Freistaat
SACHSEN

Bericht des Beauftragten für Informationssicherheit des Landes 2025

Berichtszeitraum: August 2024 – Juli 2025

Inhalt

1 Einführung

Seit Inkrafttreten des Sächsischen Informationssicherheitsgesetzes (SächsISichG) im Jahr 2019 berichtet der Beauftragte für Informationssicherheit des Landes (BfIS Land) jährlich dem Sächsischen Landtag und damit der Öffentlichkeit über seine Tätigkeit und den Stand der Informationssicherheit in der Sächsischen Verwaltung im Jahresbericht Informationssicherheit. Dabei wurde der Bericht bislang auch dazu genutzt, um weitere über die gesetzlichen Anforderungen hinausgehende Informationen zu kommunizieren, z. B. zur Bedrohungslage und zu statistischen Daten im jeweiligen Berichtszeitraum, der sich von August bis Juli erstreckt.

Beginnend mit dem vorliegenden Bericht wird sich der BfIS Land auf die in § 5 Absatz 8 Satz 1 SächsISichG benannten Berichtspflichten konzentrieren. Weitere Informationen, insbesondere statistische Daten von Schutzsystemen, sollen künftig in Monatsscheiben – und damit aktueller als es in einem einmal jährlich erscheinenden Jahresbericht möglich ist – auf der Webseite „Dashboard Informationssicherheit“ veröffentlicht werden.

Nachdem im letzten Berichtszeitraum die Änderung des SächsISichG durch den Sächsischen Landtag beschlossen worden ist, wurde im vorliegenden Zeitraum die Umsetzung der neuen gesetzlichen Aufgaben nach der NIS-2-Richtlinie, insbesondere für BfIS Land und für das Sicherheitsnotfallteam (SAX.CERT), begonnen und strukturell verankert – jedoch unter erheblichem Ressourcendruck. Ein zusätzlicher Personalaufwuchs zur Bewältigung der erweiterten Aufgabenstellungen ging mit der Gesetzesänderung nicht einher. Stattdessen wurden die gesetzlichen Anforderungen durch organisatorische Anpassungen, interne Umschichtungen und Priorisierungen realisiert. Eine nachhaltige und vollumfängliche Umsetzung der NIS-2-Anforderungen setzt jedoch perspektivisch eine personelle und finanzielle Verstärkung voraus.

Auch die Evaluierung des SächsISichG, die im Berichtszeitraum erfolgreich abgeschlossen werden konnte, lässt erkennen, dass es an einigen Stellen noch an der Umsetzung der normativen Vorgaben mangelt, vielfach wegen beschränkter Ressourcen. In einer zunehmend digitalisierten Welt mit einer digitalen Verwaltung sollte uns deshalb grundsätzlich an einer ausreichend abgesicherten IT gelegen sein. Dazu braucht es sowohl eine gut orchestrierte Organisation und technische Schutzmaßnahmen nach aktuellem Stand – von den 20 Prozent, die das BSI anteilig am IT-Budget für Sicherheitsmaßnahmen als notwendig erachtet[1], sind die Behörden im Freistaat Sachsen insgesamt ziemlich entfernt.

[1] so die Präsidentin des BSI, Claudia Plattner, auf der IT-Sicherheitsmesse IT-SA 2023 in Nürnberg; https://www.vdi-nachrichten.com/technik/informationstechnik/bsi-chefin-plattner-firmen-sollten-20-prozent-des-it-budgets-fuer-cybersecurity-vorsehen/

2 Tätigkeitsbericht des Beauftragten für Informationssicherheit des Landes

Neben den in Kapitel 3 benannten Maßnahmen des Sicherheitsnotfallteams SAX.CERT und den statistischen Daten zur Anzahl von Fällen der Verarbeitung personenbezogener Daten, die durch den Einsatz erweiterter Angriffserkennungssysteme angefallen sind, dient der Jahresbericht zuvorderst dazu, den Sächsischen Landtag nach § 5 Absatz 8 über die Tätigkeit des BfIS Land allgemein zu informieren.

Der BfIS Land ist laut SächsISichG unter anderem für die Erstellung des Informationssicherheitsmanagementsystems (ISMS Land) der Sächsischen Staatsverwaltung zuständig und erarbeitet verbindliche Mindeststandards zur Informationssicherheit für die staatlichen Stellen. Er initiiert und koordiniert landesweite Sensibilisierungs- und Schulungsmaßnahmen und Projekte zur Informationssicherheit. Darüber hinaus berät er die Beauftragten für Informationssicherheit (BfIS) der Behörden bei der Erfüllung ihrer Aufgaben.

2.1 Umsetzung der Anforderungen nach der NIS-2-Richtlinie in Sachsen

Im Freistaat Sachsen wurden die normativen Anforderungen der NIS-2-Richtlinie an die öffentliche Verwaltung fristgemäß umgesetzt. Sachsen war damit das erste Bundesland in Deutschland, das die europäischen Vorgaben der NIS-2-Richtlinie für die Landesverwaltung in nationales Recht überführt und im SächsISichG integriert hat, um die Cybersicherheit in der öffentlichen Verwaltung zu stärken. Bei der Umsetzung der NIS-2-Richtlinie konnte auf bereits bestehende Strukturen und Regelungen zurückgegriffen werden. Dabei wurden die bestehenden Regelungen zielgerichtet weiterentwickelt und in ihrer Reichweite und Wirkung so angepasst, dass sie auch über den unmittelbar von der NIS-2-Richtlinie erfassten Kreis hinaus zur Anwendung kommen, um die bisherige Strategie eines ganzheitlichen Sicherheitsniveaus für die Behörden im Freistaat fortzuführen und den gestiegenen Anforderungen einer modernen, krisenfesten Verwaltung gerecht zu werden.

Das Gesetz zur Änderung des Sächsischen Informationssicherheitsgesetzes wurde im Juni 2024 – und damit im Berichtszeitraum des letzten Jahresberichts – vom Sächsischen Landtag beschlossen. Die Änderungen traten mit der aus der NIS-2-Richtlinie vorgegebenen Umsetzungsfrist im Oktober 2024 in Kraft und gelten damit seit dem Berichtszeitraum dieses Jahresberichts. Der neu eingefügte § 7 Absatz 4 SächsISichG regelt die Identifizierung staatlicher Stellen als wichtige Einrichtungen der öffentlichen Verwaltung der Regionalebene im Sinne der NIS-2-Richtlinie. Der erstmalige Identifizierungsprozess wurde im Berichtszeitraum abgeschlossen. Insgesamt wurden 20 staatliche Stellen gemäß § 7 Absatz 4 SächsISichG als relevant eingestuft und gemäß § 5 Absatz 1 Satz 3 SächsISichG als Anzahl erstmalig durch den BfIS Land an das Bundesamt für Sicherheit in der Informationstechnik (BSI) fristgerecht gemeldet.

