktion. Unternehmen können auf gebündelte Informationen im Sinne der Hilfe zur Selbsthilfe und auf kostenlose Angebote einer Erstberatung zugreifen. Zudem wird in Form einer Notfallkarte gezeigt, wie nach einem Vorfall der Geschäftsbetrieb zügig wiederaufgenommen werden kann. Derzeit sind im „Cyber-Sicherheitsnetzwerk Sachsen" über 20 Digitale Ersthelfer sowie zertifizierte Vorfall-Praktiker und Vorfalls-Experten registriert, die Unternehmen je nach Art des Vorfalls zur Seite stehen können. Weitere IT-Dienstleister aus vertrauenswürdigen sächsischen Netzwerken erweitern diesen Kreis. Nach der Initiierung ist nun die stetige Vergrößerung dieses Netzwerks eine wichtige Maßnahme, damit eine nennenswerte Zahl an Unternehmen von der Zusammenarbeit und den Angeboten profitieren kann. Die Zahl der im „Cyber-Sicherheitsnetzwerk Sachsen" aktiven Akteure (Digitale Ersthelfer, Vorfall-Praktiker und -experten sowie zertifizierte IT-Dienstleister) soll weiter kontinuierlich zulegen.

Zum Schutz der Unternehmen vor Cyberangriffen tragen die staatlichen Behörden wesentlich bei, indem sie die ihnen vorliegenden aktuellen Informationen zu Cyberbedrohungen und -Trends in geeigneter Form mit der Wirtschaft teilen. Durch den Austausch von Bedrohungsdaten sind Unternehmen in der Lage, sich besser vorzubereiten und effektiver auf neue Bedrohungen zu reagieren. Das LfV bietet sich als Sicherheitspartner für alle sächsischen Unternehmen an. Zu diesem Zweck geht das LfV aktiv auf potenziell gefährdete Unternehmen zu. Inhalte einer Sicherheitspartnerschaft können Vorträge, Individualberatungen, Onlineangebote und Broschüren sein. Darüber hinaus unterstützt das LfV alle Interessenten bei der Analyse ihrer Einrichtungen auf spionagerelevante Schwachstellen, bei der Entwicklung individueller Abwehrlösungen und bei der Aufklärung von Verdachtsfällen. In der Vergangenheit gab es mit den „Wirtschaftsschutztagen" Veranstaltungen des LfV gemeinsam mit den Industrie- und Handelskammern in Sachsen, bei denen sich Bedienstete des Verfassungsschutzes als Ansprechpartner zu allen Fragen in Sachen Wirtschaftsspionage/Wirtschaftsschutz mit Vorträgen und Info-Ständen präsentierten. Um mehr IHK-Mitglieder zu erreichen, soll die Zusammenarbeit intensiviert werden.

Das SN4C im LKA bietet mit der ZAC Unterstützung für Unternehmen, Behörden und Verbände des Freistaates Sachsen. Die ZAC nimmt Sicherheitsvorfälle mit Bezug zu Cybercrime auf, leitet polizeiliche Maßnahmen zur Strafverfolgung ein und berät zur Vorbeugung und dem Erkennen von Gefahren durch Cybercrime. Ein wichtiges Anliegen der ZAC ist auch die Förderung der vertrauensvollen Zusammenarbeit zwischen Wirtschaftsunternehmen, Behörden und der Polizei.

Auch wenn die Regulierung der Betreiber kritischer Anlagen in Bezug auf Cybersicherheit dem Bund obliegt, wird der Freistaat Sachsen im Bedarfsfall bei Sicherheitsvorfällen in diesem Bereich mit notwendiger Koordinierung von Reaktionen ergänzend mitwirken. So ist mit dem Bund ein Prozess entwickelt worden, in dem das SAX.CERT als zentrale Meldestelle des Landes Meldungen zu schwerwiegenden Ausfällen entgegennimmt und bewertet. In diesem Rahmen werden die Stellen der Ressorts mit einer Zuständigkeit für einen KRITIS-Sektor einbezogen, damit Cybervorfälle bei durch den Bund regulierten Unternehmen und ihre Auswirkungen auf Sachsen beurteilt sowie kleine Betreiber aus dem gleichen Sektor in geeigneter Weise über gegebenenfalls existierende Sicherheitslücken in IT-Systemen gewarnt werden können. Um das Sicherheitsbewusstsein in diesem Bereich generell zu stärken, werden Betreiber kritischer Anlagen in kommunaler Trägerschaft oder unter Beteiligung von Kommunen insbesondere zu den gesetzlichen Anforderungen des Bundes vom Freistaat informiert und unterstützt. Hierbei werden neben dem SAX.CERT in seiner Rolle als zentrale Kontaktstelle auch für die allgemeine Sicherheit von kritischen Infrastrukturen zuständigen Akteure in der Staatsverwaltung im Sinne eines All-Gefahren-Ansatzes eingebunden.

4.4. Digitalisierungsbezogene Kompetenz

In der heutigen Welt sind große Teile der Gesellschaft von digitalen Technologien und Geräten umgeben, die die Menschen in vielen Bereichen des täglichen Lebens unterstützen. Gleichzeitig gibt es Bedrohungen im digitalen Raum, wie z. B. betrügerische Phishing E-Mails, Verschlüsselung von Daten durch Ransomware oder Missbrauch von persönlichen Daten. Digitalisierungsbezogene Kompetenzen helfen jedem Einzelnen dabei, diese Bedrohungen zu erkennen und zu bewerten, sichere IT-Systeme zu nutzen, angemessene Schutzmaßnahmen zu ergreifen und im Falle eines Sicherheitsvorfalls richtig zu reagieren. Diese Kompetenz stellt somit eine Fähigkeit dar, sicher und selbstbestimmt in einer digitalisierten Umgebung zu handeln.

Es gibt viele Möglichkeiten, um digitalisierungsbezogene Kompetenzen (verstanden als Teil einer allgemeinen Medienkompetenz) zu erwerben und zu verbessern. Dazu gehören z. B. spezifische Unterrichtsstunden in der Schule oder Lehrangebote der Hochschulen, besondere Aktionstage oder -wochen, Weiterbildungen und Kurse zu spezifischen digitalen Tools und Technologien, Online- Tests, Selbsteinschätzungen oder E-Learning-Kurse im Internet. Es ist wichtig, sich kontinuierlich weiterzubilden und digitale Fähigkeiten auszubauen, um sich vor den ständig wachsenden Bedrohungen im digitalen Raum zu schützen.

Ziel der Cybersicherheitsstrategie Sachsen ist es, dass die sächsische Bevölkerung in den betroffenen Altersgruppen selbstbestimmt und kompetent Computer, Smartphones, vernetzte IT-Geräte und IT-Dienste nutzen kann. Sie baut insofern auf der Sächsischen Landesstrategie zur Medienbildung im außerschulischen Bereich „MESA – Medienbildung in Sachsen" aus dem Jahr 2019 auf (s. Kapitel 2.3.4.). Digitalisierungsbezogene Kompetenzen mit Bezug zur Cybersicherheit sind Teil einer umfassenden Medienkompetenz. Der Freistaat Sachsen fördert den Erwerb digitalisierungsbezogener Kompetenzen unter Einbeziehung von Sicherheitsaspekten vor allem in vier Bereichen:

4.4.1. Schulische Bildung

Medienkompetenz gilt als Schlüsselqualifikation für eine gleichberechtigte und selbstbestimmte Teilhabe am gesellschaftlichen Leben. Die Handlungsfelder zur Förderung der Medienkompetenz in Sachsens Schulen sind durch die Konzeption des Sächsischen Staatsministeriums für Kultus (SMK) zur „Medienbildung und Digitalisierung in der Schule" untersetzt. Die Konzeption integriert den Kompetenzrahmen zu „Kompetenzen in der digitalen Welt" der Ständigen Konferenz der Kultusminister der Länder in

der Bundesrepublik Deutschland – kurz Kultusministerkonferenz – (KMK) aus dem Jahr 2016. Dementsprechend ist Medienbildung in den sächsischen Lehrplänen als Querschnittsaufgabe und überfachliches Ziel in den Fächern, des fächerverbindenden Unterrichts und der außerunterrichtlichen Angebote von Schule, z. B. in der Medienprojektarbeit, angelegt. Sie erfolgt integrativ und ist somit explizit nicht nur Bestandteil der Fächer Informatik bzw. Technik/Computer. Dabei ergänzen sich Medienbildung und informatische Bildung wechselseitig. Die in den Lehrplänen formulierten Inhalte und Ziele der Medienbildung sollen die Schülerinnen und Schüler – beginnend in der Grundschule und dann über alle Schulformen und Klassenstufen hinweg – befähigen, ihre Medienkompetenz zunehmend selbstständiger einzuschätzen, einzuordnen und weiterzuentwickeln. Der Kompetenzrahmen „Kompetenzen in der digitalen Welt" besteht aus sechs Bereichen, darunter der Bereich „Schützen und sicheres Agieren", indem auch Cybersicherheitsthemen vermittelt werden.

