Freistaat
SACHSEN

Bericht über die Evaluierung des Sächsischen Informationssicherheits-gesetzes (SächsISichG)

Stand: 11/2024

Inhalt

1 Zusammenfassung

Mit dem Sächsischen Informationssicherheitsgesetz (SächsISichG) vom 2. August 2019 (Sächsisches Gesetz- und Verordnungsblatt (SächsGVBl.) S. 630) hat der Freistaat Sachsen als eines der ersten Länder ein eigenständiges Informationssicherheitsgesetz geschaffen, das zudem nicht nur die Staatsverwaltung, sondern auch die Kommunen und andere nicht-staatliche Stellen einbezieht und damit die Gewährleistung von Informationssicherheit ganzheitlich denkt. Dies hat sich grundsätzlich bewährt, denn mit dem Gesetz wurden nicht nur die Strukturen der Informationssicherheit gestärkt. Es hat sich in den letzten gut fünf Jahren auch ein starkes Bewusstsein für die Informationssicherheit entwickelt, welches sich im Ländervergleich sehen lassen kann. Zu diesem Bewusstsein gehört auch der im Gesetz vorgesehene kontinuierliche Verbesserungsprozess mit Evaluierung und Berichterstattung an den Sächsischen Landtag, der dazu beitragen soll, die Informationssicherheit im Freistaat auch in den nächsten fünf Jahren weiter zu stärken. Die zwischenzeitlich im SächsISichG umgesetzten Anforderungen aus der Richtlinie (EU) 2022/2555, Network Information Systems Security Directive (NIS-2-Richtlinie)[1], die ab dem 1. Oktober 2024 gelten, haben zudem eindrucksvoll gezeigt: Mit dem SächsISichG lag nicht nur bereits eine Regelung vor, in die die Anforderungen der europäischen Ebene gut integriert werden konnten, sondern das sächsische Gesetz war so fortschrittlich und vorausschauend konzipiert, dass es nur an vergleichsweise wenigen Stellen geändert werden musste.

Auswirkungen des Gesetzes auf die Organisation der Informationssicherheit und Empfehlungen für Verbesserungen

Das SächsISichG hat in den letzten fünf Jahren zweifellos den stärksten Impuls zur Professionalisierung der Organisationsstruktur der Informationssicherheit gegeben. Mit der Verpflichtung zur Bestellung von Informationssicherheitsbeauftragten[2] und der Bereitstellung von sechs Stellen für einzelne Ressorts durch den Haushaltsgesetzgeber wurden im Laufe der Jahre erstmals in allen Ministerien und weiteren wichtigen Staatsbehörden Rollen besetzt, die das Thema Informationssicherheit in ihren Behörden vorantreiben konnten. Auch der zentrale operative Akteur, das Sicherheitsnotfallteam (SAX.CERT), wurde durch einen deutlichen Stellenzuwachs gestärkt. Im Einzelnen kann die Entwicklung der viergliedrigen Informationssicherheitsorganisation auf Landesebene und die Entwicklung der Informationssicherheitsorganisation in den Kommunen wie folgt bewertet werden:

Beauftragter für Informationssicherheit des Landes (BfIS Land)

Die zentrale strategische Instanz BfIS Land ist etabliert und wirksam. Die gesetzliche Verankerung eines Vertreters, wie sie für die BfIS der staatlichen Stellen bereits besteht, sollte auch auf den BfIS Land ausgedehnt werden, um Abwesenheitszeiten des Rolleninhabers abzusichern.

Seit dem 1. Oktober 2024 wurde BfIS Land zusätzlich die Rolle einer Aufsichtsbehörde übertragen. Er wird damit seitdem nicht nur bei Sicherheitsvorfällen gegenüber den Leitern der öffentlichen Stellen anordnend tätig, sondern auch bei festgestellten Mängeln hinsichtlich der Anforderungen an die Informationssicherheit im Rahmen von Audits oder Revisionen. Diese Rolle kann aus einer Linienorganisation heraus nur eingeschränkt wahrgenommen werden. Hier bietet sich zukünftig eine organisatorische Verankerung in unabhängiger Position im Bereich des Beauftragten für Informationstechnologie der Staatsregierung (CIO) an.

Sicherheitsnotfallteam (SAX.CERT)

Das SAX.CERT erfüllt seine Aufgaben nach dem SächsISichG, bedient sich dabei allerdings externer Unterstützung. So werden beispielsweise Sicherheitstests und Scans im Sächsischen Verwaltungsnetz (SVN) nicht routinemäßig durch das SAX.CERT selbst durchgeführt. Auch

[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] Aufgrund der besseren Lesbarkeit wird im Folgenden auf die explizite Nennung weiblicher und männlicher Personen- oder Personengruppenbezeichnungen verzichtet. Sofern nicht ausdrücklich gekennzeichnet, sind stets beide Geschlechter gemeint.

forensische Untersuchungen werden im Auftrag des SAX.CERT durch Dritte durchgeführt. Dies ist bei schwerwiegenden Vorfällen kritisch zu sehen, da nur eine schnelle Analyse eine gute Grundlage für schnelle Folgeentscheidungen ist.

Zudem stehen für die neuen Aufgaben wie die Rufbereitschaft ab dem 1. Oktober 2024 keine zusätzlichen personellen Ressourcen zur Verfügung. Das heute extern bei einem Dienstleister eingekaufte Sicherheitsbetriebszentrum (sog. Security Operations Center (SOC) soll zukünftig, wie in vielen anderen Bundesländern, bereits heute etabliert, intern im SAX.CERT verankert werden. Damit wird Kompetenz im SAX.CERT aufgebaut und gebunden, die auch im Falle einer Vorfallbearbeitung zu einer schnellen und fundierten Analyse und Lösungsvorschlägen führt. Es wird empfohlen, das SAX.CERT sowohl für die seit dem Jahr 2019 bestehenden als auch für die im Oktober 2024 hinzugekommenen Aufgaben personell zu stärken.

Beauftragte für Informationssicherheit (BfIS) der staatlichen Stellen

In fast allen staatlichen Stellen ist ein BfIS benannt oder zumindest ein Ansprechpartner für das Thema Informationssicherheit bei den zentralen Akteuren wie BfIS Land und SAX.CERT bekannt. Die zeitlichen Anteile der mit der BfIS-Rolle betrauten Bediensteten und damit die Umsetzung der Anforderungen aus dem Gesetz sind jedoch von Behörde zu Behörde sehr unterschiedlich. Dies gilt auch für die in § 7 Abs. 1 SächsISichG genannten 15 besonders wichtigen Behörden, die einen hauptamtlichen BfIS zu bestellen haben. Einige dieser Behörden haben bereits vor mehr als 10 Jahren professionelle Strukturen aufgebaut, während andere diese Rolle erst mit Stellen-zuweisungen nach dem Jahr 2019 besetzt hatten.

Mit der unterschiedlichen Umsetzungsreife der Anforderungen aus dem Gesetz geht natürlich auch der Stand des Informationssicherheitsmanagementsystems (ISMS) einher. Auffallend ist, dass eine Software, die im besten Fall zur Steuerung und Dokumentation eines ISMS eingesetzt werden sollte, überwiegend nur in den Behörden eingesetzt wird, die einen hauptamtlichen Beauftragten benannt haben. Es wird geprüft, die Nutzung für die Behörden kostenfrei, aber verpflichtend zu machen, um den weiteren Ausbau der ISMS der staatlichen Stellen zu unterstützen.

Die zahlreichen Rückmeldungen aus dem staatlichen Bereich zu fehlenden oder unzureichenden personellen und finanziellen Ressourcen können zwar nicht abschließend auf Plausibilität geprüft werden, spiegeln aber die bereits im Rahmen der Abstimmungen zum SächsISichG 2019 sowie zur Novellierung des SächsISichG 2024 eingegangenen Bedarfsmeldungen der Ressorts wider. Der Aufbau der Informationssicherheitsorganisation ist in den meisten Ressorts noch nicht abgeschlossen. Um ein zufriedenstellendes Niveau der Informationssicherheit im Freistaat Sachsen zu erreichen, müssen in den kommenden Jahren personelle und finanzielle Ressourcen nachgesteuert werden.

Arbeitsgruppe Informationssicherheit (AG IS)

Die AG IS wird als sehr wichtiger Baustein für die Fortschreibung und Weiterentwicklung der Themen zur Umsetzung der Informationssicherheit im Freistaat Sachsen angesehen. Seit Inkrafttreten des SächsISichG fasste das Gremium, in dem alle Ressorts sowie weitere Einrichtungen aus der Verwaltung vertreten sind, 21 Beschlüsse, darunter elf Mindeststandards, die in der Folge als verbindliche landesweite Leit- und Richtlinien durch den LA ITEG beschlossen wurden. Damit ist man dem Ziel eines möglichst einheitlichen Sicherheitsniveaus über Ressortgrenzen hinweg nähergekommen.

BfIS in den Kommunen

Fünf Jahre nach Inkrafttreten des SächsISichG sind in ca. 59 % der sächsischen Gemeinden und Verwaltungsgemeinschaften BfIS bestellt. Dieser Aufwuchs von ca. 20% vor Inkrafttreten des Gesetzes geht auf vielfältige Aktivitäten von BfIS Land im Zusammenwirken mit Akteuren auf der kommunalen Ebene wie den Spitzenverbänden SSG und SLKT zurück: So wurde nicht nur über kommunale Publikationen und elektronische Rundschreiben auf die Pflicht zur Benennung eines BfIS aufmerksam gemacht, sondern parallel dazu ein Unterstützungsnetzwerk mit technischen Serviceleistungen des SAX.CERT und kostenfreien Schulungsangeboten des BfIS Land sowie

regelmäßigen Netzwerktreffen aufgebaut, um den Mehrwert an dieser gesetzlichen Verpflichtung zu verdeutlichen. Herausforderung für die Zukunft ist, die Zahl der Kommunen mit einem BfIS weiter zu erhöhen. Die Zeitanteile, die den Bediensteten für die Rolle des BfIS zur Verfügung stehen, sind allerdings überwiegend unzureichend. Kritisch zu bewerten ist zudem, dass selbst in den Verwaltungen der zehn Landkreise und drei kreisfreien Städte nicht alle BfIS mit Vollzeitstellen und eigenem Personal ausgestattet sind. Zumindest in Kommunen dieser Größenordnung müssen professionelle Informationssicherheitsorganisationen aufgebaut werden, das zeigen die enormen Auswirkungen von Sicherheitsvorfällen wie in der Vergangenheit im Landkreis Anhalt-Bitterfeld oder im Rhein-Pfalz-Kreis. Hier ist die kommunale Selbstverantwortung gefordert. Dies gilt sowohl für organisatorische als auch für entsprechende technische Maßnahmen. Unbedingtes Ziel sollte es sein, die Kommunen mit ihrer gesamten IT an das Kommunale Datennetz (KDN) anzuschließen und damit das Schutzniveau für alle IT-Komponenten zu erhöhen. Größeren Kommunen wird darüber hinaus empfohlen, erweiterte Angriffserkennungssysteme zum Schutz des eigenen Behördennetzes zu implementieren. Das SächsISichG bietet hierfür seit dem Jahr 2019 die rechtliche Grundlage, die jedoch kaum genutzt wird.

Auswirkungen des Gesetzes auf die Maßnahmen der Informationssicherheit und Empfehlungen für Verbesserungen

Die Evaluierung zeigt, dass es richtig war, in § 4 Abs. 1 SächsISichG angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zur Gewährleistung der Informationssicherheit als Vorgaben zu definieren und um die Anforderung zu ergänzen, den jeweils aktuellen Stand der Technik zu berücksichtigen. Damit wird bereits seit dem Jahr 2019 ein hohes Qualitätsniveau angestrebt, das nun auch zentraler Bestandteil der Anforderungen der NIS-2-Richtlinie ist.

Mit den Regelungen der §§ 12 und 13 SächsISichG über Datenverarbeitungsbefugnisse zur Erkennung und Abwehr von Gefahren für informationstechnische Systeme im Freistaat Sachsen wurden spezielle und detaillierte Regelungen getroffen, die den Einsatz von Systemen zur erweiterten Angriffserkennung ermöglichen. Ohne diese Regelungen bestünden Rechtsunsicherheiten im Umgang mit Telekommunikationsdaten. Für die mit der Datenverarbeitung verbundenen Grundrechtseingriffe wurden normenklare und verhältnismäßige Rechtsgrundlagen geschaffen. Da die Befugnisnormen bisher ausreichend erscheinen, wurde von der im Gesetz verankerten **Experimentierklausel** seit Inkrafttreten des Gesetzes kein Gebrauch gemacht.
In den zentralen Schutzsystemen des SVN sind bereits seit einigen Jahren erweiterte Angriffserkennungssysteme im Einsatz, die das Sicherheitsniveau deutlich erhöht haben. Auf der dezentralen Ebene der staatlichen und nicht-staatlichen Stellen werden entsprechende Systeme jedoch noch zu selten eingesetzt.

Die im SächsISichG in den §§ 15-17 verankerten Meldepflichten haben die Meldekultur im Freistaat über die Jahre gestärkt. Rückblickend ist seit Inkrafttreten des SächsISichG ein stetiger Anstieg der jährlichen Meldungen zu verzeichnen. Dies ist auf eine zunehmende Sensibilisierung und bessere Kenntnis der staatlichen und nichtstaatlichen Stellen hinsichtlich der Meldepflichten zurückzuführen. Um das Lagebild zu vervollständigen und schnell auf Vorkommnisse reagieren zu können, wird die Staatsregierung von der Ermächtigung des § 16 Abs. 2 SächsISichG Gebrauch machen und eine Meldepflichtenverordnung erlassen. Diese soll Verfahren und Inhalte des Meldeprozesses vereinheitlichen, nach Kritikalität priorisieren und Schnittstellen für die technisch erhobenen Informationen definieren.

Änderungsbedarf am SächsISichG

Mit dem SächsISichG wurde ein ganzheitliches und nachhaltiges Gesetz zur Stärkung der Informationssicherheit im Freistaat Sachsen geschaffen, das in den letzten gut 5 Jahren seit seinem Inkrafttreten nicht nur wirkungsvoll war, sondern auch in seiner Systematik und mit den formulierten Anforderungen sehr weitsichtig aufgestellt ist. So musste das Gesetz nur an vergleichsweise

wenigen Stellen geändert werden, um den weitreichenden europäischen Vorgaben der NIS-2-Richtlinie zur Informations- und Cybersicherheit zu genügen.

Auch die Ergebnisse der Evaluierung zeigen, dass die gesetzlichen Normen ausreichend sind. Unbefriedigende oder kritikwürdige Sachstände in der Informationssicherheit deuten fast ausschließlich auf Umsetzungsdefizite hin. Daher nehmen diese auch den Schwerpunkt des vorliegenden Evaluierungsberichts ein. Nichtsdestotrotz wird auch empfohlen, an einigen wenigen Stellen des Gesetzes Änderungen zu prüfen. Dazu zählt die gesetzliche Festschreibung der Vertreterrolle des BfIS Land, die Aufnahme von Regelungen zur Einbeziehung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bei der Analyse des Datenverkehrs sowie die Ausweitung der Meldepflicht bei zumindest erheblichen Sicherheitsvorfällen auf alle Kommunen, auch außerhalb des KDN.

2 Ausgangssituation

Die Sächsische Staatsregierung erfüllt mit dem folgenden Bericht ihren Auftrag aus § 21 des SächsISichG. Danach ist die Sächsische Staatsregierung verpflichtet, dem Sächsischen Landtag einerseits über die durch das Gesetz erzielten Auswirkungen zu berichten und ihm andererseits Vorschläge zur Weiterentwicklung zu unterbreiten.

Mit dem SächsISichG vom 2. August 2019 wurden erstmals detaillierte gesetzliche Rahmenbedingungen für die Gewährleistung der Informationssicherheit in der Verwaltung des Freistaates Sachsen geschaffen. Das Gesetz verpflichtet alle Behörden und Gerichte des Freistaates Sachsen als staatliche Stellen sowie die seiner Aufsicht unterstehenden Körperschaften, Anstalten und rechtsfähigen Stiftungen des öffentlichen Rechts (Träger der Selbstverwaltung) als nicht-staatliche Stellen, angemessene Informationssicherheit zu gewährleisten. Dadurch sollen die Informationssicherheit in den staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen erhöht und Gefahren für ihre informationstechnischen Systeme abgewehrt werden.

Die Sicherung der informationstechnischen Systeme der staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen vor Angriffen ist wesentlich für das Funktionieren des Staates. Angriffe auf die informationstechnischen Systeme können die Handlungsfähigkeit der Verwaltung erheblich negativ beeinflussen. Das unberechtigte Abfließen von staatlichen oder kommunalen Informationen stellt neben der Verletzung des Rechts auf informationelle Selbstbestimmung einer Person auch ein Risiko für die administrative Grundordnung des Staates dar.

Im Folgenden wird dargestellt, welchen Stand die Informationssicherheit vor Inkrafttreten des SächsISichG hatte und welche Notwendigkeiten gesehen wurden, die Informationssicherheit in einem eigenständigen Gesetz zu regeln. Welche Ziele steckte man sich im Jahr 2019 hierzu, welche Impulse sollten gesetzt werden? Daran anschließend wird die Entwicklung des Informationssicherheitsrechts, also in erster Linie die Entwicklung von Gesetzen zur Informations- und Cybersicherheit auf europäischer, Bundes- und Länderebene, nachgezeichnet. Abschließend werden in diesem Eingangskapitel der gesetzliche Evaluierungsauftrag und die Rahmenbedingungen der Evaluierung beschrieben.

2.1 Ausgangssituation vor Inkrafttreten des SächsISichG

Dieses Kapitel dient der Betrachtung des Status Quo der Informationssicherheit in der sächsischen Verwaltung in den Jahren vor 2019. Welche rechtlichen Grundlagen gab es zu seiner Zeit, die einen Einfluss auf die Organisation und Gestaltung der Informationssicherheit hatten? Welche Akteure und Aufgaben waren bereits angelegt und wie wurden diese auch tatsächlich besetzt und ausgefüllt? Wie stellte sich die Bedrohungslage vor dem Jahr 2019 dar und mit welchen technischen Mitteln versuchte man, Cyberangriffe oder andere Ursachen für die Einschränkung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit der Daten gar nicht erst zur Geltung kommen zu lassen?

2.1.1 Rechtliche Grundlagen

Auf Gesetzesebene gab es vor dem Jahr 2019 nur im „**Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen“** (Sächsisches E-Government-Gesetz (SächsEGovG))[3] einige Vorgaben zur Informationssicherheit. So waren bereits seit Inkrafttreten dieses Gesetzes unter § 5 Absatz 1 SächsEGovG die Erstellung und Pflege von Informationssicherheitskonzepten für die staatlichen Behörden und die Träger der Selbstverwaltung vorgeschrieben, sofern sie personenbezogene Daten automatisiert verarbeiten. Zudem wurde unter § 9 SächsEGovG seit dem Jahr 2018[4] festgelegt, dass die staatlichen Behörden angemessene organisatorische und technische

[3] Sächsisches E-Government-Gesetz vom 9. Juli 2014 (SächsGVBl. S. 398)
[4] § 9 geändert durch Artikel 9 des Gesetzes vom 26. April 2018 (SächsGVBl. S. 198)

Vorkehrungen und sonstige Maßnahmen zur Einhaltung der Informationssicherheit nach § 2 Absatz 2 des BSI-Gesetzes für die in ihren informationstechnischen Systemen verarbeiteten Daten zu treffen haben. Das galt nach § 13 Absatz 1 des SächsEGovG entsprechend auch für die an E-Government beteiligten Träger der Selbstverwaltung. Zur Erreichung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus waren für die staatlichen Behörden darüber hinaus die Standards und Kataloge des BSI maßgeblich.

Weitaus detaillierter und daher auch mit weitreichenderer Wirkung für die Informationssicherheit in der Landesverwaltung ist die "**Verwaltungsvorschrift der Sächsischen Staatsregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung**" (VwV Informationssicherheit, kurz VwV IS)[5] zu sehen. Sie legte bereits im September 2011 die notwendigen Strategien und Organisationsstrukturen fest, um die Informationssicherheit in der sächsischen Landesverwaltung zu gewährleisten, und definierte einen ganzheitlichen Prozess, der sicherstellt, dass Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gewahrt bleiben. Dabei stützte sich die VwV auf die Standards des BSI und verpflichtete die Landesbehörden, diese Vorgaben umzusetzen.

Die Vorschrift galt für Behörden und Einrichtungen des Freistaates Sachsen, jedoch nicht für Gerichte, Hochschulen, die Schulen in kommunaler Trägerschaft, Forschungseinrichtungen, den Verfassungsgerichtshof des Freistaates Sachsen, den Rechnungshof, die Verwaltung des Landtags oder den Sächsischen Datenschutzbeauftragten. Jede Behörde war dafür verantwortlich, die Vorschriften gemäß ihrer Aufgabenstellung anzupassen und umzusetzen. Die Verantwortung für die Einhaltung der Informationssicherheit lag bei der jeweiligen Behördenleitung, die die entsprechenden Regelungen erlassen und den Bediensteten zugänglich machen musste. Auch die Bediensteten waren verpflichtet, verantwortungsvoll mit IT-Systemen und Daten umzugehen. Verstöße konnten disziplinarrechtliche Folgen nach sich ziehen. Zudem waren externe Dienstleister, die für die Landesverwaltung tätig sind, ebenfalls an die Sicherheitsvorgaben gebunden.

Zur Unterstützung der Informationssicherheitsmaßnahmen musste in jeder obersten Landesbehörde ein BfIS ernannt werden. Dieser war verantwortlich für die Steuerung des Informationssicherheitsprozesses, die Überprüfung der Sicherheitsvorgaben und die Entwicklung von Sicherheitskonzepten. Er fungierte als Ansprechpartner für Bedienstete und sorgte für die Durchführung von Sensibilisierungs- und Schulungsmaßnahmen. Zudem koordinierte eine AG IS ressortübergreifende Themen. Sie bestand aus dem BfIS Land sowie den BfIS der Sächsischen Staatskanzlei (SK), der Staatsministerien, der Polizei und des Staatsbetriebes Sächsische Informatik Dienste (SID). Die AG IS sollte Entwicklungen im Bereich der Informationssicherheit beobachten und Maßnahmen zur Verbesserung vorschlagen. Zudem wurde die Rolle eines SAX.CERT beschrieben. Dieses Team, das im SID angesiedelt wurde, sollte bei Sicherheitsvorfällen aktiv werden. Es sollte durch die Bereitstellung von Lösungen bei Vorfällen unterstützen, über Sicherheitslücken informieren und Maßnahmen zur Behebung von Sicherheitsrisiken koordinieren.

In der VwV IS wurde auch BfIS Land als zentrale Instanz für die Informationssicherheit in der sächsischen Landesverwaltung beschrieben. BfIS Land war zu der Zeit im Staatsministerium der Justiz und für Europa angesiedelt (ab dem Jahr 2015 dann im Sächsischen Staatsministerium des Innern (SMI)) und sollte die Verantwortung für die operative und koordinierende Umsetzung aller Aufgaben im Bereich der Informationssicherheit tragen, die ihm vom Lenkungsausschuss IT und E-Government (LA ITEG) übertragen wurden. Eine seiner wesentlichen Aufgaben war die Steuerung des Informationssicherheitsprozesses innerhalb der gesamten Landesverwaltung, was bedeutete, dass er die Koordination und Überwachung der Maßnahmen zur Gewährleistung der Sicherheit der IT-Systeme und Daten zu übernehmen hatte.

Darüber hinaus sollte BfIS Land als zentrale Ansprechperson für alle ressortübergreifenden Fragen der Informationssicherheit fungieren und für die Koordination entsprechender Maßnahmen verantwortlich zeichnen. Er leitete daher die AG IS. Bei ressortübergreifenden Sicherheitsvorfällen war BfIS Land laut VwV ermächtigt, bei Gefahr im Verzug Maßnahmen anzuordnen, um die Sicherheit

[5] VwV Informationssicherheit vom 7. September 2011 (Sächsisches Amtsblatt mit Amtlichem Anzeiger S. 1294)

wiederherzustellen. Das durfte beispielsweise auch die Sperrung von Anwendungen oder Netzverbindungen umfassen. Durch diese zentrale Rolle übernahm BfIS Land die Hauptverantwortung für die Sicherheit der IT-Infrastruktur des Freistaates Sachsen und sorgte dafür, dass die Informationssicherheit auf Landesebene einheitlich und effektiv umgesetzt wird.

Zeitlich gesehen nach der VwV IS, aber noch vor dem SächsEGovG reihte sich als dritte rechtliche Grundlage für die Informationssicherheit im Freistaat Sachsen die **Leitlinie für Informationssicherheit** nebst diesbezüglichen Umsetzungsplan ein, die der **IT-Planungsrat** (IT-PLR) in seiner 10. Sitzung im März 2013 beschlossen hatte.[6] Da der IT-PLR ein Verfassungsgremium zur einheitlichen Gestaltung der IT zwischen Bund und Ländern darstellt und seine Beschlüsse verbindlichen Charakter haben, waren fortan die in der Leitlinie festgelegten Ziele auch für die Landesverwaltung zu beachten. Im Jahr 2018 wurde die Leitlinie fortentwickelt und mit neuen Aufgaben und einem Umsetzungsplan unterlegt, dessen Ziele bis zum Jahr 2025 erreicht sein sollen.[7]

2.1.2 Organisation der Informationssicherheit in Sachsen

Seit Einführung der VwV IS im Jahr 2011 verfügte der Freistaat Sachsen über eine Leitlinie für die Landesverwaltung, die eine viergliedrige Organisation mit dem BfIS Land, dem SAX.CERT, den BfIS der Ressorts und der AG IS vorsah, welche im Zusammenspiel Vorgaben und Maßnahmen zur Erhöhung der Informationssicherheit abstimmte.

BfIS Land und SAX.CERT

BfIS Land als zentrale strategische Sicherheitsinstanz in der Informationssicherheitsorganisation der Landesverwaltung war vor Inkrafttreten des SächsISichG mit einem eigenen Referat im SMI, ab August 2018 in der SK angesiedelt. Das Referat „Informationssicherheit in der Landesverwaltung, Cybersicherheit“ bestand dabei neben dem Referatsleiter aus drei Bediensteten der Laufbahngruppe (LG) 2.2 und einer Bediensteten LG 1.2. Das Budget des Referats im Haushaltsjahr 2019 belief sich auf gut 1 Millionen Euro, wovon gut 600.000 Euro in Anspruch genommen wurden. Zudem führte BfIS Land die Fachaufsicht über das SAX.CERT im SID und trieb technische und nichttechnische Projekte zur Erhöhung der Informationssicherheit voran. Da das SAX.CERT zu der Zeit personell völlig unzureichend besetzt war, fielen darunter auch zahlreiche Themen, die grundsätzlich in die Zuständigkeit des SAX.CERT gehörten. Zu diesen technischen Projekten zählten u. a. die Projekte „HoneySens“ (Aufspürung von Hackern im internen Netz), „Identity Leak Checker Client“ (Aufdeckung von Identitätsdiebstählen) sowie das „Security Dashboard“ (Grafische Darstellung einer Übersicht über die Gefährdungslage der IT in der Landesverwaltung).

Zudem kümmerte sich BfIS Land um die Wahrnehmung des Themas in der verwaltungsinternen, aber auch allgemeinen Öffentlichkeit. Als vorrangig auf der strategischen Ebene tätige Instanz war BfIS Land außer in Ausnahmefällen jedoch nicht weisungsbefugt für die Informationssicherheit in den Ressorts. Die Verantwortung für die Umsetzung von Informationssicherheitsmaßnahmen in Sachsen lag insofern fast ausnahmslos bei den Ressorts. Das vielfältige Aufgabengebiet des BfIS Land spiegelt sich in der Mitarbeit und Mitgliedschaft in zahlreichen Gremien und Initiativen auf Bundes- und Landesebene sowie zwischen diesen Ebenen und auch mit dem kommunalen Bereich wider.

Das Ziel Sensibilisierung war in der VwV IS unter dem Titel „Prinzip des informierten Beschäftigten“ festgelegt. Demnach lag ein zentraler Baustein zu mehr Sicherheit in der Sensibilisierung vor Gefahren bei der alltäglichen Nutzung von PC, Smartphone und Internet einerseits und in der Vermittlung von Kompetenzen zur Gefahrenabwehr andererseits. Aufgrund dieses Auftrags organisierte BfIS Land mit der Großveranstaltung INFOSIC bereits seit dem Jahr 2012 sogenannte „Live-Hackings“, die sich ausdrücklich an alle Bediensteten von Landes- und Kommunalbehörden richteten. Die gesamte Veranstaltungsreihe wurde dabei aus Projektmitteln des IT-PLR unterstützt.