Mit der Implementierung einer Cybersicherheitsstrategie auf Landesebene hat der Freistaat Sachsen die noch offene Verpflichtung aus Artikel 7 der NIS-2-Richtlinie erfüllt. Am 6. Mai 2025

beschloss das Kabinett die Cybersicherheitsstrategie Sachsen[2], mit der erstmals alle Aktivitäten von sächsischen Behörden zum Schutz vor Bedrohungen aus dem Cyberraum gebündelt werden. Zudem benennt sie langfristige Ziele und konkrete Maßnahmen, um die Cybersicherheit im Freistaat Sachsen zu erhöhen. Die Strategie ist das Ergebnis einer engen Zusammenarbeit aller Ministerien unter der Federführung der Sächsischen Staatskanzlei.

Nach der Einleitung werden die rechtlichen und strategischen Rahmenbedingungen in der Cybersicherheitsstrategie erläutert. Darüber hinaus wird das Verhältnis zu anderen Strategien dargestellt. Die neun Handlungsfelder der Cybersicherheitsstrategie Sachsen richten sich nach den Vorgaben der Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien der Innenministerkonferenz und konkreten Einzelanforderungen der NIS-2-Richtlinie. Im Kapitel 3 wird die Zielstellung der Cybersicherheitsstrategie Sachsen dargestellt. Es werden Visionen formuliert, aus denen sich ein Leitbild ergibt: „Der Freistaat Sachsen schützt sich vor Cyberangriffen, unterstützt Wirtschaft und Gesellschaft bei Cybervorfällen durch Bildungs- und Sensibilisierungsangebote und informiert sie zu Lagebild, Präventionsmaßnahmen und Gefährdungen.“ Daran anknüpfend werden Ziele und Maßnahmen festgelegt. Im Kapitel 4 werden ausgehend von einer themenbezogenen Bestandsaufnahme die Handlungsfelder der Cybersicherheitsstrategie beschrieben, mit denen entsprechend des in Kapitel 3 dargestellten Leitbildes die dahinterliegenden Ziele erfüllt werden sollen. Zuletzt wird aufgezeigt, wie der Fortschritt der Maßnahmen überwacht und die Strategie gemäß den Vorgaben der NIS-2-Richtlinie fortgeschrieben werden soll.

Informationssicherheit als zentrales Handlungsfeld der Cybersicherheitsstrategie Sachsen

Das Thema Informationssicherheit ist in der Cybersicherheitsstrategie Sachsen in einem eigenen Handlungsfeld verortet. Im Bereich „Informationssicherheit in der Staatsverwaltung und in den Kommunen“ werden Schwerpunkte in den Themen „Informationssicherheitsmanagement“, „Sensibilisierung und Fortbildung“, „Ausbau der Analyse- und Reaktionskompetenzen im SAX.CERT“, „IT-Notfallmanagement zwischen Land und Kommunen verzahnen“ sowie unter dem Punkt „Rechtlichen Rahmen erneuern“ gesetzt und dazu passende Ziele und konkrete Maßnahmen formuliert. Die Umsetzung der Maßnahmen bezogen auf alle neun Handlungsfelder der Cybersicherheitsstrategie Sachsen wird nach 5 Jahren evaluiert und auf dem Weg dahin jährlich dokumentiert und damit auch in den kommenden Jahresberichten aufgegriffen werden.

2.2 Evaluierung des Sächsischen Informations-sicherheitsgesetzes

Mit dem SächsISichG vom 2. August 2019 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. Dabei ist in § 21 Absatz 1 SächsISichG der Auftrag an die Staatsregierung formuliert, sich alle fünf Jahre mit den Auswirkungen des Gesetzes zu beschäftigen und Vorschläge zur Weiterentwicklung zu unterbreiten,

[2] Cybersicherheitsstrategie Sachsen, https://www.egovernment.sachsen.de/download/Cybersicherheitsstrategie_Sachsen.pdf

indem dem Landtag ein Evaluierungsbericht vorzulegen ist. Am 8. April 2025 wurde der Bericht vom Kabinett behandelt und dem Sächsischen Landtag zugeleitet.[3]

Datengrundlage der Evaluierung waren einerseits die Ergebnisse einer Onlinebefragung mittels Fragebögen im Beteiligungsportal, an der insgesamt 114 staatliche und nicht-staatliche Stellen teilgenommen hatten. Andererseits kamen die Ergebnisse einer Expertenbefragung hinzu, die durch den Beauftragten für Informationstechnologie des Freistaates Sachsen (CIO), den BfIS Land und die kommunalen Spitzenverbände beantwortet wurden. Zudem wurde in den letzten fünf Jahren durch zahlreiche interne Datensätze die Entwicklung der Informationssicherheit dokumentiert. Wichtigstes Ziel der Evaluierung war es, dem gesetzlichen Evaluierungsauftrag vollumfänglich nachzukommen. Neben dem Umsetzungsstand des SächsISichG und den Auswirkungen einzelner Regelungen des Gesetzes wurden auch die Kosten und der Nutzen des Gesetzes sowie mögliche Weiterentwicklungspotentiale des SächsISichG im Evaluierungsbericht dargestellt.

Insgesamt lässt die Evaluierung erkennen, dass mit dem Gesetz die Strukturen der Informationssicherheit gestärkt wurden und sich ein starkes Bewusstsein für die Informationssicherheit innerhalb der verschiedenen Ebenen der Verwaltung entwickelt hat. Der im Gesetz vorgesehene kontinuierliche Verbesserungsprozess mit Evaluierung und Berichterstattung an den Sächsischen Landtag soll nun dazu beitragen, die Informationssicherheit im Freistaat auch in den nächsten fünf Jahren weiter zu stärken. Die zwischenzeitlich im SächsISichG umgesetzten Anforderungen aus der NIS-2-Richtlinie der EU haben zudem eindrucksvoll gezeigt, dass mit dem SächsISichG nicht nur bereits eine Regelung vorlag, in die die Anforderungen der europäischen Ebene gut integriert werden konnten. Das sächsische Gesetz war auch so fortschrittlich und vorausschauend konzipiert, dass es nur an vergleichsweise wenigen Stellen geändert werden musste.