Die in den Lehrplänen verankerten Bezüge zur schulischen Medienbildung werden zudem durch qualitativ hochwertige Medienbildungsprojekte externer Partner unterstützt, sodass eine aktive und reflexionsfördernde Auseinandersetzung der Schülerinnen und Schüler mit aktuellen Themen der Digitalisierung in Gesellschaft und Bildung gelingt. Ziel ist der Erwerb von Handlungskompetenz auch im Bereich Cybersicherheit.

Im Fach Informatik allgemein sowie an den M.I.T.-Oberschulen und Gymnasien im Spezielleren können Schülerinnen und Schüler über die Förderung der Medienkompetenz hinaus weitergehende Kenntnisse und Fähigkeiten mit Bezug zur Cybersicherheit erwerben.

Im Rahmen des Safer Internet Day, einem von der Europäischen Kommission initiierten jährlichen internationalen Aktionstag für mehr Sicherheit im Netz, werden sachsenweit Veranstaltungen organisiert, die einen nachhaltigen Beitrag für mehr Cybersicherheit und ein besseres Internet für Kinder und Jugendliche leisten. Sie richten sich an Schülerinnen und Schüler, Lehrkräfte und Eltern und werden vom Landesamt für Schule und Bildung in Zusammenarbeit mit verschiedenen Partnern durchgeführt.

Die Bildungsinitiative „Medienscouts in Sachsen" engagiert sich für die Ausbildung von Kindern und Jugendlichen, die sich an ihren Schulen freiwillig für die Medienkompetenzförderung einsetzen. Dabei werden alle Schularten einbezogen, Lehrkräfte durch Fortbildung bei der Ausbildung von Medienscouts unterstützt und bei der Suche nach außerschulischer medienpädagogischer Unterstützung beraten. Es werden Materialien für die Schule zur Aufnahme des Medienscout-Konzeptes in das schulische Medienbildungskonzept bereitgestellt.

4.4.2. Außerschulische Projekte

Um auch im außerschulischen Bereich in den unterschiedlichsten Bereichen digitalisierungsbezogene Kompetenzen vermitteln zu können, ist es mitentscheidend, die Fähigkeiten der in diesen Bereichen arbeitenden Menschen zu entwickeln. Die Stärkung der Medienkompetenz wird in der überörtlichen Jugendhilfeplanung des Freistaates Sachsen für die Jahre 2021-2025 als thematischer Arbeitsschwerpunkt definiert. Auch in der kommenden überörtlichen Jugendhilfeplanung soll das Thema als Arbeitsschwerpunkt fortgeführt werden. Mit den thematischen Arbeitsschwerpunkten benennt der überörtliche Planungsträger handlungsorientierte Zielvorgaben für die überörtliche Bildungsarbeit. In diesem Zusammenhang fördert der Freistaat Sachsen auf Grundlage der Förderrichtlinie überörtlicher Bedarf zwei themenspezifischen Fachstellen in den Bereichen erzieherischer Kinder- und Jugendschutz, Medienerziehung und Medienkompetenz. Im Zentrum stehen Angebote der medienpädagogischen Fortbildung und Beratung für Fachkräfte der Jugendhilfe, Träger der Jugendhilfe, Kinder und Jugendliche sowie deren Eltern.

Daneben werden über die Koordinierungsstelle Medienbildung (KSM) verschiedene Angebote v. a. für Kinder und Jugendliche vermittelt, z. B. Feriencamps, Workshops und Vorträge im Rahmen der drei in Sachsen bestehenden „Jugend hackt Labs", und Anbieter von Online-Kursen, die cybersicherheitsrelevante Themen aufbereiten. Die KSM unterstützt die Netzwerkbildung in der Medienbildungslandschaft Sachsens. Die KSM macht die medienpädagogischen Angebote in Sachsen sichtbar und vernetzt außerschulische Akteurinnen und Akteure, berät die sächsische Bevölkerung und weist auf wichtige Informationen im Bereich Medienbildung hin.

4.4.3. Erwachsenenbildung

Erwachsenenbildung ist für die Cybersicherheitsstrategie Sachsen ein zentraler Bereich der Vermittlung von digitalisierungsbezogenen Kompetenzen in Bezug auf das Thema Cybersicherheit. Immerhin gehen 85 Prozent der sächsischen Bevölkerung altersbedingt nicht mehr zur Schule. Bereits Menschen, die heute über 30 Jahre alt sind, konnten zu ihrer Schulzeit keine heute wichtigen auf Cybersicherheit bezogenen Kompetenzen erwerben. Daher bieten die sächsischen Volkshochschulen Bildungsangebote zu außerberuflichen Digitalkompetenzen an. Beispiele sind u. a. Smartphone- Kurse für Seniorinnen und Senioren, Angebote zum sicheren Online-Shopping, Online-Banking, EMail- Kommunikation und zum Surfverhalten. Inhalt dieser Kurse, Schulungen und Workshops ist u. a. auch die präventive Cybersicherheit.

Damit folgen die Volkshochschulen der Sächsischen Landesstrategie zur Digitalen Transformation von Volkshochschulen, in der Kompetenz in Cybersicherheit als Teil der allgemeinen Medienkompetenz integraler Bestandteil des strategischen Handlungsfeldes „Bildung zur Digitalisierung" ist. Allerdings gehören insbesondere präventive auf Cybersicherheit bezogene Kompetenzen zu einem Weiterbildungsfeld, bei dem eine Diskrepanz zwischen Bildungsbedarfen und Bildungsbedürfnissen festzustellen ist. Oft werden die eigenen Kompetenzlücken und Bildungsbedarfe nur unzureichend oder gar nicht erkannt. Dies führt dazu, dass die objektiv vorhandenen Bildungsbedarfe der Bevölkerung nicht ausreichend zu individuellen und subjektiv wahrgenommenen Bildungsbedürfnissen und mithin zur Veranlassung / Motivation zur freiwilligen Teilnahme an einschlägigen Bildungsangeboten führen. Eine Teilnahmegebühr senkt diese Motivation zusätzlich, sodass entsprechende Bildungsangebote häufig nur entgeltfrei realisiert werden können. Es sind daher Bildungs- und Informationsformate erforderlich, die zum einen ohne finanzielle Hürden zugänglich sind und zum anderen neue methodisch-didaktische Ansätze nutzen. Auch Formate der aufsuchenden Bildungsarbeit sind im besonderen Maße erforderlich. Der Freistaat Sachsen wird daher prüfen, inwieweit er seine Förderinstrumente weiterentwickeln sollte, um den Zugang zu den Angeboten der Volkshochschulen zu vergrößern.

In Zusammenarbeit mit den Volkshochschulen veranstaltet die Sächsische Staatskanzlei in Form einer öffentlichen Sensibilisierungskampagne bereits seit dem Jahr 2016 in loser Folge sogenannte Live-Hackings für Bürger. An der Cybersicherheits-Roadshow, die durch ganz Sachsen tourt, nehmen zudem die Verbraucherzentralen in Sachsen und weitere Einrichtungen wie das BSI oder die Sächsische Datenschutz- und Transparenzbeauftragte teil. Orientierung hierfür bietet der Europäische Monat der Cybersicherheit (European Cyber Security Month, kurz ECSM), der jährlich mit Schwerpunkt im Oktober stattfindet. Der ECSM ist eine europaweite Informations- und Sensibilisierungskampagne, die den Bürgerinnen und Bürgern u. a. das Thema Cybersicherheit mit verschiedenen Veranstaltungen und Publikationen näherbringen möchte. Der Freistaat Sachsen hatte sich hier als erstes Bundesland in Deutschland an der Kampagne beteiligt. Bei den in Sachsen organisierten ca. zweistündigen Veranstaltungen zeigten Computerexperten leicht verständlich einfache Tricks und Handgriffe, damit private IT-Nutzer ihre Informationen und Daten auf Computer, Tablet und Smartphones vor fremdem Zugriff geschützt halten können und keine leichten Opfer für Cyberkriminelle werden. Seit dem Jahr 2016 wurden insgesamt 88 Veranstaltungen in 17 unterschiedlichen Städten angeboten. An den Live-Hackings nahmen insgesamt über 8.500 Bürgerinnen und Bürger teil. In vielen Städten wurden zudem zwei bis drei Veranstaltungen an einem Tag angeboten und dabei die früheren Veranstaltungen z. B. für Schülerinnen und Schüler, Auszubildende oder auch Bedienstete von Behörden reserviert. Diese Veranstaltungsreihe soll in den kommenden Jahren in Zusammenarbeit mit den vorbenannten Einrichtungen fortgesetzt werden. Allein die staatlichen Einrichtungen sollen Sensibilisierungsmaßnahmen für 5.000 Menschen aller Altersgruppen pro Jahr durchführen bzw. unterstützen.

