SÄCHSISCHE STAATSKANZLEI | Freistaat SACHSEN

Jahresbericht Informationssicherheit 2024

des Beauftragten für Informationssicherheit des Landes

Berichtszeitraum: August 2023 – Juli 2024

Inhaltsverzeichnis

1 Einführung

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

Mit dem Sächsischen Informationssicherheitsgesetz (SächsISichG) besteht eine starke rechtliche Basis, die nicht nur die staatlichen Behörden, sondern auch die Kommunen reguliert: So wird die organisatorische Verortung von Beauftragten für Informationssicherheit (BfIS) ebenso festgelegt wie der Einsatz angemessener organisatorischer und technischer Vorkehrungen sowie sonstiger Maßnahmen zur Gewährleistung der Informationssicherheit. Auch die Kommunen sind gesetzlich verpflichtet, zum Beispiel ein Informationssicherheitsmanagementsystem (ISMS) aufzubauen und technische Systeme zur Abwehr von Cyberangriffen zu betreiben bzw. betreiben zu lassen.

Seit Inkrafttreten des 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.

Kernbotschaften des Jahresberichts Informationssicherheit 2023/2024

Sächsisches Informationssicherheitsgesetz übernimmt NIS-2-Anforderungen

Die EU-Richtlinie NIS-2, die seit Januar 2023 in Kraft ist, musste von den Mitgliedsstaaten bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden. Übergeordnetes Ziel der Richtlinie ist es, Unternehmen sowie Institutionen vor Cyberangriffen zu schützen und allgemein die Cybersicherheit in der EU zu modernisieren und auszubauen. Mit der NIS-2-Richtlinie wurde der Anwendungsbereich der Cybersicherheitsregulierung erstmals auf bestimmte Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene, also die Landesverwaltung, ausgedehnt. Die Umsetzung der NIS-2-Richtlinie auf nationaler Ebene ist ein komplexer Prozess, der sowohl die Bundes- und Landesverwaltung als auch die Wirtschaft betrifft und vor Herausforderungen stellt. Es kann daher als großer Erfolg gewertet werden, dass im Freistaat Sachsen die Anforderungen der NIS-2-Richtlinie an die

öffentliche Verwaltung fristgerecht umgesetzt wurden. Sachsen hat als erstes Bundesland in Deutschland die europäischen Vorgaben der NIS-2-Richtlinie für die Landesverwaltung in nationales Recht umgesetzt und in das SächsISichG integriert, um die Cyber-Sicherheit in der öffentlichen Verwaltung zu stärken.

Das Gesetz zur Änderung des Sächsischen Informationssicherheitsgesetzes wurde im Juni 2024 vom Sächsischen Landtag beschlossen. Die Änderungen treten mit der Umsetzungsfrist der NIS-2-Richtlinie im Oktober 2024 in Kraft.

IT der öffentlichen Verwaltung in Sachsen bleibt unter Angriffsdruck von außen

Die Schutzsysteme des Sächsischen Verwaltungsnetzes (SVN) konnten auch im aktuellen Berichtszeitraum eine hohe Anzahl von Angriffen abwehren: Von den über 110 Mio. eingehenden E-Mails wurden bereits 59 % direkt am Internet-Gateway des SVN abgewiesen, da der Verdacht auf Schadsoftware bestand. Von den weiteren Schutzsystemen wurden über 6 Mio. E-Mails als Spam und rund 1,6 Mio. E-Mails vom Reputationsdienst als unseriös markiert. Zusätzlich wurden gut 18.000 Viren im Mailverkehr und 3.000 Viren im Internetverkehr erkannt und blockiert.

Darüber hinaus wurden auch wieder einige gezielte Überlastangriffe (DDoS) auf sächsische Behörden registriert: In diesen Fällen versuchten Hackergruppen, die aus dem Internet erreichbaren Server über einen längeren Zeitraum mit hohem Traffic zu blockieren. Die Schutzsysteme des SVN konnten diese Angriffe zuverlässig abwehren, so dass es nur zu zeitlich sehr begrenzten Einschränkungen kam. Herausragend war ein koordinierter Distributed Denial-of-Service-Angriff (DDoS-Angriff) auf mehrere deutsche Großstädte im Oktober 2023. Der Angriff wurde von den Angreifenden kurzfristig angekündigt. Das Sicherheitsnotfallteam (SAX.CERT) kontaktierte die betroffenen sächsischen Kommunen und informierte über den bevorstehenden Angriff.

Schwachstellen in Software bleiben fortwährende Sicherheitsaufgabe: Beispielhaft dafür stehen die im Frühjahr 2024 bekannt gewordenen Schwachstellen in der Webkonferenz-Software Webex des US-amerikanischen Unternehmens Cisco. Diese Schwachstellen ermöglichten unberechtigten Dritten, Gespräche der Bundeswehr abzuhören und sich auch bei anderen Nutzerinnen und Nutzern (nahezu) unbemerkt in Konferenzsitzungen einzuschalten. Auch wenn die über die Presse ausführlich bekannt gewordenen Vorfälle sich auf andere Webex-Versionen als die im SVN eingesetzte bezogen, wurden mit dem Hersteller umgehend Härtungsmaßnahmen für die Systeme abgestimmt und umgesetzt.

Aber auch der Lieferant kann selbst ein Risiko darstellen: Von einem durch den US-amerikanischen Hersteller CrowdStrike unzureichend geprüften Software-Update einer Cybersicherheitslösung, welches im Juli 2024 weltweit zu erheblichen IT-Ausfällen geführt hat, war die Sächsische Verwaltung zwar nicht betroffen. Dieser Vorfall zeigt aber, dass der Fokus zukünftig auch ganz erheblich auf der Kontrolle der Einhaltung von Sicherheitsmaßnahmen in der Lieferkette von IT-Produkten liegen muss.

Zusammenarbeit stärkt Informationssicherheit

Nach der seit 2018 bestehenden Absichtserklärung zur vertieften Kooperation haben im November 2023 das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Freistaat Sachsen ihr Zusammenwirken auf ein neues verbindlicheres Niveau gestellt und eine Kooperationsvereinbarung unterzeichnet. Grundpfeiler ist eine intensive Zusammenarbeit, die auf einem schnellen und möglichst umfassenden gegenseitigen Informationsaustausch basiert. Im sächsischen Freital unterhält das BSI bereits einen Standort, an dem Bereiche wie 5G-Sicherheit oder digitaler Verbraucherschutz angesiedelt sind. Insgesamt umfasst die Kooperationsvereinbarung acht Handlungsfelder: So soll unter anderem die Zusammenarbeit bei der Cyberabwehr intensiviert, bei IT-Sicherheitsvorfällen unterstützt und gemeinsam für das Thema Cyber- und Informationssicherheit sensibilisiert werden. Sachsen war zu dem Zeitpunkt das sechste Bundesland, mit dem das BSI eine solche Vereinbarung abschloss.

Im Rahmen der Kooperationsvereinbarung wurde die Zusammenarbeit mit der Stadt Chemnitz intensiviert, die durch die Ausrichtung der Europäischen Kulturhauptstadt 2025 erhöhte Anforderungen an die Cybersicherheit in Verbindung mit den Unternehmen und verschiedenen gesellschaftlichen Akteuren vor Ort sieht. Das BSI wurde in die Sicherheitsberatungen zur Großveranstaltung eingebunden und unterstützt die Planungen mit seiner Expertise im Bereich der Cyber- und Informationssicherheit.

2 Gefährdungslage

Die Sicherheit des SVN ist fortwährend verschiedenen und wechselnden Gefährdungen ausgesetzt. Daher gilt es, mögliche Gefährdungen kontinuierlich zu identifizieren, daraus resultierende Risiken zu bewerten und geeignete Maßnahmen zur Risikominderung abzuleiten und umzusetzen. Diese Beobachtung erfolgt durch das SAX.CERT. Das SAX.CERT legt besonderen Fokus auf das SVN sowie das Kommunale Datennetz (KDN) und stellt in diesem Bericht die Erkenntnisse aus dem Zeitraum August 2023 bis Juli 2024 zusammen.

Dabei ist festzustellen, dass sich die Anzahl der versuchten und erfolgreichen Angriffe auf die Sächsische Verwaltung im Vergleich zum Vorjahr kaum verändert hat. Gleichzeitig konnten aber weitere Gefährdungen für die Informationssicherheit identifiziert werden. Beispielhaft hierfür sind:

Angriff auf Microsoft Exchange Online[1]

Bereits zum Ende des letzten Berichtszeitraums wurde bekannt, dass ein kryptographischer Schlüssel von Microsoft von Angreifenden erbeutet und genutzt wurde. Erst im Laufe dieses Berichtszeitraums wurde aber die Tragweite der Zugriffsrechte bekannt. Der kryptographische Schlüssel erlaubte die Erstellung zulässiger Anmeldeinformationen für Microsoft Exchange Onlinedienste und ließ damit Zugriff auf weite Teile der sogenannten Azure-Cloud und die dortigen Exchange-Konten zu. Die US-amerikanische Agentur für Cybersicherheit und Infrastruktursicherheit hat in ihrer Untersuchung erhebliche Versäumnisse seitens Microsoft sowohl in Sicherheitsmechanismen, der Fallaufarbeitung, als auch der Kommunikation festgestellt. Der Vorfall zeigt, dass auch große Anbieter von Cloudleistungen erfolgreich angegriffen werden.

Manipulation der xz-Bibliothek[2]

Ein über mehrere Jahre vorbereiteter Angriff vermutlich staatlicher Akteure hatte das Ziel, einen versteckten Zugang (Backdoor) zu Linux-basierten Betriebssystemen einzurichten. Diese Betriebssysteme werden weltweit insbesondere für Server eingesetzt. Die Backdoor hätte den Angreifenden ungehinderten Zugang zu diesen Servern ermöglicht und damit sowohl Datendiebstahl als auch Manipulation. Sie wurde allerdings kurz vor Übernahme in die Produktivversionen der Betriebssysteme entdeckt und konnte somit keine Wirkung entfalten. Dieser Vorfall zeigt, dass auch Open-Source-Projekte erfolgreich angegriffen werden.

---

[1] https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf (zuletzt abgerufen am 25.09.2024)

[2] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-223608-1032.pdf (zuletzt abgerufen am 25.09.2024)

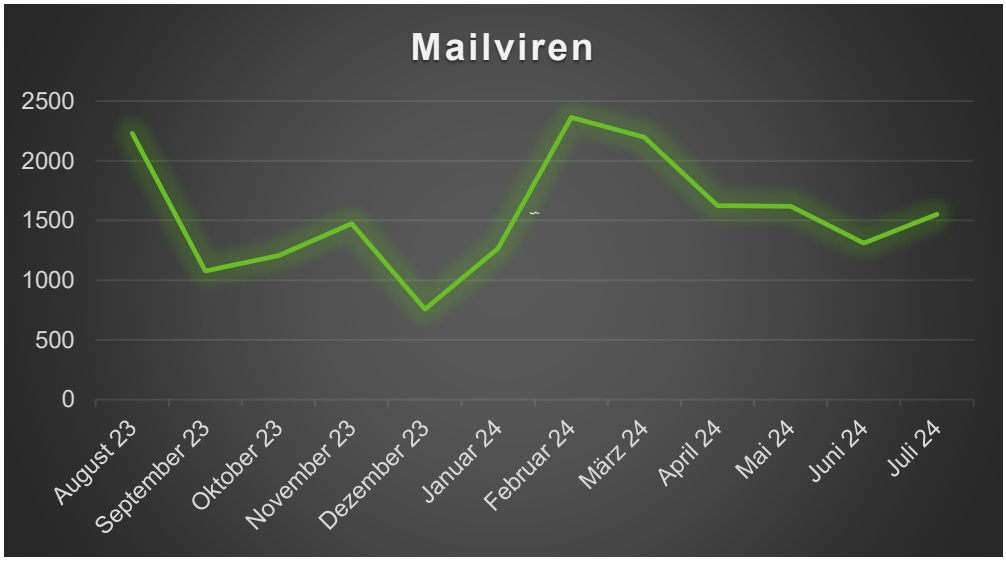
Die Behörden des Freistaates Sachsen waren von keinem dieser Ereignisse betroffen. Jedoch ist festzustellen, dass eine immer komplexer werdende System- und Softwarelandschaft, akribische Angriffsvorbereitungen und letztlich auch der Faktor Mensch zu einer immer komplexer werdenden Gefährdungs- und Bedrohungslage führt. Angriffsvektoren eröffnen sich aus unerwarteten Richtungen. Diese Unvorhersehbarkeit von Angriffen erfordert auch eine ständige Prüfung der Schutzsysteme über eine Schwerpunktüberwachung an den zentralen Übergangspunkten des SVN/KDN zum Internet hinaus, hin zur Überwachung von Auffälligkeiten im Netzverkehr innerhalb des SVN/KDN.