[6] https://www.it-planungsrat.de/fileadmin/beschluesse/2013/Beschluss2013-01_Leitlinie_Informationssicherheit_Hauptdokument.pdf (zuletzt abgerufen am 30.10.2024)
[7] https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-05_TOP_09_Umsetzungsplan.pdf (zuletzt abgerufen am 30.10.2024)

Über die Jahre wurde die INFOSIC die größte Sensibilisierungsveranstaltung für Informationssicherheit im Freistaat Sachsen. Wurden in den Anfangsjahren in Leipzig und in Chemnitz jährlich knapp 700 Teilnehmer begrüßt, erhöhte sich die Zahl im Jahr 2015 in Dresden auf 1.800 Teilnehmer und in den Jahren 2016 und 2017 auf jeweils knapp 3.000 Teilnehmer. Durch diese und andere dezentral vom BfIS Land organisierte bzw. unterstützte Veranstaltungen wurden bis dato über 10.000 Bedienstete aus der öffentlichen Verwaltung in Sachsen direkt erreicht. Mit dieser Teilnehmerzahl belegte der Freistaat Sachsen im Bundesvergleich einen Spitzenplatz. Als weiteres Angebot startete Anfang 2018 darauf aufbauend ein Online erreichbares E-Learning-Modul, mit dem Bedienstete von ihrem Arbeitsplatz aus wichtige Kenntnisse erlernen konnten, um im Umgang mit der IT möglichst sicher zu agieren. Damit wurden tausende weitere Bedienstete geschult.

Das SAX.CERT als zentrale operative Instanz in der Informationssicherheitsorganisation der Landesverwaltung stellte den Behörden derweil technische Services zur Verbesserung der Informationssicherheit zu Verfügung. So informierte es in monatlichen Lageberichten über die Sicherheitskennzahlen in Sachsen, Fehler in Software, Lücken in öffentlichen Webverfahren sowie infizierte Computer oder kompromittierte Benutzerdaten, und unterstützte die Behörden bei der Eindämmung von Schadensfällen. Hierfür betrieb das SAX.CERT einen Warn- und Informationsdienst für die Ressorts sowie ein elektronisches Melde- bzw. Ticketsystems für Sicherheitsvorfälle. Zudem unterstützte es den Betrieb der Sicherheitssysteme des SVN. Für ein möglichst umfassendes Lagebild tauschte das SAX.CERT Informationen über Schadereignisse mit CERTs des Bundes und der Länder aus. Das SAX.CERT war seit Anbeginn im SID angesiedelt und hatte vor Inkrafttreten des Gesetzes lediglich zwei feste Stellen LG 2.1, unterstützt durch zwei externe Bedienstete.

Staatliche Stellen (Behörden und Gerichte des Freistaates Sachsen)

Sehr differenziert in Qualität und Quantität stellte sich die Situation in den Behörden der Landesverwaltung dar. Laut VwV IS war in jeder obersten Staatsbehörde ein BfIS zu ernennen, zusätzlich beim Landes-IT-Dienstleister SID und im Landespolizeipräsidium, aufgrund der herausgehobenen Bedeutung dieser Bereiche jeweils sogar ein hauptamtlicher BfIS. Während die Ministerien der erstgenannten Pflicht nicht bzw. nicht zu jeder Zeit nachkamen, war die Hauptamtlichkeit im SID und Polizei jederzeit gegeben. Die Polizei hatte bereits seit dem Jahr 2005 den ersten hauptamtlichen BfIS und in der Folge weitere hauptamtliche Stellen sowohl im Polizeiverwaltungsamt als auch in nachgeordneten Dienststellen des Innenressorts geschaffen, der SID seit dem Jahr 2011. Auch darüber hinaus gab es weitere Behörden, die nach eigenen Angaben bereits vor dem Inkrafttreten des SächsISichG im Jahr 2019 diese Rolle hauptamtlich besetzt hatten: das SMI, das Staatsministerium für Umwelt und Landwirtschaft, das Staatsministerium für Finanzen, das Statistische Landesamt des Freistaates Sachsen (StaLa), das Landesamt für Umwelt, Landwirtschaft und Geologie, die Landestalsperrenverwaltung des Freistaates Sachsen, die Leitstelle für Informationstechnologie der sächsischen Justiz (LIT), das Landesamt für Steuern und Finanzen und das Landesrechenzentrum Steuern. Damit hatten immerhin sechs der 15 später im Gesetz unter § 7 Absatz 1 SächsISichG definierten wichtigen Behörden teilweise weit vor dem Jahr 2019 einen wichtigen Schritt in Richtung Professionalisierung unternommen. Das zeigt sich darin, dass es zumeist diese Behörden waren, die ein ISMS aufbauten und ihrerseits Leit- und Richtlinien zu Anwendungsfeldern der Informationssicherheit in Kraft setzten. Im Bereich des Landwirtschaftsressorts kam hinzu, dass die Zertifizierungsanforderung der EU-Zahlstelle bei der Etablierung einer Informationssicherheitsorganisation katalysierend wirkte.

Vereint waren die vorgenannten Akteure in der AG IS als Plattform der ressortübergreifenden Zusammenarbeit. Die AG IS war als koordinierendes Gremium für alle ressortübergreifenden Aspekte der Informationssicherheit eines der wichtigsten Arbeitsmittel des BfIS Land. Ihr gehörten neben dem BfIS Land als Vorsitzender auch die BfIS der SK und Staatsministerien, der Polizei und des SID als stimmberechtigte Mitglieder an. Als Mitglieder ohne Stimmrecht saßen je ein Vertreter des SAX.CERT, der Verwaltung des Sächsischen Landtags, des Sächsischen Rechnungshofes und des Sächsischen Datenschutzbeauftragten sowie der Vorsitzende des Arbeitskreises Sächsisches Verwaltungsnetz (AK SVN) und ein gemeinsamer Vertreter der sächsischen Kommunen in der AG IS. Zu wichtigen Fragen fasste die AG IS Beschlüsse, die dem Arbeitskreis der IT-Koordinatoren für

IT und E-Government der Ressorts (AK ITEG) zum Ausbau und Weiterentwicklung der Informationssicherheit vorgelegt wurden. So wurde eine Richtlinie zur Meldung von Sicherheitsvorfällen an das SAX.CERT beschlossen, die Möglichkeit der temporären Nutzungseinschränkung unsicherer Internetdienste vereinbart und verbindliche Listen für zu blockierende, da potenziell schädliche Internetseiten erstellt. Zudem beriet die AG IS sowohl den AK ITEG als auch den LA ITEG zu Fragen der Informationssicherheit.

Träger der Selbstverwaltung als nicht-staatliche Stellen

Zwar mussten mit dem SächsEGovG gemäß § 13 bereits die am E-Government beteiligten Träger der Selbstverwaltung angemessene organisatorische und technische Maßnahmen zur Einhaltung der Informationssicherheit für die in ihren informationstechnischen Systemen verarbeiteten Daten treffen. Allerdings wurden die grundlegenden organisatorischen Maßnahmen wie die Einsetzung eines BfIS trotz gesetzlicher Festlegung nicht bei allen betroffenen Trägern der Selbstverwaltung umgesetzt. Die im Rahmen der Evaluierung des SächsEGovG im Jahr 2017 durchgeführte Online-Befragung der Träger der Selbstverwaltung wies daher niedrige Ergebniswerte auf. Danach hatten nur ca. 20 % der Kommunen einen BfIS namentlich benannt. Über IT-Sicherheitskonzepte verfügten rund 50 % der auf die Onlinebefragung antwortenden kommunalen Träger der Selbstverwaltung und 29 % der auf die Onlinebefragung antwortenden sonstigen Träger der Selbstverwaltung. Rund die Hälfte der antwortenden sonstigen Träger der Selbstverwaltung (54 %) und der kommunalen Träger der Selbstverwaltung (47 %) gaben an, eine IT-Sicherheitsleitlinie eingeführt zu haben. Weiterhin hatten rund 58 % der sonstigen Träger der Selbstverwaltung und 40 % der befragten kommunalen Träger der Selbstverwaltung IT-Sicherheitskonzepte implementiert.[8]

2.1.3 Lage der Informationssicherheit

Die Behörden der Sächsischen Landesverwaltung waren damals wie heute miteinander über das SVN verbunden. Das heißt: Kommunizieren die Behörden untereinander, werden die Daten ausschließlich über das SVN transportiert, abseits vom Internet. Das SVN wiederum ist über einen zentralen Zugang auch mit dem Internet verbunden. Dieser Anschluss wird benötigt, damit die Landesbehörden mit Dritten wie z. B. Bürgern oder Unternehmen auf elektronischem Weg kommunizieren können. Der über den zentralen Zugang zum Internet ins SVN eingehende Datenverkehr hatte im Jahr 2017 ein Volumen von rund 1 Petabyte. In diesem riesigen Datenstrom verstecken sich dabei auch Cyberangreifer, die versuchen z. B. per Schadsoftware in einer E-Mail oder mit anderen technischen Angriffsarten in das SVN und bis hin zu einzelnen Behördenrechnern vorzudringen.

Um Angriffe abzuwehren und ein möglichst hohes Maß an Informationssicherheit zu gewährleisten, bilden das SVN und die internen Netze der Behörden zusammen ein mehrstufiges Sicherungssystem, bei dem neben herkömmlichen Virenschutzprogrammen auch individuell angepasste Schutzmaßnahmen greifen. Die am zentralen Übergang zum Internet erhobenen Daten zeigten, dass auf die an das SVN angeschlossenen Behörden täglich Cyberangriffe stattfanden. Dabei war das SVN hauptsächlich ungezielten Massenangriffen ausgesetzt. Dazu zählen z. B. Erpressungstrojaner und allgemeine Spähprogramme. Deutlich seltener befand sich das Behördennetz im Fokus gezielter Angriffskampagnen.

Im Jahr 2018 wurden fast 80 Millionen Spam-Mails durch die zentralen Schutzsysteme des SVN abgewehrt, während weitere 6,5 Millionen Spam-Mails intern erkannt und als Spam markiert wurden, was eine Steigerung von 63 % im Vergleich zum Vorjahr darstellte. Bei der Erkennung von Viren im Internetverkehr wurden über 35.000 Viren identifiziert, was einem Anstieg von 44 % gegenüber dem Vorjahr entsprach. Im E-Mail-Verkehr wurden knapp 100.000 Viren entdeckt, eine drastische Zunahme von 171 % im Vergleich zum Vorjahr.

Diese Zahlen basieren auf den zentralen Schutzsystemen des SVN, weitere vergleichbare Daten von den zusätzlichen Schutzsystemen auf Ebene der Behörden lagen nur teilweise vor. So meldeten im November 2018 der SID und die Polizei zusätzlich knapp 7.000 Viren im E-Mail-Verkehr, die von

[8] Bericht über die Evaluierung des SächsEGovG, Drucksache (Drs.) 6/9859; S. 49

den zentralen Schutzsystemen des SVN nicht erkannt wurden. Bereits damals lautete das Fazit in einem Monatsbericht des SAX.CERT aus dem Dezember 2018: „Um eine vollständige und korrekte Übersicht der Bedrohungslage zu gewährleisten, muss im neuen Jahr das Reporting der Ressorts deutlich stärker mit dem der zentralen Systeme des SVN verknüpft werden."

Neben den automatisiert erhobenen Daten von erfolgreich abgewehrten Viren, bestand seit Januar 2016 bereits die Pflicht aller Behörden der Landesverwaltung, Sicherheitsvorfälle per Formular an das SAX.CERT zu melden (Beschluss des AK ITEG 01/2016). Eine Meldepflicht bestand für festgelegte Vorfälle und als Reaktion auf vom SAX.CERT veröffentlichte Warnmeldungen. In den Jahren bis Inkrafttreten des SächsISichG erhielt das SAX.CERT jährlich zwischen elf und 19 Meldungen über sicherheitsrelevante Vorfälle in den Ressorts. Die meisten dieser Meldungen betrafen Schadprogramme, die im Anhang von E-Mails auf Arbeitsplätze gelangten und dort aktiv werden konnten.

2.2 Schaffung des SächsISichG

Im Vorwort zum Jahresbericht Informationssicherheit 2017 konstatierte der BfIS Land: „Eine weitere wesentliche Herausforderung in der Zukunft bleibt aber auch die Stärkung der gesamten Informationssicherheitsorganisation in der Verwaltung. Hier stößt die mittlerweile seit über sechs Jahren bestehende VwV an ihre Grenzen. Deshalb soll bis Anfang 2019 ein SächsISichG in Kraft treten, dass klare Verantwortlichkeiten und Zugriffsmöglichkeiten der zentralen Sicherheitsakteure schafft, und damit die Informationssicherheit auf ein höheres Niveau hebt. Auch die Sensibilisierung der Bediensteten zu Cybergefahren wird hier noch stärker als bisher als wichtiges Element benannt werden."[9]

2.2.1 Erkannte Notwendigkeiten für die Schaffung des SächsISichG

Wegen der sich ständig verschärfenden Bedrohungslage, parallel bestehender Defizite bei der Umsetzung von Sicherheitsmaßnahmen in Teilen der Landesverwaltung und bei den Trägern der Selbstverwaltung, welche u. a. im Rahmen der Evaluierung des SächsEGovG deutlich wurden[10], aber auch wegen fehlender datenschutzrechtlicher Befugnisnormen wurde die Notwendigkeit gesehen, die Regelungen zur Gewährleistung der Informationssicherheit deutlich zu erweitern. Aufgrund der Komplexität der beabsichtigten Regelungen zur Informationssicherheit unter Einbeziehung der Träger der Selbstverwaltung wurde von Anfang an ein eigenes Informationssicherheitsgesetz für erforderlich angesehen. Einschlägige Vorschriften des SächsEGovG sollten dabei in das neue eigenständige Gesetz überführt werden.

Mit der zunehmenden Digitalisierung der Verwaltung werden umfassend personenbezogene und sonstige zu schützende Daten elektronisch gespeichert und übermittelt. Der Schutz dieser Daten und der zu ihrer Verarbeitung eingesetzten informationstechnischer Systeme ist zu einer fundamentalen Anforderung der Landesverwaltung geworden, um die Rechtmäßigkeit, Funktionsfähigkeit und vor allem ihre Verlässlichkeit sicherzustellen. Diverse Hackerangriffe im In- und Ausland zeigten, wie schnell Systeme infiziert und Informationen in die falschen Hände gelangen könnten. Den immer ausgereifteren Hackerangriffen sollte mit dem eigenständigen Gesetz erfolgreich begegnet werden. Allerdings muss die Verwaltung angemessene Abwehrmaßnahmen überhaupt treffen dürfen. Hierzu bedurfte es neuer gesetzlicher Regelungen, insbesondere datenschutzrechtlicher Befugnisse. Diese Regelungen waren zwingend erforderlich, da Angriffstechnologien mit den bis dahin etablierten technischen Verfahren - wie portbasierten Firewalls, Virenscannern und Vermittlerserver (sogenannte Proxy-Server) - und im bestehenden Rechtsrahmen nicht mehr zuverlässig abgewehrt werden konnten.

Mit dem Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen[11] sollten die bisherige VwV IS sowie die entsprechenden Regelungen im SächsEGovG zusammengefasst und

[9] Jahresbericht des Beauftragten für Informationssicherheit des Landes 2017, März 2018, S. 7
[10] Bericht über die Evaluierung des SächsEGovG, (Drs.) 6/9859; S.51
[11] Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen vom 2. August 2019 (SächsGVBl. S. 630)

erheblich erweitert, die Gerichte und vor allem die nicht-staatlichen Stellen wie die Kommunen in den Anwendungsbereich einbezogen, die Befugnisse der BfIS und des SAX.CERT ausgeweitet, Rechtsgrundlagen für die den zulässigen Einsatz moderner Erkennungs- und Abwehrtechnologien geschaffen und verschiedene Meldepflichten über Sicherheitsvorfälle eingeführt werden.

Ziel war es, ein zukunftsfähiges Gesetz zu schaffen, welches den Herausforderungen der Cybersicherheit trotzt sowie künftige technischen Entwicklungen berücksichtigt. Das Gesetz sollte Impulsgeber für eine Stärkung der Informationssicherheit in der öffentlichen Verwaltung in Sachsen sein.

2.2.2 Regelungsinhalte des SächsISichG im Überblick

Die Regelungsinhalte finden sich in den folgenden Abschnitten:

Abschnitt 1: Allgemeine Vorschriften (§§ 1 - 4)
Unter den Anwendungsbereich (§ 2) fallen die Behörden und Gerichte des Freistaates Sachsen als staatliche Stellen sowie die seiner Aufsicht unterliegenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts als nicht-staatliche Stellen. Für Beliehene gilt das Gesetz nur, soweit sie an das SVN oder KDN angeschlossen sind. Durch die Einbeziehung der Gerichte ist der Anwendungsbereich weiter als im SächsEGovG.

Bezogen auf die Grundsätze der Informationssicherheit (§ 4) wurden im Wesentlichen die bestehenden Regelungen aus dem SächsEGovG übernommen. Danach müssen die staatlichen Stellen angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zur Einhaltung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit für die in ihren informationstechnischen Systemen verarbeiteten Daten treffen.

Die BSI-Standards in Verbindung mit dem BSI-Grundschutz sind weiterhin zu berücksichtigen. Neu ist hingegen, dass für technische Maßnahmen der Stand der Technik maßgeblich sein soll. Außerdem sollen nun alle staatlichen Stellen ein ISMS erstellen. Die Absicherung eines angemessenen Informationssicherheitsniveaus wird auch für die nicht-staatlichen Stellen, also auch die kommunalen Träger der Selbstverwaltung, vorgeschrieben. Das entsprach den Regelungen im damals gültigen SächsEGovG.

Abschnitt 2: Organisation der Informationssicherheit (§§ 5 - 10)
Die Informationssicherheitsorganisation hatte sich im staatlichen Bereich bereits der seit dem Jahr 2011 bestehenden VwV IS und den Vorgaben des IT-PLR etabliert und wurde daher im Gesetz beibehalten. BfIS Land blieb weiterhin die zentrale strategische Stelle für die Informationssicherheit im Freistaat Sachsen.

Das SAX.CERT wurde als die zentrale Stelle für operative Fragen der Informationssicherheit aller staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen auf eine gesetzliche Grundlage gestellt. Sein Aufgabenbereich wurde u. a. um die Erfassung und Analyse von Sicherheitsgefährdungen erweitert, um ein aktuelles Bild der Sicherheitslage im Freistaat zu erstellen. Das SAX.CERT wurde außerdem zentrale Meldestelle nach dem BSI-Gesetz und im VerwaltungsCERT-Verbund (VCV), aber auch für Sicherheitsvorfälle in den staatlichen oder nicht-staatlichen Stellen. Zudem wurde festgelegt, dass sowohl SAX.CERT als auch BfIS Land den nicht-staatlichen Stellen beratend zur Verfügung stehen. Neben dem BfIS Land erhielt auch das SAX.CERT Befugnisse, nötige Anordnungen zu treffen und erforderliche Maßnahmen zur Abwehr von Gefahren für die Informationssicherheit zu ergreifen.

In das SächsISichG wurde für die staatlichen Stellen die verpflichtende Ernennung der BfIS aufgenommen. Aufgrund der besonderen Stellung in der Landesverwaltung soll in bestimmten staatlichen Stellen wie den Staatsministerien, der Polizei und dem SID ein hauptamtlicher BfIS eingesetzt werden. Nicht-staatliche Stellen sollen ebenfalls eine Informationssicherheitsorganisation aufbauen. Dabei können kleine nicht-staatliche Stellen flexibel agieren: Sie dürfen einen gemeinsamen Beauftragten ernennen oder die Aufgabe an Externe übertragen

Die AG IS hatte sich als beratendes Gremium bewährt und wurde daher in das Gesetz ausdrücklich aufgenommen. Daher berät es den BfIS Land weiterhin und empfiehlt Maßnahmen zur Sicherstellung angemessener Informationssicherheit. Dabei sichern zwei Vertreter der Kommunen in der AG IS die Vertretung der nicht-staatlichen Behörden.

Abschnitt 3: Maßnahmen zur Sicherstellung der Informationssicherheit (§§ 11 - 14)

Für den Schutz der Verwaltungsnetze bedarf es u. a. einer Analyse des Datenverkehrs insbesondere am Übergang zum Internet. Das Gesetz schafft die erforderlichen Rechtsgrundlagen, wonach Daten, die beim Betrieb von informationstechnischen Systemen der staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen anfallen, durch diese erhoben und automatisiert ausgewertet werden dürfen, soweit dies zur Verhinderung oder Abwehr von Angriffen auf die informationstechnischen Systeme erforderlich ist. Auch wurden Rechtsgrundlagen geschaffen, die es ermöglichen, Datenströme nachzuverfolgen, wenn Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung festgestellt werden. Dabei orientierten sich die Regelungen an vorhandene Vorschriften im BSI-Gesetz und an Gesetzen bzw. Gesetzentwürfen zum Thema Informationssicherheit anderer Bundesländer.

Abschnitt 4: Meldepflichten (§§ 15 - 17)

Ein wirksamer Schutz vor Angriffen ist nur möglich, wenn allgemeine Gefährdungen sowie die eigene konkrete Gefährdungslage im Überblick bekannt sind. Daher wurden in Abschnitt 4 behördenübergreifende Meldepflichten sowie Meldepflichten der staatlichen und nicht-staatlichen Stellen geregelt.

Abschnitt 5: Schlussvorschriften (§§ 18 - 21)

Die Schlussvorschriften enthielten den notwendigen Hinweis auf die Einschränkung von Grundrechten gemäß dem Zitiergebot, eine Experimentierklausel und eine Vorschrift zur Evaluierung. Das Gesetz enthielt zudem Übergangsfristen bis zur vollständigen Wirksamkeit, um erforderliche technische und organisatorische Umsetzungsschritte zu gewährleisten.

Berichtspflichten an den Sächsischen Landtag

Der von der Staatsregierung im Februar 2019 eingebrachte Gesetzentwurf, der dem SächsISichG zugrunde liegt[12], wurde während der Ausschussberatungen um Berichtspflichten des BfIS Land an den Sächsischen Landtag ergänzt.[13] Danach hat er den Sächsischen Landtag jährlich über seine Tätigkeit und die in den Landesbehörden getroffenen Maßnahmen der Datenverarbeitung zu unterrichten (§ 5 Absatz 8 Satz 1 SächsISichG). Hintergrund für die Aufnahme der Regelung war, dass die Datenverarbeitungsbefugnisse Eingriffe in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung darstellen. Um diesen Eingriff in die Grundrechte zu kompensieren, wurde BfIS Land zur jährlichen Berichterstattung an den Landtag verpflichtet. Damit werden hinreichend Transparenz und Kontrolle gewährleistet und auf der Grundlage des Gesetzes ergriffene Maßnahmen einer parlamentarischen Kontrolle zugänglich gemacht. Um den statuierten Berichtspflichten nachkommen zu können, wurden auch die staatlichen und nicht-staatlichen Stellen, soweit sie Befugnisse aus §§ 12 und 13 SächsISichG in eigener Verantwortung wahrnehmen, verpflichtet, den BfIS Land zu unterrichten.

Änderungen am SächsISichG aufgrund der Anforderungen der NIS-2-Richtlinie

Mit dem Gesetz zur Änderung des Sächsischen Informationssicherheitsgesetzes [14] wurden europarechtliche Vorgaben aus der NIS-2-Richtlinie im Freistaat Sachsen umgesetzt. Die NIS-2-Richtlinie verfolgt einen ganzheitlichen, gefahrenübergreifenden Ansatz, der nicht lediglich die einzelne kritische Anlage schützen soll, sondern das Unternehmen bzw. die Einrichtung gesamthaft betrachtet. Übergeordnetes Ziel ist damit der Schutz von Unternehmen sowie Institutionen und allgemein die Modernisierung und Ausweitung der Cybersicherheit in der EU. Der Anwendungsbereich der Cybersicherheitsregulierung ist mit der NIS-2-Richtlinie erstmals auf bestimmte Einrichtungen der öffentlichen Verwaltung der Regionalebene ausgeweitet worden.

[12] Sächsischer Landtag, Drs 6/16724
[13] vgl. Sächsischer Landtag, Beschlussempfehlung und Bericht des Innenausschusses zur Drs 6/16724; Drs 6/18105
[14] Gesetz zur Änderung des Sächsischen Informationssicherheitsgesetzes vom 5. Juli 2024 (SächsGVBl. S. 590)

Dabei bot das SächsISichG nicht nur eine bestehende Regelung, die die europäischen Anforderungen nahtlos integrieren konnte, sondern war auch so fortschrittlich und weitsichtig, dass nur wenige Änderungen erforderlich waren. Da das SächsISichG bereits für alle Verwaltungsebenen verpflichtende Anforderungen zur Informationssicherheit vorgesehen hatte, wurden die Anforderungen der NIS-2-Richtlinie auf alle staatlichen Stellen ausgeweitet. Die Umsetzung geht damit über eine reine Richtlinienumsetzung hinaus. Das bereits umfassend bestehende Regelungswerk für staatliche Stellen wurde mit der Gesetzesanpassung zukunftsweisend weiterentwickelt.

Die gemäß § 4 Absatz 1 SächsISichG zu treffenden, abstrakt beschriebenen angemessenen Maßnahmen wurden durch verpflichtende Maßnahmen konkretisiert und priorisiert, u. a. zur Bewältigung von Sicherheitsvorfällen oder zum Management von Sicherheitslücken, vgl. § 4 Absatz 1a SächsISichG.

Als zuständige Behörde gemäß Artikel 8 Absatz 1 der NIS-2-Richtlinie auf Ebene des Landes für die Aufsicht über die gemäß Artikel 2 Absatz 2 Buchstabe f Ziffer ii der NIS-2-Richtlinie identifizierten Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene wurde BfIS Land bestimmt, vgl. § 5 Absatz 1 Satz 2 Nummer 5 SächsISichG. Insbesondere wurde mit der Änderung sein Revisionsrecht ergänzt, vgl. § 5 Absatz 7 SächsISichG.

Als Computer Security Incident Response Team (CSIRT) im Sinne der Richtlinie wurde das SAX.CERT ernannt, vgl. § 6 Absatz 1 Satz 2 Nummer 1 SächsISichG. Das SAX.CERT erfüllte bereits eine Reihe der unter der NIS-2-Richtlinie beschrieben Aufgaben. Bei der Benennung und Einrichtung des SAX.CERT als CSIRT ist jedoch sicherzustellen, dass es über angemessene Ressourcen sowie Personalausstattung und technische Kapazitäten verfügt, um die Aufgaben eines CSIRT zu erfüllen.

2.3 Entwicklung des Informationssicherheitsrechts in Deutschland und Europa

Der Rechtsrahmen für die Informationssicherheit hat sich in den vergangenen Jahren dynamisch entwickelt und nicht zuletzt u. a. auch durch EU-Rechtsetzungsverfahren erheblich an Relevanz gewonnen. Die Entwicklung des Informationssicherheitsrechts in Deutschland und Europa war geprägt von einer kontinuierlichen Anpassung an die wachsenden Herausforderungen der Digitalisierung und Cyberbedrohungen.

Ein zentraler Meilenstein war das **IT-Sicherheitsgesetz**[15], das im Jahr 2015 auf Bundesebene in Kraft trat. Das Gesetz zielte darauf ab, die IT-Sicherheit in Deutschland zu verbessern, insbesondere für Kritische Infrastrukturen (KRITIS) wie Energieversorgung, Gesundheitswesen und Telekommunikation. Es regelte aber auch die Stärkung der IT-Sicherheit in der Bundesverwaltung. Das **IT-Sicherheitsgesetz 2.0**[16] aus dem Jahr 2021 stärkte die Rolle des BSI als zentrale Cybersicherheitsbehörde. Es führte neue Regelungen für die Cybersicherheit in Mobilfunknetzen ein, erhöhte die Anforderungen an die IT-Sicherheit und erweiterte den Kreis der kritischen Infrastrukturen.

Das vom Bund geplante NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz[17] zielt darauf ab, die NIS-2-Richtlinie in nationales Recht für Unternehmen und die Bundesverwaltung umzusetzen. Es wird weitere, über den bisher geltenden Ordnungsrahmen hinaus geltende Anforderungen an Unternehmen und Bundesbehörden stellen, um die Cybersicherheit in Europa zu stärken.

[15] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I S. 1324)
[16] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122)
[17] Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, BT-Drs. 20/13184

Die Europäische Union (EU) setzt durch ihre Cybersicherheitsstrategie[18], ihre Richtlinien und Verordnungen starke Impulse im Bereich der Cybersicherheit, um die Widerstandsfähigkeit gegen Cyberbedrohungen in allen Mitgliedstaaten zu stärken. Wesentliche Impulse durch die EU erfolgten durch die NIS-Richtlinie[19], NIS-2-Richtlinie[20], den Rechtsakt zur Cybersicherheit[21] und den Cyber Resilience Act[22] (CRA).

Mit dem CRA wird es erstmals für Software und Hardware-Produkte mit digitalen Elementen verbindliche grundlegende Cybersicherheitsanforderungen für den Marktzugang zum europäischen Binnenmarkt geben. Durch die zukünftige Anwendung harmonisierter Standards (Security-by-Design) und einem verbindlichen Umgang mit Schwachstellen soll der CRA das Vertrauen der Verbraucher in digitale Produkte sowie die Verbraucherrechte stärken.

Neben den europarechtlichen und bundesweiten Regelungen hatten auch die Bundesländer die Notwendigkeit erkannt, Regelungen zur Informationssicherheit für ihre Verwaltungen in ihren E-Government-Gesetzen aufzunehmen. Sachsen war jedoch eines der ersten Bundesländer, welches ein eigenständiges Gesetz zur Informationssicherheit geschrieben hat. Eigenständige Gesetze zur Informations- oder Cybersicherheit gibt es bislang in fünf Ländern.

Die Entwicklung des Informationssicherheitsrechts in Deutschland zeigt eine klare Tendenz zur Stärkung der Informations- und Cybersicherheit auf allen Ebenen. Durch die Kombination aus bundesweiten Gesetzen und spezifischen Regelungen in den Bundesländern wird ein umfassender Schutz vor Cyberbedrohungen angestrebt. Dies ist essenziell, um die Digitalisierung sicher und vertrauenswürdig zu gestalten.