Das SMS ist zudem Partner des „DigitalPakt Alter", eine gemeinsame Initiative des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ) und der Bundesarbeitsgemeinschaft der Seniorenorganisationen auf Grundlage der Empfehlungen des Achten Altersberichtes des BMFSFJ. Das bundesweite Netzwerk engagiert sich aktiv für die digitale Teilhabe älterer Menschen. Bestehende Angebote vor Ort werden hierüber bekannt und damit zugänglich gemacht. Neue Erfahrungsorte können sich bewerben und gefördert werden und Anbieter finden Unterstützung für ihre Öffentlichkeitsarbeit sowie zahlreiche Schulungsmaterialien – hier auch im Bereich der Medienkompetenzbildung und für digitale Sicherheit.

4.4.4. Berufliche Bildung und Weiterbildung

Aus- und Fortbildungsprogramme für Lehrkräfte sind unerlässlich, um sicherzustellen, dass sie die neuesten Entwicklungen in der Cybersicherheit verstehen und dieses Wissen an ihre Schüler weitergeben können. Daher wird Cybersicherheit als Teil digitalisierungsbezogener Kompetenzen im Rahmen des Vorbereitungsdienstes für Lehrämter berücksichtigt. So sind Kompetenzentwicklungsziele in der zweiten Phase der Lehrkräftebildung für den Gesamtbereich der Medienbildung angelegt. Das verbindliche Curriculum umfasst in diesem Kontext u. a. das Thema Schutz und Sicherheit in der digitalen Welt. Ebenso ist Medienbildung im Portfolio der staatlichen Lehrkräftefortbildung ein Schwerpunktthema. Unterschiedliche Veranstaltungen u. a. auch zu Datenschutz und Datensicherheit können hier abgerufen werden.

Der Freistaat Sachsen sensibilisiert und schult auch insgesamt seine Bediensteten sowie die der Kommunen zum Thema Informationssicherheit (s. Kapitel 4.1.2.). So wird bereits seit sechs Jahren ein E-Learning zur „Informationssicherheit am Arbeitsplatz" angeboten, an dem bis dato über 30.000 Bedienstete teilgenommen haben. Daneben werden regelmäßig sogenannte Live-Hacking-Veranstaltungen ausgerichtet, an denen sich in den Hochzeiten vor der Corona-Pandemie rund 3.000 Teilnehmer pro Jahr angemeldet haben. Hier wird der Freistaat seine Angebote fortsetzen und zielgruppenspezifischer ausrichten. Ziel ist es, das E-Learning für Bedienstete allgemein, aber auch für besondere Gruppen, wie Führungskräfte und IT-Fachkräfte, weiterzuentwickeln. Des Weiteren soll die Sensibilisierung zur Informationssicherheit in zentralen landesweiten wie auch in behördenspezifischen Veranstaltungen wieder verstärkt angeboten werden. Mit diesen Maßnahmen und weiteren Schulungsangeboten zur Informationssicherheit des Fortbildungszentrums Meißen kommt der Freistaat Sachsen dem strategischen Ziel der Strategie der digitalen Transformation der Sächsischen Staatsverwaltung nach, ein abgestimmtes System an Angeboten der Fort- und Weiterbildung vorzuhalten.

4.5. Verbraucherschutz

Vernetzte Geräte werden im Alltag von Verbraucherinnen und Verbrauchern zunehmend eingesetzt, so etwa vom Smartphone über Smart Toys bis hin zu kompletten Smart-Home-Systemen. Doch viele Menschen fühlen sich nicht ausreichend geschützt und sind es tatsächlich auch nicht. Technische Systeme werden immer komplexer und die mit ihnen verbundenen Datenverarbeitungen immer schwieriger zu überblicken. Gesetzlich festgeschriebene, einheitliche und von anerkannten Stellen kontrollierte Mindestanforderungen für die IT-Sicherheit sind deshalb wichtige verbraucherschützende Maßnahmen.

Aufgabe des Verbraucherschutzes ist es unter anderem, sich für Regulierung, anbieterunabhängige Qualitätssiegel für sichere Produkte und für eine Marktüberwachung einzusetzen. Außerdem gehören die Information, die Beratung einschließlich nötiger Warnungen der Verbraucherinnen und Verbraucher sowie die Rechtsdurchsetzung dazu, damit digitale Produkte und Dienste sicher genutzt werden können. In dieser Rolle ist der Verbraucherschutz ein wichtiger Akteur in der Vermittlung digitalisierungsbezogener Kompetenzen (s. Kapitel 4.4.). In diesem Kontext soll die öffentliche Wahrnehmung für Verbraucherschutz begleitend durch landesweite Kampagnen gesteigert werden, denen ein übergeordnetes sächsisches Kampagnenkonzept zugrunde liegt.

Wesentliche Akteure im Verbraucherschutz mit Bezug auf die Cybersicherheit sind in Deutschland das BSI mit seinem Fachbereich Digitaler Verbraucherschutz und die Verbraucherzentralen. Als Qualitätssiegel für IT-Produkte gilt in Deutschland das IT-Sicherheitskennzeichen, das vom BSI vergeben wird.

Damit IT-Sicherheit gelingen kann, sind die Fähigkeiten, Einschränkungen und Gewohnheiten von Nutzerinnen und Nutzern einzubeziehen. Um das Ziel zu erreichen, den Verbraucherschutz zur Cybersicherheit in Sachsen zu intensivieren, soll die Maßnahme umgesetzt werden, durch regelmäßige, zielgruppenorientierte Veranstaltungsformate alle betroffenen Bevölkerungsschichten zu sensibilisieren. Gemeinschaftliche Kommunikationsmaßnahmen und Aktionen sind hierbei Gewähr für eine erfolgreiche Umsetzung.

Konkrete Maßnahmen der Staatsverwaltung sind in den Kapiteln 4.4.1. und 4.4.3. benannt. Darüber hinaus wirken in Sachsen das BSI und die Verbraucherzentrale Sachsen im Rahmen einer Übereinkunft zur vertieften Zusammenarbeit z. B. bei der Umsetzung eines gemeinsamen Projekts zur Steigerung des Schutzniveaus für Verbraucherinnen und Verbraucher zusammen.

4.6. Fachkräfte

Fachkräfte für Cybersicherheit arbeiten in Bereichen, die Organisationen und Einzelpersonen vor Gefahren von Cyberangriffen schützen. Dies umfasst den Schutz von Daten, persönlichen Informationen, finanziellen Transaktionen und kritischer Infrastruktur. Cybersicherheitsexperten tragen dazu bei, die wirtschaftliche und gesellschaftliche Stabilität zu gewährleisten, indem sie Unternehmen vor finanziellen Verlusten durch Datendiebstahl und Betrug schützen bzw. dafür sorgen, dass Behörden und kritische Infrastrukturen verlässlich funktionieren und dadurch sowohl die öffentliche Daseinsvorsorge als auch das allgemeine Vertrauen in die Demokratie gewährleistet sind.

Spezielle Fachkräfte sind gerade auch für den Freistaat Sachsen wichtig, der mit seiner hohen Dichte an erstklassigen Forschungseinrichtungen, als führender europäischer Halbleiter-Standort, mit seiner stark wachsenden Software- und Kreativbranche, einer dynamischen Startup-Szene und seinem innovativen Mittelstand insbesondere im High-Tech-Sektor eine vielfältige Unternehmenslandschaft beheimatet, die für einen hohen Grad an Digitalisierung steht. Um diese zukunftsorientierte Wirtschaftslandschaft langfristig in Sachsen zu halten, muss ein stetiger Zugewinn an Knowhow unterstützt werden. Die Frage der Fachkräftesicherung ist wesentlich für die Zukunft der sächsischen Unternehmen und für die Gesellschaft.

Ziel ist es, dem bestehenden IT-Fachkräftemangel wirksam zu begegnen, um einerseits den Wissenschafts- und Wirtschaftsstandort zu festigen und andererseits die Digitalisierung und die Cybersicherheit im Freistaat Sachsen langfristig durch gut ausgebildetes Fachpersonal zu sichern.

Um hochqualifizierte Fachkräfte in der Cybersicherheit zu gewinnen, ist es wichtig, eine gezielte Strategie mit unterschiedlichen Maßnahmen zu verfolgen. Dabei ist ein ganzheitlicher Ansatz gefordert, der Vergütung, berufliche Entwicklung, Unternehmenskultur und die Möglichkeit zur beruflichen Weiterentwicklung berücksichtigt.

Zentraler Orientierungsrahmen für alle Aktivitäten der Fachkräftesicherung und -gewinnung ist die „Fachkräftestrategie 2030 für den Freistaat Sachsen“[29], die von der Fachkräfteallianz Sachsen, der die relevanten Sozialpartner, Wirtschafts- und Arbeitsmarktakteure angehören, und der Sächsischen Staatsregierung getragen wird. Das Zentrum für Fachkräftesicherung und Gute Arbeit Sachsen mit Sitz in Chemnitz bietet Leistungen und Informationen rund um das Thema Fachkräfte für die kleinund mittelständisch geprägte Wirtschaft sowie für die Beschäftigten in Sachsen an.