2.1 Lagebild in der Staatsverwaltung

Das SVN ist prinzipiell ein vom Internet unabhängiges internes Netz der Staatsbehörden und hat durch diese Struktur ein vergleichsweise hohes Niveau an Informationssicherheit aufzuweisen. Gleiches gilt für das KDN. Jedoch sind diese Netze natürlich auch mit dem Internet verbunden, um z. B. die Kommunikation zwischen Behörden und Bürgerinnen und Bürgern oder auch Unternehmen und anderen Institutionen zu gewährleisten. Gerade vor dem Hintergrund, dass sich die öffentliche Verwaltung stetig weiter digitalisiert und zunehmend Behördenleistungen auch online abrufbar sind, haben Behörden und ihre IT-Netzwerke immer mehr Verbindungen in das Internet. Da aber gerade aus dem Internet heraus Angriffe auf die IT-Infrastruktur der Verwaltung drohen, kommen leistungsfähige Schutzsysteme in den zentralen Diensten des SVN und KDN zum Einsatz. Diese sichern die Übergänge aus dem internen Netz der Staatsverwaltung von und zum Internet gegen zielgerichtete Bedrohungen ab. Ergänzt werden diese zentralen Schutzsysteme durch dezentrale Virenscanner in den Rechenzentren der Behörden und des zentralen staatlichen IT-Dienstleisters sowie auf den Endgeräten der Bediensteten. Ergänzt wurden diese Schutzsysteme im Berichtszeitraum durch eine Überwachung des Active Directory, dem zentralen System zur Authentifizierung und Autorisierung, welches regelmäßig Ausgangspunkt erfolgreicher Ransomware-Angriffe war.

Zwischen August 2023 und Juli 2024 wurden von über 112 Millionen ankommenden E-Mails (Vorjahreszeitraum: 110 Mio.) rund 66,3 Mio. bzw. 59 % (Vorjahreszeitraum: 67,5 Mio. bzw. 61 %) an der Internetübergangsstelle des SVN direkt abgewiesen, weil sie unter dem Verdacht standen, für das SVN schädlich zu sein. Weitere knapp 6,2 Mio. E-Mails (Vorjahreszeitraum: 5,3 Mio.) wurden von den dezentralen Systemen als Spam-Mail erkannt und entsprechend markiert. Damit lag der Anteil von unerwünschten Nachrichten am Mail-Aufkommen mit gut 64 % knapp unter dem Wert des Vorjahres (66 %).

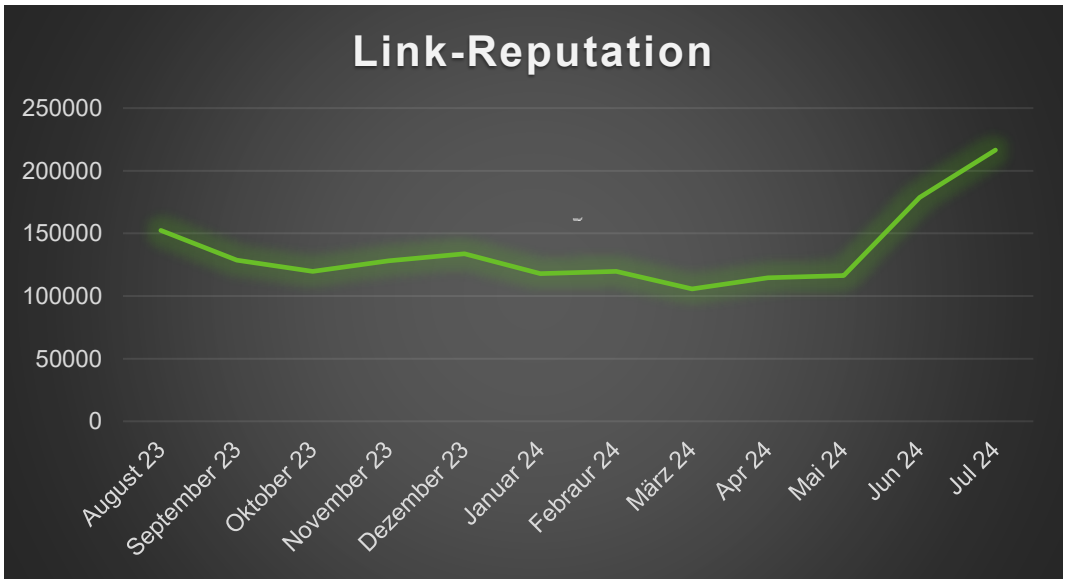
Abbildung 1: Entdeckte Schadprogramme im Mailverkehr



Daneben wurden gut 18.000 Viren im Mailverkehr abgefangen (Vorjahreszeitraum: 30.000).

Seit der Zerschlagung der großen Botnetze von Emotet 2021 und von QBot in 2023 durch Sicherheitsbehörden sind große Phishing-Mail-Wellen eher die Ausnahme geworden. Die Anzahl der Schadmails hat sich fast halbiert. Im August 2023 sowie im Februar 2024 gab es größere Phishing-Mail-Wellen, bei denen bis zu 600 Schadmails am Tag erkannt wurden.

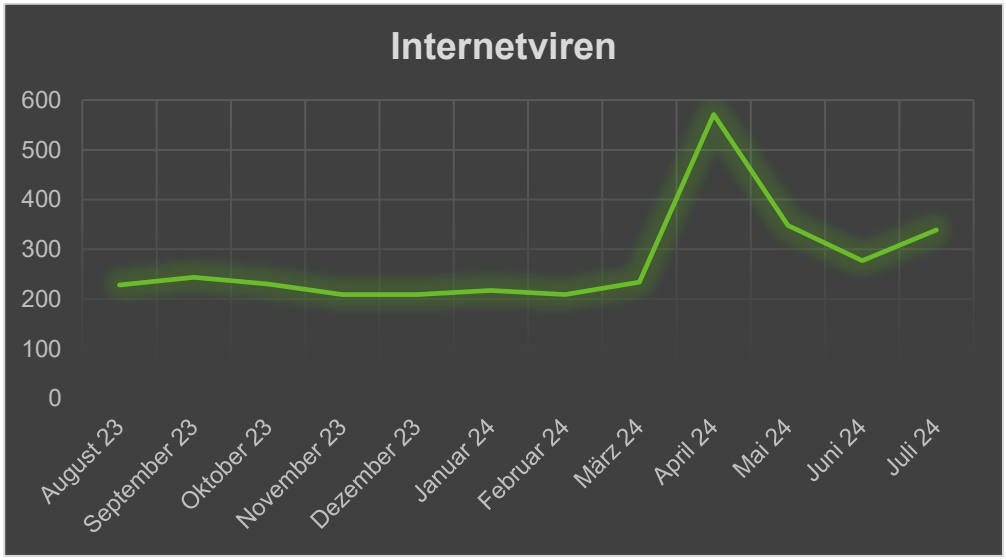
Abbildung 2: Markierte E-Mails mit verdächtigen Links



Ergänzend wurden durch den Dienst zur Prüfung der Reputation von Links eingehender E-Mails bereits rund 1,6 Mio. E-Mails gekennzeichnet und die enthaltenen Links unschädlich gemacht.

Neben verseuchten E-Mails ist auch ein in Webseiten oder Downloads versteckter Schadcode eine der wesentlichen Gefahren für die IT der Verwaltungen. So wurden im Internetverkehr, wenn z. B. Bedienstete auf ihren dienstlichen Geräten eine Webseite aufrufen, über 3.000 Viren erkannt. In den zwölf Monaten zuvor waren es noch knapp 12.000 Viren.

Abbildung 3: Entdeckte Schadprogramme im Internetverkehr



Die Reduzierung der Zahl ist u. a. auf einen Sondereffekt im vorangegangenen Berichtszeitraum zurückzuführen. Dort wurden zeitweise Downloads von intensiv genutzten aber legitimen Webseiten als Schadcode eingestuft.

2.2 Angriffsmethoden und -mittel

Die grundsätzlichen Methoden und Mittel zum Angriff auf das SVN bleiben im Vergleich zum Vorjahr unverändert. So wurden an den Schnittstellen des SVN zum Internet ungezielte, breit im Internet gestreute Tests der Sicherheitsmechanismen des SVN durch unautorisierte Dritte festgestellt. Diese betreffen auch andere Institutionen, Unternehmen oder Privatpersonen. Daneben waren insbesondere gezielte Angriffe u. a. im Bereich des Social Engineerings zu beobachten.

2.2.1 Ransomware

Ransomware ist als APT (Advanced Persistent Threat – fortgeschrittene, hartnäckige Bedrohung) eine der größten Risiken für die Funktionsfähigkeit von IT-Infrastrukturen und damit für die Arbeitsfähigkeit von Behörden. Ransomware sind mit Schadsoftware ausgestattete Trojaner, mit deren Hilfe Angreifende den Zugriff auf Daten oder ganze Computersysteme verhindern können. Dabei werden die Daten verschlüsselt, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Vor der Verschlüsselung werden die Daten der gekaperten Systeme auf IT-Systeme der Hacker kopiert. Die Angreifenden drohen mit der Veröffentlichung von sensiblen Daten bzw. bieten die Daten im Netz zum Verkauf an, sollten die Erpressungsversuche nicht zum Erfolg führen. Ransomware-Angriffe bergen vor allem dann ein enormes Schadpotenzial, wenn sie auf schlecht gesicherte IT-

Systeme treffen (z. B. ohne aktuelle Sicherheitsupdates und Schutzmaßnahmen wie eine Mehr-Faktor-Authentisierung) und die Mitarbeiterinnen und Mitarbeiter z. B. bei der Bearbeitung von E-Mails angehängte Dokumente oder Links im Text nicht richtig auf Vertrauenswürdigkeit einschätzen können. Verfügt die betroffene Behörde am Ende über keine regelmäßige Datensicherung, sind die Daten ohne Entschlüsselungscode nicht mehr nutzbar. Selbst wenn Backups vorliegen, eingespielt werden und die Verschlüsselung damit umgangen werden kann, droht in solchen Fällen immer noch die Veröffentlichung sensibler Daten durch den vorangegangenen Datendiebstahl. Für die öffentliche Verwaltung gilt es, ein solches Szenario unbedingt zu vermeiden.

Deutschlandweit musste eine angespannte Lage in Bezug auf Ransomware festgestellt werden. So waren beispielsweise allein bei dem erfolgreichen Angriff auf die Südwestfalen-IT mehr als 70 angeschlossene Kommunen in Nordrhein-Westfalen über einen längeren Zeitraum massiv beeinträchtigt. Auch eine sächsische Kommune war im Berichtszeitraum von einem Ransomware-Vorfall betroffen. Die betroffenen Systeme waren jedoch nicht am KDN angeschlossen. Die Daten auf den Servern wurden seitens der Kommune bereits verschlüsselt abgelegt, sodass diese für den Angreifenden wertlos waren. Die Systeme konnten innerhalb weniger Tage wiederhergestellt werden. Die Experten des SAX.CERT haben den Vorfall eng begleitet.

2.2.2 Social Engineering und Phishing-Mails

Über den Berichtszeitraum verteilt gab es immer wieder Fälle von Social Engineering, also Betrugsversuchen über E-Mail und/oder Telefonanrufe, um insbesondere Finanztransaktionen auf Konten der Angreifenden zu bewirken. Ein Schwerpunkt bildet dabei der Angriff auf Auftraggeber-/Auftragnehmer-Beziehungen der Staatsverwaltung. Hierbei nutzten die Angreifenden sowohl ihre Kenntnisse über Verwaltungsabläufe, als auch öffentlich zugängliche Informationen über Vertragsbeziehungen zwischen den Staatsbehörden und Dienstleistern.