2.2.1 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 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 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:

[3] Bericht über die Evaluierung des Sächsischen Informationssicherheitsgesetzes (SächsISichG), https://www.egovernment.sachsen.de/download/Evaluierungsbericht_SaechsISichG.pdf

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 CIO-Bereich 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), aber forensische Untersuchungen im Auftrag des SAX.CERT durch Dritte durchgeführt.

Das heute extern bei einem Dienstleister eingekaufte Sicherheitsbetriebszentrum (sog. Security Operations Center) soll zukünftig, wie in vielen anderen Bundesländern bereits 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.

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 Absatz 1 SächsISichG genannten 15 besonders wichtigen Behörden, die einen hauptamtlichen BfIS zu bestellen haben. Einige dieser Behörden haben bereits vor mehr als zehn Jahren professionelle Strukturen aufgebaut, während andere diese Rolle erst mit Stellenzuweisungen nach dem Jahr 2019 besetzt hatten.

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 Lenkungsausschuss IT und E-Government (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. 72 %[4] der sächsischen Gemeinden und Verwaltungsgemeinschaften BfIS bestellt. Dieser Aufwuchs von ca. 46 % vor Inkrafttreten des Gesetzes geht auf vielfältige Aktivitäten von BfIS Land im Zusammenwirken mit Akteuren auf der kommunalen Ebene wie den Spitzenverbänden Sächsischer Städte- und Gemeindetag (SSG) und Sächsischer Landkreistag (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 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.

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

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 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

[4] Stand: 14. Oktober 2025

wurden spezielle und detaillierte Regelungen getroffen, die den Einsatz von Systemen zur erweiterten Angriffserkennung ermöglichen. Ohne diese Regelungen bestünden Rechtsunsicherheiten im Umgang mit Kommunikationsdaten. 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 nicht-staatlichen 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 Absatz 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 fünf 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 Evaluierungsberichtes ein. Nichtsdestotrotz wird 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 BSI bei der Analyse des Datenverkehrs sowie die Ausweitung der Meldepflicht bei zumindest erheblichen Sicherheitsvorfällen auf alle Kommunen, auch außerhalb des KDN.

2.3 Revisionen und Anordnungen

Zur Überprüfung der Wirksamkeit der organisatorischen und technischen Maßnahmen nach § 4 Absatz 1 und Absatz 1a SächsISichG kann der BfIS Land gemäß § 5 Absatz 7 SächsISichG eigene Revisionen durchführen. Darüber hinaus kann er gegenüber an das SVN angeschlossenen staatlichen Stellen gemäß § 5 Absatz 3 SächsISichG Anordnungen treffen oder Maßnahmen ergreifen, um Gefahren für die informationstechnischen Systeme, die mit dem SVN verbunden sind, abzuwehren. Maßnahmen, die auch die nicht-staatlichen Stellen betreffen, bedürfen hierbei der

Herstellung des Benehmens mit dem BfIS des KDN (§ 5 Absatz 4 SächsISichG). Im Berichtszeitraum hat der BfIS Land nachfolgende Prüfungen vorgenommen und eine Anordnung im obigen Sinn umgesetzt.

2.3.1 Revisionen

Gemäß § 5 Absatz 7 Satz 4 SächsISichG wurde BfIS Land unterrichtet, dass die EU-Zahlstelle des Staatsministeriums für Umwelt und Landwirtschaft im Berichtszeitraum erfolgreich das zweite Überwachungsaudit für das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz des BSI abgeschlossen hat. Für den nächsten Berichtszeitraum steht die Rezertifizierung an.

BfIS Land auditierte im Berichtszeitraum die Umsetzung verschiedener organisatorischer und technischer Maßnahmen zur Informationssicherheit.

Die Prüfung des ISMS des Staatsbetriebes Sächsische Informatik Dienste wurde im Berichtszeitraum fortgesetzt. Die Fortschritte wurden dem BfIS Land in einem regelmäßigen Turnus vorgestellt.

Im Berichtzeitraum wurde zudem mit der Prüfung des Informationssicherheitskonzeptes Amt24 begonnen.

Im Rahmen der technischen Revisionen wurden das Active Directory überprüft, das aus Sicht der Informationssicherheit eine wichtige Komponente in der Architektur der Landesverwaltung darstellt. Das System ist die zentrale Komponente für die Verwaltung von Nutzern, Rechnern und Berechtigungen und damit regelmäßig Ausgangspunkt für APT-Angriffe (fortgeschrittene, andauernde Bedrohung). Für die Prüfung wurde der realitätsnahe Ansatz eines sogenannten Red-Teaming gewählt. Hierbei verhält sich das Red-Team wie ein echter Angreifer und versucht über Schwachstellen im System die IT zu übernehmen. Die hierbei aufgedeckten Schwachstellen in den Konfigurationen verschiedener Systeme wurden umgehend beseitigt. Dabei wurde ebenfalls festgestellt, dass trotz intensiver Anstrengungen zur Verbesserung der IT-Sicherheit die Detektion von Angriffen weiter verbessert werden muss.

2.3.2 Anordnungen

Im Berichtszeitraum hat der BfIS Land eine Anordnung gegenüber einer staatlichen Stelle getroffen.

Dem BfIS Land und dem SAX.CERT wurde ein Sicherheitsereignis nach § 15 SächsISichG angezeigt. Das Sicherheitsereignis wurde als hochkritisch eingestuft. Mit Unterstützung externer technischer Berater wurden umgehend Maßnahmen ermittelt und als Anordnungen an die zuständige Systembetreuung gegeben. Der Mangel konnte innerhalb kürzester Zeit beseitigt werden. Ein Sicherheitsvorfall im Sinne des § 3 Absatz 5 SächsISichG konnte nicht festgestellt werden.