29 https://publikationen.sachsen.de/bdb/artikel/33962/documents/52881

Eine wettbewerbsfähige Vergütung für Fachkräfte im Bereich Cybersicherheit stellt eine wichtige Maßnahme dar. Cybersicherheitsexperten sind gefragte Fachleute und eine attraktive Vergütung ist ein entscheidender Faktor, um sie zu gewinnen. Dazu gehören auch weitere Faktoren, wie Flexibilität bei der Arbeitszeit und die Möglichkeit zum mobilen Arbeiten bzw. Home-Office. Dieses Paket an Maßnahmen muss auch die Staatsverwaltung als Arbeitgeber bzw. Dienstherr stärker in den Fokus nehmen, z. B. über eine bessere tarifliche Eingruppierung bzw. beamtenrechtliche Einstufung von IT-Experten.

Auch die berufliche Weiterentwicklung gilt es zu schärfen und den Mitarbeitern systematischer als bislang anzubieten. Die Welt der Cybersicherheit ist ständig im Wandel und Fachkräfte schätzen Arbeitgeber, die ihre Weiterbildung fördern. Daher wird die Staatsverwaltung in diesem Feld ihre Angebote fortführen und ausbauen. So wird die Fortbildung von jährlich 60 ausgebildeten Fachkräften in den Verwaltungen von Land und Kommunen im IT-Grundschutz des BSI bzw. in vertiefenden Cybersicherheitsthemen aus einem zentralen Budget finanziert.

Darüber hinaus sollte der Freistaat seine Möglichkeiten nutzen, die Ausbildung von Cybersicherheitsfachkräften zu unterstützen und tätigkeitsbezogen auch selbst in die Hand zu nehmen. Hier spielt in erster Linie die Unterstützung von Hochschulen und anderen Aus- und Fortbildungseinrichtungen eine wichtige Rolle, um die Zahl dringend benötigter Fachkräfte für den Schutz der Unternehmen und Behörden in Sachsen zu erhöhen.

Für die Staatsverwaltung stellen ergänzend hierzu eigene berufsqualifizierende Studiengänge oder Vorbereitungsdienste eine Möglichkeit dar, Fachkräfte zu qualifizieren und zu binden. So gibt es an der Hochschule Meißen (FH) u. a. den Studiengang „Digitale Verwaltung", in welchem auch Informationssicherheit gelehrt wird. An der Hochschule der Sächsischen Polizei (FH) wird im Vorbereitungsdienst „Computer- und Internetkriminalitätsdienst" zur Bekämpfung der Cyberkriminalität ausgebildet. Allgemein auf die digitale Kompetenz bezogen wird in der „Strategie zur digitalen Transformation der sächsischen Staatsverwaltung"[30] das Ziel formuliert, ein abgestimmtes System aus grundständigen und berufsbegleitenden Ausbildungsangeboten zu unterstützen und die Gewinnung von Synergien aus der Kooperation mit Maßnahmen der Fort- und Weiterbildung zu fördern. Das sollte Kompetenzen zur Cybersicherheit mitumfassen.

30 https://publikationen.sachsen.de/bdb/artikel/43191/documents/65495

4.7. Forschung und Entwicklung / Hochschulen

Hochschulen und Forschungseinrichtungen sind bedeutende Träger für Innovationen in der Cybersicherheit. In Instituten und speziellen Forschungsgruppen an Hochschulen sowie bei außeruniversitären Forschungseinrichtungen wird zur Cybersicherheit geforscht, werden praxisnahe Kooperationen mit Unternehmen eingegangen, um konkrete Probleme zu lösen und auch Zukunftsthemen in den Blick genommen. Insgesamt forschen mehr als 30 Akteure der sächsischen Hochschul- und Forschungslandschaft an einschlägigen Themen.

Forschung und Entwicklung sind wichtig für die Cybersicherheit, da sie dazu beitragen, allen Menschen ein sicheres und selbstbestimmtes Leben in der digitalen Welt zu ermöglichen. Die Forschung zu IT-Sicherheit ist der Schlüssel, um Wirtschaft, Gesellschaft und staatliche Einrichtungen im Bereich der inneren und äußeren Sicherheit in Deutschland auf zukünftige Bedrohungen im digitalen Raum vorzubereiten. Forschungsprojekte können Erkenntnisse liefern, die dabei helfen, digitale Infrastrukturen möglichst zuverlässig und krisensicher aufzustellen sowie die Cyberresilienz und -kompetenz in der Gesellschaft zu steigern. Voraussetzung ist, dass alle Hochschulen über sichere ITInfrastrukturen verfügen, damit Forschung und Lehre nicht durch Cyberangriffe betroffen werden und hierüber z. B. wertvolle Daten abfließen.

In Deutschland gibt es außerhalb des Freistaates Sachsen bereits an mehreren Standorten Forschungszentren zur Cybersicherheit von nationaler Bedeutung, die größtenteils durch Bundesmittel finanziert werden. Solche Strukturen bestehen in Sachsen nicht, allerdings gibt es auch andere Faktoren, um Forschung und Entwicklung in der Cybersicherheit weiter voranzubringen: eine vielfältige Hochschullandschaft, Forschungsinstitutionen, ein der Thematik nahestehendes System an Branchen und Unternehmen sowie ausreichend Fachkräfte bzw. Forschende.

Sachsen besitzt diese Mischung und den für Forschung und Entwicklung so wichtigen Nährboden. In der Hochschullandschaft wird zur Cybersicherheit an den Technischen Universitäten in Chemnitz und Dresden gelehrt und geforscht, wie auch an den Hochschulen in Mittweida und Zittau/Görlitz. An diesen Standorten ergänzen und verstärken von Bund und Ländern finanzierte außeruniversitäre Forschungseinrichtungen, u. a. solche der Fraunhofer-Gesellschaft, die Forschung in diesem Bereich. In Dresden ist mit dem landesfinanzierten Barkhausen-Institut zudem eine der führenden Forschungseinrichtungen mit dem Fokus auf das Internet der Dinge angesiedelt. In der sächsischen Landeshauptstadt befindet sich mit

dem Silicon Saxony e. V. auch das landesweit größte Branchennetzwerk an Technologie-Unternehmen von IT-Providern bis hin zu global agierenden Unternehmen der Halbleiter- und Chip-Industrie.

Ziel ist es, diese Vernetzung weiter zu intensivieren. Sachsens Forschungsförderung, die grundsätzlich themenoffen angelegt ist, ermöglicht es den Hochschulen und außerhochschulischen Forschungseinrichtungen Förderungen aus europäischen Mitteln (v. a. Europäischer Fonds für regionale Entwicklung – EFRE, Fonds für einen gerechten Übergang - JTF) oder auch aus Landesmitteln zu beantragen. Da gerade die Interdisziplinarität einen Fokus der staatlichen Förderung darstellt, wird hier den Akteuren die Möglichkeit eröffnet, Themen der Cybersicherheit multidimensional und mit breiter Perspektive, z. B. durch die Einbeziehung der Sozial-, Rechts- und Geisteswissenschaften, zu erforschen. Gerade dieser Ansatz könnte eine Lücke füllen, die im bundesdeutschen Kontext besteht, und dafür sorgen, die Akzeptanz von neuen Lösungen in der Cybersicherheit deutlich zu erhöhen und in die gesellschaftliche Breite und damit zur Anwendung zu bringen. Die themenoffenen Fördergegenstände Promotionen und Nachwuchsforschungsgruppen innerhalb der ESF-Plus Förderung des SMWK bieten ebenfalls Ansatzpunkte für das Thema Cybersicherheit.

Von besonderem Wert für die sächsische Forschungslandschaft ist in diesem Zusammenhang auch das aus Landesmitteln finanzierte Barkhausen-Institut. Das Institut schafft im Rahmen seiner anwendungsorientierten Grundlagenforschung zu Informations- und Kommunikationstechnologien Innovationen und beeinflusst als Innovationszentrum im Forschungsbereich des Internets der Dinge die breite Forschungslandschaft. Sein Ziel ist es, Vertrauenswürdigkeit für zukünftige, von der Digitalisierung geprägte Gesellschaften zu ermöglichen. Um dieses Ziel zu erreichen, liefert das Barkhausen- Institut die technologischen Grundlagen, um Vertrauenswürdigkeit zu einer grundlegenden Anforderung an alle mit dem Internet verbundenen Geräte zu machen. Das Institut forscht zu Themen der Cybersicherheit und ist in dieser Ausrichtung europaweit einmalig. Damit wird es seinem Anspruch gerecht, ein sichtbares sächsisches Kompetenzzentrum für alle zu sein, die die gesellschaftlich und wirtschaftlich fundamentale Herausforderung der Vertrauenswürdigkeit in der Digitalisierung annehmen.