[18] aktuelle Cybersicherheitsstrategie „The EU´s Cybersecurity Strategy for the Digital Decade“ vom 16. Dezember 2020; https://digital-strategy.ec.europa.eu/de/node/435

[19] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1)

[20] 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 Richt-linie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABI. L 333 vom 27.12.2022, S. 80; L, 2023/90206, 22.12.2023)

[21] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikations-technik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (ABl. L 151, 7. Juni 2019, S. 15)

[22] Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheits-anforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024)

Die nachfolgende Übersicht stellt die aktuelle Gesetzgebung in den Ländern mit Bezug zur Informations- oder Cybersicherheit dar:

Bundesland	Gesetz
Baden-Württemberg	Gesetz für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz - CSG) vom 4. Februar 2021 (GBl. 2021, 182)
Bayern	Bayerisches Digitalgesetz (BayDiG) vom 22. Juli 2022 (GVBl. S. 374, BayRS 206-1-D), das zuletzt durch Art. 10 des Gesetzes vom 21. Juni 2024 (GVBl. S. 114) geändert worden ist
Berlin	Gesetz zur Förderung des E-Government (E-Government-Gesetz Berlin - EGovG Bln) vom 30. Mai 2016 (GVBl. S. 282), zuletzt geändert durch Gesetz vom 27.09.2021 (GVBl. S. 1122)
Brandenburg	Gesetz über die elektronische Verwaltung im Land Brandenburg (Brandenburgisches E-Government-Gesetz - BbgEGovG) vom 23. November 2018 (GVBl.I/18, [Nr. 28]), zuletzt geändert durch Artikel 2 des Gesetzes vom 14. Mai 2024 (GVBl.I/24, [Nr. 17], S.5)
Bremen	-
Hamburg	-
Hessen	Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG) vom 29. Juni 2023; (GVBl. S. 433) FFN 210-105
Mecklenburg-Vorpommern	Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (E-Government-Gesetz Mecklenburg-Vorpommern - EGovG M-V) vom 25. April 2016 (GVOBl. M-V 2016, 198), zuletzt geändert durch Artikel 1 des Gesetzes vom 9. April 2024 (GVOBl. M-V S. 110) EGovG M-V
Niedersachsen	Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) vom 24. Oktober 2019 (Nds. GVBl. S. 291)
Nordrhein-Westfalen	-
Rheinland-Pfalz	Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (E-Government-Gesetz Rheinland-Pfalz - EGovGRP) vom 15. Oktober 2020
Saarland	Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland - IT-SiG SL) vom 15. Mai 2019
Sachsen	Sächsisches Informationssicherheitsgesetz vom 2. August 2019 (SächsGVBl. S. 630), das zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 22. Juli 2024 (SächsGVBl. S. 706) und durch das Gesetz vom 5. Juli 2024 (SächsGVBl. S. 590) geändert worden ist
Sachsen-Anhalt	-
Schleswig-Holstein	-
Thüringen	Thüringer Gesetz zur Förderung der elektronischen Verwaltung (Thüringer E-Government-Gesetz - ThürEGovG -) vom 10. Mai 2018 (GVBl. 2018, 212, 294)

Tabelle 1 - Übersicht über aktuelle Informations- und Cybersicherheitsgesetzgebung der Länder

2.4 Beschreibung des gesetzlichen Auftrages und Rahmenbedingungen der Evaluierung

Die Aufgabe des Evaluierungskonzeptes besteht darin, die Staatsregierung zu befähigen, die gesetzlich vorgeschriebene Evaluierung des SächsISichG durchzuführen und hierüber an den Landtag zu berichten. Für die vorliegende Evaluierung wurde in einem mehrstufigen Verfahren ein möglichst breites Stimmungsbild der betroffenen Verpflichteten des Gesetzes und aller weiteren Akteure eingeholt, um im Ergebnis aussagekräftige und zutreffende Evaluierungsergebnisse ermitteln zu können.

Die Anforderungen an die Evaluierung des SächsISichG 2024 leiten sich direkt aus dem in § 21 Absatz 1 SächsISichG definierten Evaluierungsauftrag ab. Die Staatsregierung hat danach einen Bericht vorzulegen, in dem sie darlegt,

1. welche Auswirkungen dieses Gesetz auf die Informationssicherheit in den Behörden im Freistaat Sachsen hat,
2. welche Projekte auf Basis der Experimentierklausel des § 19 SächsISichG durchgeführt wurden,
3. welche Kosten und welcher Nutzen bei der Umsetzung des Gesetzes entstanden sind und
4. ob eine Weiterentwicklung der Vorschriften dieses Gesetzes erforderlich ist.

Wichtigstes Ziel der Evaluierung des SächsISichG im Jahr 2024 sollte es sein, dem gesetzlichen Evaluierungsauftrag aus § 21 Absatz 1 SächsISichG vollumfänglich nachzukommen. Neben dem Umsetzungsstand des SächsISichG und den Auswirkungen einzelner Regelungen des Gesetzes waren demnach auch die Kosten und der Nutzen des Gesetzes sowie mögliche Weiterentwicklungspotentiale des SächsISichG zu evaluieren.

2.4.1 Erläuterung des Vorgehens

Um die Berücksichtigung der gesetzlichen Anforderungen aus § 21 SächsISichG im Rahmen des Erstellungsprozesses des Evaluierungskonzeptes sicherzustellen, wurden der Konzepterstellung folgende Prämissen zugrunde gelegt:

- Stringente Orientierung an den gesetzlichen Regelungen: **Die für die Durchführung der Evaluierung definierten Indikatoren orientieren sich eng an den Vorschriften des SächsISichG. So können Aussagen zur Wirksamkeit des Gesetzes anhand des Umsetzungsstandes der gesetzlichen Regelungen und dem Grad der Zielerreichung getroffen werden.**
- **Berücksichtigung strategischer Ziele zur digitalen Transformation der sächsischen Staatsverwaltung:** Im Rahmen der Evaluierung wurden neben dem Koalitionsvertrag 2019 bis 2024 auch die strategischen Ziele der beabsichtigten Strategie zur digitalen Transformation der sächsischen Staatsverwaltung berücksichtigt, um eine ganzheitliche Perspektive auf die Entwicklungen und Zielsetzungen zur Informationssicherheit/IT-Sicherheit im Freistaat zu gewährleisten.
- Machbarkeit und Verhältnismäßigkeit: **Handlungsleitend waren die Grundsätze der Machbarkeit und Verhältnismäßigkeit in Bezug auf die Erhebung der Daten. Sofern Informationen zentral vorlagen, wurden diese zentral erhoben. Die Datenerhebung bei den einzelnen staatlichen Stellen und nicht-staatlichen Stellen (beispielsweise im Rahmen einer Online-Befragung) erfolgte entsprechend nur dort, wo Informationen nicht zentral vorlagen und der Erkenntnisgewinn im Vergleich zum Aufwand der Erhebung vertretbar erschien.**

Ein weiteres Ziel der Evaluierung war es, die Wirkung der Rechtsnormen im Hinblick auf die Gewährleistung der Informationssicherheit der Verwaltung in Sachsen zunächst zu dokumentieren, um darauf aufbauend die zukünftige Ausgestaltung entsprechender Strategien und rechtlicher Rahmenbedingungen möglichst bedarfsgerecht fortzuentwickeln.

Ziel der Evaluierung war es aber auch, die Sachgerechtigkeit, Praktikabilität und Normenklarheit des SächsISichG zu überprüfen. Daneben war der Erfüllungsaufwand, der durch die Neuregelung des SächsISichG entstanden ist, nachzumessen.

2.4.2 Methodisches Vorgehen

Im Rahmen der Evaluierung wurden die Wirkungen des SächsISichG untersucht. Mittels einer umfangreichen Datenerhebung bzw. -analyse von Primär- und Sekundärdaten wurde die Grundlage für die Evaluierung sowie letztlich für die Ableitung von Vorschlägen zur Weiterentwicklung des Gesetzes gelegt.

Die Ermittlung der Auswirkungen der Regelungen erfolgte anhand eines Wirkmodells, dass im Wesentlichen auf den Prämissen des logischen Modells (Grundlagen, Umsetzung, Output, Outcome und Impact) basiert.

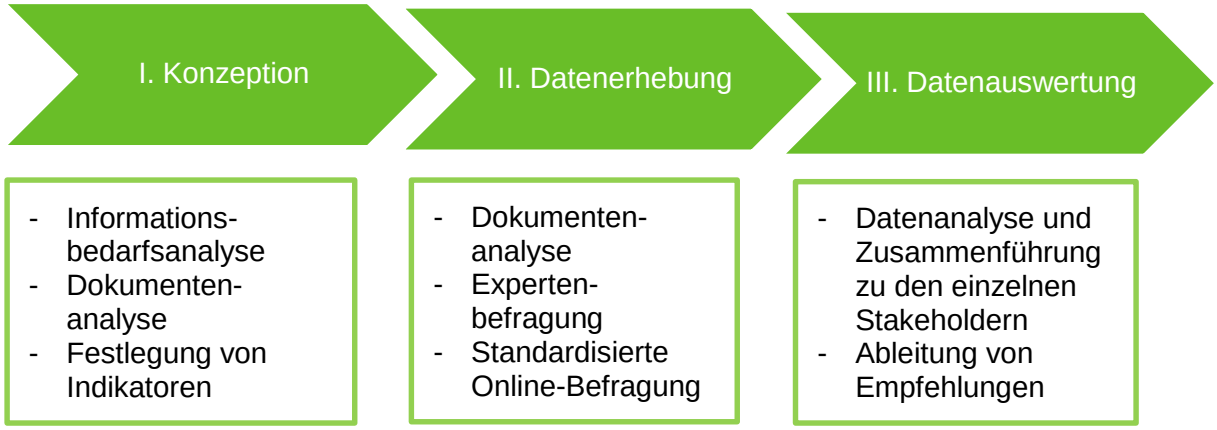

Abbildung 1 - Methodischer Ansatz der Evaluierung des SächsISichG im Jahr 2024

Als Untersuchungsdesign wurde der Vorher-Nachher-Vergleich gewählt. Mit dem Vorher-Nachher-Vergleich kann anhand von Zeitreihen die Zielerreichung dargestellt werden. Der damit einhergehende Daten- und Informationsbedarf wurde durch unterschiedliche Verfahren zur Erhebung der Daten gedeckt:

- eigens konzeptionierte und fortlaufende amtliche Statistik, z. B. Meldung der ernannten BfIS,
- Leitfadengestützte Interviews,
- Online-Befragungen.

Ausgehend von den Ergebnissen wurden Indikatoren für die Zielerreichung gebildet. Im Rahmen einer Informationsbedarfsanalyse wurde für die einzelnen Indikatoren festgestellt, an welchen Stellen entsprechende Informationen bereits vorliegen und welche Daten zusätzlich erhoben werden sollten. Ziel war es, für alle Adressatengruppen des Gesetzes (staatliche Stellen und nicht-staatliche Stellen) möglichst umfassend die erreichten Ergebnisse in der Umsetzung, die vollzogenen Unterstützungsmaßnahmen sowie die Bewertung der Zielerreichung darstellen zu können. Aus den Ergebnissen der Informationsbedarfsanalyse leiteten sich für die Phase der Datenerhebung drei unterschiedliche Untersuchungsmethoden ab: eine Dokumentenanalyse, eine Expertenbefragung sowie eine standardisierte Online-Befragung.

Dokumentenanalyse

Im Rahmen der Konzeption der Evaluierung und der Informationsbedarfsanalyse wurden relevante Dokumente für die Evaluierung der Regelungsbereiche des SächsISichG identifiziert. Die Dokumentenanalyse umfasste insbesondere folgende Dokumente:

- Gesetzentwurf zur Neuordnung der Informationssicherheit im Freistaat Sachsen (Drs. 6/16724)
- Gesetzentwurf zur Änderung des SächsISichG (Drs. 7/16207)
- Stellungnahme des Sächsischen Normenkontrollrates zum Gesetzentwurf zur Neuordnung der Informationssicherheit im Freistaat Sachsen
- Strategie Digitale Transformation der Verwaltung Sachsen
- Sachsen Digital 2030: besser schneller, sicher - Digitalstrategie für den Freistaat Sachsen
- Jahresberichte des Beauftragten für Informationssicherheit 2020-2023
- vorliegende Beschlüsse und Berichte (z. B. der AG IS und des LA ITEG)
- Koalitionsvertrag Freistaat Sachsen 2019 – 2024

Expertenbefragung

Dem Grundsatz der Verhältnismäßigkeit und Machbarkeit folgend wurden zentral vorliegende Informationen auch zentral abgefragt. Entsprechend wurden in der Konzeption der Evaluierung auskunftsfähige Ansprechpartnerinnen und Ansprechpartner für Expertenbefragungen identifiziert. Neben dem BfIS Land in der SK und dem SAX.CERT beim SID wurden die Mitglieder der AG IS, einschließlich der Vertreter für die kommunale Ebene, als auch der CIO einbezogen.

Standardisierte Online-Befragung

Für die Evaluierungsaspekte, in denen keine zentralen Dokumente oder auskunftsfähige Expertinnen und Experten identifiziert werden konnten, wurde eine flächendeckende standardisierte Online-Befragung der Adressatengruppen des SächsISichG vorgenommen. Dabei wurde jeweils ein eigener Fragebogen für die Befragung der staatlichen Stellen (Ressorts und nachgeordnete Einrichtungen), der kommunalen Träger der Selbstverwaltung, der Hochschulen sowie sonstiger Träger der Selbstverwaltung konzipiert, da sich die abzufragenden Themenkomplexe und Fragestellungen zum Teil unterscheiden. Die Online-Befragung erfolgte über das Beteiligungsportal des Freistaates Sachsen.

3 Ergebnisse der Evaluierung nach § 21 SächsISichG

Die Evaluierung der Auswirkungen des SächsISichG erfolgt, wie in Kapitel 2.4.2 dargestellt, dreigeteilt. Datengrundlage sind einerseits die Ergebnisse der an die staatlichen und nicht-staatlichen Stellen online im Beteiligungsportal Sachsen adressierten Fragebögen. Dazu kommen die Ergebnisse der Expertenbefragungen. Zudem dokumentieren zahlreiche Datensätze, die dem BfIS Land vorliegen, die Entwicklung der Informationssicherheit in den letzten fünf Jahren. Hierzu gehören beispielhaft der öffentlich publizierte Jahresbericht Informationssicherheit, der jährlich dem Sächsischen Landtag übermittelt wird, als auch zahlreiche interne Dokumente wie der Monatsbericht des SAX.CERT, Beschlüsse der AG IS und des LA ITEG, Anordnungen, Leit- und Richtlinien zur Informationssicherheit sowie Gesetzesbegründungen.

Im Rahmen der Online-Befragung wurden staatliche Stellen und nicht-staatliche Stellen über das Beteiligungsportal des Freistaates Sachsen mit je einem eigenen Fragebogen im Zeitraum vom 29. August bis 20. September bzw. 4. Oktober 2024 befragt.

Die Rücklaufquote stellt sich differenziert nach Organisationstypen wie folgt dar:

Organisationstyp	Anzahl beteiligter Stellen	Anzahl beantworteter Fragebögen	Rücklaufquote in %
Staatliche Stellen (Behörden und Gerichte)	150	50	33 %
Kommunen	428	47	11 %
Hochschulen	18	7	39 %
Sonstige Träger der Selbstverwaltung	37	10	27 %
Gesamt	633	114	18 %

Tabelle 2 - Rücklaufquoten der Online-Befragung

Zur Befragung der staatlichen Stellen wurden über das Beteiligungsportal 50 Formulare ausgefüllt. Im Ergebnis beteiligten sich alle Ministerien und die SK, sowie 14 nachgeordnete Behörden des Freistaates Sachsen an der Evaluierung. Aus der Justiz wurden 19 und aus dem Bereich der Polizei acht Formulare ausgefüllt. Auf der Seite der nicht-staatlichen Stellen beteiligten sich insgesamt 64 Einrichtungen an der Evaluierung, gestaffelt nach Kommunen, Hochschulen und sonstigen Trägern der Selbstverwaltung. Die damit insgesamt erreichte Zahl von 114 Rückmeldungen (Rücklaufquote 18 %) ist positiv zu werten. Die erste Evaluierung des SächsEGovG hatte zum Vergleich bei zahlenmäßig weniger beteiligten Stellen eine Rücklaufquote von 15 % erreicht. Die zweite Evaluierung des SächsEGovG verzeichnete hingegen eine leicht höhere Rücklaufquote von 25 % (120 Rückläufer) bei jedoch weniger befragten Behörden und Einrichtungen. Im Ergebnis stand damit ausgehend von der standardisierten Online-Befragung der staatlichen und nicht-staatlichen Stellen eine ausreichende Datengrundlage für die Bewertung der ausgefüllten Fragebögen zur Verfügung.

Zur weiteren Datenerhebung wurden jeweils auskunftsfähige Ansprechpartner bzw. Experten im SAX.CERT, die einzelnen Mitglieder der AG IS sowie der CIO des Freistaates Sachsen persönlich befragt. Mit diesen zusätzlichen Expertenbefragungen konnten weitere Hintergrund- und Kontextinformationen sowie Einschätzungen zum Nutzen des SächsISichG gewonnen werden. Die aus den Befragungen gewonnen zusätzlichen Informationen wurden unter Kapitel 3.1 und Kapitel 3.2 im Rahmen der Auswertung zusammenfassend gewürdigt.

3.1 Auswirkungen des Gesetzes auf die Informationssicherheitsorganisation in Sachsen

Unzweifelhaft den stärksten Impuls setzte das SächsISichG in den letzten fünf Jahren für die Professionalisierung der Organisationsstruktur der Informationssicherheit. Mit der Pflicht zur Benennung von BfIS und der Bereitstellung von sechs Stellen für einzelne Ressorts durch den Haushaltsgesetzgeber wurden über die Jahre hinweg erstmals in allen Ministerien und weiteren wichtigen Staatsbehörden Rollen besetzt, die damit das Thema Informationssicherheit in ihren Behörden treiben konnten. Auch der zentrale operative Akteur SAX.CERT wurde durch eine deutliche Erhöhung seiner Stellen gestärkt.

In diesem Kapitel wird dargestellt, in welcher Weise die vom Gesetz benannten Rollen in der Informationssicherheit die ihnen zugedachten Aufgaben wahrgenommen haben und welche Herausforderungen bei der Aufgabenwahrnehmung und der Zusammenarbeit zwischen den Rollen und Gremien aufgetreten sind.

3.1.1 Beauftragter für Informationssicherheit des Landes

BfIS Land bildet die zentrale strategische Instanz in der Informationssicherheitsorganisation der staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen. Er wird vom CIO des Freistaates Sachsen ernannt und hat für die Erfüllung seiner Aufgaben bei diesem ein direktes Vorspracherecht. Er ist zugleich auch Referatsleiter des Referats „Informations- und Cybersicherheit, Kritische Infrastrukturen“.

BfIS Land:

- berät, fördert und unterstützt die in die AG IS berufenen BfIS staatlichen Stellen bei deren Aufgabenerfüllung,
- initiiert und koordiniert landesweite Sensibilisierungs- und Schulungsmaßnahmen (siehe Kapitel 3.2.2) sowie Projekte zur Informationssicherheit,
- berät und unterstützt den CIO in Fragen der Informationssicherheit,
- ist zuständige Behörde nach der NIS-2-Richtlinie für die Aufsicht über die staatlichen Stellen (seit Oktober 2024),
- übt die Fachaufsicht über das SAX.CERT aus,
- trifft Anordnungen oder ergreift Maßnahmen bis hin zu vorübergehenden Netztrennungen, um Gefahren für die mit dem SVN oder KDN verbundenen informationstechnischen Systeme abzuwehren,
- führt eigene Revisionen bei staatlichen Stellen durch und kann (seit Oktober 2024) Anordnungen treffen oder Maßnahmen ergreifen, falls diese die Anforderungen der Informationssicherheit nicht in ausreichendem Maße umsetzen,
- ist für die Erstellung des ISMS für die sächsische Staatsverwaltung zuständig; dazu erarbeitete Mindeststandards legt er nach Anhörung der AG IS dem LA ITEG zur Entscheidung vor,
- unterrichtet den Landtag jährlich über seine Tätigkeit, über vom SAX.CERT getroffene Anordnungen und ergriffene Maßnahmen sowie zu Informationssicherheitszwecken verarbeitete personenbezogene Daten,
- unterrichtet den LA ITEG, den IT Kooperationsrat und die AG IS über die allgemeine Lage und seine Tätigkeit (siehe Kapitel 3.1.4) und
- unterrichtet die Öffentlichkeit über wesentliche Entwicklungen der Informationssicherheit im Freistaat Sachsen.

Im Evaluierungszeitraum wurden vier Bedienstete als BfIS Land berufen. Der jetzige Rolleninhaber bekleidet die Funktion seit September 2021. Für die teilweise längeren Zeiten zwischen den Wechseln wurden die Aufgaben vom stellvertretenden Referatsleiter übernommen.

Das Referat, welches Aufgaben über den gesetzlichen Umfang des SächsISichG hinaus zu erfüllen hat, wuchs im Berichtszeitraum um eine Stelle auf und umfasst nun vier Bedienstete der LG 2.2 und einen Bediensteten der LG 2.1.

Für die Informationssicherheit verfügt BfIS Land über ein eigenes Budget im Einzelplan der SK. Im Doppelhaushalt 2019/2020 (DHH) betrug der zugewiesene Anteil für die Titelgruppe „98 – Informationssicherheit“ 1.008.500 Euro, für das Jahr 2020 dann unter Berücksichtigung der neuen Aufgaben aus dem Gesetz 1.023.500 Euro. Dieses Budget wurde bis ins Jahr 2024 in gleicher Höhe fortgeschrieben.

BfIS Land berät die BfIS der Ressorts und unterstützt diese durch Handlungsempfehlungen, Leitfäden u. ä. Neben den in Kapitel 3.1.4 beschriebenen Mindeststandards erstellte er beispielsweise Sicherheitsempfehlungen zur Umsetzung der Homeoffice-Regelung zu Beginn der Corona-Pandemie und ressortübergreifende Rahmenvorgaben bei der Nutzung privater Endgeräte zu dienstlichen Zwecken als Ausnahme zur VwV Dienstordnung, empfahl die Nutzung eines Dokumentationstools für die ISMS der Ressorts und gab eine Empfehlung zum Nachfolgeprodukt eines Verschlüsselungstools für Dokumente mit dem Geheimschutzgrad „Verschlusssache – Nur für den Dienstgebrauch“. Die BfIS wurden bei Bedarf auch einzeln beraten.

Zur weiteren Absicherung des Netzes initiierte und koordinierte BfIS Land verschiedene Projekte, so die Einführung einer Mehrfaktorauthentifizierung für Exchange-Dienste, die IT-sicherheitstechnische Härtung des Landesverzeichnisdienstes und die Einführung erweiterter automatisierter Überwachungsfunktionen im Security Information & Event Managementsystem (SIEM). Die gesetzliche Verankerung gab BfIS Land hierzu die entsprechende Durchsetzungsmöglichkeit.

Der Austausch zwischen CIO und BfIS Land erfolgte zum einen regelmäßig im Vorfeld der Gremiensitzungen von LA ITEG und IT-Kooperationsrat. Zudem informierte BfIS Land den CIO anlassbezogen bei erheblichen Sicherheitsvorfällen oder kritischen Lagen wie der Bedrohung von einer Vielzahl von Softwareanwendungen durch eine Schwachstelle einer Open Source Komponente, der Log4J-Bibliothek, oder auch nach dem russischen Angriff auf die Ukraine.

Schließlich erstellt BfIS Land regelmäßig, gemeinsam mit dem Landeskriminalamt Sachsen und dem Landesamt für Verfassungsschutz sowie koordiniert durch das SAX.CERT, ein Lagebild für die Cybersicherheit des Freistaates Sachsen und legt dieses dem CIO sowie dem Staatsminister des Innern vor.

BfIS Land übt die Fachaufsicht über das im nächsten Kapitel genauer beschriebene SAX.CERT aus. Dazu gibt es, zusätzlich zum operativen Tagesgeschäft, einen wöchentlichen Austausch zur Abstimmung der Aufgaben.

BfIS Land hat von seinem Recht, Anordnungen zu treffen und Maßnahmen zur Gefahrenabwehr anzuordnen, seit Verabschiedung des Gesetzes mit zwölf Anordnungen maßvoll Gebrauch gemacht. So wurde bereits im Oktober 2019 eine Anordnung getroffen, potenziell gefährliche veraltete Dateiformate der Microsoft-Office-Suite in E-Mails zu unterbinden. Mit dem Angriff Russlands auf die Ukraine stieg die Gefahr einer hybriden Bedrohung, auch hier ordnete BfIS Land entsprechende Sicherungsmaßnahmen an. Selbst die komplette Trennung von Fachverfahren und Verwaltungsangeboten vom Internetübergang des SVN war im Zuge der Bedrohung durch die Log4J-Schwachstelle zum Jahreswechsel 2021/2022 notwendig. Aufgrund einer erfolgreichen Ransomware-Attacke auf eine Sächsische Kommune ordnete BfIS Land ebenfalls eine vorübergehende Netztrennung an.

Mit der Änderung des SächsISichG ab 1. Oktober 2024 darf BfIS Land zudem die Einhaltung der Anforderungen nach § 4 Absatz 1 und 1a SächsISichG überprüfen und bei Verstößen gegenüber

der von den Verpflichtungen betroffenen staatlichen Stelle anordnen, erforderliche und verhältnismäßige Maßnahmen zu ergreifen Bisher hat BfIS Land bereits regelmäßig die Einhaltung der erlassenen Mindeststandards abgefragt, die Jahresberichte der BfIS der Ressorts geprüft und auch jährlich den Umsetzungsstand der Leitlinie des IT-PLR zur Informationssicherheit in der öffentlichen Verwaltung erfasst. Zukünftig wird dies durch Audits und Revisionen zu verstärken sein, um die neuen gesetzlichen Auflagen zu erfüllen.

Dem LA ITEG legte BfIS Land nach Anhörung der AG IS zwölf landesweite Mindeststandards zur Entscheidung vor. Die Beschlussvorschläge waren sehr gut vorabgestimmt, es bestand daher nur selten Diskussionsbedarf im LA ITEG. Die Beschlüsse wurden einstimmig gefasst. Allerdings bestand ein hoher Informationsbedarf, diesem wurde durch die Erörterung vor Beschlussfassung Rechnung getragen. Des Weiteren wurden Beschlüsse zu Sicherheitsprojekten gefasst, die dann verbindlich in allen Ressorts umgesetzt werden.

BfIS Land kam seiner jährlichen Berichtspflicht an den Landtag nach. Zusätzlich zu den gesetzlich verpflichtenden Angaben enthält der jeweilige Jahresbericht zur Informationssicherheit auch ein allgemeines Bild zur Gefährdungslage mit den beobachten Angriffsszenarien auf das SVN, den Tätigkeitsbericht des BfIS Land, den Umsetzungsstand des SächsISichG sowie den Blick auf zukünftige und zusätzliche rechtliche Verpflichtungen, z. B. auf EU-Normen und Festlegungen des IT-PLR.

Die Unterrichtung des LA ITEG und des IT Kooperationsrats erfolgte ebenfalls in den jeweiligen Gremiensitzungen. Regelmäßig trug BfIS Land hier zur Lage der Informationssicherheit im Freistaat Sachsen vor und berichtete über seine Tätigkeit im Bereich Schulung/Sensibilisierung, stellte den Stand von IT-Sicherheitsprojekten vor und informierte über sich ändernde Rahmenbedingungen aufgrund von geplanten und vollzogenen Rechtsetzungsverfahren der EU und des Bundes.

Mit der Veröffentlichung des Jahresberichts erfüllt BfIS Land die Verpflichtung, die Öffentlichkeit über wesentliche Entwicklungen der Informationssicherheit der Verwaltung im Freistaat Sachsen zu unterrichten. Daneben werden regelmäßig Antworten auf Presseanfragen zur Informationssicherheit von BfIS Land dem Regierungssprecher fachlich zugearbeitet und Hör- und Fernsehfunkbeiträge begleitet.

BfIS Land vertritt die sächsische Verwaltung in Belangen der Informationssicherheit in der AG Informationssicherheit des IT-PLR.

Bewertung

Die zentrale strategische Instanz BfIS Land ist etabliert und wirksam.

Zur Vermeidung von Einschränkungen der Aufgabenerfüllung bei Abwesenheit des BfIS Land sollte die gesetzliche Verankerung eines Vertreters, wie sie für die BfIS der staatlichen Stellen bereits besteht, auch auf den Landesbeauftragten erweitert werden.

Das dem BfIS Land übertragene Budget war prinzipiell auskömmlich. Bedingt durch die Corona-Pandemie blieben in den Jahren 2021 und 2022 Mittel insbesondere für landesweite Sensibilisierungsmaßnahmen in Präsenz ungenutzt. Die personelle Ressource war mit dem Aufgabenportfolio bis zum 30. September 2024 ausreichend dimensioniert. Die seitdem umfangreicheren Aufgaben insbesondere als Aufsichtsbehörde über die staatlichen Stellen mit erweiterten Revisionsrechten und Anordnungspflichten erfordern allerdings zukünftig einen weiteren personellen und finanziellen Ausbau.