2.4 Mindeststandards und Rahmenvorgaben

BfIS Land erstellt gemäß § 5 Absatz 6 SächsISichG für die staatlichen Stellen verbindliche Mindeststandards zur Informationssicherheit und legt diese nach Anhörung der AG IS dem LA ITEG zur Entscheidung vor. Im Sinne der Teilziffer 32 e) der Verwaltungsvorschrift der Sächsischen

Staatsregierung zur Regelung des Dienstbetriebes für die Behörden des Freistaates Sachsen (VwV Dienstordnung) kann BfIS Land zudem ressortübergreifende Rahmenvorgaben erstellen.

2.4.1 Mindeststandards

Die Richtlinien und Konzepte legen für organisatorische sowie technische Bereiche verbindliche Mindeststandards zur Informationssicherheit fest und gelten nach Beschluss des LA ITEG grundsätzlich unmittelbar. Die BfIS der Behörden prüfen beschlossene Mindeststandards hinsichtlich einer behördeninternen Konkretisierung und adressatengerechten Veröffentlichung. Im Einzelfall kann ein Mindeststandard auf Antrag des zuständigen BfIS beim BfIS Land zeitlich befristet unterschritten werden.

Derzeit sind insgesamt 14 landesweite Mindeststandards, Richtlinien und darauf aufbauende Konzepte zur Informationssicherheit in Kraft (siehe folgende Tabelle).

Tabelle 1 – Mindeststandards zur Informationssicherheit beim Freistaat Sachsen

Rahmendokument zum ISMS Land	Richtlinie zur Schulung und Sensibilisierung
Richtlinie zur ISMS-Dokumentation	Sensibilisierungs- und Schulungskonzept
Richtlinie Definition der Schutzbedarfs-kategorien	Rahmenrichtlinie zur sicheren Grundkonfiguration für mobile Endgeräte (Smartphone/Tablet)
Richtlinie zur Durchführung von Risikoanalysen	Konzept zur Durchführung von simulierten Phishing-Kampagnen (Phishing-Konzept)
Richtlinie zur Authentifizierung im Nutzerkonto des Landes-AD – AKTUALISIERT	Richtlinie zur Informationssicherheit auf Auslandsreisen – NEU
Richtlinie zur Authentifizierung von Administratoren in Konten des Landes-AD – NEU	Leitlinie IT-Notfallmanagement
Richtlinie zur Löschung und Vernichtung von Datenträgern	Richtlinie IT-Notfallstab (Land)

Den nicht-staatlichen Stellen (kommunale Gebietskörperschaften, Anstalten sowie Stiftungen des öffentlichen Rechts) wird gemäß § 5 Absatz 6 Satz 3 SächsISichG die Anwendung der beschlossenen Mindeststandards empfohlen.

In Zusammenarbeit mit der Sächsischen Anstalt für kommunale Datenverarbeitung (SAKD) wurden im Laufe des Jahres 2025 die Voraussetzungen dafür geschaffen, dass die vom Freistaat Sachsen beschlossenen Mindeststandards und Richtlinien den nicht-staatlichen Stellen zur Verfügung gestellt werden können. Die oben aufgeführten Mindeststandards und Richtlinien werden ab sofort in anonymisierter Form über das Projektportal der SAKD zur Nachnutzung im anpassbaren und nachnutzbaren Word-Format bereitgestellt.

2.4.2 Rahmenvorgaben

Im Berichtszeitraum wurden durch BfIS Land keine ressortübergreifenden Rahmenvorgaben im Sinne von Teilziffer 32 e) der VwV Dienstordnung erlassen. Derzeit sind zwei ressortübergreifende Rahmenvorgaben hinsichtlich der Nutzung privater Endgeräte für dienstliche Zwecke für die Generierung sicherer Einmalpasswörter (sogenannter OTP-Token) sowie für die dienstliche Nutzung der Anwendung Threema Work für IT-notfallrelevante Stellen zur IT-Notfallkommunikation in Kraft.

2.5 Gremienarbeit

Zentrales Gremium der strategischen Informationssicherheit beim Freistaat Sachsen bildet die Arbeitsgruppe Informationssicherheit (AG IS). Gemäß § 10 Absatz 3 SächsISichG leitet der BfIS Land dieses Gremium. Aufgabe der AG IS ist es, den BfIS Land in Fragen der Informationssicherheit zu beraten.

Im Berichtszeitraum fanden insgesamt zwölf Sitzungen der AG IS statt. Es wurden vier Beschlüsse gefasst. Unter den Beschlüssen befinden sich zwei neue sowie eine überarbeitete Richtlinie (siehe Tabelle 1). Die drei Richtlinien wurden gemäß § 5 Absatz 6 SächsISichG dem LA ITEG zum verbindlichen Beschluss für die gesamte Sächsische Staatsverwaltung vorgelegt und im Berichtszeitraum in Kraft gesetzt. Mit der Aktualisierung des bestehenden Sensibilisierungs- und Schulungskonzepts wurde von der AG IS im Berichtszeitraum zudem ein Beschluss in eigener Zuständigkeit gefasst.

In den Sitzungen der AG IS wurden mehrfach Großprojekte wie bspw. SVN NG oder auch ePM.SAX vorgestellt, um die Maßnahmen im Bereich der Informationssicherheit in diesen Projekten zu bewerten. Auch tauschte sich die AG IS regelmäßig zur Anpassung von zentralen Schutzsystemen oder der Änderung von Prozessen im Bereich der Informationssicherheit aus. So wurde die Sperre der automatischen Weiterleitung von E-Mails nach Extern vorbereitet, der zukünftige Umgang mit dynamischen Sperrlisten besprochen und das Beseitigen erkannter Schwachstellen diskutiert. Zudem stand der Einsatz der Deutschen Verwaltungscloud sowie der mögliche Einsatz des BundesMessengers beim Freistaat Sachen auf der Tagesordnung. Darüber hinaus informierte BfIS Land in den jeweiligen Sitzungen zur allgemeinen Lage der Informationssicherheit und zu ausgewählten Sicherheitsereignissen und Sicherheitsvorfällen im Freistaat Sachsen.

Neben der AG IS nimmt BfIS Land beratend an weiteren Gremien wie dem Arbeitskreis für IT und E-Government (AK ITEG), der Arbeitsgruppe Informationstechnische Basisinfrastruktur (AG IBIS), dem Arbeitskreis SVN und dem IT-Kooperationsrat teil. BfIS Land ist zudem Mitglied in der Arbeitsgruppe Informationssicherheit des IT-Planungsrates (AG InfoSic).