Den Grad der Vernetzung zu steigern, sollte auch für das Niveau der Informationssicherheit der Akteure selber gelten: So hat sich das SMWK laut Strategie zur digitalen Transformation im Hochschulbereich das Ziel gesetzt, die für die IT-Sicherheit der Hochschulen zuständigen Stellen miteinander zu vernetzen und Formen der Kooperation zu etablieren, die den Austausch der Hochschulen über Sicherheitsvorfälle oder -bedrohungen befördert.

4.8. Intensivierung der Vernetzung der Cybersicherheitsakteure

Die Cybersicherheitsarchitektur des Freistaates Sachsen besteht aus verschiedenen Akteuren, die wiederum Teil des nationalen und internationalen Sicherheitssystems sind. Der BfIS Land, das SAX.CERT und die BfIS der Staatsbehörden sind wichtige Akteure, die sich mit der Informationssicherheit in der sächsischen Staatsverwaltung befassen. Das SN4C im LKA befasst sich mit der Bekämpfung der Cyberkriminalität in Sachsen. Die Vernetzung dieser und weiterer Verantwortlicher im Bereich der Cybersicherheit innerhalb des Freistaates ist wichtig, da sie durch den Austausch von Wissen und Ressourcen zur Erhöhung der Sicherheit vor Cyberangriffen beitragen kann. Eine optimierte Cybersicherheitsarchitektur unterstützt den Schutz der Informationstechnologie im Freistaat Sachsen durch strategische Steuerung und Überwachung der landesweiten Sicherheitsmaßnahmen unter Gewährleistung der Geheimschutzinteressen.

In Bezug auf das Handlungsfeld 1 „Informationssicherheit in der Staatsverwaltung und in den Kommunen" dieser Strategie bestehen in Sachsen sowohl gesetzlich normierte Vernetzungsstrukturen als auch informelle Austauschformate. Die gesetzlich normierte Vernetzung der wesentlichen Verantwortlichen der Informationssicherheit auf Landesebene erfolgt über die AG IS. Hier werden in erster Linie gemeinsame Leit- und Richtlinien erarbeitet, die nach Beschlussfassung durch den LA ITEG von allen Staatsbehörden verbindlich umzusetzen sind. Damit wird ein ISMS auf gleichem Niveau für alle staatlichen Behörden geschaffen. Die Vernetzung mit den sächsischen Kommunen ist dagegen informeller Natur: So bietet der BfIS Land in Zusammenarbeit mit dem SAX.CERT seit 2022 monatlich eine Sprechstunde für Kommunen an, in der aktuelle Themen und konkrete technische und organisatorische Unterstützungsangebote besprochen werden.

Um das Cybersicherheitsniveau insgesamt zu erhöhen, wurden in den vergangenen Jahren Vernetzungsstrukturen zwischen allen für Cybersicherheitsthemen zuständigen Behörden im Freistaat Sachsen geschaffen. So wurde zur Bewältigung von akuten Cybersicherheits-Lagen die sogenannte Operative Koordinierungsgruppe Cybersicherheit gegründet, in der aus dem Sächsischen Staatsministerium des Innern (SMI) das für Verbrechensbekämpfung zuständige Referat, das LKA, das LfV, das SAX.CERT und der BfIS Land zusammenwirken. Diese Gruppe kommt 14-täglich zusammen, um auch ohne Anlassbezug einen kontinuierlichen Austausch auf operativer Ebene sicherzustellen. Darüber hinaus kommen mindestens in jedem Halbjahr die oben benannten Akteure sowie die Generalstaatsanwaltschaft Cybercrime, die DiAS und das für das allgemeine Krisenmanagement zuständige Referat im SMI zum Austausch zusammen, um neben der gegenseitigen Information zur Lage auch strategische Themen der Cybersicherheit zu erörtern.

Diese Zusammenarbeit aller Cybersicherheitsakteure in Sachsen werden wir weiter intensivieren und darüber konkrete Services und Projektergebnisse erreichen. Innerhalb der Staatsregierung soll ein ressortübergreifendes Koordinierungsgremium zur Abwehr von Cyberangriffen eingerichtet werden. Die daran beteiligten Akteure SN4C, das Sicherheitsnotfallteam SAX.CERT sowie die Digitalagentur Sachsen sollen gestärkt werden. Diese Koordinierungsstelle soll u. a. ein regelmäßiges Cyber- Lagebild für den Freistaat Sachsen zusammenführen, in das IT-Krisenmanagement auf Landesebene eingebunden sein und als zentrale Ansprechstelle für die Zusammenarbeit mit anderen Ländern und dem Bund dienen. Mittelfristig sollen die Daten in einem besonders gesicherten Portal zusammenlaufen.

4.9. Nationale und internationale Kooperationen

Nationale und internationale Kooperationen im Bereich der Cybersicherheit bezeichnen die Zusammenarbeit von Institutionen oder Behörden verschiedener staatlicher Ebenen, die wiederum unterschiedliche fachliche Inhalte haben können, z. B. politische, wirtschaftliche oder technische. Solche Formen der Zusammenarbeit sind von großer Bedeutung, da sie dazu beitragen, die Sicherheit im digitalen Raum zu erhöhen. Die Zusammenarbeit zwischen verschiedenen Organisationen und Ländern ermöglicht es, Wissen und Ressourcen zu teilen und dadurch Synergien zu schaffen, um gemeinsam stark gegen Cyberangriffe vorzugehen. Eine Möglichkeit, die Zusammenarbeit auf nationaler Ebene zu stärken, ist die koordinierte Zusammenarbeit der Verwaltungen im Bereich der ITSicherheit. Eine weitere Möglichkeit ist die Förderung der internationalen Zusammenarbeit. Es gibt jedoch keine allgemeingültige Methode, um Kooperationen im Bereich der Cybersicherheit zu erreichen. Die Umsetzung hängt von vielen Faktoren ab, z. B. von der Art der Organisationen, die zusammenarbeiten, und von den Zielen, die sie verfolgen.

Im Bereich der Informationssicherheit der Behörden (s. Kapitel 4.1.) arbeitet der Freistaat Sachsen sowohl mit anderen Bundesländern als auch mit dem Bund zusammen. So werden in der AG Informationssicherheit des IT-Planungsrates Leitlinien zur Informationssicherheit und entsprechende Umsetzungspläne erarbeitet, die von Bund und Ländern verbindlich umzusetzen sind. Darüber hinaus agiert der Freistaat Sachsen bilateral z. B. mit dem Freistaat Bayern, indem Hospitationen zwischen dem dortigen Landesamt für Sicherheit in der Informationstechnik und dem sächsischen Sicherheitsnotfallteam SAX.CERT durchgeführt werden, um den Austausch zu stärken und spezielle Sicherheitsprozesse oder Tools des anderen kennenzulernen. Bereits seit vielen Jahren arbeitet das SAX.CERT mit dem CERT des Bundes und den CERTs der Länder im Verwaltungs-CERT-Verbund für einen kontinuierlichen Austausch zur Lage der Informationssicherheit in der öffentlichen Verwaltung zusammen. Gemeinsam

mit dem BSI hat der Freistaat Sachsen die seit 2018 bestehende Partnerschaft im November 2023 durch den Abschluss einer Kooperationsvereinbarung auf eine neue, verbindlichere Ebene gehoben. Diese dient dazu, die Zusammenarbeit in insgesamt acht Handlungsfeldern mit konkreten Projekten für die nächsten Jahre zu verstetigen. Beide Partner werden intensiver bei der Cyberabwehr zusammenwirken, sich bei IT-Sicherheitsvorfällen unterstützen und gemeinsam die Bürgerinnen und Bürger zum Thema Cyber- und Informationssicherheit stärker aufklären, beispielsweise mit Sensibilisierungsvorträgen und Veranstaltungen. In allen acht Handlungsfeldern der Kooperationsvereinbarung mit dem BSI sollen in den nächsten zwei Jahren konkrete Ergebnisse erreicht werden.

Der Freistaat Sachsen wird seinen Willen zur engeren Kooperation sowohl mit anderen Ländern als auch mit dem Bund weiter artikulieren. Da es in einem globalen Cyberraum nicht effizient ist, in einem Bundesland gleichwertige Cybersicherheitsstrukturen zu denen des Nationalstaats wie auch der Europäischen Union aufzubauen – zumal die Gewinnung von Fachkräften in der Cybersicherheit absehbar schwieriger werden wird – ist es zweckmäßig, dass die Länder sowohl untereinander als auch mit der Bundesebene eine aufeinander abgestimmte Cybersicherheitsarchitektur aufbauen, die Synergien ermöglicht und Doppelarbeit vermeidet.