Positiv zu bewerten ist, dass trotz verschiedener Versuche in diesem Berichtszeitraum kein Schadensfall festzustellen war. Diese positive Entwicklung wird auf eine stärkere Sensibilisierung der im Fokus der Angreifenden stehenden Verwaltungsbereiche zurückgeführt.

Weiterhin ist festzustellen, dass Angreifende vermehrt mittels sogenannter Phishing-Mails versuchen, sich als vertrauenswürdige Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Phishings ist es, im weiteren Verlauf an persönliche Daten, wie z. B. Zugangsdaten, eines Bediensteten zu gelangen oder ihn zur Ausführung einer schädlichen Aktion zu bewegen. In der Folge wird dann beispielsweise Identitätsdiebstahl begangen oder eine Schadsoftware (z. B. Ransomware) installiert. Neben dem ungezielten Phishing mittels massenhaft versendeter E-Mails war im Berichtszeitraum zu beobachten, dass Angreifende gezielt auf tatsächlich erfolgter Kommunikation ein sogenanntes Spear-Phishing aufbauen. Grundlage für diese Angriffe waren schlecht geschützte E-Mail-Postfächer von Dritten, die in Kommunikationsverläufe eingebunden waren. So haben Angreifende Zugriff auf Inhalte und Mailadressen und können diese Informationen gezielt für weitere Angriffsschritte nutzen.

2.2.3 DDoS-Angriffe

Im aktuellen Berichtszeitraum konnten wieder verschiedene gezielte Überlastangriffe mittels Botnetzen detektiert werden. Dabei wurde von Hackergruppen mit hoher Verkehrslast über einen längeren Zeitraum versucht, die vom Internet aus erreichbaren Server zu blockieren. Nach voreingestellter Latenzzeit konnten die Schutzsysteme der im SVN genutzten Internet Service Provider diese Angriffe zuverlässig abwehren. Es kam nur zu geringen Einschränkungen. Als besonders erwähnenswert ist eine koordinierte DDoS-Attacke auf mehrere deutsche Großstädte im Oktober 2023. Der Angriff wurde seitens der Hacker kurzfristig angekündigt. Das SAX.CERT hat sich mit den betroffenen sächsischen Kommunen in Verbindung gesetzt und diese über den anstehenden Angriff informiert.

Die Angriffserkennungssysteme des SVN detektierten in dieser Kategorie auch wieder eine Reihe verschiedener Angriffsmuster und -vektoren, mit denen die aus dem Internet zugänglichen Komponenten und Dienste des SVN auf bekannte Schwachstellen gescannt wurden. Dies ist typisch für Angreifende, die diese Schwachstellen dann kommerziell im Darknet als „Cybercrime as a Service“ zur Ausnutzung anbieten, aber auch für Sicherheitsorganisationen, die gezielt auf Defizite hinweisen, wenn Schwachstellen gefunden wurden.

2.2.4 Schwachstellen in Software

Die Vielzahl eingesetzter Software in der Staatsverwaltung führt dazu, dass täglich Sicherheitslücken bekannt werden, die zu einer Gefährdung des SVN führen können. Die wichtigste Gegenmaßnahme ist hier die möglichst zeitnahe Installation der vom Hersteller zur Verfügung gestellten Korrekturen („Patches“). Das SAX.CERT bietet hierzu allen Behörden der Staats- und Kommunalverwaltung einen kostenlosen Warndienst zu über 2.000 Soft- und Hardwareprodukten an, der per E-Mail gezielt zu den vom Nutzenden ausgewählten Produkten warnt, sobald hier neue Lücken bekannt werden (siehe 4.1). Welche Risiken bei offenen Sicherheitslücken auftreten, zeigt exemplarisch folgender Fall im Berichtszeitraum:

Im Frühjahr 2024 wurden aufeinanderfolgend mehrere Schwachstellen in Cisco Webex bekannt. So gab es Berichte in Medien über abgehörte Gespräche der Bundeswehr sowie zur Möglichkeit der Teilnahme und Einsichtnahme in Metadaten zu Videokonferenzen in Webex. Während ein Teil der Probleme auf fehlerhafte Konfigurationen und individuelles Fehlverhalten mit vertraulichen Informationen zurückzuführen ist, wurden auch tatsächliche Schwachstellen bekannt. Mit dem Hersteller wurden umgehend Härtungsmaßnahmen für die Systeme abgestimmt und die Behörden dafür sensibilisiert, die Webkonferenzen datensparsam zu konfigurieren und z. B. die Teilnahme nur über geschützte Kommunikationskanäle zu ermöglichen.

3 Tätigkeitsbericht des Beauftragten für Informationssicherheit des Landes

Der BfIS Land ist laut SächsISichG unter anderem für die Erstellung des ISMS 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 der Behörden bei der Erfüllung ihrer Aufgaben.

Um dies leisten zu können, stellt er einen Rahmenvertrag zu Beratungsleistungen in der Informationssicherheit zur Verfügung, aus dem die staatlichen Stellen Beratungs- und Unterstützungsleistungen abrufen können. Schwerpunkte des Rahmenvertrages sind Beratungen darauf spezialisierter Firmen zur Erstellung von Informationssicherheitskonzepten, zur Implementierung eines ISMS sowie zu technischen Aspekten der Informationssicherheit. Zur Gewährleistung hinreichender Transparenz ist der BfIS Land zur jährlichen Berichterstattung über seine Tätigkeit an den Landtag verpflichtet.

3.1 Revisionen und Anordnungen

Zur Prüfung der Wirksamkeit des ISMS und des Standes der Erfüllung der Mindeststandards darf BfIS Land gemäß § 5 Absatz 7 SächsISichG Auskünfte verlangen und eigene Revisionen durchführen. Gegenüber an das SVN angeschlossenen staatlichen Stellen kann er 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 Anordnungen im obigen Sinn umgesetzt.

3.1.1 Revisionen

BfIS Land auditierte im Berichtszeitraum die Umsetzung verschiedener technischer Maßnahmen. So wurden durch das SAX.CERT zwei Scans der Konfiguration und Sicherheitseinstellungen vom Landesverzeichnisdienst durchgeführt. Dabei Identifiziertes wurde den Verantwortlichen zur Behebung mitgeteilt und die Abarbeitung durch das SAX.CERT kontrolliert.

Die EU-Zahlstelle des Staatsministeriums für Energie, Klimaschutz, Umwelt und Landwirtschaft hatte sich im Berichtszeitraum der regelmäßigen jährlichen Prüfung durch das BSI unterzogen. Das Prüfergebnis wurde gemeinsam mit BfIS Land ausgewertet und Maßnahmen abgestimmt.

Weiterhin wurde das ISMS des Staatsbetriebes Sächsische Informatik Dienste geprüft. Dabei getroffene Feststellungen werden auch hier durch die Verantwortlichen nachgearbeitet und durch den BfIS Land nachgehalten.

3.1.2 Anordnungen

Im Berichtszeitraum mussten zwei Anordnungen durch den BfIS Land getroffen werden, die dem Schutz des SVN/KDN dienten. Zum einen wurde eine Netztrennung angeordnet, um das KDN vor den Auswirkungen eines Vorfalles in einer sächsischen Kommune zu schützen. Nach Behebung des Vorfalles wurde die Netztrennung wieder aufgehoben.

Zum weiteren wurden Prüfungs- und Risikominderungsmaßnahmen gegenüber einer staatlichen Stelle angeordnet, um die Eskalation eines Sicherheitsereignisses zu einem Sicherheitsvorfall zu verhindern. Ein Schaden war hier nicht eingetreten.

3.2 Mindeststandards und Rahmenvorgaben

Gemäß § 5 Absatz 6 SächsISichG erstellt BfIS Land verbindliche Mindeststandards zur Informationssicherheit für die staatlichen Stellen und legt sie nach Anhörung der Arbeitsgruppe Informationssicherheit dem Lenkungsausschuss IT- und E-Government (LA ITEG) zur Entscheidung vor. Die Arbeitsgruppe Informationssicherheit (AG IS) unterstützt den BfIS Land dabei. Den nicht-staatlichen Stellen, zuvorderst den Kommunen, wird die Anwendung der Mindeststandards empfohlen. Im Berichtszeitraum wurden in der Arbeitsgruppe Informationssicherheit drei neue Richtlinien und die Aktualisierung einer bestehenden Leitlinie gemeinsam erarbeitet. Diese und zwei weitere Richtlinien aus dem Vorjahreszeitraum wurden durch den LA ITEG als verbindliche Mindeststandards für die Staatsverwaltung beschlossen. Zudem wurde von der AG IS ein Beschluss in eigener Zuständigkeit gefasst:

Richtlinie: ISMS-Dokumentation

Dokumente, die im Rahmen des übergreifenden ISMS des Freistaates Sachsen erstellt, bearbeitet und verwaltet werden, müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein. Die Richtlinie ISMS-Dokumentation beschreibt Mindestanforderungen an den Aufbau und die Gliederung der Dokumente des ISMS Land sowie zu deren Lenkung. Der einheitliche Aufbau der Dokumente dient der einfacheren Handhabung und dem besseren Verständnis. Die Vorgaben zur Kennzeichnung gewährleisten ein schnelles Wiederauffinden der Dokumente und die Anforderungen an das Änderungsmanagement stellen eine regelmäßige Aktualisierung im Sinne der kontinuierlichen Verbesserung sicher. Die Anforderungen an die ISMS-Dokumentation orientieren sich an den Vorgaben der BSI-Standards 200-1 sowie 200-2.

Richtlinie: Durchführung von Risikoanalysen

Eine Risikoanalyse im Kontext der Informationssicherheit hat die Aufgabe, relevante Gefährdungen für den Informationsverbund zu identifizieren und die daraus möglicherweise resultierenden Risiken abzuschätzen. Ziel ist es, die Risiken durch angemessene Gegenmaßnahmen auf ein akzeptables Maß zu reduzieren, die Restrisiken transparent darzustellen und das Gesamtrisiko systematisch zu steuern. Die Richtlinie zur Durchführung von Risikoanalysen stellt diesbezüglich einen Mindeststandard dar und beschreibt einen einheitlichen und strukturierten Ansatz zur Methodik von Risikoanalysen. Sie dient der Schaffung eines gemeinsamen Verständnisses für den Prozess der Risikoanalyse und stellt sicher, dass relevante Faktoren im Rahmen der Durchführung von Risikoanalysen berücksichtigt werden. Die neue Richtlinie orientiert sich an den Vorgaben des BSI-Standards

200-3. Sie ersetzt und erweitert die Richtlinie „Risikoanalyse: Maßstäbe und Begriffe“ aus Juni 2019, die noch auf dem alten BSI-Standard 100-3 basierte.

Leitlinie IT-Notfallmanagement (Land)

Die bereits im Jahr 2022 vom LA ITEG freigegebene Leitlinie zum IT-Notfallmanagement (Land) hat im Kontext der LÜKEX 2023 (siehe 3.7) eine Fortschreibung erfahren. Die Leitlinie definiert wichtige Begriffe und beschreibt im Kern die Rollen und Zuständigkeiten zum Aufbau einer geeigneten Organisation zur IT-Notfallvorsorge und IT-Notfallbewältigung auf Ebene des Freistaates Sachsen. Die im Rahmen der LÜKEX 2023 identifizierten Verbesserungspotenziale wurden inhaltlich in die Leitlinie eingearbeitet. So prüft nun vor Ausrufung eines landesweiten IT-Notfalles durch den Beauftragten für Informationstechnologie des Freistaates Sachsen (CIO) ein sogenanntes Kernteam, ob bei kritischen Lagen tatsächlich ein IT-Notfall vorliegt, was zur Konstituierung des IT-Notfallstabes Land führen würde. Zudem wurden Bezüge zum zwischenzeitlich verabschiedeten BSI-Standard 200-4 zum Business Continuity Management hergestellt.