2.6 Sensibilisierung und Schulung

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 organisiert BfIS Land seit vielen Jahren die Großveranstaltung INFOSIC mit den sogenannten „Live-Hackings“, die sich ausdrücklich an alle Mitarbeiterinnen und Mitarbeiter von Landes- und Kommunalbehörden richteten. Dabei geht es zum einen darum, vor Gefahren bei der alltäglichen Nutzung von PC, Smartphone und Internet zu sensibilisieren und andererseits

Kompetenzen zur Gefahrenabwehr zu vermitteln. Im Jahr 2024 wurden aufgrund der Corona-Pandemie und ihrer Nachwirkungen nach 2019 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 Mitarbeiter selber organisieren.

Zu den Schulungsmaßnahmen, die sich an die Sensibilisierungsveranstaltungen anschließen, gehört seit gut sechs Jahren das E-Learning-Angebot zur Informationssicherheit am Arbeitsplatz. Es steht allen Mitarbeiterinnen und Mitarbeitern der Staatsverwaltung und der Kommunen nach Selbstanmeldung im E-Learning-Portal zur Verfügung. Bis Ende Juli 2025 haben über 34.000 Nutzerinnen und Nutzer die Teilnahmebescheinigung erworben (bis Juli 2024 waren es über 30.000) und über 28.000 Nutzerinnen und Nutzer den Online-Test zum Sächsischen Informationssicherheitsschein erfolgreich absolviert (bis Juli 2024 waren es über 25.500).

Betrachtet man die Verteilung der Teilnehmenden auf die Behörden im Freistaat, so weisen die Behörden der Staatsverwaltung fast 4.000 Teilnehmer mehr auf als die Kommunen. Von den Kommunen haben jedoch gut 1.000 Bedienstete mehr den Online-Test zum Sächsischen Informationssicherheitsschein absolviert als von den staatlichen Behörden. Die Behörden mit den meisten Teilnehmenden im Berichtszeitraum waren das Sächsische Staatsministerium für Justiz, das Statistische Landesamt und das Sächsische Staatsministerium des Innern. Bei den Kommunen waren es die Landeshauptstadt Dresden und die Landkreise Mittelsachsen und Nordsachsen.

Das bestehende E-Learning-Angebot wird noch im laufenden Jahr durch neue Inhalte ersetzt. Neben dem allgemeinen Modul für alle Mitarbeiterinnen und Mitarbeiter wird künftig ein zusätzliches Modul speziell für die Behördenleitungen bereitgestellt. Hintergrund ist die geänderte Rechtslage im SächsISichG, die ihnen im Zuge der Umsetzung der NIS-2-Richtlinie eine besondere Verantwortung zuweist (§ 4 Absatz 3 SächsISichG). Im Weiteren ist ein drittes Modul geplant, das sich gezielt an Mitarbeiterinnen und Mitarbeiter mit Aufgaben im IT-Bereich richtet.

2.7 Unterstützung für Kommunen

In Deutschland liegt die Verantwortung für die Informationssicherheit grundsätzlich bei jeder Verwaltung selbst. Die Eigenverantwortung der Kommunen gründet auf dem verfassungsrechtlich verankerten Prinzip der kommunalen Selbstverwaltung. Allerdings gewährt das Kommunalverfassungsrecht den Kommunen dabei keine uneingeschränkte Gestaltungsfreiheit. Denn aus ihrer Eigenverantwortung und der Pflicht zur Erfüllung öffentlicher Aufgaben ergeben sich zugleich Sorgfaltspflichten im Bereich der Informationssicherheit.

Der BfIS Land hat frühzeitig erkannt, dass Kommunen bei dieser Aufgabe umfassend unterstützt werden müssen. Deshalb stellt er ihnen – sowohl auf technischer als auch organisatorischer Ebene – kostenlose Leistungen zur Verfügung. Besonders wichtig ist dies, wenn – wie in Sachsen – die Mehrheit der Kommunen in einem gemeinsamen Informationsverbund mit der Staatsverwaltung organisiert ist: So ist das KDN eng an das SVN angebunden. In einem solchen Verbund tragen alle Beteiligten gemeinsame Verantwortung für das Sicherheitsniveau, da Schwächen eines einzelnen Mitglieds die gesamte Gemeinschaft gefährden können. Hier gilt: Das schwächste Glied bestimmt die Sicherheit des Ganzen. Ein Prinzip, dass auch für die Umsetzung des Onlinezugangsgesetzes

(OZG) gilt, bei der vernetzte Verfahren eine zentrale Rolle spielen. Informationssicherheit kann daher nur dann ganzheitlich gewährleistet werden, wenn Land und Kommunen eng zusammenarbeiten und gemeinsam ein angemessenes Schutzniveau sicherstellen.

Der Freistaat Sachsen unterstützt die Kommunen in diesem Zusammenhang im Rahmen seiner rechtlichen und finanziellen Möglichkeiten durch verschiedene Maßnahmen, die auf einer zentralen Webseite „Informationssicherheit in Kommunen“ gebündelt dargestellt sind. Dazu zählen insbesondere die technischen Leistungen des SAX.CERT. Darüber hinaus begleitet BfIS Land die Kommunen seit Jahren etwa bei der Qualifizierung von BfIS sowie bei der Sensibilisierung und Schulung von Beschäftigten (siehe vorheriges Kapitel).

Ein weiteres Angebot ist die seit fast zwei Jahren etablierte Online-Sprechstunde, die nahezu an jedem ersten Freitag im Monat stattfindet. Sie dient dazu, aktuelle Themen der Informationssicherheit und die Angebote des SAX.CERT zu präsentieren sowie konkrete Fragen und Bedarfe der Kommunen aufzunehmen. Gleichzeitig bietet sie den Verantwortlichen, die in ihren Verwaltungen oft als Einzelkämpfer agieren, eine wertvolle Plattform zum Austausch. Auf diese Weise können sie voneinander lernen, Erfahrungen teilen und praktische Unterstützung erhalten.

BfIS Land unterstützt die kommunale Plattform der SAKD für Richtlinien und Best-Practices in der Informationssicherheit

Zur Erhöhung des Niveaus der Informationssicherheit werden den Kommunen nunmehr über die kommunale Plattform der SAKD Richtlinien und Best-Practices in der Informationssicherheit zur Verfügung gestellt. BfIS Land stellt diese, wie im Kapitel Mindeststandards ausgeführt (Tz. 2.4.1), in anonymisierter Form im anpassbaren Word-Format fortlaufend zur Nachnutzung bereit.