Im Bereich der Cybersicherheit der Wirtschaft (s. Kapitel 4.3.) kooperiert das LKA Sachsen gemeinsam mit fünf weiteren Landeskriminalämtern und dem Verband der deutschen Informations- und Telekommunikationsbranche Bitkom e. V. in der Sicherheitskooperation Cybercrime. Durch gemeinsame Anstrengungen und Know-how-Austausch soll der Gefährdung des Wirtschaftssektors durch Cybercrime begegnet werden. Die Kooperation steht in regelmäßigem Austausch, sie bestreitet gemeinsame Veranstaltungen wie Messen sowie Fachtagungen und organisiert gegenseitige Hospitationen. Die Aktivitäten der Sicherheitskooperation führen zur Intensivierung des Wissenstransfers und zur Erweiterung von technischen Kompetenzen. Darüber hinaus wird die vertrauensvolle Zusammenarbeit von Wirtschaft und Polizei gefördert und das Bewusstsein um die Gefahren von Cybercrime gestärkt.

5. Evaluierung und Fortschrittsüberwachung

In diesem Kapitel soll der Blick dafür geschärft werden, dass mit dem Inkrafttreten der Cybersicherheitsstrategie Sachsen die Arbeit nicht endet, sondern weitergeführt werden muss. So sind die in der Strategie benannten Ziele und konkreten Maßnahmen zu verfolgen und ihre Umsetzung zu bewerten. Dabei sind Trends und Entwicklungen zu identifizieren. Die rasante Evolution von Technologien im Cyberraum, z. B. durch Innovationen wie KI und die zunehmende Vernetzung durch das Internet der Dinge wird eine fortlaufende Anpassung der hier formulierten Sicherheitsansätze erfordern. Zudem wird die verstärkte Zusammenarbeit auf nationaler und internationaler Ebene zur Bewältigung globaler Bedrohungen an Bedeutung gewinnen.

Gemäß Artikel 7 Absatz 4 der NIS-2-Richtlinie haben die Mitgliedstaaten ihre nationalen Cybersicherheitsstrategien regelmäßig, mindestens aber alle fünf Jahre auf der Grundlage wesentlicher Leistungsindikatoren zu bewerten und erforderlichenfalls zu aktualisieren. Demnach wird auch die Cybersicherheitsstrategie Sachsen spätestens fünf Jahre nach Inkrafttreten durch die für Cybersicherheit koordinierend zuständige Stelle in der Staatsverwaltung unter Beteiligung der unter Kapitel 6 benannten Behörden und sonstigen Akteure einer Evaluierung unterzogen.

Zudem ist innerhalb der fünf Jahre Geltungsdauer der Cybersicherheitsstrategie vorgesehen, den Fortschritt der Umsetzung der Maßnahmen durch die Koordinierungsrunde Cybersicherheit kontinuierlich zu überwachen.

Die Evaluierung der Cybersicherheitsstrategie Sachsen ist von entscheidender Bedeutung, um sicherzustellen, dass die in der Strategie benannten Ziele und konkreten Maßnahmen in den einzelnen Handlungsfeldern umgesetzt werden. Zudem soll dieser Prozess auch eine kritische Reflexion über die Wirksamkeit der Ziele und Maßnahmen beinhalten und Einblicke in Bereiche zulassen, die möglicherweise verbessert werden müssen. Im Folgenden werden verschiedene Schlüsselaspekte beleuchtet, die während der Evaluierung der Cybersicherheitsstrategie berücksichtigt werden.

Effektivität der Sicherheitsmaßnahmen

Es ist nicht nur zu prüfen, ob zusätzliche technische oder organisatorische Sicherheitsmaßnahmen umgesetzt wurden, sondern auch, ob diese eine zielerreichende Wirkung haben.

Technologische Aktualisierung

Evaluierung der Anpassungsfähigkeit an neue Technologien.

Leistungskennzahlen

Auswertung von Leistungskennzahlen (gebündelt benannt in Kapitel 3.2.), um den Fortschritt und den Erfolg der Strategie zu messen.

Budget und Ressourcen

Überprüfung der Verteilung von Budget und Ressourcen im Verhältnis zu den Sicherheitszielen.

6. Beteiligte

Die Cybersicherheitsstrategie Sachsen wurde federführend durch die Sächsische Staatskanzlei, Referat 45 „Informations- und Cybersicherheit, kritische Infrastrukturen" erstellt. Folgende staatliche Stellen waren an der Erstellung beteiligt und verantworten einzelne Umsetzungsmaßnahmen in den genannten Handlungsfeldern. Mit der Benennung der Beteiligten an der Erstellung der Cybersicherheitsstrategie Sachsen wird die Anforderung nach Artikel 7 Absatz 1 Buchstabe f) der NIS-2-Richtlinie erfüllt.

Behörde	Referat / Bereich	Handlungsfeld
Sächsische Staatskanzlei	Referat 45 „Informations- und Cybersicherheit, kritische Infrastrukturen"	Federführung
Staatsbetrieb Sächsische Informatik Dienste	SAX.CERT	Staatsverwaltung und Kommunen
Sächsisches Staatsministerium des Innern	Referat 44 „Krisenmanagement, Bund-Länder-Zusammenarbeit"	Wirtschaft und KRITIS
Landeskriminalamt Sachsen		Gefahrenabwehr, Strafverfolgung und Verfassungsschutz
Landesamt für Verfassungsschutz		Gefahrenabwehr, Strafverfolgung und Verfassungsschutz
Sächsisches Staatsministerium für Kultus	Referat 32 „Digitalisierung, Medienbildung"	Digitalisierungsbezogene Kompetenz
Sächsisches Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung		Gefahrenabwehr, Strafverfolgung und Verfassungsschutz
Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr	Referat 41 „Grundsatzfragen Digitalisierung"	Wirtschaft und KRITIS
	Referat 38 „Innovationspolitik"	Forschung und Entwicklung / Hochschulen
	Referat 23 „Fachkräfte"	Fachkräfte
Digitalagentur Sachsen	Digitale Transformation	Wirtschaft und KRITIS
Sächsisches Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt	Referat 25 „Verbraucherschutz"	Verbraucherschutz
	Referat 42 „Kinder und Jugendliche"	Digitalisierungsbezogene Kompetenz

Sächsisches Staatsministerium für Energie, Klimaschutz, Umwelt und Landwirtschaft	Beauftragter für Informationssicherheit	Staatliche Verwaltung und Kommunen
Sächsisches Staatsministerium für Wissenschaft, Kultur und Tourismus	Referat 41 „Grundsatzangelegenheiten“	Forschung und Entwicklung / Hochschulen
	Referat 33 „Digitale Transformation im Hochschulbereich und Wissenschaftliche Bibliotheken“	Forschung und Entwicklung / Hochschulen
Sächsische Datenschutz- und Transparenzbeauftragte	Justiziariat / Verwaltung	Verbraucherschutz

Außerhalb der Staatsverwaltung wurden folgende Akteure bei der Erstellung der Cybersicherheitsstrategie Sachsen konsultiert.

Handlungsfeld	Beteiligte Stellen
Staatsverwaltung und Kommunen	Landkreis Nordsachsen, Landkreis Erzgebirge, Landkreis Zwickau, Sächsische Anstalt für kommunale Datenverarbeitung, Landeshauptstadt Dresden, Chemnitz
Gefahrenabwehr, Strafverfolgung und Verfassungsschutz	-
Wirtschaft und KRITIS	Mittelstand-Digital Zentrum Chemnitz, Cluster IT Mitteldeutschland, Handwerkskammer zu Leipzig, Handwerkskammer Dresden, Nordostchemie-Verbände
Digitalisierungsbezogene Kompetenz	Volkshochschulverband, Koordinierungsstelle Medienbildung, BITS 21
Verbraucherschutz	Bundesamt für Sicherheit in der Informationstechnik
Fachkräfte	-
Forschung und Entwicklung / Hochschulen	HTW Dresden, HS Mittweida, TU Dresden, Barkhausen-Institut
Vernetzung	-
Kooperation	-