Richtlinie: Schulung und Sensibilisierung

Angesichts der zunehmenden Digitalisierung der Verwaltung und den damit einhergehenden Risiken für Angriffe auf die IT-Systeme ist eine verstärkte und strukturierte Wissensvermittlung der Bediensteten zur Informationssicherheit erforderlich. Die Richtlinie greift diesen Bedarf auf, definiert unterschiedliche Zielgruppen und beschreibt die Anforderungen an Schulungs- und Sensibilisierungsinhalte für diese Zielgruppen. Das Sensibilisierungs- und Schulungskonzept benennt konkrete Maßnahmen und Angebote zur Schulung und Sensibilisierung im Kontext der Informationssicherheit, die durch behörden- und ressortspezifische Vorgaben, entsprechend dem Arbeitsumfeld der Beschäftigten, ergänzt werden müssen.

Richtlinie: IT-Notfallstab (Land)

Die Richtlinie IT-Notfallstab regelt die personelle Besetzung des IT-Notfallstabes Land, das konkrete Verfahren zur Konstituierung und Auflösung sowie die Aufgaben und Handlungsbefugnisse im IT-Notfall. Zudem dokumentiert die Richtlinie die Regeln für die Stabsarbeit. Die Richtlinie wurden unter Beteiligung der IT-Notfallbeauftragten der Ressorts erarbeitet und mit den Erkenntnissen aus der LÜKEX 2023 (siehe 3.7) final abgeglichen, bei der das Kernteam des IT-Notfallstabes erstmals aufgerufen worden war, ergänzt um die Vertreter der übenden Ressorts. Die Richtlinie IT-Notfallstab stellt einen Ausfluss der Leitlinie IT-Notfallmanagement dar, welche konkrete Vorgaben zum Aufbau einer schnellen und effektiven IT-Notfallbewältigungsorganisation im IT-Notfall festlegt.

Identifizierungskonzept für die Sächsische Staatsverwaltung

Um die Vorgaben der NIS-2-Richtlinie durch den Freistaat Sachsen vollständig umzusetzen, wird neben der Änderung des SächsISichG (siehe 7.1.1) ein sogenanntes Identifizierungskonzept erforderlich. In den Anwendungsbereich der NIS-2-Richtlinie können Einrichtungen der öffentlichen Verwaltung des Freistaates Sachsen als wichtige Einrichtungen fallen, die nach einer risikobasierten Bewertung Dienste erbringen, die Auswirkungen auf kritische wirtschaftliche oder gesellschaftliche Tätigkeiten haben könnten. Um diese Einrichtungen förmlich identifizieren zu können, wurde ein

landeseigenes Identifizierungskonzept erarbeitet, welches sich am Beschluss 2023/39 des IT-Planungsrates vom 3. November 2023 orientiert.

Die obersten Staatsbehörden werden auf der Grundlage des erarbeiteten Identifizierungskonzeptes – einem „Top-Down-Ansatz“ folgend – verpflichtet, die in ihren jeweiligen Geschäftsbereichen betroffenen staatlichen Stellen förmlich zu identifizieren und dem BfIS Land zu übermitteln. Der Inhalt der Übermittlung ist gesetzlich festgelegt und umfasst den Namen, die Anschrift und aktuellen Kontaktdaten des BfIS sowie die IP-Adressbereiche der staatlichen Stellen. Die erstmalige Identifizierung nehmen die obersten Staatsbehörden zum 17. Januar 2025 und danach alle zwei Jahre vor. Die Anzahl der identifizierten staatlichen Stellen ist gemäß Artikel 3 Absatz 5 der NIS-2-Richtlinie bis zum 17. April 2025 an die Europäische Kommission zu übermitteln.

Rahmendokument zum übergreifenden Informationssicherheitsmanagementsystem

Zentraler Baustein des ISMS Land bildet das sogenannte Rahmendokument zum übergreifenden ISMS, welches den Rahmen für den Aufbau und die Weiterentwicklung des übergreifenden ISMS Land setzt und die Schnittstellen zu den ISMS der staatlichen Stellen beschreibt. Zusätzlich werden im Rahmendokument in den vier Teilprozessen Dokumentenmanagement, Aufrechterhaltung und Verbesserung, Kompetenzmanagement sowie Incident Management Leitlinien, Richtlinien und Konzepte beschrieben, die im ISMS Land mindestens zu entwickeln sind, um die Informationssicherheit beim Freistaat Sachsen sicherzustellen und schrittweise auszubauen.

Rahmenrichtlinie – Sichere Grundkonfiguration für mobile Endgeräte (Smartphone/Tablet)

Im Berichtszeitraum wurde von der AG IS in eigener Zuständigkeit eine Änderung an der Rahmenrichtlinie Sichere Grundkonfiguration für mobile Endgeräte (Smartphone/Tablet) verabschiedet. Einige Vorgaben waren nicht mehr zeitgemäß, sodass diese einer Überarbeitung bedurften. So wurde die Anlage zur Rahmenrichtlinie, welche die Mindestanforderungen an die Grundkonfiguration mobiler Endgeräte beim Freistaat Sachsen beschreibt, an wenigen Stellen überarbeitet, um das Handling der Anwender mit mobilen Endgeräten zu verbessern.

Weitere Rahmenvorgaben

Der BfIS Land hat im Berichtszeitraum eine ressortübergreifende Rahmenvorgabe nach Nr. 32 e) VwV Dienstordnung erlassen. Diese erlaubt ausgewählten Bediensteten im Freistaat Sachsen für Notfallsituationen die Nutzung privater Endgeräte für dienstliche Zwecke. Dazu ist eine bestimmte Softwarelösung auf dem mobilen Endgerät der Bediensteten zu installieren, mit der ein redundanter Kommunikationskanal genutzt werden kann, falls das SVN nicht zur Verfügung stehen sollte.

3.3 Gremienarbeit

Auf Landesebene hält der BfIS Land den Vorsitz der Arbeitsgruppe Informationssicherheit. Um eine angemessene Informationssicherheit in den staatlichen Behörden zu realisieren, ist ein landesweites ISMS auf Basis der jeweils geltenden BSI-Standards aufzubauen. Dieses landesweite ISMS verzahnt die ISMS auf Ebene der staatlichen Behörden. Die AG IS ist Austausch- und Beratungsgremium bei der Erarbeitung von landesweiten Richtlinien und Standards. Im Berichtszeitraum trafen sich die BfIS der Ressorts und die weiteren Teilnehmer der AG IS zu insgesamt elf Sitzungen: Der

Sitzungsturnus wurde im März 2023 auf monatlich geändert. Damit kommt die AG IS seit April 2023 in der Regel monatlich zusammen – wobei sich Sitzungen in Präsenz und per Webkonferenz abwechseln.

Gemäß § 5 Abs. 6 SächsISichG brachte BfIS Land im Berichtszeitraum in den drei Sitzungen des Lenkungsausschusses IT- und E-Government, dem Koordinierungsgremium auf Amtschefebene für ressortübergreifende Entscheidungen zu Fragen der IT und zum E-Government der obersten Staatsbehörden, sowie auch im Umlaufverfahren die in Kapitel 3.2 benannten Mindeststandards ein. Diese wurden durch das Gremium als ressortübergreifende Mindeststandards beschlossen. Darüber hinaus informierte BfIS Land in den jeweiligen Sitzungen zur allgemeinen Lage der Informationssicherheit und zu ausgewählten Sicherheitsereignissen sowie Sicherungsmaßnahmen.

Neben diesen zwei wesentlichen Gremien für die Erstellung und verbindliche Beschließung von Mindeststandards in der Informationssicherheit ist BfIS Land zudem an weiteren Gremien beteiligt und informiert dort regelmäßig über seine Tätigkeit oder bringt die Interessen aus Sicht der Informationssicherheitsorganisation vor, z. B. im Arbeitskreis IT und E-Government, im Arbeitskreis SVN oder auch in der Arbeitsgruppe Informationstechnische Basisinfrastruktur.

In Bezug auf die Verwaltung außerhalb der staatlichen Stellen berichtet BfIS Land im IT-Kooperationsrat regelmäßig den kommunalen Spitzenverbänden Sächsischer Städte- und Gemeindetag und Sächsischer Landkreistag zur Bedrohungslage in Sachsen. Zudem informiert er auf Einladung des Sächsischen Landkreistages die Arbeitsgruppe der BfIS der Landkreise und kreisfreien Städte regelmäßig über wichtige strategische oder operative Themen der Informationssicherheit.

3.4 Sensibilisierung und Fortbildung

Viele der im Kapitel 2.2 dargestellten Angriffsmethoden und -mittel benötigen für ihren Erfolg neben unsicheren Systemen immer auch die ungewollte Mitwirkung des Menschen als Nutzenden der Informationstechnik. In diesem Bewusstsein konzentrieren sich Cyberkriminelle stark auf den Faktor Mensch und nicht nur auf technische Schwachstellen. So werden beispielsweise an die Bediensteten der Staatsverwaltung täglich Unmengen schädlicher E-Mails verschickt. Auch wenn ein großer Teil davon bereits an der Grenze des SVN oder von behördeneigenen dezentralen Schutzsystemen zurückgewiesen wird, gibt es auch E-Mails, die nicht als schädlich erkannt werden. Die Bediensteten sind in diesem Fall die letzte Verteidigungslinie. Sie benötigen Anhaltspunkte, um mögliche Gefahren zu erkennen. Nur wenn es gelingt, den Bediensteten das Wissen und die Sensibilität zu vermitteln, die Angriffsversuche zu erkennen, können sie die Angriffe abwehren und ggf. Daten ihrer Behörde schützen bzw. das Funktionieren ihrer IT gewährleisten. Daher sind und bleiben Sensibilisierung und Schulung wesentliche Maßnahmen zur Erhöhung der Informationssicherheit.

Sowohl das SächsISichG als auch das IT-Grundschutz-Kompendium des BSI beschreiben, dass die Sensibilisierung der IT-Anwenderinnen und -Anwender eine elementar wichtige Sicherheitsmaßnahme für den täglichen Umgang mit IT-Systemen darstellt. Dies bedeutet zunächst, dass ein Problembewusstsein für die Bedrohungslage und die Risiken für die Informationssicherheit geschaffen werden muss. Darauf aufbauend ist es dann Ziel und Herausforderung zugleich, eine Verhaltensän-

derung hin zu einem sicheren Umgang mit IT zu erreichen. Da die wenigsten Verwaltungsmitarbeiterinnen und -mitarbeiter IT-Experten sind, kann das notwendige Wissen am besten über einfache Regeln und nachvollziehbare Sicherheitsmaßnahmen vermittelt werden.

3.4.1 E-Learning zur Informationssicherheit

Das E-Learning-Angebot zur Informationssicherheit am Arbeitsplatz, das seit nunmehr fast fünf Jahren allen Mitarbeiterinnen und Mitarbeitern der Staatsverwaltung und der Kommunen nach einfacher Selbstanmeldung im E-Learning-Portal zur Verfügung steht, konnte auch im Berichtszeitraum einen weiteren Anstieg der Teilnehmerzahlen verzeichnen. Bis Ende Juli 2024 haben über 30.000 Nutzerinnen und Nutzer die Teilnahmebescheinigung erworben (bis Juli 2023 waren es über 26.000) und knapp 25.500 Nutzerinnen und Nutzer den Online-Test zum Sächsischen Informationssicherheits-Schein erfolgreich absolviert (bis Juli 2023 waren es über 22.000).

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 Absolventinnen und Absolventen des Online-Tests liegen die Kommunen leicht vorne. Die Behörden mit den meisten Teilnehmenden im Berichtszeitraum waren in der Staatsverwaltung die Justiz, die Landesdirektion und das Umweltministerium, bei den Kommunen waren es Dresden, Hoyerswerda, Torgau und der Landkreis Nordsachsen.

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 Mitarbeiterinnen und Mitarbeiter 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 SächsISichG). Im Laufe des kommenden Jahres soll zudem als drittes Modul ein E-Learning für Mitarbeiterinnen und Mitarbeiter mit Aufgaben im IT-Bereich angeboten werden.