BfIS Land veranstaltet mit BSI zweite Roadshow Kommunen zur IT-Sicherheit

Wie bereits bei der ersten Roadshow Kommunen des BSI mit den Ländern im Jahr 2022 war Sachsen auch bei der zweiten Reihe des Formats der Premierenstandort in Deutschland. An der gemeinsamen virtuellen Roadshow von BSI und Sächsischer Staatskanzlei nahmen rund 140 Vertreterinnen und Vertreter sächsischer Kommunen teil. CIO Frau Dr. Dylakiewicz hob in ihrer Eröffnung hervor, dass bereits deutliche Fortschritte bei der Verbesserung der Informationssicherheit erzielt worden seien. Mit dem Informationssicherheitsgesetz und den Unterstützungsangeboten, etwa durch das SAX.CERT, sei ein solides Fundament geschaffen worden.

In einem gemeinsamen Beitrag von BSI, SSG und der Stadt Markranstädt wurde dargestellt, wie die Digital-Lotsen das vom BSI entwickelte Modell „Weg in die Basis-Absicherung“ für die sächsischen Kommunen angepasst haben und seitdem für dessen praktische Umsetzung werben. Der Bürgermeister der Gemeinde Mulda verdeutlichte zudem, dass Informationssicherheit Chefsache ist und selbst kleinere Kommunen in der Lage seien, ihre IT wirksam abzusichern. Weitere Vorträge befassten sich mit IT-Krisenmanagement und dem Einsatz erweiterter Angriffserkennungssysteme. Insgesamt verdeutlichte die Roadshow, dass Informationssicherheit realisierbar ist, wenn alle Akteure zusammenwirken.

2.8 Kooperation mit dem BSI

Eben genannte Veranstaltung fand im Rahmen der seit Ende 2023 bestehenden Kooperationsvereinbarung mit dem BSI statt. Die Kooperationsvereinbarung erstreckt sich über insgesamt acht verschiedene Handlungsfelder: So soll etwa intensiver bei der Cyberabwehr zusammengewirkt, bei IT-Sicherheitsvorfällen unterstützt oder gemeinsam zum Thema Cyber- und Informationssicherheit sensibilisiert werden. Im Berichtszeitraum wurde in den folgenden Kooperationsfeldern zusammengewirkt:

Unterstützung bei Ereignis- und Umfeldanalyse für Rechenzentrums-Neubau

Seit März 2025 unterstützt das BSI bei der Prüfung der baulichen Aspekte (materieller Geheimschutz) für den Rechenzentrums-Neubau mit seiner Expertise. Auch während der eigentlichen Bauphase soll diese Unterstützung fortgesetzt werden.

VerwaltungsCERT-Verbund

Der Freistaat Sachsen und das BSI beteiligen sich aktiv an der Mitarbeit im VerwaltungsCERT-Verbund (VCV) und informieren sich proaktiv über Cybersicherheitsvorfälle. So beteiligt sich das SAX.CERT aktiv am Teilen seiner operativen Ergebnisse im VCV-Chat sowie an den VCV-Arbeitstreffen. Warnmeldungen des BSI werden durch das SAX.CERT an die zuständigen Stellen auf staatlicher und kommunaler Ebene ausgesteuert und je nach Kritikalität auch nachgehalten. Die vom BSI an das Land gesendeten Informationen, Umfragen und Sicherheitshinweise werden je nach Betroffenheit an die BfIS der Kommunen versandt.

Hospitationen

Durch gegenseitige Hospitationen werden Vernetzung und Wissensaustausch in Cybersicherheitsthemen vertieft und gestärkt. Das BSI und der Freistaat Sachsen ermöglichen Hospitationen bei der jeweiligen Stelle. Eine Hospitation durch das SAX.CERT im CERT-Bund wurde im November 2024 durchgeführt.

3 Bericht zu den ergriffenen Maßnahmen nach § 5 Absatz 8 SächsISichG

Zur Gewährleistung von Transparenz und parlamentarischer Kontrolle schreibt § 5 Absatz 8 SächsISichG eine jährliche Berichtspflicht an den Sächsischen Landtag vor. Hintergrund ist u. a. der beim Einsatz von erweiterten Angriffserkennungssystemen mit der Datenverarbeitung verbundene Eingriff in Grundrechte. Diese Berichtspflichten sollen sicherstellen, dass der Landtag regelmäßig über die Anwendung und Auswirkungen der gesetzlichen Befugnisse informiert wird – insbesondere im Hinblick auf Grundrechtseingriffe durch Datenanalysen und Angriffserkennungssysteme. Zum Ausgleich der Grundrechtseingriffe in den §§ 12, 13 des SächsISichG ist BfIS Land verpflichtet, dem Sächsischen Landtag jährlich Bericht über die nach dem Gesetz ergriffenen Maßnahmen zu erstatten – insbesondere über die Datenverarbeitung in bestimmten Fällen, sei es durch das SAX.CERT oder durch andere staatliche oder nicht-staatliche Stellen.

3.1 Berichtspflichten nach § 5 Absatz 8 Nr. 3 bis 9

Die gemäß § 5 Absatz 8 Nummern 3 bis 9 SächsISichG zu übermittelnden Informationen betreffen vor allem statistische Angaben zu konkreten Verarbeitungsfällen personenbezogener Daten im Zusammenhang mit dem Einsatz erweiterter Angriffserkennungssysteme. Diese Systeme kommen mittlerweile vermehrt sowohl beim SAX.CERT als auch bei staatlichen und nicht-staatlichen Stellen zum Schutz der Informationssicherheit zum Einsatz.

Erweiterte Angriffserkennungssysteme ermöglichen die kontinuierliche Überwachung und Analyse sicherheitsrelevanter Daten und setzen sich aus Komponenten wie Intrusion Detection Systemen (IDS), Security Incident and Event Management-Systemen (SIEM) sowie Endpoint-Security-Lösungen mit EDR- oder XDR-Funktionalitäten zusammen. Zusätzlich können diese Systeme durch Analystenteams in sogenannten Security Operations Centern (SOC) ergänzt werden, die sicherheitskritische Ereignisse bewerten und darauf reagieren.