7. Glossar

Begriff	Beschreibung / Erläuterung
Computer Emergency Response Team (CERT)	Ein CERT ist ein Sicherheitsnotfallteam, das aus IT-Spezialisten besteht, welche die Aufgaben der Abwehr von Cyberangriffen, die Reaktion auf IT-Sicherheitsvorfälle sowie die Umsetzung präventiver Maßnahmen wahrnehmen. Beim Freistaat Sachsen übernimmt das SAX.CERT die Aufgaben des Sicherheitsnotfallteams.
Cyberangriff	Ein Cyberangriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyberraum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.
Cybercrime	Als Cybercrime im weiteren Sinne werden nach Definition des BKA Delikte bezeichnet, die lediglich unter Nutzung von Informationstechnik begangen werden und bei denen das Internet vorwiegend Tatmittel ist. Delikte, die sich gegen das Internet und informationstechnische Systeme richten, werden hingegen als sogenannte Cybercrime im engeren Sinne bezeichnet.
Cyberraum	Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann.
Cybersicherheit	Cybersicherheit ist die IT-Sicherheit der im Cyberraum auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme
Cyberspionage	Cyberspionage wird primär als Mittel zum Erfassen von sensiblen oder vertraulichen Daten, Geschäftsgeheimnissen oder anderen Arten von geistigem Eigentum verwendet, die vom Angreifer zum Erreichen eines Wettbewerbsvorteils eingesetzt oder zur finanziellen Bereicherung verkauft werden können. Ziel solcher Angriffe ist die Informationsbeschaffung in Politik, Verwaltung, Wirtschaft, Wissenschaft, Technik oder Militär. Gerade kleine und mittlere Unternehmen sind immer wieder von Knowhow- Abfluss durch Cyberspionage betroffen.
E-Learning	E-Learning, oder auch eLearning, ist ein Begriff aus dem Bildungswesen mit einer sehr allgemeinen Grundbedeutung. Demnach werden unter E-Learning alle Formen von Lernen verstanden, bei denen elektronische oder digitale Medien für die Präsentation und Distribution von Lernmaterialien und/oder zur Unterstützung zwischenmenschlicher Kommunikation zum Einsatz kommen. Vorteile des E-Learnings betreffen zum einen die zeitliche und örtliche Unabhängigkeit des Lernenden und zum anderen die Nutzung von Skaleneffekten beim Anbieter des E-Learnings. Zudem können die Teilnehmer des E-Learnings eigene Lernrhythmen anwenden.

Incident Response	Incident Response, auch Vorfallsreaktion genannt, bezieht sich auf den Prozess der Reaktion auf Cybersicherheitsvorfälle oder andere unerwartete Ereignisse in einem IT-System. Ein Vorfall kann von verschiedenen Ursachen ausgelöst werden, wie z. B. durch Malware oder Trojaner-Infektionen, Netzwerkangriffen, Datenverlust oder von menschlichen Fehlern. Im Regelfall umfasst der Incident Response Prozess die Behebung des Schadens sowie die Definition und Umsetzung von vorbeugenden Maßnahmen, damit sich der Vorfall genauso oder in ähnlicher Weise nicht wiederholen kann.
Informationssicherheit	Informationssicherheit im Sinne des Sächsischen Informationssicherheitsgesetzes bedeutet Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der in informationstechnischen Systemen verarbeiteten Informationen und Daten. Informationen können in elektronischer, gedruckter oder gesprochener Form vorliegen.
Informationssicherheits-managementsystem	Ein Informationssicherheitsmanagementsystem ist die Aufstellung von verbindlichen Prozessen und Regeln, die die Informationssicherheit in einer staatlichen oder nicht-staatlichen Stelle dauerhaft steuern, kontrollieren, aufrechterhalten und fortlaufend verbessern.
Integrität	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf Daten angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen" angewendet. Der Begriff „Information" wird dabei für „Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autorenschaft oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zur verfassenden Person verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.
Interoperabilität	Als Interoperabilität bezeichnet man die Fähigkeit eines Systems mit unterschiedlichen anderen Systemen, Techniken oder Organisationen möglichst nahtlos zusammenzuarbeiten. Dies spiegelt sich bei der Verwendung des Begriffs im Kontext des Internets der Dinge wider. Dort wird er meist mit der Produkteigenschaft gleichgesetzt, dass Geräte und Dienste eigenständig miteinander kommunizieren können, unabhängig von Hersteller, Betriebssystem, Hierarchie oder Topologie.
Indicators of Compromise (IoC)	Indicators of Compromise (IoC, oder im Deutschen auch „Kompromittierungsindikatoren" genannt) sind die digitalen Spuren, die mit hoher Wahrscheinlichkeit auf einen unberechtigten Zugriff auf einen Computer hinweisen.
IoT	Unter Internet der Dinge oder Internet of Things (IoT) versteht man informations- und sensortechnisch aufgerüstete Gegenstände, die aus der physischen und virtuellen Welt Daten erfassen, verarbeiten und speichern und miteinander vernetzt sind.
IT-Forensik	IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Datennetzen zur Aufklärung von Sicherheitsvorfällen in IT-Systemen. IT-Sicherheitsvorfälle forensisch zu untersuchen, ist immer dann notwendig, wenn entstandene Schäden bestimmt, Angriffe abgewehrt, zukünftige Angriffe vermieden und Angreifende identifiziert werden sollen.

IT-Grundschutz	Der IT-Grundschutz hilft dabei, das Niveau der Informationssicherheit in einer Institution anzuheben und aufrechtzuerhalten. Er ist der bewährte Standard zum Aufbau eines ISMS. Mit einem ISO 27001-Zertifikat auf der Basis des IT-Grundschutzes kann eine Institution belegen, dass die umgesetzten Maßnahmen zur Informationssicherheit anerkannten internationalen Standards entsprechen und dadurch zusätzliches Vertrauen bei Kunden und Partnern schaffen.
IT-Notfall	Ein IT-Notfall ist ein Schadensereignis oder die unmittelbare Gefahr des Eintritts eines Schadensereignisses, bei welchem kritische IT-Prozesse nicht wie vorgesehen funktionieren. Die Funktionsfähigkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb maximal tolerierbarer Ausfallzeiten nicht wiederhergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt.
IT-Notfallhandbuch	Das IT-Notfallhandbuch soll die Zuständigen einer Organisation in die Lage versetzen, einen geordneten IT-Notbetrieb zu erreichen und die Rückkehr in den Normalbetrieb zu ermöglichen. Alle Regelungen, die den Notbetrieb in den Organisationseinheiten betreffen, sind in den weiterführenden Dokumenten zur Geschäftsfortführung, zum Wiederanlauf und zur Wiederherstellung geregelt.
IT-Notfallvorsorge	Zur IT-Notfallvorsorge zählen vorbeugende Maßnahmen, die den Schaden oder die Eintrittswahrscheinlichkeit von Risiken reduzieren, wie auch Maßnahmen, um ein schnelles und sinnvolles Reagieren auf einen Vorfall zu ermöglichen. Das IT-Notfallvorsorgekonzept bildet die Grundlage zur Umsetzung von Strategien, die die kontinuierliche Verfügbarkeit von IT-Diensten und Systemen sicherstellen. Es beschreibt die vorliegenden Bedingungen und beinhaltet alle bei der Konzeption anfallenden Informationen. Alle organisatorischen und konzeptuellen Aspekte sowie alle Maßnahmen und Tätigkeiten des Notfallmanagements, die nicht zur direkten Bewältigung eines Notfalls beitragen, sollten im IT-Notfallvorsorgekonzept beschrieben werden.
IT-Sicherheit	Die IT-Sicherheit stellt auf die Sicherheit technischer Produkte, also der Informationstechnik, ab. Sie stellt damit eine Unterkategorie der Informationssicherheit dar.
IT-System	IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.
Kontinuitätsstrategie	Die Kontinuitätsstrategie definiert die Rahmenbedingungen für die Aufrechterhaltung der Geschäftstätigkeit in einer Notfallsituation. Sie befasst sich mit der Untersuchung und Auswahl unterschiedlicher technischer und organisatorischer Alternativen für die Geschäftskontinuität.
KRITIS	Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der wirtschaftlichen Tätigkeit, der öffentlichen Sicherheit oder andere schwerwiegende Folgen für das Gemeinwesen eintreten würden.
MISP	Als Malware Information Sharing Platform (MISP) bezeichnet man eine Austauschplattform von Sicherheitsereignissen und Schwachstellen zur Verbesserung der Informationsaustauschund Analysefähigkeiten.