3.4.2 Sensibilisierung Phishing

Zu den E-Learning-Angeboten stellen weitere Sensibilisierungen und Tests zu besonderen Angriffsmethoden eine sinnvolle Ergänzung dar. Insbesondere, wenn sie es schaffen, den Bediensteten im Rahmen seines Arbeitsalltages mit den Herausforderungen der Informationssicherheit zu konfrontieren. Deshalb konzipierte BfIS Land mit einem Rahmenvertragspartner eine Social Engineering Kampagne, mit der die Resilienz der Bediensteten auf Phishing E-Mails getestet wird. So wurden im Dezember 2023 an die Mitarbeiterinnen und Mitarbeiter einer Behörde eine vermeintliche E-Mail des Behördenleiters mit einer Einladung zu einer Weihnachtsfeier versandt – allerdings mit einer gefälschten Absenderadresse von außerhalb des Verwaltungsnetzes. Auch wenn circa die Hälfte der Bediensteten die Einladung sofort als gefälscht einschätzte, wurden in den ersten Stunden nach Zustellung in nicht unerheblichem Umfang die Links in der E-Mail angeklickt, systemtechnisch gesperrte Inhalte manuell aktiviert oder auch technisch in SPAM-Ordner einsortierte E-Mails wieder in den Posteingang verschoben. Abschluss der Kampagne war eine Auswertung in einem Online-Video, in dem auf typische Merkmale gefälschter E-Mails hingewiesen wurde. Das Konzept zur Durchführung solcher Kampagnen stellt BfIS Land allen staatlichen Behörden zur Nachnutzung bereit.

3.4.3 Sensibilisierung von Führungskräften

Auf Einladung der Hochschule und des Fortbildungszentrums Meißen sowie des Sächsischen Städte- und Gemeindetages trug BfIS Land bei einer Bürgermeisterveranstaltung in Meißen im Juni 2024 zur Informationssicherheitslage vor. Etwa 50 Bürgermeisterinnen und Bürgermeister sächsischer Kommunen informierten sich unter dem Titel „Informationssicherheit in den Kommunen: Perspektiven, Anforderungen und Unterstützung aus Sicht der Staatsverwaltung“, wie die Staatsverwaltung die Kommunen bei der Umsetzung der Anforderungen an die Informationssicherheit unterstützt. Aber auch, welchen Beitrag die Kommunen selbst zur Erfüllung dieser Anforderungen leisten müssen und welche Verantwortung dafür die Behördenleitung trägt.

Im Juni 2024 nahm der BfIS Land an einer Dienstberatung der obersten Führungsebene des Staatsministeriums für Regionalentwicklung (SMR) unter dem Motto Cyber- und Informationssicherheit teil. Nach einem Vortrag eines Experten des Landesamtes für Verfassungsschutz zu den Erkenntnissen im Bereich Spionage und Desinformation erläuterte BfIS Land die Informationssicherheitslage innerhalb der Staatsverwaltung und ging auf aktuelle Risiken, Angriffsmuster sowie diesbezüglich getroffene technische bzw. organisatorische Maßnahmen zur Absicherung des Verwaltungsnetzes ein. Der BfIS des SMR ergänzte die Sensibilisierung der Hausspitze um die im SMR selbst umgesetzten bzw. geplanten Projekte im Bereich der Informationssicherheit.

3.4.4 Fortbildungen für BfIS

Mit dem seit Mitte 2019 bestehenden SächsISichG ist die Professionalisierung der Informationssicherheitsorganisation in der Staatsverwaltung und in den Kommunen spürbar vorangeschritten. Das lässt sich nicht nur an den Zahlen der gemeldeten BfIS und ihrer Stellvertreter in den Behörden ablesen (siehe 6.2 und 6.3), sondern auch daran, dass es auch ISMS-Teams gibt, in denen die damit einhergehenden Tätigkeiten sinnvollerweise auf mehrere Schultern verteilt sind. Dadurch besteht in den Behörden ein erhöhter Fortbildungsbedarf. BfIS Land fragt diesen Bedarf regelmäßig ab und finanziert im Rahmen seiner haushalterischen Möglichkeiten die Ausrichtung von Fortbildungsmaßnahmen. Im Berichtszeitraum wurden sowohl zwei Seminare "IT-Grundschutz-Praktiker" nach BSI-Curriculum für BfIS aus der Kommunalverwaltung als auch zwei solcher Seminare für BfIS bzw. Beteiligte an ISMS-Teams aus der Staatsverwaltung ausgerichtet, womit insgesamt knapp 60 Teilnehmerinnen und Teilnehmer für ihre Tätigkeiten fortgebildet wurden. Fast alle schlossen die Fortbildung mit der Qualifizierung zum „IT-Grundschutz-Praktiker“ nach den Prüfungskriterien des BSI ab.

3.5 Unterstützung für die Kommunen

Grundsätzlich ist in Deutschland jede Verwaltung für ihre Informationssicherheit selbst verantwortlich. Diese Eigenverantwortung der Kommunen beruht nicht zuletzt auf dem verfassungsrechtlichen Grundsatz der kommunalen Selbstverwaltung. Allerdings lässt das Kommunalverfassungsrecht den Kommunen keine unbegrenzte Gestaltungsfreiheit. Denn aus der Eigenverantwortung der Kommunen und ihrer Verpflichtung zur Erfüllung bestimmter öffentlicher Aufgaben ergeben sich auch kommunale Sorgfaltspflichten im Bereich der Informationssicherheit. BfIS Land hat frühzeitig erkannt, dass es angezeigt ist, den Kommunen möglichst viele unterstützende Leistungen – sei es im technischen oder organisatorischen Bereich – kostenlos anzubieten.

Dies ist insbesondere dann geboten, wenn sich – wie in Sachsen – die überwiegende Zahl der Kommunen in einem gemeinsamen Informationsverbund mit der Staatsverwaltung befindet: So ist das KDN eng mit dem SVN verknüpft. Innerhalb dieses Informationsverbundes besteht eine gemeinsame Verantwortung für das Sicherheitsniveau, da Defizite bei einem Verbundmitglied Auswirkungen auf andere Verbundmitglieder haben können – das schwächste Glied in der Kette bestimmt das Sicherheitsniveau. Ähnliches gilt für die Ebenen übergreifenden Verfahren im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG): Auch hier geht es um Informationsnetze. Daher gilt: Die ganzheitliche Gewährleistung der Informationssicherheit kann nur erfolgreich bewältigt werden, wenn Land und Kommunen eng zusammenarbeiten und gemeinsam zur Herstellung und Aufrechterhaltung eines angemessenen Sicherheitsniveaus beitragen.

Der Freistaat Sachsen stellt den Kommunen deshalb zur Verbesserung ihrer Informationssicherheit im Rahmen seiner rechtlichen und finanziellen Möglichkeiten verschiedene Unterstützungen und Anreize zur Verfügung, die auf einer zentralen Webseite zum Thema „Informationssicherheit in Kommunen“ dargestellt sind.[3] Hierzu zählen in erster Linie verschiedene technische Unterstützungsleistungen des SAX.CERT, wie in Kapitel 4 beschrieben. Aber auch BfIS Land unterstützt die Kommunen seit mehreren Jahren z. B. bei der Fortbildung von Informationssicherheitsexperten, wie in Kapitel 3.4.4 genannt.

Zudem richtet BfIS Land seit knapp zwei Jahren an fast jedem ersten Freitag im Monat eine Online-Sprechstunde zur IT-Sicherheit 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 Einzelkämpfende in ihren jeweiligen Behörden agieren, die Möglichkeit geben, sich untereinander zu vernetzen und ggf. von bereits vorhandenen Erfahrungen oder konkreten Hilfestellungen anderer zu profitieren. So wurde im Berichtszeitraum u. a. über die Erfahrungen einer sächsischen Kommune bei der Beteiligung am Pilot-Projekt des BSI zum neuen Einstiegsprogramm in den IT-Grundschutz mit den Namen „Wege in die Basis-Absicherung“ informiert. Eine andere Kommune stellte ihre Erfahrungen mit einem Tool zur Ermittlung des Entwicklungsstandes ihres ISMS vor. Zudem wurden die Vertreter der Kommunen regelmäßig über den Stand der Umsetzung der NIS-2-Richtlinie in Deutschland informiert und die möglichen Auswirkungen auf die Kommunen erläutert.

3.6 Kooperationsvereinbarung mit dem BSI

Am 22. November 2023 haben das BSI, vertreten durch seine Präsidentin Claudia Plattner, und der Freistaat Sachsen, vertreten durch CIO Staatssekretär Prof. Thomas Popp, eine Kooperationsvereinbarung unterzeichnet. Mit der Vereinbarung heben beide Partner ihren Austausch auf ein neues Niveau. Grundpfeiler ist dabei eine intensive Kooperation, die auf einem schnellen und möglichst umfassenden gegenseitigen Informationsaustausch basiert. Im sächsischen Freital unterhält das BSI bereits einen Standort, in dem Bereiche wie 5G-Sicherheit oder der Digitale Verbraucherschutz

[3] https://www.egovernment.sachsen.de/informationssicherheit-in-den-kommunen.html (zuletzt abgerufen am 25.09.2024)

angesiedelt sind. 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. Sachsen war zu dem Zeitpunkt das sechste Bundesland, mit dem das BSI eine solche Vereinbarung geschlossen hat.

In den acht Monaten bis zum Ende des Berichtszeitraumes wurden in den folgenden Kooperationsfeldern die ersten konkreten Vorhaben begonnen:

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 leitet das SAX.CERT an die zuständigen Stellen auf staatlicher und kommunaler Ebene weiter. Die vom BSI an das Land gesendeten Informationen, Umfragen, Sicherheitshinweise werden je nach Betroffenheit an die BfIS der Kommunen weitergeleitet. Informationen, die das SAX.CERT vom BSI erhält, werden nur unter Berücksichtigung der Geheimhaltungsvereinbarungen geteilt.

Sensibilisierungsvorträge

Das BSI unterstützt circa zweimal im Jahr den Freistaat Sachsen durch themenspezifische Sensibilisierungsvorträge, die sich an alle BSI-Zielgruppen richten können. Demnach haben sich einige Vertreter des BSI mit einem Vortrag und der Teilnahme an der Podiumsdiskussion bei der Auftaktveranstaltung „Digital? Aber sicher!“ im Rahmen der sächsischen Roadshow Cybersicherheit in Dresden am 16. Oktober 2023 eingebracht. Weitere angedachte Formate für Vorträge des BSI sind IT-Gremien der Staatsverwaltung als auch auf kommunaler Ebene.

Informationssicherheitsmanagementsystem

Im Umfeld der Kulturhauptstadt Europas Chemnitz 2025 (KHE 2025) werden für die Stadt Chemnitz und den Freistaat Sachsen in Verbindung mit Unternehmen und verschiedenen gesellschaftlichen Akteuren vor Ort erhöhte Anforderungen an die Cybersicherheit gesehen. Das BSI wird in die Sicherheitsberatungen zur Großveranstaltung KHE 2025 eingebunden und unterstützt mit seiner Expertise im Bereich der Cyber- und Informationssicherheit bei den Planungen. Im Berichtszeitraum hat die Stadt Chemnitz unter Beteiligung aller an der KHE 2025 beteiligten Behörden und Einrichtungen mit dem BSI der Stadt und BfIS Land Workshops zum ISMS durchgeführt. Daneben findet insbesondere eine Qualitätssicherung der Dokumente des ISMS der KHE 2025 durch das BSI statt.

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 für November 2024 vereinbart.

3.7 LÜKEX 2023

Die in regelmäßigem Abstand in Deutschland stattfindende länder- und ressortübergreifende Krisenmanagementübung (LÜKEX) für den Bevölkerungsschutz soll das gemeinsame Krisenmanagement von Bund und Ländern auf strategischer Ebene verbessern. Zuletzt gab es Übungen zu den Szenarien „Gasmangellage in Süddeutschland“ und „Sturmflut an der deutschen Nordseeküste“. Die ursprünglich bereits für 2022 vorgesehene und aufgrund des Angriffs Russlands auf die Ukraine verschobene Übung zum Thema „Cyberangriff auf das Regierungshandeln“ wurde nunmehr im September 2023 durchgeführt.