Stellen, die Maßnahmen nach §§ 12 und 13 SächsISichG in eigener Zuständigkeit durchführen, sind verpflichtet, entsprechende Fallzahlen an den BfIS Land zu melden. Die Meldung umfasst sowohl tatsächliche Verarbeitungsfälle als auch sogenannte Nullwerte, die anzeigen, dass keine relevanten datenverarbeitenden Tätigkeiten erfolgt oder gemeldet wurden.

Die Zunahme der gemeldeten Fallzahlen ist auf die verstärkte Verbreitung dieser Systeme bei staatlichen und nicht-staatlichen Stellen zurückzuführen. Insbesondere die verschärfte Bedrohungslage im Cyberraum – geprägt durch gezielte Angriffe auf öffentliche Einrichtungen und die zunehmende Professionalisierung krimineller Akteure – macht eine frühzeitige Erkennung und wirksame Abwehrmaßnahmen unerlässlich. Erweiterte Angriffserkennungssysteme leisten hierzu einen entscheidenden Beitrag und unterstützen zugleich die Einhaltung gesetzlicher Vorgaben zum Schutz personenbezogener Daten.

Zur Erleichterung der gesetzlich vorgeschriebenen Meldungen hat der BfIS Land ein neues Unterstützungsangebot geschaffen. Über das Beteiligungsportal Sachsen wurde eine strukturierte Abfrage bereitgestellt, die eine systematische Erfassung und Übermittlung der Berichtsdaten ermöglicht. Zusätzlich fand eine Informationsveranstaltung statt, in der die Anforderungen der Berichtspflicht erläutert wurden.

Tabelle 2 – Berichtspflichten nach § 5 Absatz 8 Satz 1 Nr. 4 bis 8 SächsISichG

Anzahl der Fälle	SAX.CERT	staatliche Stellen	nicht-staatliche Stellen
der Wiederherstellung des Personenbezuges pseudonymisierter Protokolldaten, § 5 Absatz 8 Satz 1 Nummer 4	0	0	0
der Wiederherstellung des Personenbezuges pseudonymisierter Inhaltsdaten, § 5 Absatz 8 Satz 1 Nummer 5	0	0	0
der manuellen Auswertung von Daten mit Personenbezug gemäß § 13 Absatz 4; § 5 Absatz 8 Satz 1 Nr. 6	635	5	241
der durchgeführten Benachrichtigungen gemäß § 13 Absatz 5, § 5 Absatz 8 Satz 1 Nr. 7	410	5	40
der unterbliebenen Benachrichtigungen gemäß § 13 Absatz 5, § 5 Absatz 8 Satz 1 Nr. 7	225	0	201
der nachgeholten Benachrichtigungen gemäß § 13 Absatz 5, § 5 Absatz 8 Satz 1 Nr. 7	0	0	0
der Übermittlung von Daten gemäß § 13 Absatz 6 und 7, § 5 Absatz 8 Satz 1 Nr. 8	0	0	0

Daten, die den Kernbereich privater Lebensgestaltung gemäß § 13 Absatz 8 SächsISichG betreffen, wurden im Berichtszeitraum weder von einer staatlichen noch nicht-staatlichen Stelle erlangt, § 5 Absatz 8 Satz 1 Nummer 9 SächsISichG.

3.2 Maßnahmen des SAX.CERT gemäß § 6 Absatz 3

Nach § 5 Absatz 8 Nummer 1 SächsISichG ist zu den durch das SAX.CERT getroffenen Anordnungen und ergriffenen Maßnahmen gemäß § 6 Absatz 3 SächsISichG zu berichten. Im Berichtszeitraum hat das SAX.CERT keine eigenen Anordnungen und Maßnahmen nach § 6 Absatz 3 SächsISichG durchgeführt.

3.3 Verarbeitung personenbezogener Daten durch das SAX.CERT gemäß § 6 Absatz 4

Gemäß § 5 Absatz 8 Nummer 2 SächsISichG ist das BfIS Land verpflichtet, dem Sächsischen Landtag jährlich die Anzahl der Fälle zu übermitteln, in denen personenbezogene Daten zu anderen Zwecken verarbeitet wurden als zu demjenigen, zu dem sie ursprünglich erhoben wurden. Grundlage hierfür ist § 6 Absatz 4 SächsISichG, der eine datenschutzrechtliche Ermächtigung zur zweckändernden Verarbeitung personenbezogener Daten darstellt.

Diese Regelung erlaubt es dem SAX.CERT, personenbezogene Daten über den ursprünglichen Erhebungszweck hinaus zu nutzen, sofern dies zur Erfüllung seiner Aufgaben im Bereich der Informationssicherheit erforderlich ist. Die zweckändernde Verarbeitung erfolgt insbesondere zur Erkennung, Analyse und Untersuchung von Sicherheitsvorfällen, wie etwa bei der Auswertung von Schadsoftware, der Identifikation von Sicherheitslücken oder Angriffe auf Computersysteme. Hierzu zählen die Datenverarbeitungen bei Sicherheitsvorfällen (z. B. eigene oder forensische Untersuchungen) oder die Untersuchung von verdächtigen E-Mails.

Im Berichtszeitraum wurden insgesamt 1.092 Fälle dokumentiert, in denen personenbezogene Daten zweckändernd verarbeitet wurden. Diese Zahl umfasst sämtliche Vorgänge, bei denen eine Verarbeitung über den ursprünglichen Erhebungszweck hinaus erfolgte und die im Rahmen der gesetzlichen Aufgabenwahrnehmung des SAX.CERT notwendig waren.

3.4 Sicherheitsmeldungen gemäß §§ 16 und 17

Seit Inkrafttreten des SächsISichG gelten verschiedene Meldepflichten für die staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen sowie Beliehene, die an das SVN oder das KDN angeschlossen sind. Diese Stellen sind nach den §§ 16 und 17 SächsISichG dazu verpflichtet, Sicherheitsvorfälle zu melden.