Gerade in Krisenzeiten schätzt der CIO das unmittelbare Vorspracherecht als effektiv ein. Während in anderen Bundesländern CIO und Informationssicherheitsbeauftragter mitunter unabhängig voneinander agieren, schätzt der CIO diese direkte Kopplung als gut und bewährt ein. Dadurch wird zwischen CIO und BfIS Land ein gegenseitiger frühzeitiger Informationsaustausch gewährleistet. Als

Kabinettsmitglied kann der CIO auch die Herausforderungen der Informationssicherheit unmittelbar in der Staatsregierung einbringen.

Die organisatorische Integration als Referat in die Verwaltungsdigitalisierungsabteilung hat den Vorteil, dass BfIS Land die Zusammenarbeit innerhalb der Abteilung zu Themen der Informationssicherheit stärkt und das „Mitdenken“ des Themas und eine frühzeitige Einbindung des BfIS Land gefördert wird.

Seit dem 1. Oktober 2024 hat BfIS Land allerdings die Rolle einer Aufsichtsbehörde übertragen bekommen. BfIS Land agiert zukünftig nicht nur bei Sicherheitsvorfällen anordnend gegenüber Leitern staatlicher Stellen, sondern auch hinsichtlich festgestellter Mängel zu den Anforderungen der Informationssicherheit aus Audits oder bei Revisionen. Diese Rolle kann aus einer Linienorganisation eher eingeschränkt wahrgenommen werden. Hier bietet sich zukünftig eine organisatorische Verankerung als Stabsreferat an.

Mit seiner Beratungspflicht konnte BfIS Land die BfIS der Ressorts aktiv unterstützen und beim Aufbau eigener ISMS fördern. Das hat sich sehr gut bewährt. Die Jahresberichte der Ressorts zur Informationssicherheit zeigen hier einen erheblichen Fortschritt bei der Etablierung von entsprechenden Prozessen und Regelungen.

BfIS Land war es mit dem Recht zur Anordnung bei Gefahren für informationstechnische Systeme möglich, schnell und verlässlich Sicherheitsmaßnahmen durchzusetzen. Dieses Recht hat sich bewährt und wurde von BfIS Land mit Augenmaß vorgenommen, komplette Netztrennungen stellten hierbei das letztmögliche Mittel zur Absicherung des Verwaltungsnetzes dar. Das SAX.CERT kann BfIS Land hier aufgrund der gesetzlichen Rahmenvorgaben bei der Sicherstellung der Informationssicherheit sehr wirksam operativ unterstützen.

Die Beschlussfassung der Mindeststandards durch das Gremium der Staatssekretärsebene, dem LA ITEG, hat aus Sicht des CIO zumindest zu einer Beschäftigung mit dem Thema und damit letztlich auch zu einer erhöhten Sensibilität für das Thema Informationssicherheit in den Ressorts geführt. Mit den Mindeststandards wurde ein solides Fundament gelegt, auf dem die Ressorts ihre Informationssicherheit weiter ausgestalten können. Die Wirksamkeit der Mindeststandards verdeutlicht sich in der äußerst geringen Zahl von erfolgreich schadensverursachenden Cyberattacken.

Der Jahresbericht zur Informationssicherheit ist eine hervorragende Möglichkeit, die Abgeordneten des Sächsischen Landtags über die Lage der Informationssicherheitslage in Kenntnis zu setzen und in den jeweiligen zur Befassung festgelegten Ausschüssen direkt über die Tätigkeit des BfIS Land zu unterrichten.

Laut Einschätzung von CIO und BfIS Land trägt der Lagevortrag in LA ITEG und IT Kooperationsrat erheblich dazu bei, dass Bewusstsein für die Informationssicherheit auf oberster Führungsebene der Staatsverwaltung und der Verbandsspitzen vom Sächsischen Städte- und Gemeindetag und Sächsischen Landkreistag zu fördern.

3.1.2 Sicherheitsnotfallteam SAX.CERT

Das SAX.CERT ist die zentrale Stelle für operative Fragen der Informationssicherheit im Freistaat Sachsen und ist als SAX.CERT im SID organisatorisch angesiedelt. Zu seinen Aufgaben gehören u. a.:

- die Unterstützung bei der Bewältigung konkreter Sicherheitsereignisse und -vorfälle,
- die kontinuierliche Prüfung von IT-Systemen auf Risiken im Betrieb,
- die Information zu Sicherheitslücken in Soft- und Hardware,
- die Beobachtung und Bewertung der Lage der Informationssicherheit und die Erstellung entsprechender Empfehlungen,
- die Mitwirkung bei der technischen und technologischen Koordinierung der Informationssicherheit in den staatlichen und nicht-staatlichen Stellen sowie
- die regelmäßige Information über die Lage der Informationssicherheit im Freistaat Sachsen.

Darüber hinaus nimmt das SAX.CERT die Aufgabe der zentralen Meldestelle sowohl im Sinne des BSI-Gesetzes als auch im Sinne des IT-PLR im VCV wahr und hat damit sämtliche für die Sicherheit in der Informationstechnik erforderlichen Informationen zu Sicherheitslücken, Schadprogrammen, Angriffen und Angriffsversuche inkl. Vorgehensweise zu sammeln und auszuwerten. Die Aufgaben des SAX.CERT werden weiterhin durch den Beschluss des IT-PLR vom 9. März 2022 zum CERT-Standard bundesweit einheitlich konkretisiert. Auf Grund der Umsetzung der NIS-2-Richtlinie zum 17. Oktober 2024 und des daher geänderten SächsISichG ergeben sich neue Aufgaben.

Vom SAX.CERT wird – wie bereits vor Inkrafttreten des SächsISichG – ein monatlicher Lagebericht zur Informationssicherheit im SVN/KDN erstellt. In diesem werden sowohl Sicherheitskennzahlen (u. a. Anzahl Mailviren, Internetviren) benannt als auch die gemeldeten Sicherheitsereignisse in den Behörden in Sachsen dargestellt. Dieser Bericht hat in den letzten Jahren an Umfang der Inhalte zugenommen und wurde inhaltlich kontinuierlich verbessert. Zudem werden seit Mai 2023 separate Lageberichte für die staatlichen Stellen und die Kommunen verteilt. Jedoch ist der Bericht in seiner monatlichen Dokumentenform statisch und informiert nur nachrichtlich und nachträglich über die Lage der Informationssicherheit.

Mit dem Änderungsgesetz zum SächsISichG in Verbindung mit der NIS-2-Richtlinie hat das SAX.CERT seit 1. Oktober 2024 weitere Aufgaben zu erfüllen. So ist zukünftig eine ständige Erreichbarkeit der Dienste des SAX.CERT sicherzustellen. Darüber hinaus hat das SAX.CERT nunmehr forensische Daten zu erheben und zu analysieren sowie auf Ersuchen bestimmter Einrichtungen eine proaktive Überprüfung der Netz- und Informationssysteme vorzunehmen. Diese, sowie weitere Daten, sollten in einem SOC zusammengeführt und für ein Lagebild ausgewertet werden.

Auf Grund des Erlasses des SächsISichG, der sich daraus ergebenden Aufgaben und weiterwachsender Anforderungen, z. B. durch den o. g. Beschluss des IT-PLR, wurde das SAX.CERT personell mit zusätzlichen Ressourcen ausgestattet.
Zum Aufbau des SAX.CERT wurden den zwei Bestandsstellen im Jahr 2019 eine Stelle LG 2.2 und eine befristete Projektstelle LG 2.1 hinzugeordnet. Im DHH 2021/2022 wurden vier weitere Stellen der LG 2.1 zugeführt, deren Besetzung sich allerdings bis weit ins Jahr 2023 hinzog. Gründe dafür liegen sowohl im Fachkräftemangel für die gesuchten hochspezialisierten Sicherheitsexperten als auch an der zu niedrigen Eingruppierung der zur Verfügung gestellten Stellen. Mit dem DHH 2023/2024 wurden dem SAX.CERT deshalb zwei Stellen LG 2.2 zugewiesen, die auch besetzt werden konnten. Die aktuelle Stellenausstattung beträgt nun drei Stellen der LG 2.2 und sechs Stellen der LG 2.1.

Die finanzielle Ausstattung des SAX.CERT ist seit dem DHH 2019/2020 konstant bei jährlich 600.000 Euro geblieben. Finanziert werden damit externe Personalressourcen für die Sicherheitsvorfall-Hotline und Forensikdienste, Lizenzkosten für eingesetzte Viren- und Malwarescanner, Betriebskosten für das Detektionswerkzeug HoneySens u. ä.

Bereits vor Inkrafttreten des Gesetzes bot das SAX.CERT verschiedene Dienstleistungen für die Behörden der Staatsverwaltung an und dehnte dieses Angebot auf die vom Gesetz nun umfassten nicht-staatlichen Stellen aus. So wird gemeinsam mit dem Hasso-Plattner-Institut der Identity Leak Checker angeboten, der das Darknet auf gestohlene Identitäten mit dienstlichen E-Mail-Adressen der Staatsverwaltung und auf Antrag auch von Kommunen durchsucht. Die Anwendung Passwortchecker prüft, ob das von Bediensteten zur Nutzung geplante Passwort komplex und ausreichend lang ist, um einem Hackerangriff zu widerstehen. Mit dem Produkt HoneySens bietet das SAX.CERT ein im Behördennetz einzusetzendes Detektionssystem an, welches unerwünschten Netzwerkverkehr erkennt und meldet.

Seit dem Jahr 2020 werden zudem regelmäßige Webseitenscans zur Identifikation von Schwachstellen in Webseiten der Landes- und Kommunalverwaltung durchgeführt. Über ein Infoportal können die staatlichen und nicht-staatlichen Stellen dann abrufen, welche Schwachstellen erkannt wurden und wie diese zu beheben sind.

Im Jahr 2020 baute der SID für das SAX.CERT ein Lagezentrum auf, in dem auf mehreren Monitoren verschiedene sicherheitsrelevante Ereignisses aus verschiedenen Informationsquellen so aufbereitet werden, dass Abweichungen zum erwarteten Verhalten von IT-Systemen sehr schnell erkannt und analysiert werden können. 2022 wurde gemeinsam mit einem externen Partner ein SOC aus dem seit dem Vorjahr bestehenden Probe- in den Regelbetrieb überführt, mit dem die Kernkomponenten des SVN rund um die Uhr überwacht und auf Anomalien geprüft werden. Hierfür werden auch personenbezogene Daten überprüft. Die rechtliche Basis hat das SächsISichG dafür erfolgreich geschaffen.

Bereits seit Beginn des Evaluierungszeitraums ist das SAX.CERT aktiv in den Verbund der SAX.CERT von Bund und Ländern eingebunden, den VCV. Als zentrale Kontaktstelle gemäß BSI-Gesetz für Sicherheitsvorfälle bei KRITIS-Unternehmen agiert es allerdings erst seit dem Jahr 2023 produktiv. Vorausgegangen waren längere Abstimmungen der Länder mit dem Bund zur Prozessgestaltung.

Im Rahmen der Evaluierung wurden die staatlichen und nicht-staatlichen Stellen zur Inanspruchnahme der Leistungen des SAX.CERT befragt. Rund 65 % der Rückmeldenden gaben an, Leistungen des SAX.CERT in Anspruch zu nehmen. Gemessen an den gesamten Rückmeldungen wird insbesondere der Schwachstellenwarndienst genutzt (51 %). Ebenfalls intensiv genutzt werden der Identity Leak Checker (31 %), der Webseitenscan (32 %), der Passwortchecker (16 %) sowie der HoneySens (21 %). Die Intensität der Inanspruchnahme lässt Verbesserungspotential erkennen. Es scheint notwendig, stärker über die Leistungen des SAX.CERT in den staatlichen und nicht-staatlichen Stellen zu informieren, um das Sicherheitsniveau im Anwendungsbereich des SächsISichG zu erhöhen.

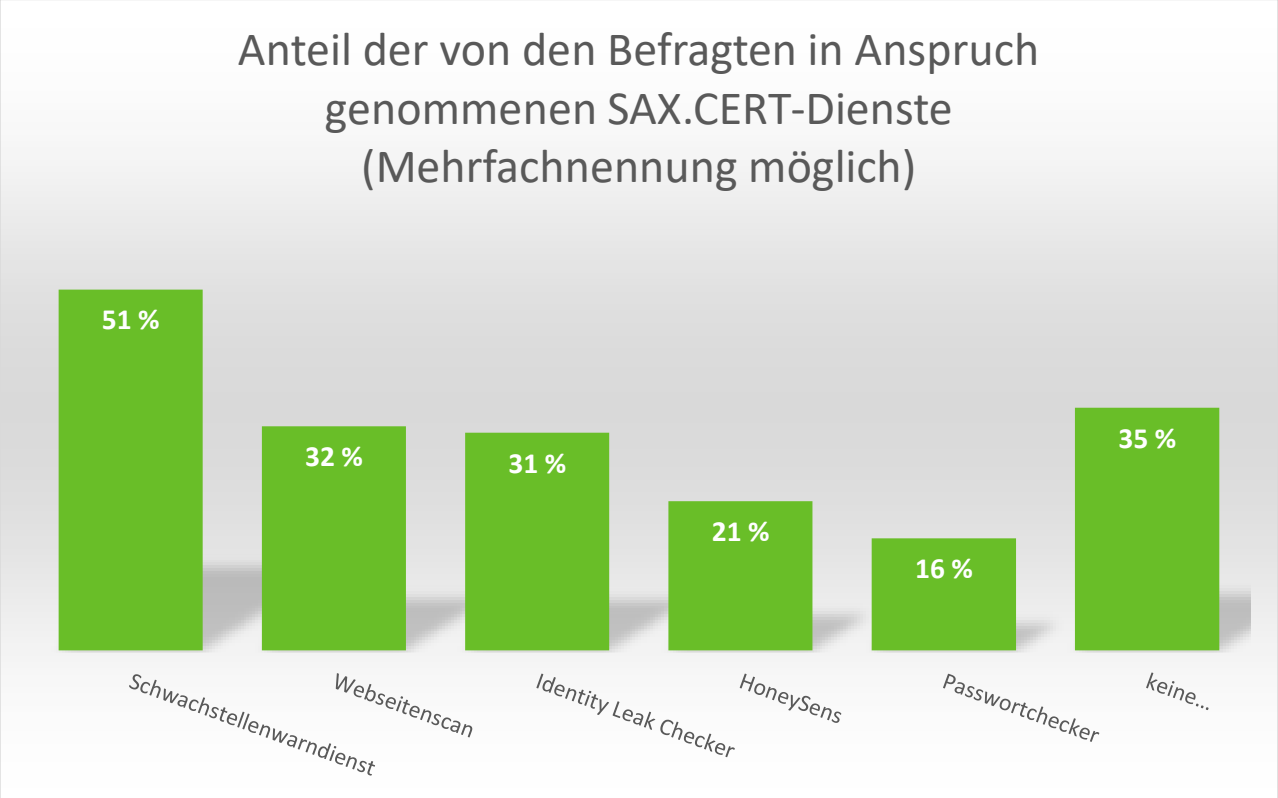

Abbildung 2 - Inanspruchnahme von Dienstleistungen des SAX.CERT

Regelmäßig werden staatliche und nicht-staatliche Stellen bei Meldungen von Sicherheitsvorfällen fachlich beraten und bei der Vorfallbewältigung unterstützt. Im Auftrag des BfIS Land übernimmt das SAX.CERT die Aussteuerung von technischen Sicherheitsmaßnahmen, z. B. bei festgestellten Mängeln im Rahmen von Audits oder bei großflächigen Vorfällen wie der Log4J-Schwachstelle.

Hinsichtlich der Informationssicherheitsorganisation besteht aus Sicht des SAX.CERT ein funktionierender bidirektionaler Informationsfluss zwischen den BfIS der staatlichen sowie nicht-staatlichen Stellen und dem BfIS Land. Ein Informationsaustausch ist sowohl über Meldeketten, durch direkte Kontakte im Fall von notwendigen Beratungen und Rückfragen zu auftretenden Informationssicherheitsereignissen sowie zu Dienstleistungen des SAX.CERT gewährleistet. Das SAX.CERT sieht hingegen eine aktivere fachliche Beteiligung der Teilnehmer der AG IS für wünschenswert.

Bewertung

Das SAX.CERT erfüllt die Aufgaben nach SächsISichG, bedient sich allerdings externer Unterstützung, um diese mit den aktuell beschränkten Ressourcen erfüllen zu können. So werden beispielsweise Sicherheitstests und -scans im SVN auf Grund fehlender Kompetenzen nur anlassbezogen durch Dritte, im Rahmen verfügbarer finanzieller Mittel, und nicht routinemäßig durch das SAX.CERT selbst durchgeführt. Auch forensische Untersuchungen nehmen Dritte im Auftrag des SAX.CERT vor. Dies führt dazu, dass zusätzlicher Zeitaufwand im Falle der Inanspruchnahme entsteht. Dies ist bei schwerwiegenden Vorfällen kritisch zu betrachten, da nur eine zügige Analyse eine gute Grundlage für schnelle Folgeentscheidungen ist. Ebenfalls kritisch einzuordnen ist die Beteiligung Dritter bei einer forensischen Untersuchung von IT-Technik, welche damit Kenntnis von eingestuften Dokumenten und Verfahren erhalten. Hier sind entsprechende zusätzliche Sicherungsmaßnahmen sowie ein hohes Vertrauen in den Dienstleister erforderlich.

Für die neuen Aufgaben seit dem 1. Oktober 2024 wie die Rufbereitschaft stehen zudem keine zusätzlichen personellen Ressourcen zur Verfügung. Das heute extern bei einem Dienstleister eingekaufte SOC sollte zukünftig, wie in vielen anderen Bundesländern auch, intern beim SAX.CERT verankert werden. Damit wird Kompetenz im SAX.CERT aufgebaut und gebunden, was

bei einer Vorfallbearbeitung ebenfalls zu einer schnellen, fundierten Analyse und Lösungsvorschlägen führt. Es wird empfohlen, dass SAX.CERT somit sowohl für die seit dem Jahr 2019 bestehenden als auch für die im Oktober 2024 hinzugekommen Aufgaben personell zu stärken.

Die gesetzlich normierte, organisatorische Zuordnung des SAX.CERT zum SID diente dem Auf- und Ausbau des Sicherheitsnotfallteams. Die organisatorische Zuordnung der Sicherheitsnotfallteams in den Ländern ist sehr unterschiedlich, sie reicht von ähnlicher Konstellation wie in Sachsen über eigene Sicherheitsbehörden bis hin zur Integration in einer obersten Landesbehörde. Es wird angeregt, die organisatorische Zuordnung zu untersuchen, um auf die wachsenden Anforderungen an die Aufgaben schnell und lageanpasst reagieren zu können.

3.1.3 Beauftragte für Informationssicherheit in den staatlichen Stellen und ISMS-Team

Die BfIS der staatlichen Stellen sind zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb ihres Zuständigkeitsbereiches. Ihre Hauptaufgabe besteht darin, den Leiter der staatlichen Stelle bei deren Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten und diese bei der Umsetzung zu unterstützen. Ihre Aufgaben sind in den Standards des BSI beschrieben und umfassen u. a.:

- den Informationssicherheitsprozess zu steuern und an allen damit zusammenhängenden Aufgaben mitzuwirken,
- die Behördenleitung bei der Erstellung der Leitlinie zur Informationssicherheit der Behörde zu unterstützen,
- die Realisierung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- der Behördenleitung und einem möglichen ISMS -Team über den Status quo der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- Sicherheitsvorfälle zu untersuchen und ggf. an das SAX.CERT zu melden (Einhaltung der Meldepflichten nach §§ 15 ff. SächsISichG),
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und koordinieren und
- den Aufbau eines geeigneten ISMS inklusive Informationssicherheitsorganisation.

Für die effektive Wahrung der Informationssicherheit insbesondere in kritischen Situationen ist die schnelle und direkte Kommunikation der BfIS mit ihrem Leiter der staatlichen Stelle unerlässlich, um Interessenkonflikte zu vermeiden. Nach dem SächsISichG ist in jeder staatlichen Stelle ein BfIS und ein Vertreter zu ernennen, vgl. § 7 Absatz 1 und 2 SächsISichG.

Im Rahmen der Evaluierung geben 47 der 50 sich beteiligenden staatlichen Stellen an, dass in ihrer Behörde ein BfIS benannt ist. Das korrespondiert in etwa mit dem vom BfIS Land erfassten Daten aus dem staatlichen Bereich. Demnach liegen dem BfIS Land von fast allen der 80 erfassten staatlichen Stellen persönliche Kontaktdaten vor. Ob diese dabei auch in jedem Fall offiziell als BfIS ernannt sind, ist nicht bekannt. Zu den einzelnen Gerichten liegen keine detaillierten Informationen vor.

Die Zahl der benannten Stellen hat sich mit Inkrafttreten des Gesetzes und den in diesem Zusammenhang zentral von der SK einigen Ressorts zur Verfügung gestellten Stellen jedoch erheblich vergrößert. Das lässt sich insbesondere bei den staatlichen Stellen ablesen, die nach § 7 Absatz 1 SächsISichG einen hauptamtlichen BfIS zu ernennen haben.

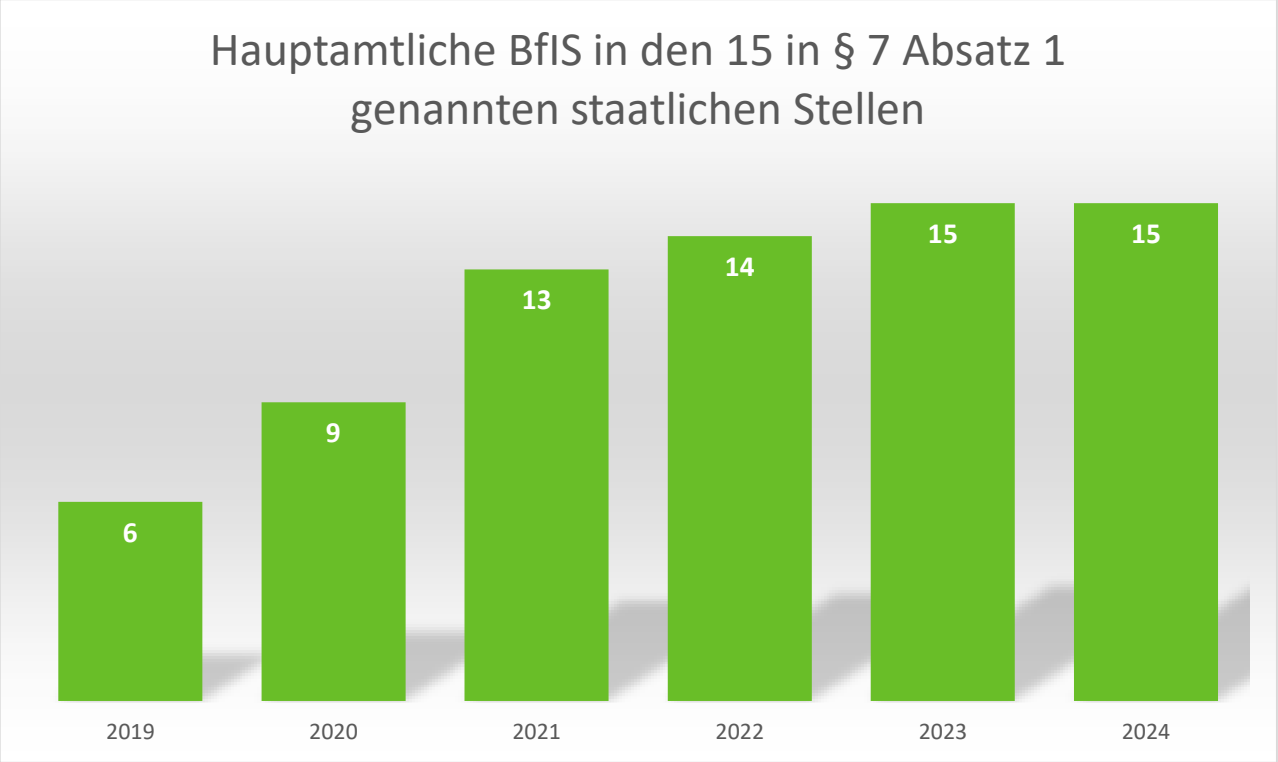

Abbildung 3 - Hauptamtliche BfIS gemäß § 7 Absatz 1 SächsISichG

Im Rahmen der Evaluierung gaben knapp die Hälfte der Behörden an, dass ihrem BfIS für seine Aufgaben zwischen 51 und 100 % des Zeitanteils zur Verfügung steht, sodass man hier von einer Hauptamtlichkeit sprechen kann. Damit stellen mehr als die eigentlich durch das Gesetz benannten Behörden dieser Rolle ausreichend Zeit zur Verfügung. Knapp 40 % sehen für die Erfüllung der Aufgaben eines BfIS nur bis zu 10 % der Arbeitszeit ihres benannten Bediensteten vor. Hierbei handelt es sich größtenteils um kleinere staatliche Stellen wie Gerichte und Justizvollzugsanstalten und einige nachgeordnete Behörden im Geschäftsbereich des SMI. In fast allen staatlichen Stellen hat der BfIS dabei ein unmittelbares Vorspracherecht bei seiner Hausleitung und kann seine Aufgaben weisungsfrei ausüben.

In der Hälfte der Behörden kann der BfIS auf ein sogenanntes Informationssicherheitsmanagement-Team zurückgreifen, was gewährleistet, dass die Themen der Informationssicherheit in der Behörde in allen wichtigen organisatorischen Einheiten mitgestaltet und mitgetragen werden. Die Abstimmung geht in vielen Fällen sogar über die eigene Organisation hinaus: Gut die Hälfte der Behörden gibt an, sich regelmäßig mit dem BfIS des zuständigen Ministeriums bzw. der übergeordneten Behörde abzustimmen, 10 % tauschen sich sogar wöchentlich aus.

Antwort	Anzahl	Prozent
nie	3	5,9%
selten (jährlich)	17	33,3%
regelmäßig (quartalsweise oder monatlich)	26	51%
wöchentlich	5	9,8%

Abbildung 4 - Austausch mit BfIS des zuständigen Ministeriums

Die BfIS der staatlichen Stellen geben fast unisono an, ihre Hausleitung in Fragen der Informationssicherheit zu beraten, die Bediensteten regelmäßig zu informieren und zu sensibilisieren sowie den Informationssicherheitsprozess zu steuern, u. a. durch das Erstellen von Sicherheitskonzepten und Richtlinien. Zudem wird die Behandlung von Sicherheitslücken und Sicherheitsereignissen als Aufgabe beschrieben. In den Behörden mit einem hauptamtlichen BfIS wird der Stand des ISMS

überwiegend als etabliert oder auf einem guten Weg beschrieben, einige befinden sich allerdings auch noch im Ausbau. Die meisten nutzen dabei eine Software zur Steuerung des ISMS. Grundsätzlich anders sieht es bei den staatlichen Stellen aus, deren BfIS nur nebenamtlich im Einsatz sind. Hier ist überwiegend kein ISMS etabliert, nur im Aufbau und kann vielerorts praktisch nicht „gelebt“ werden, da die Zeitbudgets der handelnden Personen zu gering sind. Es wird zudem überwiegend auch keine Software zur Steuerung des ISMS eingesetzt.

90 % der staatlichen Stellen geben an, dass ihnen zur Erfüllung der gesetzlichen Aufgaben Personal- und/oder Sachaufwände entstanden sind. Allerdings konnten nur die wenigsten von ihnen diese auch genauer bestimmen. Vier Behörden bezifferten ihren jährlichen Personalaufwand, entweder mit 100.000 Euro in einer Summe oder gaben den Bedarf von durchschnittlich zwei Vollzeitäquivalenten (VZÄ) an. Fünf Einrichtungen gaben Einblicke in ihren jährlichen Sachaufwand, in einer Spannweite von 5.000 bis über 100.000 Euro, wobei der Durchschnitt bei gut 30.000 Euro liegt.

Knapp 60 % der sich an der Evaluierung beteiligenden staatlichen Stellen beantworteten die Frage zu etwaigen Anpassungsbedarfen zum SächsISichG bzw. aus ihrer Sicht erforderlichen weiteren Maßnahmen, um die Informationssicherheit zu verbessern. In sehr vielen Stellungnahmen wurde auf unzureichende personelle und teilweise auch finanzielle Ausstattung in der Informationssicherheit hingewiesen. So wurde in den Rückmeldungen u. a. empfohlen, gesetzlich abzubilden, dass jeder Behörde ein VZÄ für den BfIS zur Verfügung gestellt werden muss, da die Aufgabenfülle des BfIS eine Aufgabenwahrnehmung neben einer originären Tätigkeit kaum zulassen würde. Zudem sei die Informationssicherheit auch gefährdet durch personelle Lücken in der IT der Behörden. Behörden, die nach Änderung des SächsISichG seit 1. Oktober 2024 als besonders wichtige Einrichtung identifiziert werden, würden aufgrund der damit verbundenen erhöhten Anforderungen aus der Richtlinie zudem zusätzliche Personalkapazitäten im Bereich der Informationssicherheit und des IT-Notfallmanagement benötigen. Auch wird eine gesetzliche Regelung angeregt, dass für das IT-Notfallmanagement verpflichtend Personalkapazitäten aufgebaut werden müssten. Da im Rahmen der Gesetzesänderung des SächsISichG keine Stellenbedarfe aufgenommen worden sind, kündigen viele Ressorts an, die im Rahmen der Gesetzesbehandlung gemeldeten zusätzlichen Stellenbedarfe im Stellenplan der bevorstehenden Haushaltsaufstellung anzumelden. Als Alternative zur dezentralen Bereitstellung von Stellen wird auch die Idee geäußert, eine zentrale Einheit von Informationssicherheitsbeauftragten für Behörden zu etablieren, die absehbar keine hauptamtlichen Stellen schaffen. Neben personellen wird auch die Schaffung von Ressourcen für Sachkosten gefordert: So lautet ein Vorschlag, ein Informationssicherheits-Budget für Behörden und Dienststellen zu schaffen, welches sich an einem risikobasierten Ansatz orientiert.