In Vorbereitung, Durchführung und Auswertung dieser LÜKEX waren verschiedene Organe der Informationssicherheit der Sächsischen Staatsverwaltung aktiv eingebunden. Ausgangslage des bundesweit gültigen Szenarios war ein Cyber-Angriff auf staatliche IT-Infrastrukturen, der zu Störungen und Ausfällen von Geschäftsprozessen und Verwaltungsverfahren führte. Ziel der Übung war es, trotz dieser Störungen und Ausfälle die Staats- und Regierungsfunktionen aufrechtzuerhalten. Der Übungszeitraum umfasste mehrere Tage im September 2023.

BfIS Land konzipierte die thematischen Teile zur Informationssicherheit im sächsischen Szenario und trug als Experte bei der Auftaktplanbesprechung vor. An den beiden aktiven Übungstagen der LÜKEX 2023 war BfIS Land gemeinsam mit weiteren BfIS der übenden Ressorts Teil der Übungssteuerung und stellte Übungseinlagen für den aufgrund der fiktiven Krisenlage aufgerufenen Verwaltungsstab der Staatsregierung bereit. Das SAX.CERT steuerte zusätzlich Lageberichte ein.

Zusätzlich zum bundesweiten Übungsansatz wurde die seit Januar 2022 gültige Leitlinie IT-Notfallmanagement mit dem fiktiven Ausruf eines IT-Notfalles und der Aktivierung des IT-Notfallstabes Land praktisch umgesetzt und zugleich die Richtlinie IT-Notfallstab auf Praktikabilität getestet. Die hierbei gewonnenen Erkenntnisse flossen in die Fortschreibung der Richtlinie ein.

4 Sicherheitsangebote des SAX.CERT

Neben den ständigen Leistungen des SAX.CERT können die Behörden und Gerichte des Freistaates Sachsen (staatliche Stellen) sowie die seiner Aufsicht unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (nicht-staatliche Stellen) kostenfrei weitere Dienstleistungen auf Anfrage in Anspruch nehmen. Die Nutzung dieser Dienstleistungen wird allen Stellen empfohlen, um die Informationssicherheit der eigenen Institution und des Freistaates Sachsen weiter zu stärken.

4.1 Schwachstellenwarndienst

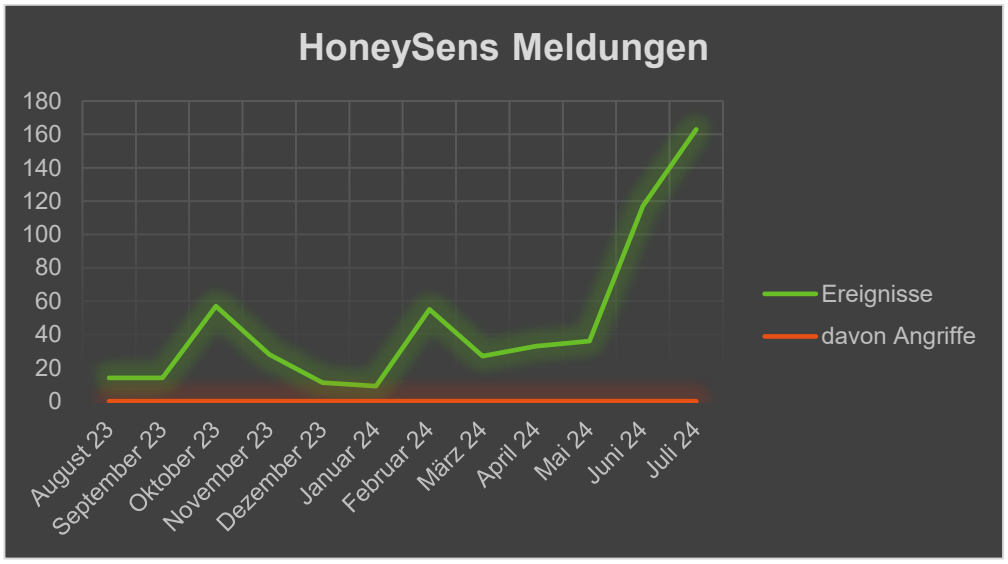
Mit dem Schwachstellenwarndienst (Vulnerability Advisory Service „dCERT“) stellt das SAX.CERT in Zusammenarbeit mit einem technischen Dienstleister tagesaktuelle Informationen zu Schwachstellen und Sicherheitslücken in IT-Systemen zur Verfügung. Über das SAX.CERT kann kostenfrei ein eigenes Nutzerkonto angelegt werden, mit dem sich die Kundin oder der Kunde aus aktuell mehr als 2.000 Hard- und Softwareprodukten eine individuelle Zusammenstellung auswählen kann. Wird für eines der ausgewählten Produkte eine neue Sicherheitslücke bekannt, versendet das Portal automatisch eine Warn-E-Mail mit ausführlichen Details und Maßnahmenempfehlungen zu dieser Schwachstelle an den betreffenden Nutzenden. Der Warndienst wurde Stand Juli 2024 von 308 Abonnenten im Freistaat Sachsen aktiv genutzt und damit von 28 Abonnenten mehr als im Vorjahreszeitraum.

4.2 HoneySens – Einbruchssensor

HoneySens ist eine Sicherheitslösung zur Erkennung von Hackerangriffen in internen Netzwerken, bestehend aus Sensoren zur Überwachung des Netzwerkes sowie einer zentralen Serverinstanz, an die die Sensoren verdächtige Zugriffsversuche melden. Interessierte können beim SAX.CERT kostenlos Sensoren beantragen, die anschließend im eigenen Netzwerk betrieben werden können. Bei sicherheitsrelevanten Zugriffen wird die Nutzerin oder der Nutzer per E-Mail und visuell über die Sensoren alarmiert. Damit kann schneller auf Angriffe reagiert bzw. das Vorgehen des Angreifenden besser nachvollzogen werden. Im Juli 2024 waren insgesamt 46 Sensoren (+6 zum Vorjahr) im produktiven Einsatz, 21 davon in der Staatsverwaltung und 25 in den Kommunen. Ein verifiziertes Eindringen in IT-Systeme wurde durch das System nicht detektiert.

Der Ausschlag der HoneySens Meldungen im Juni und Juli 2024 lässt sich damit erklären, dass im Mai 2024 zwei neue HoneySens Sensoren in Betrieb genommen wurden. Die Sensoren haben dabei Standard-Netzwerkverkehr als ungewöhnlich erkannt und damit Meldungen produziert, die als „false positive“, d. h. ungefährlich, einzustufen sind.

Abbildung 4: Zugriffe auf den Sensor HoneySens



4.3 Identity Leak Checker

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet, z. B. bei Newsletter-Betreibern, Online-Shops und Reisedienstleistern. Ein Großteil der gestohlenen Angaben wird anschließend in Darknet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen. Mit dem Identity Leak Checker bietet das SAX.CERT in Zusammenarbeit mit dem Hasso-Plattner-Institut einen individuellen Dienst zur Überprüfung von E-Mail-Adressen des Freistaates Sachsen auf die Betroffenheit derartiger Leaks an, mit dem alle Maildomains der Staatsverwaltung ständig überwacht werden. Auf Antrag können über das SAX.CERT weitere Mail-Domains in den Dienst aufgenommen werden, was im Berichtszeitraum von 42 Nutzenden (+7 zum Vorjahr) außerhalb der Staatsverwaltung wahrgenommen wurde.

4.4 Sicherheitsprüfung Webseiten

Bereits seit 2017 werden regelmäßig Internetseiten der Staats- und Kommunalverwaltung durch das SAX.CERT auf veraltete Software und bekannte Schwachstellen getestet. Derzeit befinden sich circa 6.400 Internetseiten des Freistaates und der Kommunen in der Überwachung des SAX.CERT. Beim Auftreten schwerwiegender Sicherheitslücken werden die betroffenen Webseitenbetreiber durch das SAX.CERT informiert. Bei den Kommunen erfolgt dies in der Regel über die KDN GmbH, soweit dem SAX.CERT kein direkter Ansprechpartner bekannt ist.

Innerhalb des letzten Berichtszeitraumes wurden anfangs noch 7.400 Internetseiten überwacht. Der Rückgang von 7.400 auf 6.400 überwachte Internetseiten lässt sich dadurch erklären, dass im Oktober 2023 insgesamt 1.160 Internetseiten aufgrund von Nichterreichbarkeit aus der Überwachung durch das SAX.CERT entfernt wurden. Im Gegenzug wurden im Laufe des Berichtszeitraumes immer wieder neue Domänen in die Überwachung aufgenommen, sodass die Zahl der überwachten Domänen in Summe zwar sank, jedoch der Anteil der Domänen, die mit einer Wertung versehen werden konnten, um etwa 13 % anstieg. Die Anzahl der als sicher eingestuften Internetseiten konnte

im Vergleich zum Vorjahresbericht um 4 % erhöht werden. Die Anzahl der als bedenklich eingestuften Internetseiten ging indes um circa 22 % zurück. Internetseiten, die die schlechteste Sicherheitsbewertung erhielten, konnten zwischenzeitlich auf null reduziert werden. Weisen Webseiten die schlechteste Bewertung auf, werden die Zuständigen unmittelbar aufgefordert, Sicherheitsmängel abzustellen.

4.5 Passwort-Checker

Als Sensibilisierung für die Mitarbeiterinnen und Mitarbeiter der Staatsverwaltung bietet das SAX.CERT einen Passwort-Checker auf seiner Internetseite an. Er soll Mitarbeiterinnen und Mitarbeitern dabei helfen zu überprüfen, ob ihr Passwort eine Mindestsicherheit besitzt. Dabei wurde diese Anwendung speziell so konzipiert, dass alle Berechnungen lokal im Browser über JavaScript durchgeführt werden und das eingegebene Passwort somit nicht an Dritte weitergeleitet wird. Auch wurde der Programmcode bewusst nicht verschleiert, um eine leichte Nachvollziehbarkeit und Transparenz zu gewährleisten. Ein Passwort gilt als sicher, wenn es 100 Punkte oder mehr erreicht. Der SAX.CERT Passwort-Checker ist nur aus dem SVN und KDN erreichbar.

5 Bericht zu den ergriffenen Maßnahmen laut SächsISichG

Zur Kompensation der Grundrechtseingriffe ist der BfIS Land zur jährlichen Berichterstattung der nach dem Gesetz ergriffenen Maßnahmen, u. a. der Datenverarbeitung in bestimmten Fällen, sei es durch das SAX.CERT oder durch andere staatliche wie auch nicht-staatliche Stellen, an den Sächsischen Landtag verpflichtet.

5.1 Berichtspflichten nach § 5 Absatz 8

Die meisten der Informationen nach § 5 Absatz 8 Nummern 1-10 SächsISichG beziehen sich auf statistische Angaben zu bestimmten Fällen der Verarbeitung v. a. personenbezogener Daten im Zuge der Tätigkeiten des SAX.CERT sowie der staatlichen und nicht-staatlichen Stellen zum Schutze der Informationssicherheit. Die Übermittlung etwaiger Fälle hat durch die Behörden an den BfIS Land zu erfolgen, sofern sie Maßnahmen nach §§ 12 und 13 SächsISichG in eigener Zuständigkeit ausüben. Nullwerte weisen aus, dass von den Behörden keine solchen datenverarbeitenden Tätigkeiten vorgenommen oder gemeldet wurden.

Der deutliche Anstieg der Anzahl von Fällen der nicht automatisierten Verarbeitung von Daten gemäß § 13 Absatz 4 SächsISichG bei nicht-staatlichen Stellen ist darauf zurückzuführen, dass im Berichtszeitraum bei einer Hochschule deutlich mehr Verarbeitungen gemäß § 12 Absatz 1 SächsISichG als im Vorjahr durchgeführt wurden, um einen Verdacht auf Gefahren durch Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitungen bestätigen oder widerlegen zu können.