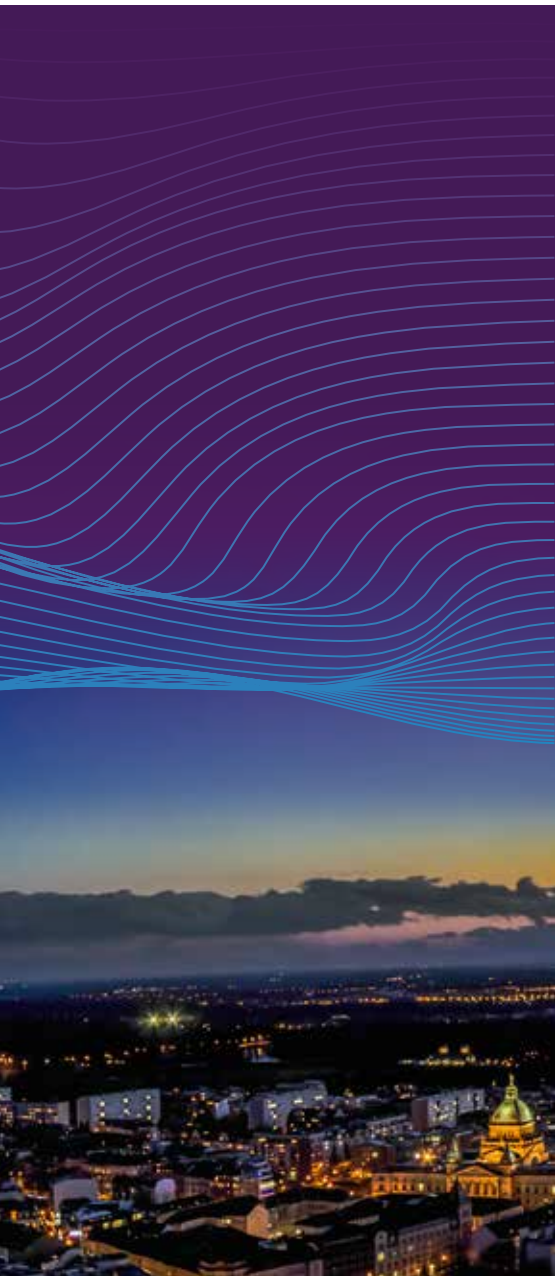
Penetrationstest	Ein Penetrationstest ist ein Verfahren, um die aktuelle Sicherheit eines IT-Netzes, eines einzelnen IT-Systems oder einer (Web-)Anwendung festzustellen. Er dient dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs einzuschätzen und dadurch die Wirksamkeit der vorhandenen Sicherheitsmaßnahmen zu überprüfen sowie weitere notwendige Sicherheitsmaßnahmen abzuleiten.
Phishing	Das Wort Phishing setzt sich aus Password und fishing zusammen, zu Deutsch: nach Passwörtern angeln. Der Angreifer versucht dabei, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten einer Internetnutzerin oder eines Internetnutzers zu gelangen und diese für seine Zwecke, meist zulasten des Opfers, zu missbrauchen.
Ransomware	Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. ransom) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.
Resilienz	Der Begriff Resilienz bezeichnet im vorliegenden Zusammenhang die Widerstandsfähigkeit von IT-Systemen gegen Sicherheitsvorfälle oder Angriffe. Die Resilienz von Systemen ergibt sich aus einem komplexen Zusammenspiel von organisatorischen und technischen Präventivmaßnahmen wie zum Beispiel Fachpersonal, ITSicherheitsbudget, verfügbare technische Infrastrukturen oder Ähnliches.
Revision	In einer Revision (revidieren = kontrollieren, prüfen) wird untersucht, ob Dokumente, Zustände, Gegenstände oder Vorgehensweisen korrekt, wirksam und angemessen sind. Im Gegensatz zum Audit muss die Revision nicht unbedingt unabhängig erfolgen. Zudem kann die Revision im Sinne einer Wartung auch bereits die Nachbesserung umfassen.
Schwachstelle	Eine Schwachstelle (englisch „vulnerability“) ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.
Schwachstellenmanagement	Unter dem Begriff Schwachstellenmanagement werden verschiedene Prozesse, Tools und Strategien zur Identifizierung, Bewertung, Behandlung und Meldung von Sicherheitsschwachstellen und Fehlkonfigurationen in der Software und den Systemen eines Unternehmens zusammengefasst.
Security Information and Event Management (SIEM)	Bei SIEM handelt es sich um eine Technologie, die in IT-Sicherheitszentren wie dem SOC eingesetzt wird. SIEM-Lösungen ermöglichen es, Log- und Ereignisdaten aus verschiedenen Quellen in Echtzeit zu sammeln, zu korrelieren, zu analysieren und zu visualisieren.
Security Operations Center (SOC)	Ein SOC ist eine Einrichtung innerhalb eines Unternehmens oder einer Organisation, die für die Überwachung und Analyse von ITSicherheitsvorfällen zuständig ist. Die Hauptaufgabe eines SOC besteht darin, Bedrohungen zu erkennen, zu analysieren und darauf zu reagieren, um die Sicherheit der IT-Infrastruktur des Unternehmens zu gewährleisten.

Sensibilisierung	Sensibilisierungen hingegen konzentrieren sich darauf, das Bewusstsein und das Verständnis für Informationssicherheit zu erhöhen. Dabei ist es im Kontext der Sensibilisierung hilfreich, den Menschen nicht als Sicherheitslücke, sondern als Abwehrschirm gegen Cyberangriffe zu sehen.
Sicherheitsereignis	Ein Sicherheitsereignis ist ein Versuch, eines der Schutzziele der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) zu verletzen.
Sicherheitskultur	Sicherheitskultur ist ein Verhaltensmerkmal einer Organisation, wie mit Fragen zur Sicherheit umgegangen wird. Die Sicherheitskultur unterliegt einem komplexen Lernprozess, in dem sich gemeinsame Ziele, Interessen, Normen, Werte und Verhaltensmuster herausbilden.
Sicherheitsvorfall	Ein Sicherheitsvorfall ist ein Ereignis, das tatsächlich nachteilige Auswirkungen auf die Informationssicherheit hat.
Social Engineering	Bei Cyberangriffen durch Social Engineering versuchen Kriminelle, ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyberkriminalität als auch bei der Spionage gehen die Angreifer geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.
Stand der Technik	Stand der Technik ist ein gängiger juristischer Begriff. Die technische Entwicklung ist schneller als die Gesetzgebung. Daher hat es sich in vielen Rechtsbereichen seit vielen Jahren bewährt, in Gesetzen auf den „Stand der Technik" abzustellen, statt zu versuchen, konkrete technische Anforderungen bereits im Gesetz festzulegen. Was zu einem bestimmten Zeitpunkt „Stand der Technik" ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards und Normen von beispielsweise DIN, ISO, DKE oder ISO/IEC ermitteln. Da sich die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung unterscheiden können, ist es nicht möglich, den „Stand der Technik" allgemeingültig und abschließend zu beschreiben.
Verfügbarkeit	Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendenden stets wie vorgesehen genutzt werden können.
Vertraulichkeit	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

8. Abkürzungsverzeichnis

Abkürzung	Langform
AG IS	Arbeitsgruppe Informationssicherheit
BfIS	Beauftragter für Informationssicherheit
BfIS Land	Beauftragter für Informationssicherheit des Landes
Bitkom	Verband der deutschen Informations- und Telekommunikationsbranche Bitkom e.V.
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
DiAS	Digitalagentur Sachsen
ECSM	European Cyber Security Month
EFRE	Europäischer Fonds für regionale Entwicklung
EU	Europäische Union
IHK	Industrie- und Handelskammern
JTF	Fonds für einen gerechten Übergang (Just Transition Fund)
IMK	Ständige Konferenz der Innenminister und -senatoren der Länder (Innenministerkonferenz)
IoC	Indicators of Compromise
IoT	Internet of Things
ISMS	Informationssicherheitsmanagementsystem
KDN	Kommunales Datennetz
KMK	Ständige Konferenz der Kultusminister der Länder (Kultusministerkonferenz)
KMU	Kleine und mittlere Unternehmen

KRITIS	Kritische Infrastrukturen
KSM	Koordinierungsstelle Medienbildung
LA ITEG	Lenkungsausschuss IT und E-Government
LKA	Landeskriminalamt Sachsen
LfV	Landesamt für Verfassungsschutz Sachsen
MESA	Landesstrategie der Sächsischen Staatsregierung zur „Medienbildung in Sachsen“
NCAZ	Nationales Cyberabwehr-Zentrum
NIS-2-Richtlinie	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)
SächsISichG	Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (Sächsisches Informationssicherheitsgesetz)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz)
SAX.CERT	Sächsisches Sicherheitsnotfallteam
SID	Staatsbetrieb Sächsische Informatik Dienste
SIEM	Security Information and Event Management
SMI	Sächsisches Staatsministerium des Innern
SMK	Sächsisches Staatsministerium für Kultus
SMWA	Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr
SMWK	Sächsisches Staatsministerium für Wissenschaft, Kultur und Tourismus
SMS	Sächsisches Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt
SN4C	Cybercrime Competence Center Sachsen
SOC	Security Operations Center
SVN	Sächsisches Verwaltungsnetz
WiBA	Weg in die Basis-Absicherung
ZAC	Zentrale Ansprechstelle Cybercrime beim Landeskriminalamt Sachsen
ZCS	Sächsische Zentralstelle zur Bekämpfung von Cybercrime bei der Generalstaatsanwaltschaft Dresden



Hinweis

Diese Publikation wird im Rahmen der Öffentlichkeitsarbeit von der Sächsischen Staatskanzlei kostenlos herausgegeben. Sie ist nicht zum Verkauf bestimmt und darf nicht zur Wahlwerbung politischer Parteien oder Gruppen eingesetzt werden.

Herausgeber

Sächsische Staatskanzlei
Referat 45 „Informations- und Cybersicherheit, Kritische Infrastrukturen“
Archivstraße 1
01097 Dresden

Redaktion

Referat 45 „Informations- und Cybersicherheit, Kritische Infrastrukturen“

Gestaltung und Satz

TORUX, Dresden

Druck

WirmachenDruck GmbH

Bildnachweis

Adobe Stock

Redaktionsschluss

31.03.2025

Bestellservice

www.publikationen.sachsen.de