Neben den Ressourcenproblemen wurden folgende Verbesserungsvorschläge bzw. Hinweise am häufigsten genannt:

- Regelung zu Interessenskonflikten bezüglich Aufgabenwahrnehmung in Personalunion (BfIS in Verbindung mit behördlichen Datenschutzbeauftragten oder IT-Notfallbeauftragten),
- Definition der Abgrenzung zum IT-Notfallmanagement bzw. zum Business Continuity Management,
- Auf- und Ausbau eines geeigneten Schulungs- und Sensibilisierungskonzeptes, intensivere Schulung und Information der BfIS; mindestens zwei verpflichtende, landesweite Schulungs- bzw. Sensibilisierungsveranstaltung zur Informationssicherheit für die Führungskräfte pro Jahr,
- Aufnahme einer Formulierung in das Gesetz, dass vor Inbetriebnahme neuer Prozesse/IT-Verfahren notwendige Konzepte/Richtlinien/Dokumentation zu erstellen/umzusetzen sind,
- zentrale Bereitstellung einer ISMS-Software,
- Ausbau übergreifender Richtlinien für organisatorische sowie technische Bereiche einschließlich verbindlicher Mindeststandards zur Informationssicherheit,

- beim Umgang mit Sicherheitsvorfällen wenig Rechtsklarheit und mithin große Unsicherheiten in der Praxis; insb. bei der Abgrenzung von Sicherheitsereignissen zu Sicherheitsvorfällen; die Betrachtungsweise ist zu pauschal, ohne die Eigenarten und Besonderheiten der verschiedenen staatlichen Stellen zu berücksichtigen,
- Ausbau von Maßnahmen, die die praktische Umsetzung der gesetzlichen Anforderungen fördern; es fehlen nicht unbedingt Richtlinien, sondern Projekte; ein Ausbau und Ergänzung einfach nutzbarer zentraler Angebote, wie beim E-Learning oder der Sensibilisierungsveranstaltungen, wäre hilfreich,
- Behörden- und Dienststellenleiter müssen für Schäden, welche aus Informationssicherheitsvorfällen resultieren und wo Ihnen grob fahrlässiges oder vorsätzliches Handeln nachgewiesen werden kann, privat haften,
- Behörden und Dienststellen des Freistaates Sachsen sollten jährlich einer zufälligen, stichprobenhaften Revision zur Informationssicherheit unterzogen werden

Bewertung

In fast allen staatlichen Stellen ist ein BfIS benannt oder zumindest ein Kontakt zum Thema Informationssicherheit für die zentralen Akteure wie BfIS Land und SAX.CERT bekannt. Allerdings weisen die Zeitanteile für die Bediensteten, die mit der BfIS-Rolle betraut sind, und damit die Umsetzung der Anforderungen aus dem Gesetz zwischen den Behörden große Unterschiede auf. Das gilt auch für die 15 in § 7 Absatz 1 genannten besonders wichtigen Behörden, die einen hauptamtlichen BfIS zu ernennen haben, da hier manche staatlichen Stellen bereits vor über 10 Jahren professionelle Strukturen aufgebaut, andere hingegen erst mit Stellenbereitstellungen durch den Haushaltsgesetzgeber nach dem Jahr 2019 diese Rolle besetzt haben. Das letzte Ministerium konnte die Anforderung erst im Jahr 2023 umsetzen. Und auch die organisatorische Verortung differenziert stark. In den meisten Behörden ist der BfIS in der Organisations-Abteilung angesiedelt, dort zuweilen im für IT zuständigen Referat. Als zweithäufigste Variante wird die Verortung in Stabsstellen oder direkt im Leitungsbereich der Behörde benannt. Aus Sicht der Informationssicherheit ist diese Verortung angemessener zu bewerten, weil hier nicht die Abhängigkeit in der Linie und ggf. zu starke Eingebundenheit in die IT zum Tragen kommt, die der gesetzlich geforderten Weisungsfreiheit in der Praxis im Wege stehen kann.

Mit der unterschiedlichen Umsetzungsreife der Anforderungen aus dem Gesetz geht natürlich auch der Stand des ISMS einher. Was dabei auffällt: die zur Steuerung und Dokumentation für ein ISMS bestenfalls zu nutzende Software wird zumeist nur in den staatlichen Stellen eingesetzt, die einen hauptamtlichen Beauftragten eingesetzt haben. Grundsätzlich anders sieht es bei den staatlichen Stellen aus, deren BfIS nur nebenamtlich im Einsatz sind. Offenbar besteht für die meisten staatlichen Stellen kein Anreiz, eine ISMS-Software einzusetzen. Zwar wird die ISMS-Software eines Anbieters zentral durch den SID bereitgestellte, muss aber durch die Behörden selbst finanziert werden. Eine Pflicht zur Verwendung besteht daher nicht. Es wird geprüft, die Nutzung durch die Behörden kostenlos zu stellen, aber verpflichtend zu machen.

Die zahlreichen Rückmeldungen aus dem staatlichen Bereich zu fehlenden oder unzureichenden personellen und finanziellen Ressourcen können zwar nicht abschließend auf Plausibilität geprüft werden, allerdings spiegeln sie die bereits im Rahmen der Abstimmungen zum SächsISichG im Jahr 2019 als auch zur Änderung des SächsISichG im Jahr 2024 eingehenden Bedarfsmeldungen der Ressorts wider. Unzweifelhaft ist, dass der Aufbau der Informationssicherheitsorganisation in den meisten staatlichen Stellen noch nicht abgeschlossen ist und die Zuführung von personellen und finanziellen Ressourcen in den nächsten Jahren notwendig sein wird, um einen zufriedenstellenden Stand in der Informationssicherheit im Freistaat Sachsen zu erreichen.

3.1.4 Arbeitsgruppe Informationssicherheit

Nach dem Inkrafttreten des SächsISichG 2019 wurde der AG IS die Funktion des gesetzlich normierten Beratungsgremiums in der Informationssicherheit zugewiesen, vgl. § 10 SächsISichG.

Die AG IS berät den BfIS Land und empfiehlt Maßnahmen zur Sicherstellung angemessener Informationssicherheit in der Landesverwaltung. Ihr gehören BfIS Land als ihr Vorsitzender sowie die BfIS der SK und Staatsministerien, des Sächsischen Rechnungshofs, der Sächsischen Datenschutzbeauftragten, des Landespolizeipräsidiums, der LIT und des SID sowie zwei Vertreter der Kommunen als stimmberechtigte Mitglieder an. Als Mitglieder ohne Stimmrecht nehmen der Leiter des SAX.CERT, der IT- und Informationssicherheitsbeauftragte des Sächsischen Landtags sowie der Vorsitzende des AK SVN regelmäßig an den Sitzungen teil. Es gibt eine Geschäftsordnung. Die Sitzungen finden monatlich statt und werden inhaltlich und organisatorisch vom BfIS Land vorbereitet. Er leitet sie auch. Von ihm gehen in aller Regel zudem die grundsätzlichen Themen aus.

Zu den Aufgaben der AG IS gehört u. a., den BfIS Land zu Fragen der Informationssicherheit zu beraten und bei der Erstellung und Weiterentwicklung von ressortübergreifenden Mindeststandards zur Informationssicherheit zu unterstützen. Für die ressortübergreifende Zusammenarbeit beschließt die AG IS Empfehlungen für Maßnahmen und Standards zur Erreichung des angestrebten oder zur Erhöhung des Informationssicherheitsniveaus. Die von der AG IS getroffenen Empfehlungen werden dem LA ITEG zur Beschlussfassung vorgelegt.

Bereits im Jahr 2009 wurde die AG IS durch Beschluss des AK ITEG als das koordinierende Gremium für ressortübergreifende Aspekte der Informationssicherheit bestimmt. Die AG IS erarbeitete seit ihrer Gründung bis zum Inkrafttreten des SächsISichG 19 Entwürfe von Beschlussvorlagen, die im Anschluss dem AK ITEG zur Stellungnahme zugeleitet wurden. Unter Berücksichtigung der Stellungnahmen des AK ITEG wurden diese Beschlussvorlagen dem LA ITEG zur Entscheidung zugeleitet. Seit Inkrafttreten des SächsISichG brachte BfIS Land elf Mindeststandards als landesweite Richt- oder Leitlinien sowie das Identifizierungskonzept nach § 7 Absatz 4 SächsISichG zur Anhörung ins Gremium, die nach positivem Votum dem LA ITEG als Beschlussempfehlung zur finalen Entscheidung zugeleitet wurden. Weitere neun Beschlüsse, so zur Geschäftsordnung und zu operativen technischen Sicherungsmaßnahmen, fasste die AG IS in eigener Verantwortung. In Summe wurden damit 21 Beschlüsse seit Inkrafttreten des SächsISichG von der AG IS gefasst (siehe Abbildung 5).

Im Ergebnis der Umfrage wird die Zusammenarbeit als gut bewertet. Der in der Geschäftsordnung der AG formulierte monatliche Turnus der Sitzungen wird als bedarfsgerecht gesehen. Das Gremium bietet für die Ressorts ausreichend gute Möglichkeiten zur Mitarbeit bei der Erstellung von Mindeststandards und Beschlussvorlagen. Einzelne Mitglieder wünschen sich allerdings eine stärkere Einbindung auch in die Vorbereitung der Sitzungen, es solle mehr Raum für Diskussionen und fachlichen Austausch geben. Zudem wird angeregt, der AG IS mehr Kompetenz im Verhältnis zum LA ITEG zu übertragen. Bei erheblichen Sicherheitsvorfällen wird ein kontinuierlicher Informationsfluss über die Behebung gewünscht.

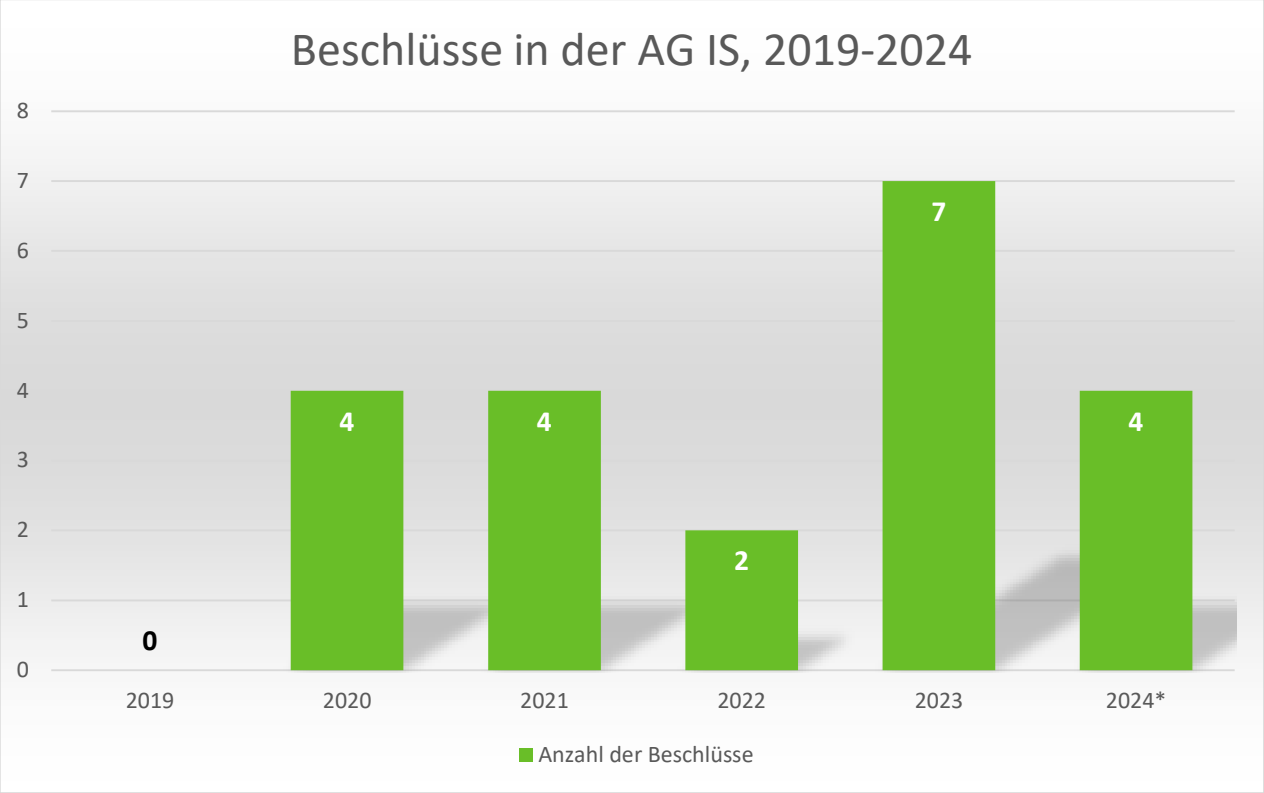

Abbildung 5 - Beschlüsse der AG IS seit Inkrafttreten des SächsISichG

Hinweis für das Jahr 2024*: Bei Redaktionsschluss lagen Daten bis einschließlich Oktober 2024 vor.

Bewertung

Allgemein wird die AG IS als wichtiger Bestandteil für die Fortschreibung und Entwicklung der Themen zur Umsetzung der Informationssicherheit im Freistaat Sachsen gesehen. Das gesteuerte einheitliche Vorgehen in der Landesverwaltung wird begrüßt, auch wenn die erarbeiteten Mindeststandards nicht immer allen AG IS-Mitglieder ausreichend tiefgehen. Allerdings erlaubt ein landesweiter Mindeststandard, dies dann in ressorteigenen Richtlinien noch weiter auszuführen und ggf. zu verschärfen.

Die Kommunen selbst sind von den Beschlussthemen häufig fachlich nicht betroffen. Die dahingehend erfolgte Änderung der Geschäftsordnung, dass die kommunalen Vertreter bei Themen, die nur die staatliche Ebene betrifft, nicht mitabstimmen, wird deshalb positiv bewertet. Allerdings wird die Ermöglichung der Teilnahme durch die kommunalen Vertreter als Informationsgewinnung gesehen, um die Kommunen über die behandelten Themen zu informieren und von Entwicklungen im staatlichen Bereich zu partizipieren.

Die im Berichtszeitraum erfolgte Einberufung von Unterarbeitsgruppen zur fachlichen Vorbereitung von Mindeststandards und technischen Sicherungsmaßnahmen wird begrüßt und als Mehrwert aufgefasst.

Es wird empfohlen zu prüfen, wie die fachliche Kompetenz der AG IS gestärkt werden kann. So könnten dem LA ITEG nur noch Vorhaben bzw. Regelungen von grundlegender Bedeutung zur Entscheidung vorgelegt werden.

3.1.5 Beauftragte für Informationssicherheit in den nicht-staatlichen Stellen

Wesentlicher Fokus in diesem Bereich liegt bei den Kommunen. Der Grad der Informationssicherheit ist hier besonders entscheidend, da die Kommunen die übergroße Zahl an staatlichen Leistungen an Bürger und Unternehmen aussteuern und ihr Funktionieren sowohl analog als auch digital dafür

unerlässlich ist. Zudem sind die Kommunen integraler Bestandteil des gemeinsamen Behördennetzes aus SVN und KDN und haben damit unter Umständen Einfluss auf die Sicherheit der technischen Infrastruktur.

Kommunen

Da die Kommunen wie jede nicht-staatliche Stelle gesetzlich verpflichtet sind, die Benennung eines BfIS zu melden, werden seit dem Jahr 2019 durch BfIS Land Daten über das Beteiligungsportal Sachsen erfasst. Demnach waren Stand 31. Juli 2024 in zwölf von 13 Landkreisen und kreisfreien Städten die BfIS-Stellen besetzt. Von den übrigen 415 Gemeinden hatten 243 einen BfIS benannt. 165 davon nutzen dabei die Möglichkeit, hierfür einen externen Bediensteten einzusetzen. Damit sind in rund 59 % der sächsischen Gemeinden bzw. Verwaltungsgemeinschaften BfIS ernannt.

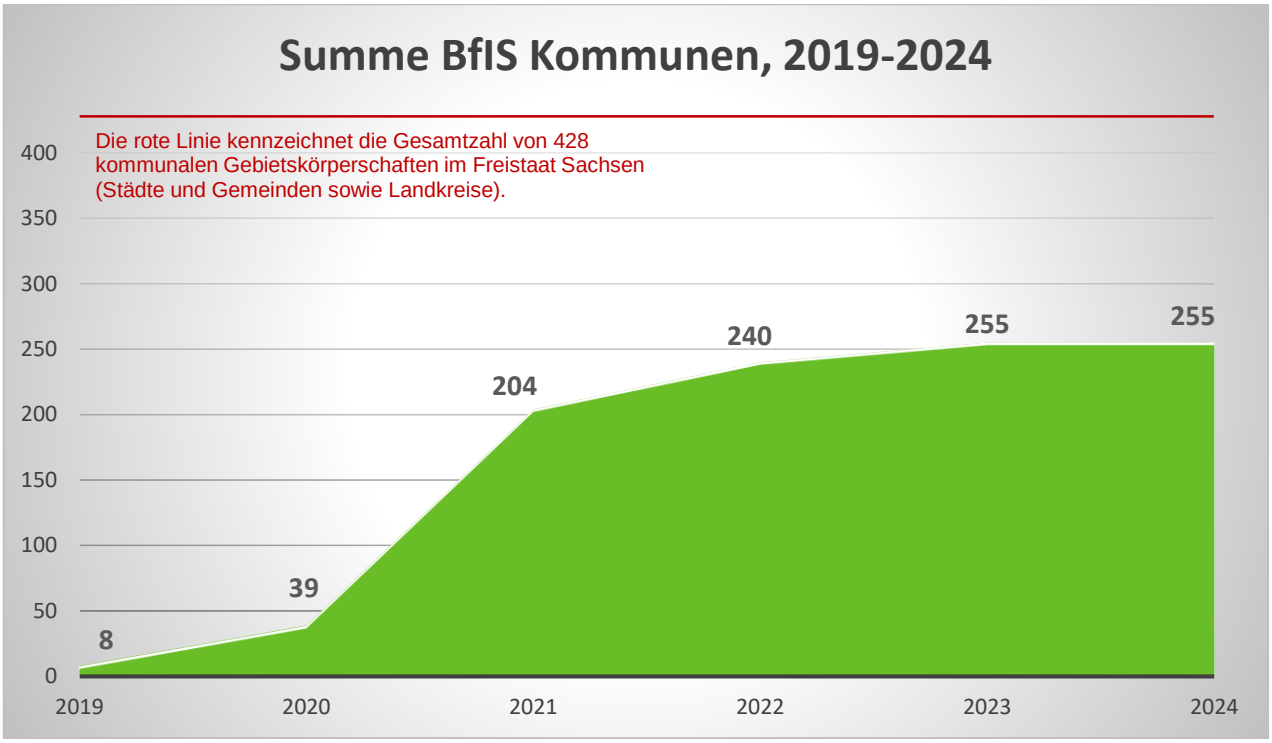

Abbildung 6 - Entwicklung der BfIS in sächsischen Kommunen

Der überwiegende Teil derjenigen Kommunen, die keinen BfIS ernannt haben, verfügt über weniger als 10.000 Einwohner. Insofern lässt sich festhalten, dass vor allem die kleineren Kommunen ihrer gesetzlichen Verpflichtung bislang nicht nachgekommen sind. Vor diesem Hintergrund ist es besonders beachtenswert, dass sich an der Evaluierung zur Hälfte kleine Kommunen mit unter 10.000 Einwohnern beteiligt haben. Quasi als Gegengewicht haben sich fast alle Landkreise und großen Städte in Sachsen an der Umfrage beteiligt, sodass die Rückmeldungen gut alle Größenstrukturen auf kommunaler Ebene repräsentieren.
Im Rahmen der Evaluierung geben 44 der 47 sich beteiligenden Kommunen an, dass in ihrer Behörde ein BfIS benannt ist. Dieser hohe Anteil spricht dafür, dass sich fast ausschließlich Kommunen an der Evaluierung beteiligt haben, die der gesetzlichen Pflicht einer Benennung eines BfIS nachkommen. Die Rückmeldungen geben daher wenig Aufschluss darüber, warum eine Kommune bislang keinen BfIS benannt hat.

Während in der offiziellen Meldung an den BfIS Land 67 % der kommunalen BfIS mit externen Bediensteten besetzt sind, liegt diese Quote in der Evaluierung bei 55 %. Der ihnen zugestandene Zeitanteil gemessen an einer Vollzeitstelle liegt in knapp 80 % der Kommunen dabei nur bei bis zu 0,1 VZÄ, also weniger als vier Stunden in der Woche. Nur sechs Kommunen melden zurück, dass sie einen hauptamtlichen BfIS mit 51 bis 100 % Stellenanteil im Einsatz haben. Bei diesen handelt es sich ausschließlich um Landkreise oder kreisfreie Städte. Das heißt im Umkehrschluss allerdings auch, dass selbst von den zwölf Rückmeldenden aus Landkreisen oder großen Städten über 50.000 Einwohner nur die Hälfte eine hauptamtliche Stelle für ihren BfIS geschaffen haben.

In fast allen Kommunen hat der BfIS ein unmittelbares Vorspracherecht bei der Verwaltungsleitung bzw. beim Bürgermeister und kann seine Aufgaben weisungsfrei ausüben. Allerdings variiert die organisatorische Verortung der BfIS stark: Einige sind direkt am Bürgermeister bzw. der

Behördenleitung oder Beigeordneten angebunden, andere in Hauptämtern, in der Inneren Verwaltung oder in einem IT-Referat verortet. In Dreiviertel der Kommunen wurde der Informationssicherheitsprozess bspw. durch Erstellung einer Informationssicherheitsleitlinie oder den Aufbau einer Informationssicherheitsorganisation initiiert, in etwa der Hälfte der Kommunen wird der BfIS durch ein Informationssicherheitsmanagement-Team unterstützt.

Entsprechend all dieser sehr unterschiedlichen Rahmenbedingungen gestalten sich die Tätigkeitsfelder des BfIS und der erreichte Stand des ISMS in der jeweiligen Verwaltung. In den Kommunen unter 10.000 Einwohnern wird das ISMS zumeist als im Ausbau oder nur rudimentär vorhanden beschrieben. Der BfIS hat zumeist beratende Funktion für die Leitung, koordiniert in einigen Fällen Schulungs- und Sensibilisierungsmaßnahmen und erstellt eigene Richtlinien zu bestimmten Themen der Informationssicherheit. Positiver wird der Stand des ISMS in Kommunen zwischen 10.000 und 50.000 Einwohnern eingeschätzt: Hier ist in den meisten Verwaltungen ein ISMS im Aufbau und es wird in vielen Fällen auch eine Software zur Steuerung des ISMS eingesetzt. Zu den am häufigsten genannten Tätigkeiten gehören auch hier die Erstellung von Sicherheitsrichtlinien, die Sensibilisierung der Bediensteten sowie die Durchführung von Schutzbedarfsanalysen. In den Kommunen über 50.000 Einwohnern und den Landkreisen sind die ISMS in der Regel deutlich weiterentwickelt, teilweise etabliert, zudem wird fast überall eine Software zur Steuerung des ISMS verwendet. Auch die Aufgaben sind weiter gefasst: Neben Beratung der Behördenleitung, Sensibilisierung der Bediensteten und Erstellung von Richtlinien werden als weitere Tätigkeiten die Durchführung interner Audits, der Aufbau eines IT-Notfallmanagements bis hin zu einem ganzheitlichen Business Continuity Management und der Planung von Notfallübungen genannt. Zudem beschäftigt man sich hier eingehender mit der Prävention und Detektion von Sicherheitsereignissen.

Für den Aufbau eines ISMS wird den Kommunen das Grundschutzkompendium des BSI gesetzlich nur zur Anwendung empfohlen. Gerade kleineren und mittelgroßen Kommunen fällt jedoch der Einstieg in den Aufbau eines ISMS schwer, wie sich aus der Befragung ergab. Um dies bundesweit zu erleichtern, hat das BSI im Jahr 2023 mit „Weg in die Basisabsicherung“ eine niederschwellige Methode als Alternative zum in der Praxis etablierten Standardvorgehen beim BSI-IT-Grundschutz entwickelt. Andere Länder unterstützen die Kommunen bei der Etablierung eines ISMS auf unterschiedliche Weise. Bayern[23] etwa bietet über das dortige Landesamt für Sicherheit in der Informationstechnik das Siegel „Kommunale IT-Sicherheit“ an, welches auf Grundlage eines landeseigenen Fragebogens gerade kleineren Kommunen den Nachweis des sicheren IT-Betriebs ermöglicht. Sachsen-Anhalt [24] startete gemeinsam mit dem BSI das IT-Sicherheitsprojekt für Kommunen und stellt für Pilotkommunen entsprechende Mittel für „Weg in die Basisabsicherung“ bereit. Auch Baden-Württemberg[25] unterstützt mit der Cybersicherheitsagentur Baden-Württemberg massiv und baut ein eigenes Beratungsangebot für Kommunen auf.

40 % der Kommunen melden zurück, dass sie sich regelmäßig mit BfIS anderer Kommunen austauschen. Da den BfIS in den Kommunen wenig Zeitanteile für ihre Arbeit zur Verfügung stehen, und auch nur in jeder zweiten Kommune eine Informationssicherheitsorganisation wie ein ISMS-Team wirkt, liegt im Austausch großes Potenzial zur Verbesserung der inhaltlichen Qualität. So richtet BfIS Land seit knapp zwei Jahren an fast jedem ersten Freitag im Monat eine Online-Sprechstunde zur Informationssicherheit in den Kommunen aus. Diese Veranstaltung dient dazu, aktuelle Themen der Informationssicherheit und die Dienstleistungen des SAX.CERT näher zu erläutern sowie Fragen und Bedarfe der Kommunen aufzunehmen. Darüber hinaus soll die Sprechstunde den Verantwortlichen aus den Kommunen, die häufig als Einzelakteur in ihren jeweiligen Behörden agieren, die Möglichkeit geben, sich untereinander zu vernetzen und ggf. von bereits vorhandenen Erfahrungen oder konkreten Hilfestellungen anderer zu profitieren. Die BfIS der Landkreise treffen sich zudem regelmäßig in einer eigenen AG IS zusammen mit den drei großen kreisfreien Städten.

[23] https://www.lsi.bayern.de/kommunen/siegel_kommunale_it_sicherheit/index.html (zuletzt abgerufen am 05.11.2024)
[24] https://mid.sachsen-anhalt.de/fileadmin/tsa_rssinclude/ministerium-fuer-infrastruktur-und-digitales_26_10_2024_pressemitteilung_sachsen-anhalt-startet-pilotprojekt-zur-erhoehung-der-it-und-informationssicherheit-in-den-kommunen.pdf (zuletzt abgerufen am 05.11.2024)
[25] https://www.cybersicherheit-bw.de/beratungsangebote-fuer-kommunen (zuletzt abgerufen am 05.11.2024)

Zum Austausch gehört auch die Integration der Kommunen bei der Meldung von Sicherheitsvorfällen: So geben knapp 70 % an, einen Prozess zur Meldung an das SAX.CERT etabliert zu haben. Ein Viertel hätte davon auch schon Gebrauch gemacht (Details zum Meldeprozess siehe Kapitel 3.3).

Bis auf vier Kommunen geben alle an, das KDN zur Kommunikation mit anderen Behörden zu nutzen. Die Zahl der an das KDN angeschlossenen Rechner variiert dabei naturgemäß sehr stark von 1 bis 10.000, allerdings geben die meisten Kommunen doch Zahlenwerte an, die darauf schließen lassen, dass sie mit einer großen Zahl ihrer Rechner an das KDN angeschlossen sind und nicht nur einige wenige Rechner für den Anschluss an das übergreifende Behördennetz vorhalten. Das kann so interpretiert werden, dass der komplette Anschluss an das KDN von Kommunen, anders als oft vorgetragen, sowohl finanzierbar ist, als auch keine Einschränkungen in der Bandbreite der Anschlüsse für die Arbeitsweise von Behörden bedeuten muss. Da das KDN im Verbund mit dem SVN als sächsisches Behördennetz an den zentralen Übergängen zum Internet eine weite Bandbreite hochqualitativer Schutzsysteme enthält, ist es unsere Auffassung, dass die Kommunen möglichst ganzheitlich an das KDN angeschlossen gehören.

Wie bei den staatlichen Stellen geben auch 90 % der Kommunen an, dass ihnen bei der Erfüllung der mit dem Gesetz einhergehenden Aufgaben seit August 2019 Personal- und/oder Sachaufwände entstanden sind. Immerhin knapp ein Viertel beziffert hierzu auch die Aufwände konkret. Elf Kommunen beziffern ihren jährlichen Personalaufwand zwischen 1.300 und 12.000 Euro, wobei die Summe von rund 5.000 Euro am häufigsten genannt wird. Beim jährlichen Sachaufwand liegt die Spannbreite deutlich höher und zwar zwischen 3.000 und 50.000 Euro, wobei Summen bis 5.000 Euro eher den Normalfall darstellen.