Tabelle 1: Anzahl von Fällen der Bearbeitung von Daten nach § 5 Absatz 8

Art der Datenverarbeitung	SAX.CERT	staatliche Stellen	nicht-staatliche Stellen
Anzahl von Fällen der nicht automatisierten Auswertung, der personenbezogenen Verarbeitung und der Wiederherstellung des Personenbezuges pseudonymisierter Daten bei Protokolldaten gemäß § 13 Absatz 2	472	0	2
Anzahl von Fällen der Speicherung und der Auswertung von Inhaltsdaten und Wiederherstellung des Personenbezuges pseudonymisierter Daten gemäß § 13 Absatz 3	299	0	0
Anzahl von Fällen der nicht automatisierten Verarbeitung von Daten gemäß § 13 Absatz 4	2	1	126
Anzahl der durchgeführten, unterbliebenen sowie nachgeholten Benachrichtigungen gemäß § 13 Absatz 5	0	0	0
Anzahl von Fällen der Übermittlung von Daten gemäß § 13 Absatz 6 und 7	0	0	0
Umgang mit unzulässig erlangten Daten, die den Kernbereich privater Lebensgestaltung betreffen, gemäß § 13 Absatz 8	0	0	0
Anzahl von gemäß §§ 15 bis 17 gemeldeten Sicherheitsereignissen und Sicherheitsvorfällen	-	63	23

5.2 Maßnahmen des SAX.CERT gemäß § 6 Absatz 3

§ 6 Absatz 3 SächsISichG stellt die zentrale Befugnisnorm des SAX.CERT dar, um die Abwehr von Gefahren für die Sicherheit der IT des SVN und des KDN zu gewährleisten. Daher darf es zur Erfüllung seiner Aufgaben gegenüber den an das SVN bzw. KDN angeschlossenen staatlichen und nichtstaatlichen Stellen erforderliche Anordnungen treffen oder Maßnahmen ergreifen, um die Gefahren für die informationstechnischen Systeme etwa durch Schadprogramme, Sicherheitslücken, unbefugte Datennutzung oder unbefugte Datenverarbeitung durch Dritte zu erkennen und abzuwehren.

Im Berichtszeitraum wurden keine Anordnungen durch das SAX.CERT erlassen. Im Rahmen der gefahrenabwehrenden Maßnahmen wurden an die Ressorts 15 Warnmeldungen abgesetzt. Zwölf Warnmeldungen wurden auch an die gemeldeten BfIS der Kommunen versandt.

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

Das SAX.CERT hat im Berichtszeitraum in 4.695 Fällen personenbezogene Daten gemäß § 6 Absatz 4 SächsISichG verarbeitet. Das bedeutet einen abermaligen Rückgang, dieses Mal um 1.301 Fälle (-22 %) im Vergleich zum letzten Berichtszeitraum.

Dabei handelt es sich in allen Fällen um E-Mails mit Schadsoftware, die von den zentralen Virenscannern des SVN ausgefiltert wurden und zu denen das SAX.CERT nähere personenbezogene Informationen beim Betreiber der zentralen Dienste des SVN angefordert hat. Insbesondere wurden dabei die E-Mail-Adresse des Absendenden und des Empfangenden sowie der Inhalt der Betreffzeile der verseuchten E-Mail angefordert, an das SAX.CERT übermittelt und von diesem verarbeitet. In einem Teil der Fälle wurde zusätzlich der Name des als Schadsoftware eingeordneten E-Mail-Anhanges verarbeitet.

Wenn sich aus diesen Informationen nähere Verdachtsfälle auf neuartige Schadsoftware mit besonderer Gefährdung des SVN ergaben, wurden die Ressorts gebeten, auch die E-Mail-Texte und die erweiterten Sendeinformationen (E-Mail-Header) einzelner E-Mails bereitzustellen. Diese Bereitstellung erfolgte dann auf freiwilliger Basis seitens der Ressorts; eine Durchsetzung unter Berufung auf das Gesetz erfolgte nicht. Die von den Ressorts bereitgestellten Daten wurden in anonymisierter Form teilweise zur Warnung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Staatsverwaltung sowie für Lageberichte verwendet.

Die datenschutzrechtliche Rechtsgrundlage für die beschriebenen Datenverarbeitungen durch das SAX.CERT findet sich in § 6 Absatz 4 SächsISichG. Dieser Absatz regelt die Verarbeitung personenbezogener Daten zum Zwecke der Sammlung, Auswertung oder Untersuchung von Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in den informationstechnischen Systemen und der dabei beobachteten Vorgehensweise oder zur Unterstützung oder Beratung zu Fragen der Informationssicherheit. Das SAX.CERT kann dadurch die mutmaßlich mit Schadcode behafteten E-Mails eingehend analysieren.

5.4 Maßnahmen zur Gefahrenabwehr nach §§ 12, 13

§§ 12 und 13 SächsISichG sind die zentralen Befugnisnormen für den Betrieb von Angriffserkennungssystemen durch die staatlichen und nicht-staatlichen Stellen sowie die Speicherung und Auswertung der mit diesen Systemen erhobenen Daten. Ausdrücklich räumt § 12 SächsISichG diese Befugnis auch dem SAX.CERT ein.

Im Berichtszeitraum wurden nach obiger Beschreibung durch das SAX.CERT geblockte Zugriffe des zentralen Proxy-Logs ausgewertet, gemeldete E-Mails eingehend nach Schadcode analysiert sowie die zentralen Mailvirenscanner-Logs ausgewertet.

Daneben ist seit Januar 2021 ein sogenanntes Security Information and Event Management (SIEM) für das SVN im Einsatz, welches vom SAX.CERT betreut wird. Das operative Vorgehen sieht vor, dass der SIEM-Dienst die Log-Daten aus angebundenen kritischen Netzsegmenten überwacht, verschiedene Ereignisse miteinander korreliert und nach konfigurierten Regeln Alarme auslöst. Die

konfigurierten Regeln werden als „Use Cases“ (deutsch: Anwendungsfall) bezeichnet. Ein klassischer „Use Case“ könnte z. B. ein „Brute-Force“-Angriff auf einen Server mithilfe eines Admin-Accounts sein.

Das Monitoring auf Sicherheitsereignisse erfolgt dabei nach einem 24x7 Betriebsmodell in einem Security Operations Center (SOC), welches die automatisierten Meldungen vorprüft und aufbereitet. Die aufbereiteten Meldungen werden vom SAX.CERT bewertet und die notwendigen Prozesse aktiviert, um die Bedrohungslage einzudämmen und Gegenmaßnahmen zu ergreifen. Unter Umständen werden dabei auch Informationen mit betroffenen Behörden geteilt, während die Koordination des Falles immer beim SAX.CERT verbleibt.

5.5 Sicherheitsmeldungen gemäß §§ 16 und 17

Mit Inkrafttreten des SächsISichG gelten verschiedene Meldepflichten für die staatlichen und nichtstaatlichen 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 unverzüglich zu melden, wenn diese:

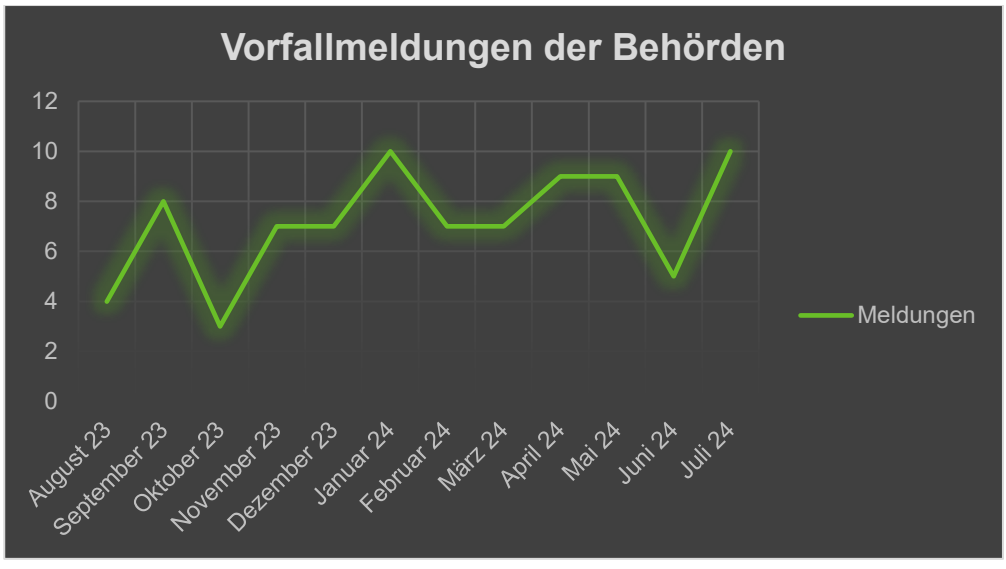
- zu einer erheblichen Beeinträchtigung der Schutzziele geführt haben oder
- behördenübergreifend zu einer erheblichen Beeinträchtigung der Schutzziele führen können.

Beispiele für derartige Sicherheitsvorfälle sind:

- Funde von bereits installierten/aktiven Viren auf Clients,
- Ausfall wichtiger Systeme oder Verfahren,
- Datenabfluss durch Malware, Hacking oder Social Engineering.

Im Berichtszeitraum wurden dem SAX.CERT über ein Meldeformular 86 Sicherheitsvorfälle und Sicherheitsereignisse gemeldet. Dabei waren 63 Meldungen der staatlichen Stellen und 23 Meldungen der nicht-staatlichen Stellen zu verzeichnen. Dies stellt einen beachtlichen Anstieg von 21 Meldung im Vergleich zum Vorjahreszeitraum dar. Die Meldungen für sich genommen lassen allerdings keine Rückschlüsse auf eine gestiegene Gefährdungslage durch spezielle Angriffsarten o ä. erkennen.

Abbildung 5: Gemeldete Vorfälle durch Staats- und Kommunalbehörden



6 Umsetzungsstand des SächsISichG

Das SächsISichG ist seit 31. August 2019 in Kraft. Die im Gesetz beschriebenen Maßnahmen zur Stärkung der Sicherheitsorganisation waren dabei bis zum 31. Dezember 2020 im Rahmen der zur Verfügung stehenden Haushaltsmittel umzusetzen. Dazu gehörten u. a. die Bestellung eines hauptamtlichen BfIS in den Ressorts und weiteren wichtigen Behörden sowie die Umsetzung eines ISMS.

6.1 Beauftragter für Informationssicherheit des Landes

Der BfIS Land bildet die zentrale strategische Instanz in der Informationssicherheitsorganisation der Behörden des Freistaates Sachsen. In seiner Zuständigkeit liegt die landesweite Förderung, Koordinierung und Abstimmung aller erforderlichen Belange der Informationssicherheit in den Behörden des Freistaates. Zur Förderung der Informationssicherheit gehört neben der Sensibilisierung der Mitarbeiterinnen und Mitarbeiter in den Behörden auch der Aufbau einer geeigneten Organisationsstruktur. Die Befugnisse des BfIS Land werden durch das SächsISichG wie folgt beschrieben:

- Beratende Unterstützung der staatlichen BfIS (§ 5 Absatz 1 Satz 2 und Satz 3 SächsISichG),
- Maßnahmenanordnung zur Gefahrenabwehr (§ 5 Absatz 3 und Absatz 4 SächsISichG),
- Festlegung von verbindlichen Mindeststandards (§ 5 Absatz 6 SächsISichG),
- Durchführung von Revisionen (§ 5 Absatz 7 Satz 2 SächsISichG).

Die im Berichtszeitraum durch BfIS Land vollzogenen Tätigkeiten sind dem Kapitel 3 zu entnehmen.

Dem Referat 45 der Sächsischen Staatskanzlei, dem BfIS Land als Referatsleiter vorsteht, waren im Berichtszeitraum vier Referentenstellen und eine Sachbearbeiterstelle zugeordnet – eine Stelle mehr, als zum Inkrafttreten des SächsISichG vor fünf Jahren. Allerdings sind die Bediensteten des Referates nicht ausschließlich für Aufgaben des BfIS Land tätig, da das Referat neben dem in diesem Bericht adressierten Themenbereich Informationssicherheit auch für Cybersicherheit und Kritische Infrastrukturen zuständig ist. Hierunter fällt u. a die rechtliche Begleitung entsprechender europäischer und bundesgesetzlicher Umsetzungsakte, die Vertretung Sachsens auf Arbeitsebene in der Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz sowie nicht zuletzt die Koordinierung von Cybersicherheitsthemen. Dies erfolgt im Austausch mit weiteren staatlichen Akteuren wie dem Cybercrime Competence Center des Landeskriminalamtes, dem Landesamt für Verfassungsschutz, der Zentralstelle Cybercrime der Generalstaatsanwaltschaft und der Abteilung Bevölkerungsschutz im Staatsministerium des Innern. So wurde im Berichtszeitraum die bereits etablierte anlassbezogene operative Koordinierungsrunde Cybersicherheit mit den Sicherheitsbehörden in ein 14-tägliches Format überführt, welche in diesem Zusammenwirken koordiniert durch das SAX.CERT ein monatliches Lagebild Cybersicherheit erstellt, mit dem der Staatsminister des Innern und der

CIO des Freistaates Sachsen zu einer ganzheitlichen Cybersicherheitslage in Verwaltung, Wirtschaft und Gesellschaft informiert werden.