Die Meldungen haben unverzüglich zu erfolgen, wenn es sich um erhebliche Sicherheitsvorfälle handelt. Mit dem Gesetz zur Änderung des Sächsischen Informationssicherheitsgesetzes wurde der Begriff des erheblichen Sicherheitsvorfalls überarbeitet, um ihn an die europaweite Terminologie anzupassen. Danach ist ein erheblicher Sicherheitsvorfall ein Sicherheitsvorfall, der schwerwiegende Betriebsstörungen der Dienste oder materielle Schäden für die betreffende Einrichtung verursacht hat oder verursachen kann oder Dritte durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann (siehe § 16 Absatz 1 Satz 3 SächsISichG).

Beispiele für zu meldende Sicherheitsvorfälle können sein:

- Funde von installierten oder aktiven Viren auf Client-PCs,
- Ausfall wichtiger Systeme oder Verfahren durch IT-Störungen,
- Datenabfluss durch Malware, Hacking oder Social Engineering,
- Ausnutzung von Schwachstellen in IT-Systemen,
- Verlust dienstlicher Endgeräte oder
- Offenlegung von schützenswerten Informationen durch Fehlkonfiguration von Systemen.

Im Berichtszeitraum wurden dem SAX.CERT über ein im Verwaltungsnetz bereitstehendes Meldeformular insgesamt 99 Sicherheitsvorfälle und Sicherheitsereignisse gemeldet. Dabei wurden 75 Vorfallmeldungen von staatlichen Stellen und 24 Vorfallmeldungen von nicht-staatlichen Stellen verzeichnet. Drei Viertel der Sicherheitsvorfälle gehen damit auf Behörden und Einrichtungen des Freistaates Sachsen zurück.

Im Vorjahreszeitraum wurden dem SAX.CERT lediglich 86 Sicherheitsvorfälle gemeldet. Dies stellt einen Anstieg um 13 Meldungen im Vergleich zum Vorjahreszeitraum von August 2023 bis Juli 2024 dar. Damit wurden im Berichtszeitraum ca. 15 % mehr Sicherheitsvorfälle gemeldet als im Vorjahr. Die bloße Anzahl der Sicherheitsvorfallmeldungen sowie die Meldungen an sich lassen allerdings keine Rückschlüsse auf eine gestiegene Gefährdungslage durch spezielle Angriffsarten oder Ähnliches erkennen.

Die Ursachen der 99 gemeldeten Sicherheitsvorfälle verteilen sich gemäß der Kategorisierung durch das SAX.CERT auf folgende Gründe:

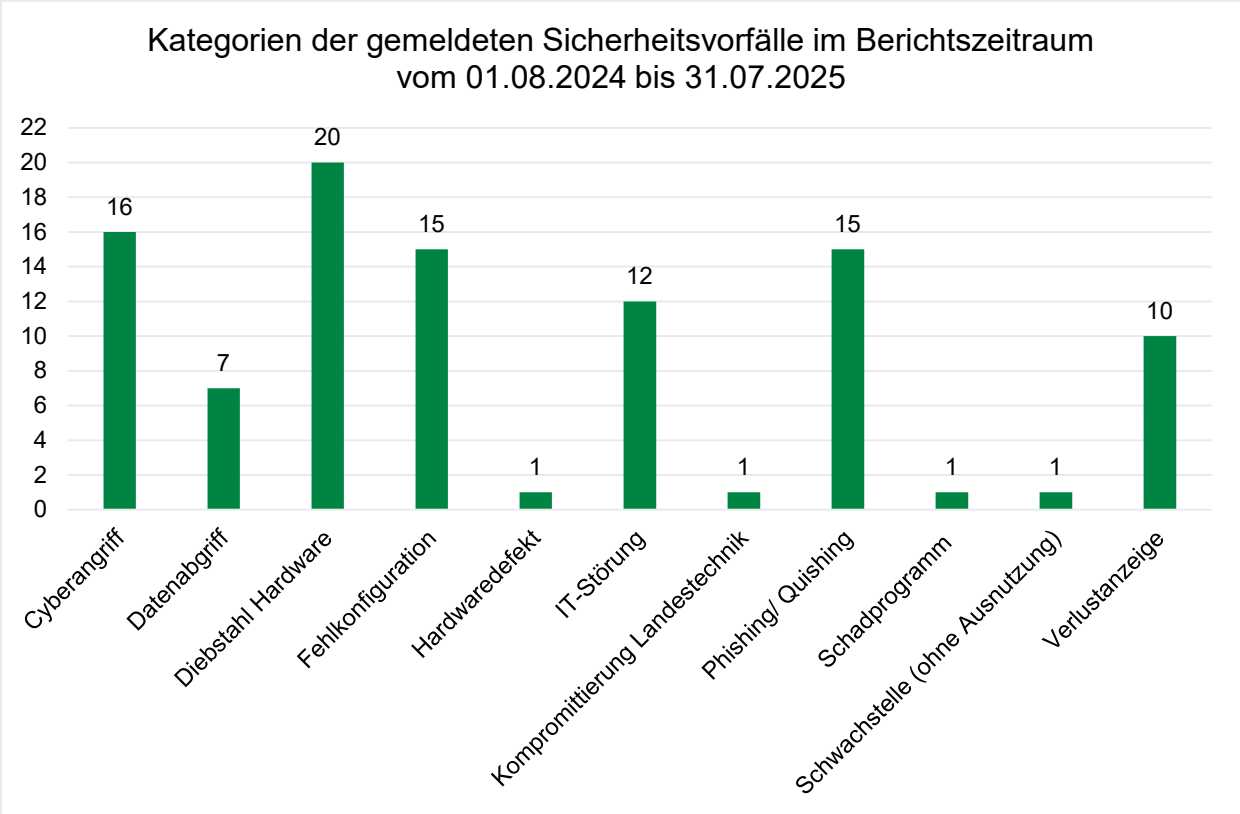

Abbildung 1 – Kategorien der Sicherheitsvorfälle

4 Abbildungs- und Tabellenverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Herausgeber

Sächsische Staatskanzlei

Archivstraße 1

01097 Dresden

Redaktion sowie Gestaltung und Satz

Referat 45: Informations- und Cybersicherheit, Kritische Infrastrukturen, IT-Haushaltsangelegenheiten

Redaktionsschluss

Oktober 2025

Bestellservice

Zentraler Broschürenversand der Sächsischen Staatsregierung

Hammerweg 30, 01127 Dresden

Telefon: +49 351 21036-71 oder -72

Telefax: +49 351 21036-81

E-Mail: publikationen@sachsen.de

www.publikationen.sachsen.de

Hinweis