Nur gut 40 % der sich an der Evaluierung beteiligenden Kommunen beantworteten die Frage zu etwaigen Anpassungsbedarfen zum SächsISichG bzw. aus ihrer Sicht erforderlichen weiteren Maßnahmen, um die Informationssicherheit zu verbessern. Vorgeschlagen werden u. a.:

- Zentralisierung der Zuständigkeiten für die Informationssicherheit in den Kommunen in der Rolle des BfIS auf Ebene der Landkreise.
- Bereitstellung einer Standard-Software für die Steuerung des ISMS
- Vorgaben bzw. Empfehlungen zum Personalaufwand zur Erfüllung der BfIS-Aufgaben in Relation zur Größe der Kommune, die Aufgabe des BfIS wird zu häufig in Personalunion mit anderen Zuständigkeiten erledigt, es fehlen Fachwissen und Erfahrung
- ein durch das Land finanziertes/gefördertes Mindestlevel an IT-Sicherheitsanforderungen
- Verbesserung der kommunalen Finanzausstattung, um personelle Ressourcen zu stärken
- mehr Informationen, Beispielunterlagen, nachnutzbare Inhalte vom Land
- die Umsetzung von Informationssicherheit in den Schulen durch den Schulträger ist gar nicht oder nur sehr eingeschränkt umsetzbar, es braucht eine andere gesetzliche Zuschreibung der Zuständigkeiten

Hochschulen

Alle der an der Umfrage teilgenommenen Hochschulen haben einen BfIS ernannt. Insgesamt wurden seit Inkrafttreten des Gesetzes BfIS-Ernennungen von 16 Universitäten und Hochschulen angezeigt. Kritisch zu sehen ist, dass bei fünf der sieben meldenden Hochschulen keine Vertreter-Rolle benannt ist und nur drei von sieben ihren BfIS hauptamtlich beschäftigen. So sehen eine Universität und eine große Hochschule nur 0,1 VZÄ für diese Rolle vor. Positiv zu bewerten ist, dass alle BfIS weisungsfrei arbeiten, direkt der Hochschulleitung berichten können und überall der Informationssicherheitsprozess initiiert ist. Hingegen ist in nur drei Hochschulen ein ISMS-Team etabliert. Die Mehrzahl der BfIS an den Hochschulen tauscht sich regelmäßig mit Kollegen anderer Hochschulen aus, auch ist in den meisten Hochschulen ein Prozess zur Meldung von erheblichen Sicherheitsvorfällen an das SAX.CERT etabliert. Nur zwei Hochschulen geben an, an das SVN angeschlossen zu sein, in beiden Fällen mit lediglich zwei oder weniger Rechnern.

Alle Hochschulen geben an, dass ihnen bei der Erfüllung der mit dem Gesetz einhergehenden Aufgaben seit August 2019 Personal- und/oder Sachaufwände entstanden sind. Beim Personalaufwand werden von drei Hochschulen Aufwände zwischen 20.000 und 90.000 Euro beziffert, beim jährlichen Sachaufwand werden Werte zwischen 10.000 und knapp 60.000 Euro benannt. In diesem Zusammenhang melden einige Hochschulen im Rahmen der Befragung auch zurück, dass die Aufgaben aus dem SächsISichG bislang nicht durch die Zuführung von Personal oder Finanzen unterstützt worden sind. So würde die notwendige Arbeit im Wesentlichen durch das vorhandene IT-Personal nebenbei, aber durchaus gewissenhaft erbracht, was zu Lasten anderer Projekte ginge. Zudem seien die Angebote des SAX.CERT für Hochschulen teilweise nicht nutzbar, weil diese nicht Teil des SVN sind.

Die Informationssicherheit der Hochschulen hat sich im Evaluierungszeitraum als angreifbar gezeigt: Die Sicherheitsvorfälle an der Westsächsischen Hochschule Zwickau und an der TU Bergakademie Freiberg im Jahreswechsel 2022/2023 gehörten zu den Fällen mit den erheblichsten Auswirkungen auf das Funktionieren der Geschäftsprozesse. Folgerichtig hat sich das Sächsische Staatsministerium für Wissenschaft, Kultur und Tourismus (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. Mit dem Änderungsgesetz zum Sächsischen Informationsgesetz sind die Hochschulen nun seit dem 1. Oktober 2024 verpflichtet, erhebliche Sicherheitsvorfälle zu melden. Bis zu diesem Zeitpunkt erfolgte eine Meldung auf freiwilliger Basis.

Weitere Träger der Selbstverwaltung

Im Rahmen der Evaluierung geben fünf der zehn sich beteiligenden Einrichtungen an, einen BfIS benannt zu haben. Dem BfIS Land gegenüber wurden seit Inkrafttreten des Gesetzes insgesamt 10 BfIS-Ernennung von Trägern der Selbstverwaltung angezeigt. Da BfIS Land seinen Fokus auf die Sicherheit des Behördennetzes und der angeschlossenen Behörden von Staatsverwaltung sowie Hochschulen und Kommunen gelegt hat, ist hier die Datenbasis am dünnsten und die Quote im Vergleich zur Zahl aller existierenden weiteren Träger der Selbstverwaltung sicherlich am geringsten. Insofern stellen die Rückmeldungen insgesamt kein aussagekräftiges Bild dar und werden daher auch nicht weiter betrachtet.

Bewertung

Fünf Jahre nach Inkrafttreten des SächsISichG sind in rund 59 % der sächsischen Gemeinden bzw. Verwaltungsgemeinschaften BfIS ernannt. Dieser Aufwuchs von ca. 20% vor Inkrafttreten des Gesetzes geht auf vielfältige Aktivitäten von BfIS Land im Zusammenwirken mit Akteuren auf der kommunalen Ebene wie den Spitzenverbänden SSG und SLKT zurück: So wurde nicht nur über kommunale Publikationen und elektronische Rundschreiben auf die Pflicht zur Benennung eines BfIS aufmerksam gemacht, sondern parallel dazu ein Unterstützungsnetzwerk mit technischen Serviceleistungen des SAX.CERT und kostenfreien Schulungsangeboten des BfIS Land sowie regelmäßigen Netzwerktreffen aufgebaut, um den Mehrwert an dieser gesetzlichen Verpflichtung zu verdeutlichen. Herausforderung für die Zukunft ist, die Zahl der Kommunen mit einem BfIS weiter zu erhöhen. Die Zeitanteile, die den Bediensteten für die Rolle des BfIS zugestanden werden, sind allerdings überwiegend unzureichend. Dass nicht einmal in den Verwaltungen der zehn Landkreise und der drei kreisfreien Städte alle BfIS mit hauptamtlichen Stellen und durch interne Bedienstete besetzt sind, wird als ungenügend bewertet. Zumindest in Kommunen dieser Größenordnung sind professionelle Informationssicherheitsorganisationen aufzubauen, das zeigen die enormen Auswirkungen von Sicherheitsvorfällen wie in der Vergangenheit im Landkreis Anhalt-Bitterfeld oder im Rhein-Pfalz-Kreis. Hier ist die kommunale Selbstverantwortung gefordert. Dies gilt neben organisatorischen auch für angemessene technische Maßnahmen. Es sollte unbedingtes Ziel sein, die Kommunen mit ihrer gesamten IT an das KDN anzuschließen und damit das Schutzniveau für alle IT-Komponenten zu stärken. Zudem wird es den großen Kommunen angeraten, erweiterte Angriffserkennungssysteme zum Schutz des eigenen Behördennetzes zu implementieren. Das SächsISichG bietet seit dem Jahr 2019 dazu die rechtliche Grundlage, die jedoch kaum in Anspruch genommen wird.

Aus Sicht der Staatsregierung wird der „Weg in die Basisabsicherung“ vor allem für kleinere Kommunen als sinnvoll dafür erachtet, den Aufbau eines ISMS vorzubereiten und das Thema Informationssicherheit in der Verwaltung sichtbar zu machen. Daher werden Initiativen wie der Digitallotsen Sachsen, den „Weg in die Basisabsicherung“ in den Kommunen zu etablieren, ausdrücklich befürwortet.

Der Bereich der Hochschulen hat im Evaluierungszeitraum erfahren müssen, welche gravierenden Einschnitte in den Betrieb von Forschung und Lehre Sicherheitsvorfälle haben können. Darauf haben Hochschulen und SMWK angemessen reagiert. Durch die Implementierung eines einheitlichen erweiterten Angriffserkennungssystems und ein die Hochschulen umfassendes Melderegime im Geschäftsbereich des SMWK wurden die Sicherheitsstrukturen deutlich professionalisiert. Mit der Änderung des SächsISichG zum 1. Oktober 2024 sind erhebliche Sicherheitsvorfälle nun auch verbindlich meldepflichtig und damit Teil des Lagebildes.

3.2 Auswirkungen des Gesetzes auf Informationssicherheitsmaßnahmen

Aus den Ergebnissen der Befragung lässt sich eine zumindest teilweise Implementierung der im SächsISichG vorgegebenen Maßnahmen zur Sicherstellung der Informationssicherheit bei den staatlichen und nicht-staatlichen Stellen ablesen. Dass es Defizite in der Umsetzung gibt, liegt eher an den Rahmenbedingungen, unter denen diese agieren müssen, als an den Inhalten des Gesetzes. Hinzu kommt, dass die für die Umsetzung von angemessenen organisatorischen und technischen Maßnahmen für die Informationssicherheit relevanten Bestimmungen bereits länger als das SächsISichG bestehen. Aus der Online-Befragung lässt sich daher nicht unmittelbar ableiten, dass das SächsISichG bei den Informationssicherheitsmaßnahmen eine direkte Anschubwirkung hatte. Mit der Schaffung von Befugnisnormen nach §§ 12, 13 SächsISichG wurden allerdings bestehende Rechtsunsicherheiten bei Datenverarbeitungen geschlossen und damit ein rechtskonformer Betrieb von Cybereinbruchserkennungs- (Intrusion Detection-) und SIEM-Systemen ermöglicht.

3.2.1 Umsetzung angemessener technischer Maßnahmen

Bereits vor Erlass des SächsISichG wurden die staatlichen und nicht-staatlichen Stellen zu angemessenen organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen zur Gewährleistung der Informationssicherheit verpflichtet, vgl. § 9 Absatz 2 SächsEGovG. Die in § 4 Absatz 1 SächsISichG im Wesentlichen übernommene Regelungen schreibt die Gewährleistung eines angemessenen Informationssicherheitsniveaus für die in der sächsischen Verwaltung eingesetzten informationstechnischen Systemen vor. Dabei statuiert die Norm grundlegende Verpflichtungen an die staatlichen und nicht-staatlichen Stellen, damit Angriffe, die die Vertraulichkeit, Integrität und Verfügbarkeit für die in ihren informationstechnischen Systemen verarbeiteten Daten beeinträchtigen, abgewehrt werden. Für technische Maßnahmen soll der Stand der Technik maßgeblich sein.

Als Stand der Technik ist ein Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen zu verstehen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, gegen die Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind einschlägige internationale und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der informationstechnischen Systeme gewährleisten, das dem bestehenden Risiko angemessen ist.

Die erforderlichen Maßnahmen stehen unter dem Angemessenheitsvorbehalt. Hierbei ist der für die staatlichen Stellen erforderliche Aufwand zu berücksichtigen. Im Rahmen der Prüfung der Angemessenheit sind Art und Ausmaß des Risikos, die Wahrscheinlichkeit des Risikoeintritts und

die Kosten der Risikovermeidung abzuwägen und zu dokumentieren. Angemessen sind die Sicherheitsmaßnahmen dann, wenn deren Schutzwirkung in einem adäquaten Verhältnis zu dem Aufwand steht, den sie verursachen. Dabei sind die Schutzbedürftigkeit der Daten und das eventuelle Gefährdungspotenzial zu berücksichtigen. Zu bewerten sind in der Regel die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigungen des Ansehens der Verwaltung und die Folgen von Gesetzesverstößen.

Angemessene zentrale technische Maßnahmen zur Gewährleistung der Informationssicherheit werden durch den Landes-IT-Dienstleister und durch den von diesem beauftragten Betreiber des Verwaltungsnetzes zentral umgesetzt und an den jeweiligen Stand der Technik fortlaufend angepasst. Im Rahmen der Onlinebefragung gaben insgesamt 48 Behörden und Einrichtung an, zusätzliche, eigene Angriffserkennungssysteme und damit eigene technische Maßnahmen einzusetzen.

Die zentralen Angriffserkennungssysteme wehren bereits im Bereich E-Mail-Verkehr und Internetverkehr einen Großteil der Eindringversuche ab. Der E-Mailverkehr wird in einer Kaskade verschiedener Virenscanner mit unterschiedlichen Technologien auf enthaltene Schadsoftware geprüft. Der Internetverkehr wird ähnlich behandelt und erkannte Schadsoftware blockiert. Die beiden folgenden Grafiken zeigen die Entwicklung der erkannten Schadsoftware. Jedoch muss auch festgestellt werden, dass gerade im Internetverkehr die Kommunikation mittlerweile regelmäßig Ende zu Ende verschlüsselt übertragen wird. Dies erschwert die Prüfung auf Schadsoftware am Netzübergang zum Internet.

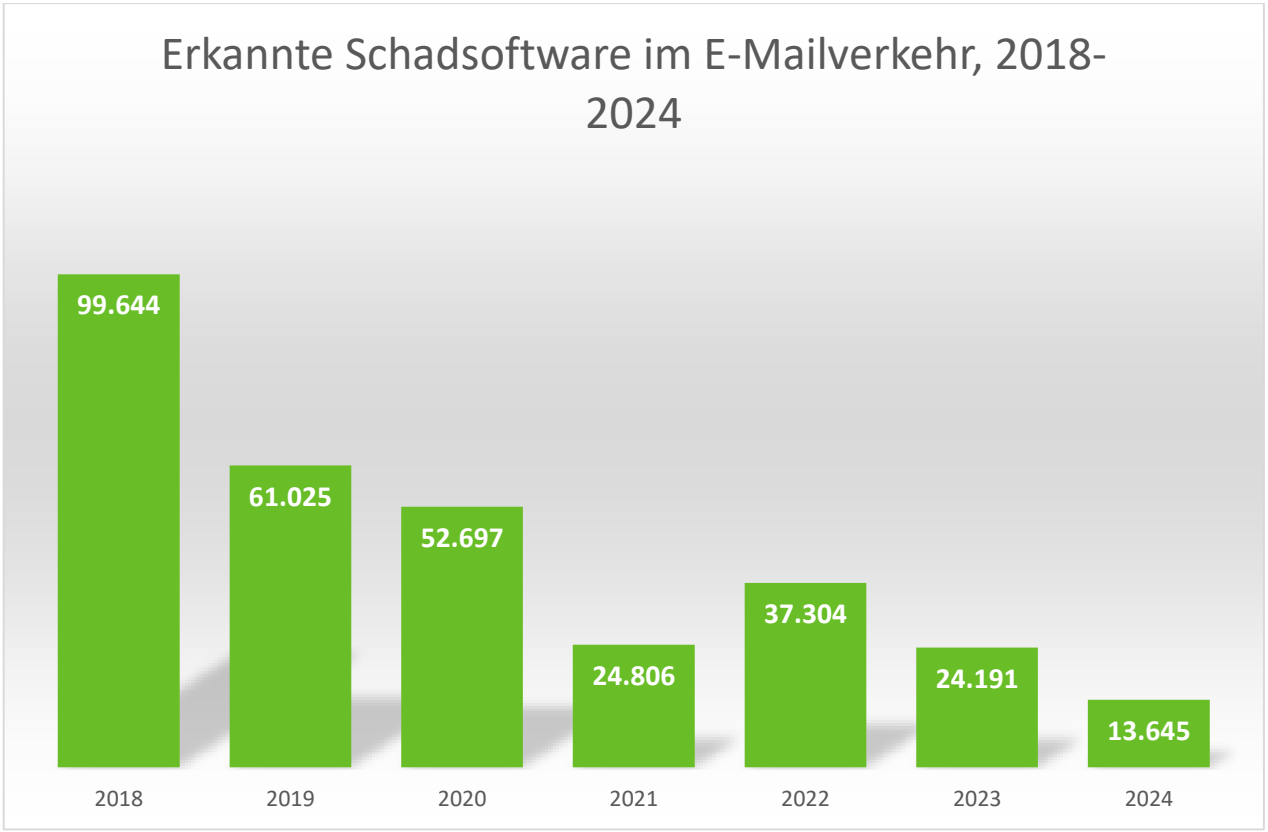

Abbildung 7 - Schadsoftware im E-Mailverkehr des SVN

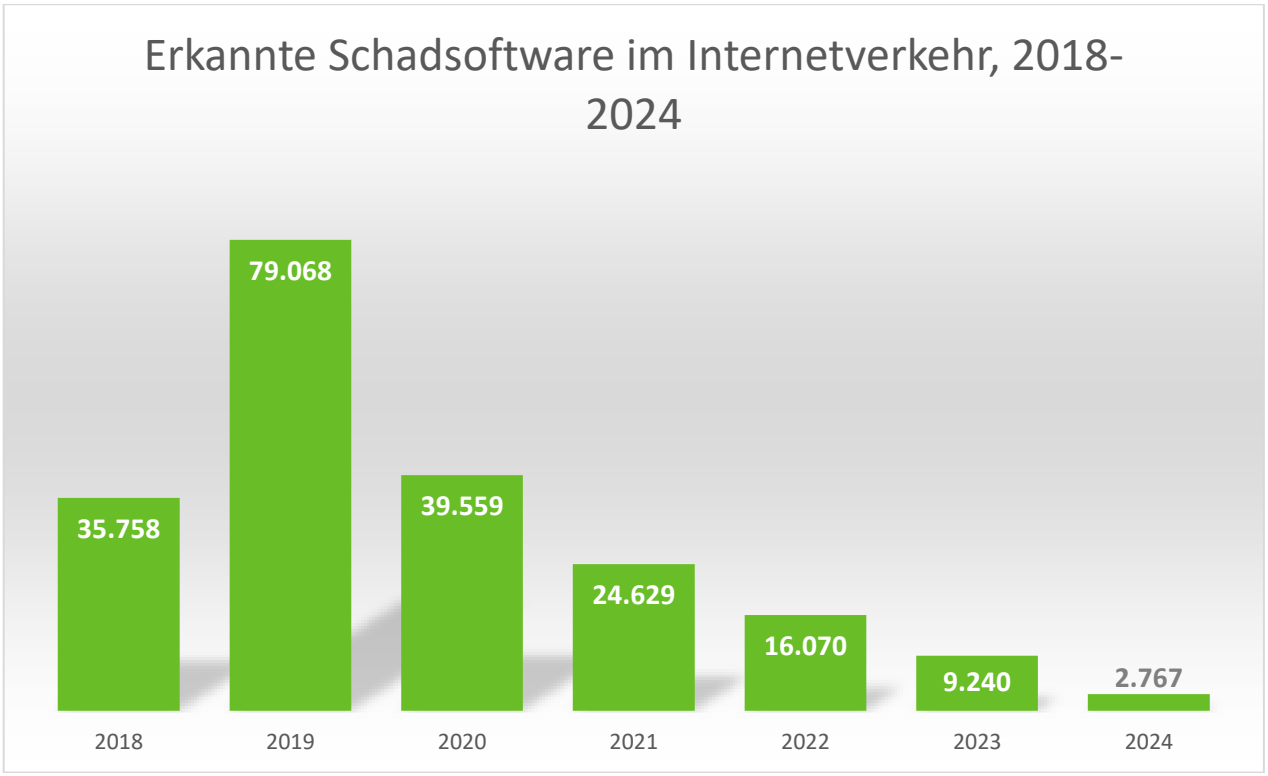

Abbildung 8 - Schadsoftware im Internetverkehr des SVN

Die folgende Grafik gibt die Behandlung des eingehenden und ausgehenden E-Mailverkehrs seit dem Jahr 2018 im SVN wieder. Die Anzahl der abgewiesenen E-Mails aufgrund verschiedener Schutzsysteme wie bspw. die Überprüfung von Realtime Blocklisten übertraf im Berichtszeitraum zu jedem Zeitpunkt die Anzahl der erwünschten/angenommenen E-Mails. Zum 1. November 2022 wurde darüber hinaus mit der Link-Reputation ein zusätzliches Schutzsystem im SVN eingeführt. Hier werden alle E-Mails aus dem Internet auf schadhafte Links überprüft.

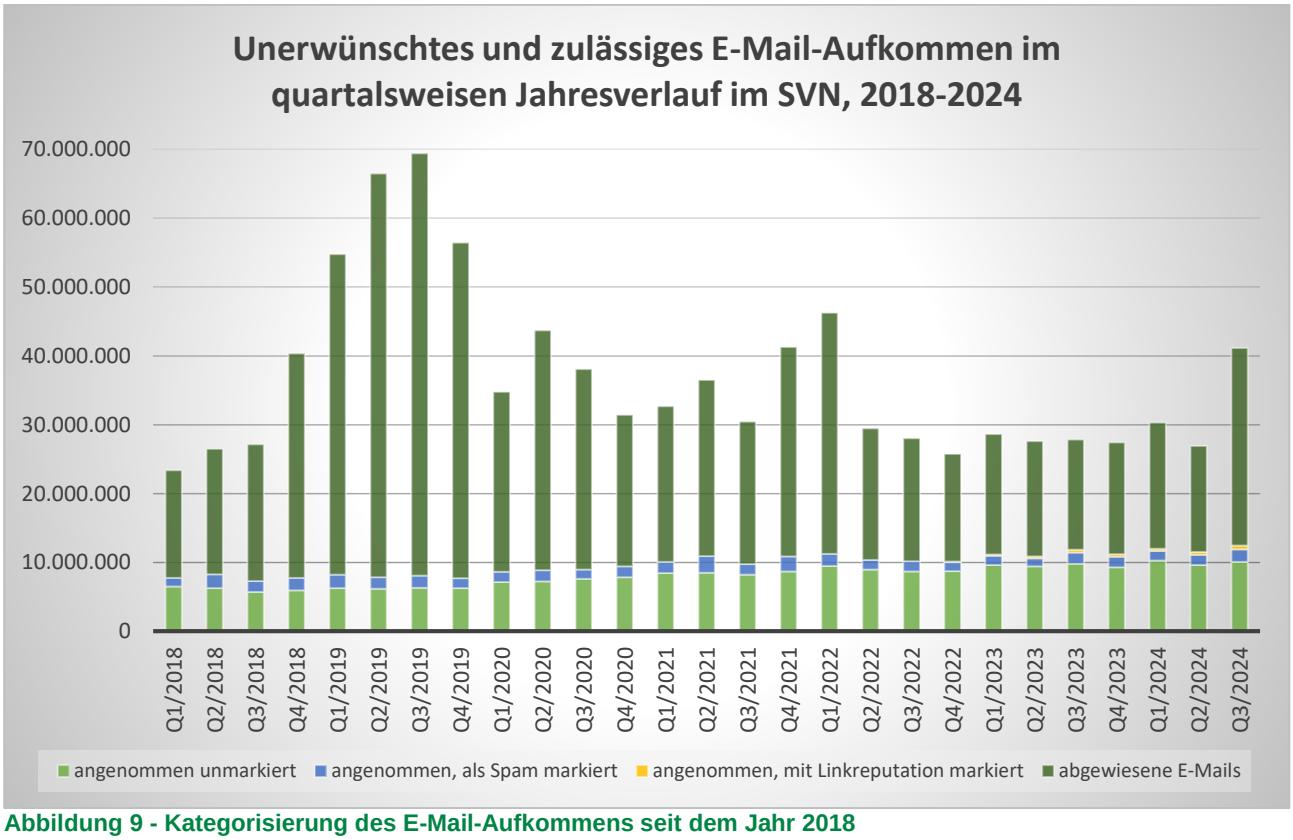

Abbildung 9 - Kategorisierung des E-Mail-Aufkommens seit dem Jahr 2018

Ergänzend zu den Schadcodescannern wurde im Jahr 2021 ein SIEM eingeführt. Dieses System dient dazu, fortlaufend Ereignisse von zentralen Kernkomponenten des Netzes zu korrelieren, auf Anomalien zu prüfen und auf mögliche Sicherheitsvorkommnisse zu bewerten.

In den Evaluierungszeitraum fällt auch die Corona-Pandemie mit einer technologischen, eruptiven Entwicklung für die staatlichen und nicht-staatlichen Stellen. Mit der kurzfristigen und massiven Einführung von Homeoffice-Arbeitsplätzen waren entsprechende Technologien für einen Zugang zum SVN/KDN zu schaffen. Neue bzw. intensiver genutzte Zugänge zum SVN boten neue Angriffsvektoren und gefährdeten die Sicherheit des SVN/KDN. Die Zugänge mussten entsprechend sicher ausgestaltet werden. So wurde ein Webinterface für den Mailzugang im SVN eröffnet, welches mit einem zweiten Authentifizierungsfaktor abgesichert wurde. Darüber hinaus wurde mittels VPN-Lösungen eine sichere, verschlüsselte und direkte Kommunikation zwischen Homeoffice und SVN möglich.

Im Zuge der neuen Arbeitsformen wurden auch die Schnittstellen des SVN/KDN zum Internet stärker in den Fokus genommen. So wurden Schnittstellen mit veralteten, fehlerbehafteten Protokollen außer Betrieb gesetzt. Alle anderen Schnittstellen wurden durch einen zusätzlichen Faktor zu Nutzernamen und Passwort abgesichert.

Zu den technischen Maßnahmen gehören darüber hinaus fortwährend Anpassungen in der Sicherheitsarchitektur, wenn dies neue Angriffsvektoren erforderlich machen. So war erkennbar, dass es seit Mitte der 2010er Jahre weltweit zu erfolgreichen und schwerwiegenden Angriffen mit ähnlichen Angriffsvektoren kam. Aus den Erkenntnissen dieser Angriffe wurden auch Rückschlüsse auf die Sicherheitsarchitektur des SVN/KDN gezogen. Die Systeme wurden mit dem Ziel gehärtet, selbst bei erfolgreichem Eindringen eines Angreifers in das SVN/KDN die Erlangung administrativer Rechte erheblich zu erschweren.

Bewertung

Die immer fortschreitende Digitalisierung bringt kontinuierlich Herausforderungen für angemessene technische Maßnahmen zur Gewährleistung der Informationssicherheit mit sich. Zudem führt die zunehmende Vernetzung von Geräten und Systemen zu immer komplexeren IT-Systemen mit einer Vielzahl an unterschiedlicher Hardware und Software. Das BSI weist in seinem Jahresbericht 2023 darauf hin, dass in dem Berichtszeitraum täglich durchschnittlich 68 neue Schwachstellen bekannt wurden, rund 24 % mehr als im vorangegangen Berichtszeitraum.[26] 53 % der dem BSI bekannt gewordenen Schwachstellen wiesen eine hohe oder kritische Bewertung auf.[27] Es ist davon auszugehen, dass derartige Hard- und Software auch um SVN/KDN in Betrieb ist und eine reale Gefährdung für das SVN/KDN darstellen.

Hinzu kommen neue Technologien sowohl für den Dienstbetrieb als auch für Angreifer, wie z. B. künstliche Intelligenz (KI) und maschinelles Lernen. Die mit KI verbundenen Nutzungsrisiken sind insbesondere bei cloudbasierten KI-Tools noch nicht klar und müssen bei Einführung entsprechender Verfahren bewertet werden. Aber auch die Nutzung bereits länger verfügbarer Technologien, wie die Ende-zu-Ende-Verschlüsselung im Internetverkehr, neue Infrastrukturbestandteile wie z. B. Cloud-Lösungen oder neue Arbeitsformen wie Mobiles Arbeiten (Homeoffice), und die damit verbundenen Risiken gilt es, bei einer Einführung zu bewerten und dem Stand der Technik entsprechende Maßnahmen zur Risikominderung umzusetzen.

Die Sicherheitsarchitektur sowie die technologischen Lösungen zur Sicherung des SVN sind folglich kontinuierlich weiter zu entwickeln, soll der aktuelle Stand der Technik erhalten bleiben.

Die Expertenbefragung der BfIS in den Behörden kommt zu ähnlichen Einschätzungen. Insbesondere der Weg in die Cloud und die Anwendung von KI-Lösungen stellen die Informationssicherheit vor neue Herausforderungen.

[26] Bundesamt für Sicherheit in der Informationstechnik - Die Lage der IT-Sicherheit in Deutschland 2023, S. 11
[27] Ebenda, S. 34

Die ursprüngliche Regelung aus dem SächsEGovG wurde in das SächsISichG übernommen. Die Evaluierung zeigt, dass es richtig war, in § 4 Absatz 1 SächsISichG angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zur Gewährleistung der Informationssicherheit als Vorgaben festzulegen und diese um die Forderung zu ergänzen, den jeweilig aktuellen Stand der Technik zu berücksichtigen. Damit wurde bereits seit 2019 ein hohes Qualitätsniveau angestrebt, welches nun auch ein zentraler Bestandteil der Anforderungen aus der NIS-2-Richtlinie ist.

3.2.2 Sensibilisierungen und Schulungen zur Informationssicherheit

Das SächsISichG schreibt in § 5 Absatz 1 dem BfIS Land die Aufgabe zu, landesweite Sensibilisierungs- und Schulungsmaßnahmen zu initiieren und zu koordinieren. Gemäß dieser Anforderung organisierte BfIS Land auch in den Jahren ab 2019 die bereits in den Vorjahren regelmäßig ausgerichtete Großveranstaltung INFOSIC mit den sogenannten „Live-Hackings“, die sich ausdrücklich an alle Bediensteten von Landes- und Kommunalbehörden richteten. Dabei geht es einerseits darum, vor Gefahren bei der alltäglichen Nutzung von PC, Smartphone und Internet zu sensibilisieren und andererseits Kompetenzen zur Gefahrenabwehr zu vermitteln.

Die Veranstaltungen der INFOSIC 2019 in großen Veranstaltungsräumen wie Hörsälen in Leipzig und Chemnitz und dem Dresdner Rundkino waren wie in den Vorjahren sehr nachgefragt. Zu den kostenlos angebotenen Live-Hacking-Veranstaltungen kamen insgesamt über 2.900 Teilnehmer und damit gut 600 mehr als im Vorjahr. Auf die Landesbehörden entfielen knapp 2.000 Teilnehmer, auf die Kommunen gut 700 und 200 auf sonstige nicht-staatliche Stellen.

Die Corona-Pandemie bedeutete in den Folgejahren nicht nur für die IT-Systeme einen Stresstest, sondern hat auch die Sensibilisierung und Fortbildung der Bediensteten erschwert. Ein bis auf den letzten Platz gefülltes Rundkino mit seinen knapp 900 Sitzen oder gar über 1.200 Teilnehmer im Kulturpalast Dresden waren nun nicht mehr möglich. Daher hat BfIS Land im Zusammenwirken mit seinen Kolleginnen und Kollegen in den Verwaltungen auf Landesebene und in den Kommunen die Werbung für das seit dem Jahr 2018 noch in kleinem Rahmen an der Hochschule Meißen (FH) und Fortbildungszentrum angebotene E-Learning-Angebot zur „Informationssicherheit am Arbeitsplatz“ massiv verstärkt.

Abbildung 10 - Werbematerialien zum E-Learning "Informationssicherheit am Arbeitsplatz"

Das E-Learning-Modul wurde mit einem verpflichtenden Teilnahmeschein und einem freiwilligen Online-Test für den Sächsischen Informationssicherheits-Schein versehen und im Oktober 2019 auf eine leistungsstarke Plattform im SID mit erweiterten Funktionalitäten (Selbstregistrierung der Teilnehmer, Erweiterung der Kapazität auf 5.000 gleichzeitige Nutzer) überführt. Bis Oktober 2024 haben auf dieser Plattform fast 31.000 Nutzerinnen und Nutzer die Teilnahmebescheinigung erworben und knapp 26.000 Nutzerinnen und Nutzer den Online-Test zum Sächsischen Informationssicherheits-Schein erfolgreich absolviert. Betrachtet man die Verteilung der Teilnehmenden auf die Behörden im Freistaat, so weisen die Behörden der Staatsverwaltung gut 3.000 Teilnehmer mehr auf als die Kommunen. Bei den Absolventen des Online-Tests liegen die Kommunen leicht vorne.

Nach Planungen des BfIS Land soll das derzeitige E-Learning-Angebot mit Beginn des Jahres 2025 von neuen Inhalten abgelöst werden. Neben dem Modul für alle Bediensteten soll es dann zusätzlich auch ein Modul für die Behördenleitungen geben, da ihnen nach Änderung des SächsISichG aufgrund der Anforderungen aus der NIS-2-Richtlinie eine besondere Verantwortung zukommt (siehe § 4 Absatz 3 Satz 3 SächsISichG). Im Laufe des kommenden Jahres soll zudem als drittes Modul ein E-Learning für Bedienstete mit Aufgaben im IT-Bereich angeboten werden.

Bei den Großveranstaltungen zur INFOSIC ist ebenso geplant, die Angebote wieder auszubauen. Nach der Corona-Pandemie fanden erste Einzelveranstaltungen, z. B. im Rahmen des IT-Sicherheitstags Sachsen im Jahr 2022 sowie im Rahmen der Roadshow Cybersicherheit unter dem Motto „Digital? Aber sicher!“ im Jahr 2023 auch für Bedienstete statt, die einige hundert Teilnehmer aus der Verwaltung erreichten. Im Jahr 2024 wurden dann erstmals wieder die klassischen INFOSIC-Veranstaltungen angeboten, mit gut 1.600 Teilnehmern in Leipzig und Dresden. Diese Veranstaltungen werden nach wie vor gut angenommen und von den Teilnehmern positiv bewertet, was auch daran liegt, dass die staatlichen Behörden solche Live-Hackings nur in den seltensten Fällen für ihre Bediensteten selber organisieren.

Um die staatlichen Behörden in ihren Bemühungen zu unterstützen, wurde im Jahr 2022 ein zentraler Rahmenvertrag für die gesamte Staatsverwaltung geschlossen, der u. a. auch Angebote zu Schulungen und Sensibilisierungen beinhaltet. Damit sind nunmehr alle Behörden in der Lage, dies vergleichsweise aufwandsarm in eigener Verantwortung abzurufen. Zudem wurde im Jahr 2023 eine Richtlinie Schulung und Sensibilisierung von der AG IS beschlossen und durch den LA ITEG bestätigt, die unterschiedliche Zielgruppen definiert und Anforderungen an Schulungs- und Sensibilisierungsinhalte für diese Zielgruppen beschreibt. Dazu zählen auch die BfIS selbst, für die eine regelmäßige fachspezifische Weiterbildung als notwendig deklariert wird. Daher hat sich BfIS Land mit Inkrafttreten des Gesetzes auch dafür eingesetzt, die Rolleninhaber in den staatlichen und auch nicht-staatlichen Stellen auf ein möglichst einheitliches Mindestniveau zu bringen und Schulungen sowohl zum IT-Grundschutz-Praktiker als auch zum Vorfall-Management und zum IT-Notfallmanagement finanziert und organisiert. Daran nahmen über 100 Bedienstete von staatlichen und 160 von nicht-staatlichen Stellen teil, die eine Rolle im ISMS ihrer Behörden bekleiden.

Bewertung

Die Maßnahmen im Bereich der Sensibilisierung und Fortbildung, die im Evaluierungszeitraum in erster Linie durch den BfIS Land verantwortet wurden, werden grundlegend positiv bewertet. § 5 Absatz 1 SächsISichG hat mit seinen Sensibilisierungs- und Schulungsanforderungen an den BfIS Land die gesetzliche Grundlage dafür gelegt, dass die großen landesweiten Sensibilisierungsmaßnahmen, die bereits seit dem Jahr 2015 angeboten wurden, fortzusetzen sind. Auch das E-Learning, welches bereits im Jahr 2018 – allerdings in kleinerem Umfang – eingeführt worden war, wurde deutlich größer skaliert. Zudem wurden für die staatlichen und nicht-staatlichen Stellen kostenlose Fortbildungsangebote für die in den Behörden wirkenden BfIS ausgerichtet.

Ein weiterer Impuls zum Thema Sensibilisierung und Schulung wird von den Änderungen des SächsISichG zu erwarten sein, welches unter § 4 Absatz 1a (neu) staatlichen Stellen Maßnahmen zu Sensibilisierung zu grundlegenden Verfahren und Schulungen auferlegt und zusätzlich in § 4 Absatz 3 Satz 3 SächsISichG vorschreibt, dass Leiterinnen oder Leiter der staatlichen Stellen

regelmäßig selbst an Schulungen zur Informationssicherheit teilnehmen müssen. Damit hat das Gesetz eine notwendige und durch Vorgaben der NIS-2-Richtlinie gedeckte Erweiterung erfahren, die die Last nicht weiter einseitig auf den BfIS Land überträgt und zudem die Behördenleitungen in die Pflicht nimmt.

3.2.3 Datenverarbeitung gemäß §§ 12, 13 SächsISichG

Zweck der Vorschriften ist es, den staatlichen und nicht-staatlichen Stellen die Befugnis zum Einsatz von Angriffserkennungssystemen einzuräumen. Der Begriff Angriffserkennungssysteme wird zwar im SächsISichG nicht verwendet, hat mittlerweile aber Eingang ins Bundesrecht gefunden (§ 2 Absatz 9b des BSI-Gesetzes). Dabei bezieht sich der Begriff auf eine große Bandbreite an technischen und organisatorischen Maßnahmen, die zur Angriffserkennung dienen. Gemeinsam ist diesen Systemen, dass sie nicht stichprobenhaft arbeiten, sondern gesamte Datenströme in Echtzeit auswerten und damit auch große Mengen grundrechtsgeschützter Daten verarbeiten. Für diese Grundrechtseingriffe wurden im SächsISichG gesetzliche Grundlagen geschaffen.

Zur Erkennung von Gefahren für die informationstechnischen Systeme im Freistaat Sachsen nach §§ 12 ff. SächsISichG wird ein dreistufiges System eingesetzt. Die drei Stufen orientieren sich an der Intensität der damit verbundenen Grundrechtseingriffe. Grundsätzlich stehen die Befugnisse der §§ 12, 13 SächsISichG jeder staatlichen und nicht-staatlichen Stelle für die von ihr betriebenen informationstechnischen Systeme zu.

Da die Befugnisnormen der §§ 12, 13 SächsISichG bislang ausreichend erschienen, um leistungsfähige Systeme zur Abwehr von Gefahren für die informationstechnischen Systeme des Freistaates Sachsen zu betreiben, wurde von der **Experimentierklausel** gemäß § 19 SächsISichG seit Inkrafttreten des Gesetzes kein Gebrauch gemacht.

Mit den Regelungen in §§ 12 und 13 SächsISichG über Datenverarbeitungsbefugnisse zur Erkennung und Abwehr von Gefahren für die informationstechnischen Systeme im Freistaat Sachsen hat der Gesetzgeber spezielle und ausführliche Regelungen getroffen, was zu begrüßen ist. Ohne diese Vorschriften bestünden rechtliche Unsicherheiten im Umgang mit Telekommunikationsdaten. Für die bei der Datenverarbeitung einhergehenden Grundrechtseingriffe wurden normenklare und verhältnismäßige gesetzliche Grundlagen geschaffen.

Die Befugnisse sind in Sachsen – anders z. B. beim BSI für den Bund – nicht zentralisiert, sondern stehen grundsätzlich jeder staatlichen oder nicht-staatlichen Stelle für ihre informationstechnischen Systeme zur Verfügung. Damit können auch die unabhängigen Behörden, wie Landesrechnungshof, die Sächsische Datenschutzbeauftragte oder die Landtagsverwaltung ihre mit dem SVN verbundenen informationstechnischen Systeme selbst überwachen.

Von den 50 teilnehmenden staatlichen Stellen meldeten 20, dass sie eigene Angriffserkennungssysteme im Einsatz haben. Ganze 40 % der Kommunen melden zurück, dass sie ebenfalls ein erweitertes Angriffserkennungssystem gemäß §§ 12 und 13 des SächsISichG im eigenen Bereich im Einsatz hätten.

Beide Angaben über den Einsatz von solchen Systemen überraschen, da weder von den staatlichen Stellen noch von den Kommunen bislang Zahlen in einem solchen Umfang im Rahmen der Berichtspflichten nach § 5 Absatz 8 Satz 2 SächsISichG zum Jahresbericht Informationssicherheit gemeldet worden sind. Hier wird mit den rückmeldenden Stellen noch zu prüfen sein, ob diese wirklich solche erweiterten Systeme im Einsatz haben oder andere Systeme fälschlicherweise als solche klassifiziert haben. Da erweiterte Angriffserkennungssysteme in der Regel zu erhöhtem Sach- und Personalaufwand führen, der nach den Erfahrungen insbesondere in den Kommunen nur schwer abbildbar ist, wird zum jetzigen Zeitpunkt in den meisten Fällen von einer falschen Interpretation der Frage ausgegangen.

Anders stellt es sich bei den Hochschulen dar. Hier wurde ein erweitertes Angriffserkennungssystem etabliert, welches alle Hochschulen nutzen können.

Die Hälfte der an der Onlinebefragung teilnehmenden Träger der Selbstverwaltung geben die Rückmeldung, dass sie Angriffserkennungssysteme einsetzen. Auch diese Aussage erstaunt, da sie sich nicht in den Rückmeldungen zum Jahresbericht Informationssicherheit widerspiegelt.

Bewertung
Die geschaffenen Rechtsgrundlagen sind für eine rechtskonforme Datenverarbeitung unerlässlich. Ungeachtet dessen sind die Befugnisnormen aufgrund der fortschreitenden Digitalisierung, der gestiegenen Cyberbedrohungen und der Zunahme der Verarbeitung personenbezogener Daten fortlaufend zu prüfen und das SächsISichG im Bedarfsfall an neue rechtliche Anforderungen bei der Datenverarbeitung anzupassen.

Dies kann sich auch aus der Notwendigkeit zum Ausbau der Analysefähigkeit ergeben. Eine besondere Expertise zur Auswertung des Netzwerkverkehrs hat dabei das BSI mit einer speziellen Technik zur Erkennung von Schadsoftware zu bieten. Die Bundesbehörde verfügt über Techniken und Analysefähigkeiten, die die Möglichkeiten und Fähigkeiten der zuständigen Landes-IT-Dienstleister bei der Ermittlung von Gefahren für die IT-Sicherheit übersteigen. Mit dem Einsatz dieser zusätzlichen Techniken und Analysefähigkeiten könnten gegenwärtige und zukünftige Bedrohungslagen für die IT-Sicherheit wirkungsvoller begegnet werden, zumal die abzuwehrenden Cyberangriffe ausgefeilter würden und zunehmend schwerer zu detektieren sind. Niedersachsen ermöglicht es seinen Behörden, das BSI mit einer ergänzenden Auswertung des Datenverkehrs zu beauftragen (vgl. § 22 Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit). Für Sachsen ist zu prüfen, ob eine ähnliche Regelung über die Auswertung von Daten durch das BSI in das SächsISichG aufgenommen werden soll.

3.3 Auswirkungen des Gesetzes auf die Meldepflichten

Bereits im November 2015 wurde mit Beschluss Nummer 08/2015 „Sicherheitsmeldungen“ der AG IS ein ressortübergreifendes Meldeverfahren für „wesentliche Sicherheitsvorfälle“ etabliert. Nach einer Reihe vordefinierter Kriterien sollten damit Sicherheitsereignisse und Sicherheitsvorfälle von den sächsischen Behörden unverzüglich an das SAX.CERT gemeldet werden, um ein realistisches Lagebild zur Informationssicherheit im Freistaat Sachsen erhalten zu können. Zur Meldung der Sicherheitsvorfälle sollte ein vom SAX.CERT bereitgestelltes Meldeformular genutzt werden.

Mit Inkrafttreten des SächsISichG im August 2019 wurden sowohl staatliche als auch nicht-staatliche Stellen des Freistaates Sachsen verpflichtet, Sicherheitsereignisse und Sicherheitsvorfälle ihrer informationstechnischen Systeme oder Prozesse an das SAX.CERT zu melden. Für nicht-staatliche Stellen gilt diese Verpflichtung, soweit deren informationstechnische Systeme mit dem SAX.CERT oder dem KDN verbunden sind, für Hochschulen seit dem 1. Oktober 2024 ausschließlich bei erheblichen Sicherheitsvorfällen. Damit wurden die Meldepflichten hinsichtlich Sicherheitsvorfällen und Sicherheitsereignissen auf eine gesetzliche Basis gestellt. Nicht verpflichtende Meldungen können von nicht-staatlichen Stellen auf freiwilliger Basis abgeben werden. Das vom SAX.CERT bereits vor Inkrafttreten des SächsISichG bereitgestellte Meldeformular wird weiterhin zur Meldung der Sicherheitsvorfälle und Sicherheitsereignisse in den Behörden genutzt.

Im Rahmen der Evaluierung geben 32 von 47 sich beteiligenden Kommunen an, dass ein Prozess zur Meldung von Sicherheitsvorfällen an das SAX.CERT etabliert ist. Dies entspricht einem Anteil von 68 %. Zwölf der 47 Kommunen geben an, in der Vergangenheit bereits Sicherheitsvorfälle an das SAX.CERT gemeldet zu haben. Von den sieben Hochschulen, die an der Befragung teilgenommen haben, ist in fünf Hochschulen ein Prozess zur Meldung von Sicherheitsvorfällen etabliert. Vier von diesen Hochschulen haben bereits Meldungen an das SAX.CERT abgegeben. Bei den Trägern der Selbstverwaltung wurden von 30 % der sich beteiligenden Einrichtungen angegeben, dass diese bereits Sicherheitsvorfälle an das SAX.CERT gemeldet haben, während in

nur 20 % dieser Einrichtungen ein Prozess zur Meldung erheblicher Sicherheitsvorfällen etabliert worden sei.

Seit der gesetzlichen Festschreibung der Meldepflichten ist eine Zunahme der an das SAX.CERT übermittelten Meldungen festzustellen. In den Jahren 2019 und 2020 ist eine Anlaufphase nach Inkrafttreten des SächsISichG erkennbar. Seit dem Jahr 2021 bewegt sich die Zahl der gemeldeten Sicherheitsvorfälle auf einem hohen Niveau. Lediglich im Jahr 2023 war eine leichte Abnahme der Meldungen von 71 auf insgesamt 63 Meldungen zu verzeichnen, was zum damaligen Zeitpunkt einem Rückgang von 11 % entspricht. Der überwiegende Teil der Vorfallmeldungen ging dabei vonseiten der staatlichen Stellen ein. Diese trugen zu 77 % der Sicherheitsvorfälle bei. Der Anteil der Kommunen, die Meldungen abgaben, liegt im Betrachtungszeitraum bei 23 %. Dabei lässt sich erkennen, dass die Anzahl der Meldungen aus dem kommunalen Umfeld seit 2019 stetig angewachsen ist. Es ist davon auszugehen, dass die wachsende Zahl dieser Meldungen vor allem aufgrund bekannterer Meldewege und aufgrund einer höheren Sensibilität der kommunalen Körperschaften für die Sicherstellung der Informationssicherheit auftritt.

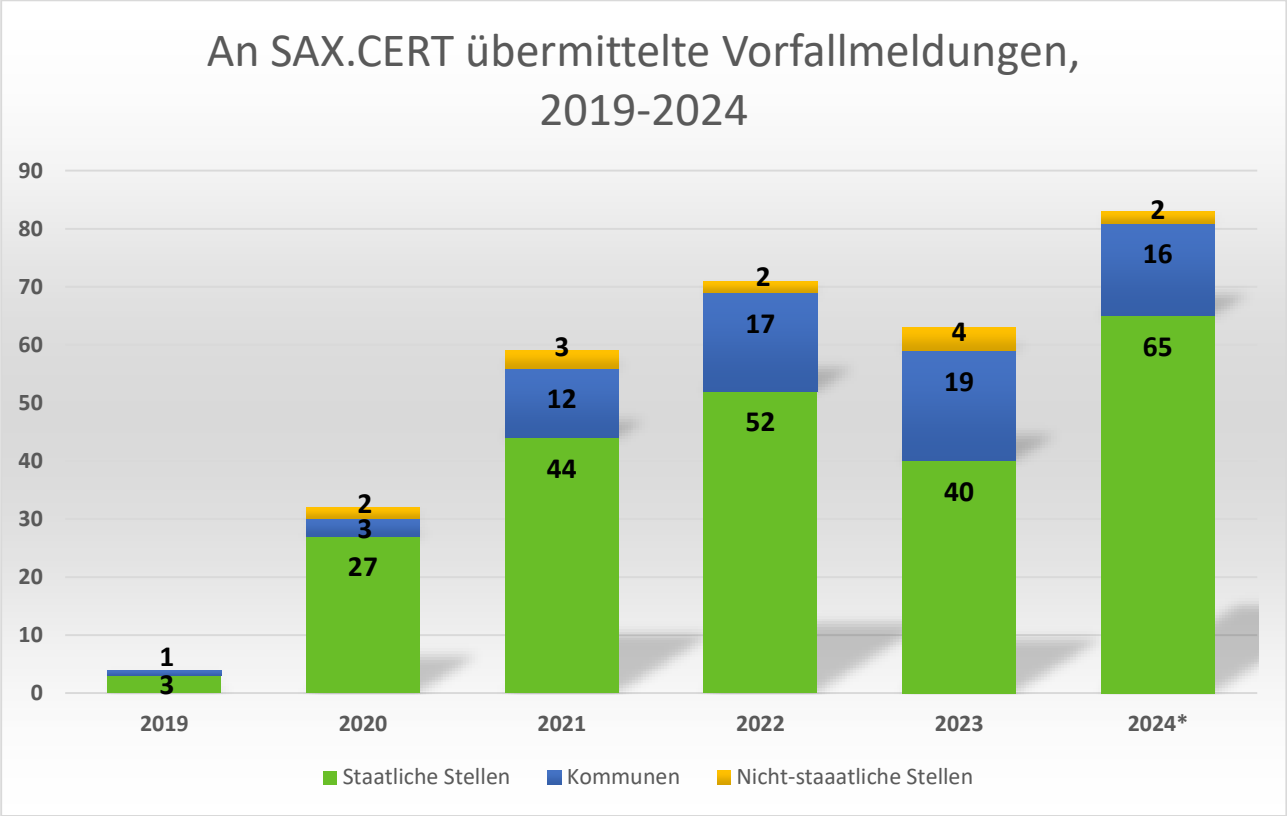

Abbildung 11 - Anzahl der an das SAX.CERT übermittelten Vorfallmeldungen

2024*: Bei Redaktionsschluss lagen Daten bis einschließlich Oktober 2024 vor.

Zur Kategorisierung der gemeldeten Sicherheitsvorfälle: Gegenstand der Meldungen sind Ereignisse, die eines der Schutzziele der Informationssicherheit, also Verfügbarkeit, Vertraulichkeit und Integrität, gefährden. Dies beinhaltet neben Angriffen durch Innen- und Außentäter beispielsweise auch technische Störungen durch Fehlbedienung oder technische Defekte. Aber auch der Verlust bzw. Diebstahl von Datenträgern, Mobilfunkgeräten und Laptops ist häufiger Meldeinhalt.

143 der 312 im Evaluierungszeitraum eingegangenen Meldungen können als Cyberangriff auf die vom Gesetz umfassten Einrichtungen gewertet werden, was mehr als zwei Angriffen pro Monat entspricht. Das Spektrum dieser Cyberangriffe ist sehr breit. Schwerpunkt sind Malware- und Virenfunde sowie Fraud-Versuche, bei denen versucht wird den Adressaten einer E-Mail zu bestimmten Handlungen zu bringen, z. B. Änderung oder Veranlassung von Zahlungsströmen. Ebenfalls gemeldet wurden Versuche, Dienste von Behörden aus dem Internet heraus mittels Überlastungsangriffen lahm zu legen.

Bewertung
In der Rückschau ist seit Inkrafttreten des SächsISichG eine konstant steigende Anzahl an Vorfallmeldungen pro Jahr zu erkennen. Dies ist der steigenden Sensibilität und besseren Kenntnis der staatlichen und nicht-staatlichen Stellen bzgl. der Meldepflichten zuzurechnen. Der Höhepunkt der Meldungen wird dabei im Jahr 2024 erreicht. Es bleibt aber weiterhin zu vermuten, dass es eine nicht unerhebliche Anzahl an Vorfällen gibt, die nicht gemeldet werden. Fehlende Meldungen können nach wie vor an vorhandener Unkenntnis über gesetzlich vorliegende Meldepflichten liegen, an mangelnder Sensibilität der meldepflichtigen Stellen oder auch an Befürchtungen vor negativen Außenwirkungen. Ein tatsächliches Lagebild über die gesamte Staats- und Kommunalverwaltung kann folglich nur bedingt erhoben werden. Nur wenn alle Sicherheitsvorfälle gemeldet werden, so kann die Lage der Informationssicherheit zuverlässig eingeschätzt werden. Zur Verbesserung der Melderate gilt es, stärker auf Aufklärung, Sensibilisierung und Transparentmachung der Ziele der Vorfallmeldungen zu setzen, um im Einzelfall angemessen auf Vorfälle reagieren zu können.

Um das Lagebild zu vervollständigen und schnell auf Vorfälle reagieren zu können, wird die Staatsregierung von der Ermächtigung nach § 16 Absatz 2 SächsISichG Gebrauch machen und eine Meldepflichtenverordnung erlassen. Diese soll die Verfahren und Inhalte des Meldeprozesses vereinheitlichen, nach Kritikalität priorisieren und Schnittstellen für technisch erhobene Informationen definieren.

Kommunale Gebietskörperschaften sind gemäß § 17 Satz 1 SächsISichG nur meldepflichtig, soweit deren informationstechnische Systeme mit dem SVN oder KDN verbunden sind. Für Vorfälle in informationstechnischen Systemen, die nicht mit dem SVN/KDN verbunden sind, gibt es keine Meldepflicht. Für Vorfälle außerhalb des SVN/KDN gingen im Berichtszeitraum nur sehr vereinzelt Vorfallmeldungen von nicht meldepflichtigen nicht-staatlichen Stellen beim SAX.CERT ein. Eine Möglichkeit zur Verbesserung des Lagebildes der sächsischen Verwaltung mit dem Ziel eines Gesamtlagebildes bestünde in der Erweiterung der Meldepflichten bei erheblichen Sicherheitsvorfällen auf den Bereich der Kommunen. Die Kommunen könnten erhebliche Sicherheitsvorfälle informationstechnischer Systeme in Netzbereichen außerhalb des KDN ebenfalls melden müssen, ähnlich wie dies bereits bei Hochschulen der Fall ist. Mit einer solchen zukünftigen Verpflichtung würde die Anzahl der Vorfallmeldungen, die aus dem kommunalen Umfeld abgegeben werden, voraussichtlich merklich ansteigen.

3.4 Kosten-Nutzen-Bewertung

Im Rahmen des Gesetzgebungsprozesses zum SächsISichG wurde vom Sächsischen Normenkontrollrat moniert, dass die mit dem Gesetz unmittelbar als notwendig dargestellten Stellenbedarfe – die damals als Ansatz beschrieben wurden, mit dem der Aufbau der Informationssicherheit bewerkstelligt werden sollte – nur unzureichend den wirklichen Bedarf abdecken würden, und daher überprüft werden müsse, ob damit die mit dem Gesetz einhergehenden Aufgaben in vollem Umfang erfüllt werden können. Die Evaluierung soll auch diesem Prüfauftrag nachkommen.

Ob die im Evaluierungszeitraum bereitgestellten Personal- und Sachkosten ausreichend waren, um die Anforderungen des Gesetzes zu erfüllen, ist nicht belastbar darzustellen. Auch eine Kosten-Nutzen-Bewertung der Informationssicherheit kann nicht spezifisch abgebildet werden, da tatsächliche Kosten für die Informationssicherheit nicht erhebbar sind. Lässt sich bei den Personalkosten eine zumindest teilweise Zuordnung zum Aufgabengebiet der Informationssicherheit herstellen, ist dies bei den Sachkosten deutlich komplexer, schließlich steckt z. B. in den Lizenzkosten jeder Software auch ein Anteil an Sicherheitskosten, der sich jedoch nicht quantifizieren lässt.

Grundsätzlich gilt in der Kosten-Nutzen-Bewertung in Bezug auf Informationssicherheit: Der Nutzen von Sicherheit besteht in der Gewährleistung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit von Informationen. Das heißt, Personal- und Sachkosten, die in die Informationssicherheit investiert werden, lassen das Erreichen der Schutzziele bestenfalls

wahrscheinlicher werden. Es ist dabei jedoch ungewiss, welche Kosten mit der Verletzung von Schutzzielen verbunden sind und ob diese die Aufwendungen für Informationssicherheitsmaßnahmen übersteigen, sodass die Investitionen in die Sicherheit auf jeden Fall als lohnenswert zu betrachten sind.

Es lassen sich hier eher näherungsweise Argumente finden, dass die Kosten für die Informationssicherheit einen hohen Nutzen haben. Zwar gab es aufgrund der Cyberangriffe auf die Hochschulen in Zwickau und Freiberg längere Ausfälle im Studien-, Forschungs- und Verwaltungsbetrieb, bei denen damit auch ein erheblicher, aber nicht genau bezifferbarer Schaden entstanden ist. In der sächsischen Landesverwaltung selbst gab es im Evaluierungszeitraum aber nur einen Sicherheitsvorfall mit einer wesentlichen Schadenssumme: Durch eine Angriffsmethode des Social Engineering entstand im Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt im Jahr 2023 ein finanzieller Schaden von über 200.000 Euro. Sprich: Die Investitionen in die Informationssicherheit haben weitgehend ihr Ziel erreicht, sodass insgesamt keine großen finanziellen Schäden eingetreten sind. Hinzu kommt, dass es auch keine Sicherheitsvorfälle gab, die andere Schäden hervorgerufen haben, wie z. B. Reputationsverlust.

Doch welche Kosten sind für die weitgehende Gewährleistung der Schutzziele der Informationssicherheit entstanden? Im Kapitel 3 wurden in mehreren Unterkapiteln sowohl Ausführungen zum Ausbau von Stellen als auch einige wenige Hinweise zu entstandenen Sachkosten gemacht. Eine systematische Erfassung zu den Personalkosten im Bereich Informationssicherheit liegt jedoch ebenso wenig vor wie eine Übersicht über die zudem aufwändig zu klassifizierenden Sachkosten in der Informationssicherheit. Einen Hinweis über die Angemessenheit der investierten Mittel kann jedoch eine im Jahr 2022 durch BfIS Land durchgeführte Erhebung in den Ressorts vermitteln. Damals wurden die Ressorts gebeten, die in Ihrem Geschäftsbereich angefallenen IT-Sicherheitskosten für das Jahr 2021 zu melden. Diese wurden den tatsächlich im Jahr 2021 angefallenen Kosten in den IT-Titeln der Behörden gegenübergestellt, soweit dass die Zahlen ermöglichten.

Die ermittelten Quoten ergaben, dass in den Behörden bzw. Ressorts zwischen 14 % bis unter 2 % anteilig für IT-Sicherheits-Maßnahmen ausgegeben wurden. Alles in allem lag die Quote bei rund 5 %, und damit insgesamt weit unter den IT-Sicherheitskosten, die von Unternehmen investiert werden oder die vom BSI empfohlen oder in Gesetzen gefordert werden. So betrug nach Angaben von statista der Anteil der Ausgaben für Cybersicherheit an den Gesamt-IT-Ausgaben in Deutschland im Jahr 2021 rund 20 %.[28] Und auch der Gesetzgeber misst den Ausgaben für die IT-Sicherheit mitunter eine Bedeutung zu: So wurde im Krankenhausfinanzierungsgesetz in Verbindung mit dem Krankenhauszukunftsgesetz, welches u. a. neue IT-Verfahren finanziell fördert, festgelegt, dass mindestens 15 % der gewährten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit zu verwenden sind.[29] Bitkom e. V. und BSI sehen unisono 20 % der IT-Kosten für die IT-Sicherheit als angemessene Quote.[30] Im Rahmen dieser Erhebung lässt sich als Ergebnis festhalten, dass die hierzu aufgebrachten Mittel in den Ressorts nicht befriedigend sind. Vor allem fehlen Budgets für die BfIS als auch Investitionen in erweiterte Schutzsysteme auf Behördenebene. Durch diese investiven Maßnahmen könnte die Informationssicherheit deutlich gestärkt werden.

Zur gesamten Kosten-Nutzen-Bewertung wurden im Rahmen der eben genannten Erhebung jährliche Sachkosten für die Informationssicherheit im Jahr 2021 von über 11 Millionen Euro ermittelt. Mit diesen Investitionen wurden also weitestgehend die Schutzziele der Informationssicherheit erreicht.
Hinzu kommen die Personalkosten, die jedoch nicht so exakt bestimmbar sind, dass ihre Angabe belastbar wäre. Schließlich tragen neben Personalkosten für die BfIS-Stellen auch Kosten für IT-Stellen, IT-nahe Stellen und teilweise auch Stellen in Organisationsbereichen dazu bei, die Informationssicherheit zu gewährleisten.

[28] Statista - das Statistik-Portal: Statistiken, Marktdaten & Studien, https://de.statista.com/statistik/daten/studie/1230132/umfrage/anteil-der-ausgaben-fuer-cybersicherheit-an-den-gesamt-it-ausgaben-in-deutschland/?locale=de (zuletzt abgerufen am 30.10.2024)
[29] Artikel 1, § 14a Krankenhausfinanzierungsgesetz, hier Absatz 3, letzter Satz
[30] https://www.bitkom.org/Kurzpositionen/Cybersicherheit-Sicherheitstechnologien (zuletzt abgerufen am 30.10.2024)

Insofern lohnt es sich, bei der Kosten-Nutzen-Bewertung nicht nur das Augenmerk auf die Kosten der Informationssicherheit zu legen, sondern auch die möglichen Kosten eines potenziellen Schadensereignisses in den Blick zu nehmen. Allein für die deutsche Wirtschaft wurde der jährliche Schaden aufgrund von Cyberangriffen zuletzt auf 267 Milliarden Euro geschätzt.[31] Und auch wenn eine ähnliche Schätzung zur öffentlichen Verwaltung in Deutschland nicht vorliegt, zeigen die einzelnen Fälle, zu denen Schadenssummen kursieren, das enorme Kostenpotenzial. So soll der Cyberangriff auf den kommunalen IT-Dienstleister Südwestfalen-IT im Oktober 2023, bei dem 72 Kommunen massiv beeinträchtigt wurden, allein für das Geschäftsjahr 2023 Mehrkosten in Höhe von 2,8 Millionen Euro erzeugt haben.[32] Die Attacke auf die digitale Infrastruktur des Landkreises Anhalt-Bitterfeld im Juli 2021 hat insgesamt Aufwendungen von rund 2,5 Millionen Euro verursacht.[33] Nicht eingerechnet sind in diese Summen der enormen immateriellen Schäden, insbesondere für die Reputation der jeweiligen Behörden oder Dienstleister.

Jeder langwierige Ausfall von Online-Services, aber auch herkömmlicher Papierverfahren einer Behörde durch einen Sicherheitsvorfall untergräbt das Vertrauen der Bürgerinnen und Bürger, von Unternehmen und anderen Einrichtungen in die öffentliche Verwaltung und damit in die Funktionsfähigkeit des Staatswesens. Die immateriellen Schäden sind daher als deutlich schwerwiegender zu bewerten, als es reine Schadenssummen für eine Verwaltung je sein können.

[31] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024 (zuletzt abgerufen am 30.10.2024)
[32] https://www.come-on.de/volmetal/meinerzhagen/it-attacke-teure-nachwehen-fuer-die-kommunen-93359184.html (zuletzt abgerufen am 30.10.2024)
[33] https://www.heise.de/news/Ransomware-kostete-Anhalt-Bitterfeld-rund-2-5-Millionen-Euro-9650816.html (zuletzt abgerufen am 30.10.2024)

4 Vorschläge zur Weiterentwicklung und Umsetzung des SächsISichG

Gemäß § 21 SächsISichG ist dem Bericht an den Landtag zu benennen, ob eine Weiterentwicklung der Vorschriften dieses Gesetzes erforderlich ist. Die Ansätze zur Weiterentwicklung werden im Folgenden differenziert in Maßnahmen zur Begleitung der Gesetzesumsetzung sowie in regulatorische Maßnahmen.

Zwar liegt der Fokus einer Evaluierung auf den regulatorischen Maßnahmen. Gleichwohl erscheinen aufgrund der in den letzten fünf Jahren gesammelten Erfahrungswerte und der Rückmeldungen im Rahmen der Evaluierung eher eine Vielzahl an begleitenden und unterstützenden Maßnahmen zur Umsetzung des Gesetzes geboten.

In der nachstehenden Tabelle werden die sich aus der Bewertung ergebenden Ansätze zur Weiterentwicklung dargestellt:

Erkannte Aufgabenkomplexe	Ansätze zur Weiterentwicklung	Maßnahme*
Stärkung der zentralen strategischen und operativen Akteure in der Informationssicherheit	Stärkung BfIS Land	R, U
	Revisionen intensivieren	U
	Stärkung des SAX.CERT	R, U
	Ausbau der Beratung zur Informationssicherheit	U
	Lagebericht zur Informationssicherheit verbessern	U
	Ausbau der Analysefähigkeit und Angriffserkennungssysteme	R, U
Zentrale Unterstützung für Informationssicherheit erhöhen, dezentrale Budgets einführen und Rollen adäquat besetzen	BfIS in den Behörden – adäquate Stellenbesetzung erreichen	U
	BfIS in den Behörden - eigenes Budget	U
	ISMS-Tool (Unterstützung durch BfIS Land)	U
Zentralisierung und Standardisierung der IT forcieren	Zentralisierung und Standardisierung der IT	U
Stärkung der Informationssicherheit in den Kommunen	KDN-Ausgestaltung und Finanzierung	U
	Unterstützung für ISMS	U
	Erweiterung der Meldepflicht	R

Tabelle 3 - Überblick über Maßnahmen zur Weiterentwicklung und Umsetzung des SächsISichG

* Maßnahme:
- Regulatorische Maßnahmen (gekennzeichnet mit R)
- Maßnahmen zur Begleitung der Gesetzesumsetzung (sog. Umsetzungsmaßnahmen, gekennzeichnet mit U)

4.1 Unterstützende Maßnahmen zur Umsetzung des SächsISichG

Anhand der Rückmeldungen im Rahmen der Evaluierung, aber auch aufgrund der Erfahrungswerte zum Stand der Informationssicherheit im Freistaat Sachsen nach Inkrafttreten des SächsISichG, ergeben sich Ansatzpunkte, mit welchen Maßnahmen man die Anforderungen aus dem Gesetz besser umsetzen könnte und welche Maßnahmen man abseits gesetzlicher Regelungen treffen sollte, um die Informationssicherheit in den Behörden im Freistaat Sachsen zu erhöhen.

4.1.1 Stärkung der zentralen Akteure in der Informationssicherheit

Stärkung BfIS Land

BfIS Land ist zwar laut SächsISichG direkt beim CIO vorspracheberechtigt, organisatorisch aber in der Abteilung zur Verwaltungsdigitalisierung und damit in der Linie verortet. Durch diese Konstellation wird BfIS Land teilweise von den Ressorts entweder als BfIS im Zuständigkeitsbereich der SK wahrgenommen oder als für operative Themen im Geschäftsbereich der SK zuständig erachtet, vor allem mit Hinblick auf den Landes-IT-Dienstleister SID. Seine zentrale strategische Rolle für die Informationssicherheit in der gesamten Staatsverwaltung und insbesondere die herausgehobene Position als Aufsichtsbehörde für alle anderen Behörden für den Bereich Informationssicherheit, auch die SK selbst, wird hierbei zu oft außer Acht gelassen.
Es wird empfohlen zu prüfen, ob die organisatorische Verortung des BfIS Land beim CIO die Aufgabenerfüllung als unabhängige zentrale strategische Instanz und als Aufsichtsbehörde besser ermöglicht.

Revisionen intensivieren

Im SächsISichG wurden mit den Änderungen zum 1. Oktober 2024 die Revisionspflichten des BfIS Land nochmals intensiviert. Allerdings wurden dem BfIS Land seit 2019 keine für diese Tätigkeit notwendigen zusätzlichen personellen Ressourcen bereitgestellt. Die Befugnis des BfIS Land zur Durchführung von Revisionen bei staatlichen Stellen führt zu einem Erfüllungsaufwand für die laufenden Prüfungstätigkeiten bei Annahme von durchschnittlich zehn Revisionen im Jahr von rund 1,5 VZÄ (ausgehend von einer Verteilung ½ LG 2.1 und ½ LG 2.2 entspricht dies insgesamt 194.575,50 Euro Sach- und Lohnkosten).
Es wird empfohlen, dem BfIS Land ausreichend personelle Ressourcen zur Umsetzung der Anforderung aus § 5 Absatz 7 SächsISichG bereitzustellen.

Stärkung des SAX.CERT

Damit das SAX.CERT seine gesetzlich festgeschriebenen Aufgaben vollumfänglich in der notwendigen Qualität erbringen kann, bedarf es einer deutlichen Stärkung der Kapazitäten. Dabei ist Sorge dafür zu tragen, dass das eingesetzte Personal über die erforderlichen Fähigkeiten und Fertigkeiten verfügt und kontinuierlich weiterentwickelt wird. Die Erfahrung zeigt, dass die kostenintensive Beschaffung von Expertise über Dienstleister nur zu temporären Verbesserungen führt und zusätzliche Aufwände für die Beschaffung, Unterweisung und Betreuung der Dienstleister erzeugt. Mit dem Ende von Beauftragungen geht i. d. R. auch die Expertise wieder verloren, die jedoch für Folgeaufgaben wieder essentiell ist.
Es wird empfohlen, dem SAX.CERT die personellen und finanziellen Ressourcen zur Verfügung zu stellen, um eine dem Stand der Technik entsprechende Ausstattung mit den dafür notwendigen IT-Experten bereitstellen zu können, damit das SAX.CERT seinen gesetzlichen Aufgaben erfüllen kann.

Ausbau der Beratung zur Informationssicherheit

Zu der im SächsISichG neu benannten Anforderung an den BfIS Land, Behörden zu Themen der Informationssicherheit zu beraten, wurden mit Verabschiedung des Gesetzes keine dafür notwendigen zusätzlichen personellen Ressourcen geschaffen. Deshalb wurde ein Rahmenvertrag für Beratungsleistungen zur Informationssicherheit mit externen Dienstleistern geschlossen, aus dem alle staatlichen Stellen abrufen können. Allerdings müssen die Behörden dafür eigene finanzielle Mittel bereitstellen. Aus der geringen Zahl an Abrufen aus dem Rahmenvertrag lässt sich schließen,

dass die wenigsten Behörden die Ressourcen haben, sich von externen Dienstleistern beraten zu lassen. Die Notwendigkeit einer zentralen und für die Behörden kostenfreien Beratungskapazität bleibt also bestehen.
Es wird empfohlen, dem BfIS Land ausreichend personelle Ressourcen zur Umsetzung der Anforderung aus § 5 Absatz 1 Satz 2 Nummer 1 SächsISichG bereitzustellen.

Lagebericht zur Informationssicherheit verbessern

Der Lagebericht des SAX.CERT ist, wie unter Kapitel 3.1.2 Sicherheitsnotfallteam SAX.CERT festgestellt, in aktueller Form als Dokument statisch und hat mit der monatlichen Berichterstattung eher statistischen und informativen Wert. Für schnelle Reaktionen auf die in der Informationssicherheit typischen, sich ständig ändernde Lagen ist diese Berichtsform ungeeignet.
Es wird empfohlen, die Mittel bereitzustellen, eine technische Grundlage im SAX.CERT zu schaffen, auf einer Online-Plattform die Lage der Informationssicherheit beschreibende Sicherheitskennzahlen aktuell darzustellen. Damit wird den dafür zuständigen Stellen in der Staats- und Kommunalverwaltung ein sicherer Zugang zu einem aktuellen Lagebild ermöglicht, darauf ausgerichtete Reaktionen können unmittelbar erfolgen.

Ausbau der Analysefähigkeit und Angriffserkennungssysteme

Im Zuge der Aufrechterhaltung des aktuellen Standes der Technik (vgl. Kapitel 3.2.1) sind kontinuierlich Maßnahmen zu prüfen, die den sich verändernden Gegebenheiten entsprechen. Dies gilt insbesondere unter Beachtung des Aufbaus des neuen Verwaltungsnetzes in den kommenden Jahren. Es scheint unerlässlich, den Fokus nicht nur auf die Schutzsysteme am zentralen Internetgateway zu legen, sondern auch verstärkt eine Angriffserkennung im Netz zu etablieren.
Es wird empfohlen, für eine effiziente Umsetzung im gesamten SVN/KDN eine standardisierte, zentral angebotene Lösung umzusetzen. Die Mittel hierfür sollten im Haushalt zentral zur Verfügung gestellt werden. Dies stellt sicher, dass Angriffserkennungssysteme über Ressortgrenzen hinweg Angriffe beobachten können, dass technische und organisatorische Schnittstellen auf ein Minimum beschränkt werden und entlastet letztlich auch die Ressorts im Bereich der Beschaffung und Wartung der Systeme.

4.1.2 Zentrale Unterstützung für Informationssicherheit - Budgets und Rollenbesetzung

BfIS in den Behörden – adäquate Stellenbesetzung erreichen

Auch wenn in allen staatlichen Stellen nach § 7 Absatz 1 SächsISichG die Rolle des BfIS nach Eigenauskunft hauptamtlich besetzt ist, sollte in diesen Behörden in einem nächsten Schritt sichergestellt werden, dass die Rolleninhaber ihre dies bezogenen Aufgaben mit 1,0 VZÄ, also zu 100 % erledigen können. In diesem Zusammenhang ist die Zusammenlegung von BfIS-Aufgaben mit anderen IT-Aufgaben oder Zuständigkeiten als IT-Notfallbeauftragter oder Business Continuity Management-Beauftragter auszuschließen.

Zudem ist darauf hinzuwirken, dass in allen staatlichen Behörden mit mehr als 300 Bediensteten, die ihre IT oder Teile ihrer IT-Infrastruktur selber betreiben, sowie in allen Behörden, die

1) besonders schützenswerte Daten verarbeiten oder
2) als Einrichtung i. S. d. Art. 2 Absatz 2 f) ii) NIS-2-Richtlinie in Verbindung mit § 7 Absatz 4 SächsISichG identifiziert worden sind,

BfIS mit mindestens 0,5 VZÄ beschäftigt werden.

BfIS in den Behörden – eigenes Budget

Sowohl die sehr geringen Abrufzahlen aus dem landesweiten Rahmenvertrag zu Beratungsleistungen zur Informationssicherheit als auch die wenigen Rückmeldungen im Rahmen der Evaluierung zur Benennung eigener Budgets lassen den Schluss zu, dass die BfIS in den meisten staatlichen Stellen nicht über eigenes Budget verfügen. Ohne eigenes Budget ist die Wirkmacht und notwendige Weisungsfreiheit der Rolle nicht vollständig gegeben.
Es wird daher empfohlen, den BfIS der staatlichen Stellen, zumindest denen, die in einer Behörde nach den im vorherigen Abschnitt dargestellten Kriterien beschäftigt sind, ein eigenes Budget zur Verfügung zu stellen. Damit könnten BfIS z. B. Sensibilisierungs- und Schulungsmaßnahmen oder auch Beratungsleistungen zu technischen oder organisatorischen Maßnahmen finanzieren, die dazu dienen, den Anforderungen aus § 4 SächsISichG nachzukommen.

ISMS-Tool (Unterstützung durch BfIS Land)

Nach § 4 Absatz 1 Satz 5 SächsISichG haben die staatlichen Stellen ein ISMS zu erstellen und zu pflegen. BfIS Land ist nach § 5 Absatz 5 SächsISichG verpflichtet, ein ISMS für die Sächsische Staatsverwaltung erstellen und zu pflegen. § 5 Absatz 7 SächsISichG sichert ihm darüber hinaus zu, die Wirksamkeit und den Stand der Erfüllung der einzelnen ISMS überprüfen zu können. Aus der Evaluierung ist ersichtlich geworden, dass die wenigsten staatlichen Stellen eine ISMS-Software zur Erfassung und Dokumentation ihres Umsetzungsstands verwenden. Damit fehlt in den meisten Fällen die Datengrundlage, auf deren Basis BfIS Land seiner Prüfverpflichtung nachkommen kann.
Es wird empfohlen, dass zentral eine ISMS-Software beschafft und finanziert wird. Die staatlichen Stellen werden verpflichtet, eine ISMS-Software zu nutzen und dem BfIS Land auf Anforderung, aber mindestens einmal jährlich darüber den Stand ihres ISMS zu übermitteln.

4.1.3 Zentralisierung und Standardisierung der IT forcieren

Zentralisierung und Standardisierung der IT

Die zentrale Bereitstellung standardisierter digitaler Infrastrukturen hilft, die IT-Landschaft der Sächsischen Staatsverwaltung effizienter und sicherer zu machen. Viele verschiedene IT-Systeme sind ein Sicherheitsrisiko. Das muss durch teure und komplexe Sicherheitslösungen ausgeglichen werden. Wenn die IT standardisiert und zentral verwaltet wird, spart das Ressourcen und macht die Arbeit effizienter. Außerdem wird die Informationssicherheit damit erhöht.

Es wird daher das folgende strategische Ziel der Strategie zur digitalen Transformation der Sächsischen Staatsverwaltung aus dem Jahr 2023 ausdrücklich geteilt: „Definierte IT-Infrastruktur-Services werden grundsätzlich zentralisiert und möglichst umweltverträglich durch den SID für die Staatsverwaltung bereitgestellt. Dabei werden die unterschiedlichen Schutzbedarfe berücksichtigt und das notwendige Maß an Informationssicherheit gewährleistet. Durch ressortübergreifende Standard-Services, bei denen Anforderungen der Informationssicherheit von Beginn an integriert sind, wird die Vielfalt an IT-Produkten begrenzt.“ [34]

4.1.4 Stärkung der Informationssicherheit in den Kommunen

KDN-Ausgestaltung und Finanzierung

Als eines der wenigen Flächenbundesländer bindet der Freistaat Sachsen die Kommunen in ein Verwaltungs- und Behördennetz ein, bei dem die kommunale Familie von den umfangreichen Schutzsystemen profitiert, die am Übergang zum Internet für das SVN und das KDN gemeinsam aufgebaut wurden. Einige kleinere Kommunen nutzen das KDN jedoch nur als Einzelplatzlösung für bestimmte Fachanwendungen und bedienen sich ansonsten eher mäßig geschützten Internetzugängen bei anderen Telekommunikations- und Internetanbietern. Die kreisfreien Städte wiederum verfügen über umfangreiche eigene physische Netze zur Kommunikation der verschiedenen Ämter untereinander. Auch wenn nicht-staatliche Stellen auf freiwilliger Basis Sicherheitsvorfälle melden können und vereinzelt auch solche Meldungen eingegangen sind, so ergibt sich aufgrund der fehlenden Verpflichtung für die Verwaltung insgesamt ein unvollständiges Lagebild. Deutschlandweit

[34] Strategie zur digitalen Transformation der Sächsischen Staatsverwaltung, 2023, S. 41 ff.

betrachtet sind die Kommunen im Bereich der Verwaltung am stärksten von Cyberangriffen gefährdet und benötigen für die Wiederherstellung ihrer Verwaltungsfähigkeit erhebliche Zeit und finanzielle Aufwendungen, falls sie beispielsweise von einer Ransomware-Attacke betroffen sind.
Empfohlen wird deshalb, insbesondere die kleineren und mittleren Kommunen komplett in das KDN und damit unter den gemeinsamen Schutzschirm mit der Staatsverwaltung einzubinden. Dies sollte spätestens im KDN der nächsten Generation berücksichtigt werden.

Unterstützung für ISMS
Die staatlichen Stellen sind gesetzlich verpflichtet, ein ISMS zu erstellen und zu pflegen und hierbei das jeweils geltende IT-Grundschutzkompendium des BSI zu berücksichtigen. Den nicht-staatlichen Stellen wird dieses Kompendium zur Anwendung empfohlen. Das BSI hat im Jahr 2023 mit „Wege in die Basisabsicherung“ eine niederschwellige Methode als Alternative zum in der Praxis etablierten Standardvorgehen beim BSI-IT-Grundschutz entwickelt und auch an einer Pilotkommune in Sachsen, Markkleeberg, getestet, um gerade kleineren und mittelgroßen Kommunen den Einstieg in den Aufbau eines ISMS zu erleichtern. Es wird empfohlen, zu prüfen, inwieweit die Staatsregierung, z. B. über Mittelzuweisungen an bestehende Programme zur Förderung des BSI-Grundschutzes in kleinen und mittleren Kommunen oder über eine eigene Förderung, die Implementierung des BSI-Grundschutzes in den Kommunen unterstützen kann.

4.2 Regulierungsbedarfe im SächsISichG

Gemäß § 21 SächsISichG liegt der Fokus, ob eine Weiterentwicklung der Vorschriften dieses Gesetzes erforderlich ist, auf den regulatorischen Maßnahmen. Entsprechend der Rückmeldungen im Rahmen der Evaluierung, aber auch aufgrund der Erfahrungen zum Vollzug des Gesetzes, ergeben sich Ansatzpunkte zur Änderung des SächsISichG in zwei Aufgabenkomplexen. Aus Gründen der Effizienz ist es sinnvoll, notwendige und sowohl gebotene Änderungen aufgrund der Evaluierung als auch solche aufgrund geänderter Rahmenbedingungen zu einer Novelle des SächsISichG zusammenzufassen, um eine konsistente Gesetzesfortschreibung zu ermöglichen.

4.2.1 Stärkung der zentralen Akteure in der Informationssicherheit

Stärkung BfIS Land
Zur Absicherung von Abwesenheitszeiten des BfIS Land sollte die gesetzliche Verankerung der Ernennung eines Vertreters auch auf den Landesbeauftragten ausgeweitet werden, ähnlich wie bei den staatlichen Stellen. Im Interesse der Gewährleistung der Handlungsfähigkeit des BfIS Land sollte daher die **Vertreterrolle des BfIS Land** analog § 7 SächsISichG gesetzlich festgeschrieben werden.

Stärkung des SAX.CERT
§ 6 Absatz 1 Satz 1 SächsISichG ordnet das **SAX.CERT organisatorisch** dem SID zu. Länder wie Nordrhein-Westfalen, Hamburg, Schleswig-Holstein, Bremen und Sachsen-Anhalt haben das Sicherheitsnotfallteam ebenfalls dem Landes-IT-Dienstleister übertragen. In anderen Ländern wird diese Aufgabe bewusst vom jeweiligen Landes-IT-Dienstleister separiert, um die Unabhängigkeit von betrieblichen Aspekten der Dienstleister zu wahren. So haben Bayern mit einem eigenen Landesamt für Sicherheit in der Informationstechnik und Baden-Württemberg mit einer Cybersicherheitsagentur explizite Organisationsstrukturen für Informationssicherheit geschaffen, Hessen hat das CERT als Referat dem Innenministerium zugeordnet.
Um der Staatsregierung zu ermöglichen, die organisatorische Zuordnung des Sicherheitsnotfallteams in Einklang mit dessen Aufgabenzuweisung bei Bedarf an die jeweilige Lage anpassen zu können, sollte die strikte gesetzliche Zuordnung zum SID aufgelöst, § 6 Abs. 1 Satz 1 SächsISichG also gestrichen werden.

Ausbau der Analysefähigkeit
Vor dem Hintergrund der deutlich gestiegenen Bedrohungslage kann der **Ausbau der Analysefähigkeit** dazu beitragen, aktuelle und zukünftige Bedrohungen der IT-Sicherheit effektiver zu bewältigen. Das BSI verfügt über fortschrittliche Techniken zur Erkennung von Schadsoftware und

zur Auswertung des Netzwerkverkehrs, die den Möglichkeiten des Landes-IT-Dienstleisters überlegen ist.
Es wird empfohlen zu prüfen, ob Regelungen in das SächsISichG aufgenommen werden sollen, die es ermöglichen, das BSI mit einer ergänzenden Auswertung des Datenverkehrs zu beauftragen.

4.2.2 Stärkung der Informationssicherheit in den Kommunen

Erweiterung der Meldepflicht

Der Freistaat Sachsen hat ein Verwaltungs- und Behördennetz aufgebaut, von dem die Kommunen profitieren. Für die Kommunen besteht eine Meldepflicht für Sicherheitsvorfälle an das SAX.CERT, soweit Kommunen das KDN in dem betroffenen Netzsegment nutzen. Kleinere Kommunen haben oft weniger gesicherte Internetzugänge und größere Städte eigene physische Netze. Das SAX.CERT erhält damit Meldungen über Sicherheitsvorfälle dieser Kommunen nur auf freiwilliger Basis. Damit ist das Bild über das Angriffsgeschehen in den Kommunen unvollständig. Neue Angriffsvektoren können vom SAX.CERT im Zweifel nicht erkannt werden. Die sinnvolle und notwendige schnelle Warnung der staatlichen und nicht-staatlichen Stellen Sachsens sowie die Information des VCV erfolgen nicht. Es ergibt sich ein unvollständiges Lagebild. Dabei sind Kommunen besonders anfällig für Cyberangriffe und benötigen erhebliche Ressourcen zur Wiederherstellung ihrer Systeme. Ziel sollte zum einen die Schaffung eines Gesamtbildes über die Lage der Informationssicherheit über die technischen Grenzen des KDN hinaus sein und zum anderen sollte ein umfassender, aktiver Beitrag zur Informationssicherheit im gesamten Land Sachsen und dem Bundesgebiet geleistet werden.
Es wird empfohlen zu prüfen, ob in der Fortschreibung des Gesetzes die Meldepflicht auf alle Kommunen für zumindest erhebliche Sicherheitsvorfälle erweitert wird.

5 Abkürzungsverzeichnis

AG IS	Arbeitsgruppe Informationssicherheit
AK ITEG	Arbeitskreis IT und E-Government
BfIS	Beauftragter für Informationssicherheit
BfIS Land	Beauftragter für Informationssicherheit des Landes
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIO	Chief Information Officer (Beauftragter für Informationstechnologie des Freistaates Sachsen)
CRA	Verordnung (EU) 2024/2847, Cyber Resilience Act
CSIRT	Computer Security Incident Response Team
DHH	Doppelhaushalt
Drs.	Drucksache
EU	Europäische Union
GVBl.	Gesetz- und Verordnungsblatt
ISMS	Informationssicherheitsmanagementsystem
ITEG	Informationstechnik und E-Government
IT	Informationstechnologie
IT-PLR	IT-Planungsrat
KDN	Kommunales Datennetz
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastrukturen
LA ITEG	Lenkungsausschuss IT und E-Government
LG	Laufbahngruppe
LIT	Leitstelle für Informationstechnologie der sächsischen Justiz
NIS-2-Richtlinie	Richtlinie (EU) 2022/2555, Network Information Systems Security Directive
SächsEGovG	Sächsisches E-Government-Gesetz
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsISichG	Sächsisches Informationssicherheitsgesetz
SAX.CERT	Sicherheitsnotfallteam
SID	Staatsbetrieb Sächsische Informatik Dienste
SIEM	Security Information and Event Management
SK	Sächsische Staatskanzlei
SMI	Sächsisches Staatsministerium des Innern
SMK	Sächsisches Staatsministerium für Kultus
SMWK	Sächsisches Staatsministerium für Wissenschaft, Kultur und Tourismus
SOC	Security Operations Center
SVN	Sächsisches Verwaltungsnetz
VCV	VerwaltungsCERT-Verbund
VwV	Verwaltungsvorschrift
VwV IS	Verwaltungsvorschrift Informationssicherheit
VZÄ	Vollzeitäquivalent

6 Tabellen- und Abbildungsverzeichnis