Mit der Umsetzung der NIS-2-Richtlinie der EU (siehe 7.1) kommen ab Oktober 2024 neue Aufgaben auf BfIS Land zu. So übernimmt dieser dann die Rolle einer Aufsichtsbehörde für die wesentlichen Einrichtungen der Staatsverwaltung und wird noch stärker als bisher die Umsetzung der Maßnahmen der Informationssicherheit in den staatlichen Stellen prüfen. Hierfür ist BfIS Land bisher nicht personell aufgestellt.

6.2 Beauftragte für Informationssicherheit in den staatlichen Stellen

Bereits seit der ersten Leitlinie Informationssicherheit des IT-Planungsrates aus dem Jahr 2013 besteht für die Sächsische Staatsverwaltung die Verpflichtung, organisatorische, technische und personelle Maßnahmen für eine angemessene IT-Sicherheit umzusetzen. Mit dem SächsISichG wurden diese Maßnahmen im August 2019 für die staatlichen Stellen verbindlich gesetzlich verankert. Auf dieser Grundlage haben die in § 7 Abs. 1 SächsISichG genannten insgesamt 15 Staatsbehörden einen hauptamtlichen BfIS zu bestellen. Die Umsetzung hatte bis zum 31. Dezember 2020 im Rahmen der verfügbaren Haushaltsmittel zu erfolgen (siehe § 20 SächsISichG). Im Berichtszeitraum war diese Stelle bei allen diesen besonders wichtigen staatlichen Stellen hauptamtlich besetzt. Bei den übrigen Behörden war im Berichtszeitraum bei fast allen Behörden und Einrichtungen ein BfIS offiziell bestellt. Allerdings ist bei den meisten Behörden nicht bekannt, mit welchem Stellenanteil der jeweilige Mitarbeiter diese Aufgabe wahrnimmt.

Die BfIS der Behörden sind für alle Belange der Informationssicherheit in ihrem Zuständigkeitsbereich zuständig. Die Hauptaufgabe des BfIS besteht darin, der Leitung der öffentlichen Stelle in Fragen der Informationssicherheit zu beraten und bei der Umsetzung zu unterstützen. Die Aufgaben sind in den Standards des BSI festgelegt. Die mögliche Einsichtnahme in sensible Protokolldaten zur Erkennung und Eingrenzung sicherheitsrelevanter Ereignisse erfordert eine organisatorisch unabhängige Ausgestaltung der Rolle des BfIS.

6.3 Beauftragte für Informationssicherheit in den nicht-staatlichen Stellen

Nach Maßgabe des § 8 SächsISichG sollen alle nicht-staatlichen Stellen einen BfIS und einen Stellvertreter ernennen. Über die Ernennung des BfIS und seines Vertreters ist der BfIS Land innerhalb eines Monates zu unterrichten. Bezogen auf die Kommunen war Stand 31. Juli 2024 in zwölf von 13 Landkreisen und kreisfreien Städten die BfIS-Stelle besetzt. Von den übrigen 415 Gemeinden hatten 243 einen BfIS benannt. 165 davon nutzen dabei die Möglichkeit, hierfür einen externen Mitarbeiter einzusetzen. Damit sind zum Ende des Berichtszeitraumes in rund 59 % der sächsischen Gemeinden bzw. Verwaltungsgemeinschaften BfIS ernannt (Vorjahr: 52 %). 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.

Neben den Kommunen haben 35 andere nicht-staatliche Stellen einen BfIS ernannt und gemeldet. Darunter sind zum überwiegenden Teil Bildungseinrichtungen wie Hochschulen und Universitäten. Hingegen haben z. B. Stiftungen und Kammern bislang noch keine Beauftragten gegenüber dem BfIS Land benannt.

6.4 Sicherheitsnotfallteam SAX.CERT

Gemäß § 6 Absatz 1 SächsISichG ist das SAX.CERT die zentrale Stelle für operative Fragen der Informationssicherheit der staatlichen und nicht-staatlichen Stellen im Freistaat, mit folgenden Aufgaben:

1. Das Aufzeigen von Lösungen bei konkreten Sicherheitsereignissen oder –vorfällen,
2. die Prüfung auf Risiken im Betrieb von informationstechnischen Systemen und die Unterstützung bei ihrer Beseitigung,
3. die Information zu Sicherheitslücken,
4. die Erfassung und Analyse der Lage der Informationssicherheit sowie die Erstellung daraus ab geleiteter Empfehlungen,
5. die Wahrnehmung der zentralen Meldestelle im Sinne des BSI-Gesetzes,
6. die Wahrnehmung der zentralen Meldestelle im Sinne des IT-Planungsrates im VCV,
7. die Mitwirkung bei der technischen und technologischen Koordinierung der Informationssicherheit in den staatlichen und nicht-staatlichen Stellen sowie
8. die regelmäßige Information über die Lage der Informationssicherheit im Freistaat Sachsen.

Wie in den Kapiteln 4 und 5 beschrieben, hat das SAX.CERT seine gesetzlichen Aufgaben zu den oben genannten Aufgaben 1 bis 4 sowie 7 und 8 erfüllt.

Zu 5.: Das SAX.CERT ist weiterhin die zentrale KRITIS-Anlaufstelle für den Freistaat Sachsen, die gemäß § 8b Abs. 2 BSI-Gesetz (BSIG) vom BSI über versuchte oder erfolgte Angriffe auf die Sicherheit der Informationstechnik von Betreibern kritischer Infrastrukturen informiert wird. Im Berichtszeitraum wurde ein schwerwiegender Sicherheitsvorfall bei einem Betreiber kritischer Infrastrukturen dem SAX.CERT gemeldet.

Zu 6.: Das SAX.CERT ist in den VCV der CERTs des Bundes und der Länder eingebunden. Hier findet ein kontinuierlicher, elektronischer Austausch und bei besonderen übergreifenden Bedrohungslagen auch gemeinsame Lagebesprechungen statt. Im Berichtszeitraum wurde durch das SAX.CERT ein sicherheitsrelevantes Ereignis aus Sachsen an den VCV gemeldet.

Für die dem SAX.CERT im Haushaltsjahr 2023 neu zugewiesenen Stellen konnten im letzten Berichtszeitraum Besetzungsverfahren erfolgreich durchgeführt werden. Stand Juli 2024 war das SAX.CERT mit zwei Referenten und sieben Sachbearbeitern besetzt, die von zwei externen Mitarbeitern unterstützt werden. Aus europäischer Rechtsetzung (siehe 7.1) wird das SAX.CERT weitere Aufgaben erhalten, die ab Oktober 2024 zu erfüllen sind und einen weiteren personellen Ausbau erfordern werden.

7 Zusätzliche und zukünftige Verpflichtungen für die Verwaltung in Sachsen

Nicht erst seit Inkrafttreten des SächsISichG gelten für die Behörden der öffentlichen Verwaltung in Land und Kommunen im Freistaat Sachsen Regelungen zur Informationssicherheit. So besteht über den IT-Planungsrat, der auf Artikel 91c GG fußt, bereits seit dem Jahr 2013 eine Leitlinie für die Informationssicherheit der öffentlichen Verwaltung des Bundes und der Länder. In den Folgejahren sind Regelungen auf europäischer Ebene dazugekommen, die sich permanent weiterentwickeln und auch Auswirkungen auf die Staatsverwaltung haben.

7.1 Umsetzung der NIS-2-Richtlinie in Deutschland

Die „Richtlinie 2022/2555 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 2016/1148“ (NIS-2-Richtlinie) ist am 16. Januar 2023 in Kraft getreten und ist bis zum 17. Oktober 2024 von den Mitgliedstaaten umzusetzen.

Mit dem Inkrafttreten wurde die bisherige NIS-Richtlinie abgelöst und durch ein weiter reichendes Regelwerk ersetzt. Ziel der Kommission war es, ein einheitliches und erhöhtes Niveau der Cyberresilienz in der EU zu schaffen und so den europäischen Binnenmarkt besser vor Cyberangriffen zu schützen. 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 Cyber-Sicherheitsregulierung ist mit der NIS-2-Richtlinie erstmals auf bestimmte Einrichtungen der öffentlichen Verwaltung der Regionalebene, also der Landesverwaltung, ausgeweitet worden.

Die Umsetzung der NIS-2-Richtlinie auf nationaler Ebene ist ein komplexer Prozess, der sowohl die Bundes- und Landesverwaltung als auch die Wirtschaft betrifft und sie vor Herausforderungen stellt.

7.1.1 Neuerung des SächsISichG ab 1. Oktober 2024

Im Freistaat Sachsen wurden die Anforderungen der NIS-2-Richtlinie an die öffentliche Verwaltung fristgemäß umgesetzt. Sachsen war 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.

Um auf Landesebene auch vor dem Hintergrund von Verflechtung und Konsolidierung der Landes-IT insgesamt ein gemeinsames, kohärentes und handbares Regime zu erreichen, wurden an alle

staatlichen Stellen Anforderungen formuliert, die sich inhaltlich an denjenigen für wichtige Einrichtungen der NIS-2-Richtlinie orientieren. Die NIS-2-Umsetzung gilt deshalb für alle staatlichen Stellen und geht somit über die reine Richtlinienumsetzung hinaus.

Das Änderungsgesetz zum SächsISichG wurde im Juni 2024 im Sächsischen Landtag beschlossen. Die Änderungen treten mit der aus der NIS-2-Richtlinie vorgegebenen Umsetzungsfrist im Oktober 2024 in Kraft. Mit der Umsetzung der NIS-2-Richtlinie setzt Sachsen ein starkes Zeichen für die Cybersicherheit und geht als Vorreiter in Deutschland voran.

7.1.2 Cybersicherheitsstrategie Sachsen

Neben der Umsetzung der oben beschriebenen Anforderungen an die Informationssicherheit in der Verwaltung auf Landesebene verpflichtet die NIS-2-Richtlinie die Mitgliedstaaten der Europäischen Union auch zur Verabschiedung einer nationalen Cybersicherheitsstrategie. Für das föderale System der Bundesrepublik Deutschland bedeutet das, dass dies auch die Cybersicherheitsstrategien der Länder umfasst. Inhaltlich befasst sich eine Cybersicherheitsstrategie mit weit mehr als der Informationssicherheit in der öffentlichen Verwaltung und geht damit deutlich über den Zuständigkeitsbereich des BfIS Land hinaus. Ziel einer Cybersicherheitsstrategie ist es vielmehr, die öffentliche Sicherheit und Ordnung im Cyberraum zu stärken und die Cybersicherheit der Bürgerinnen und Bürger sowie der Wirtschaft zu gewährleisten.

Bereits im Mai 2023 wurden unter Federführung des Referates Informations- und Cybersicherheit, Kritische Infrastrukturen, der Sächsischen Staatskanzlei im Rahmen einer Auftaktveranstaltung alle Ressorts in die Erarbeitung einer Cybersicherheitsstrategie für Sachsen einbezogen und diese in den Folgemonaten in enger Abstimmung mit den fachlich betroffenen Stellen in den Ressorts und nachgeordneten Behörden auf Arbeitsebene weiterentwickelt. Darüber hinaus wurden auch Kammern, Verbände und Hochschulen sowie weitere externe Akteure beteiligt, um in allen neun Handlungsfeldern der Strategie, die sich an den von der Innenministerkonferenz zur Anwendung in den Ländern empfohlenen Leitlinien für die Erarbeitung von föderalen Cybersicherheitsstrategien orientieren, Ziele und Maßnahmen zu formulieren, die den gesellschaftlichen und wirtschaftlichen Bedürfnissen entsprechen.

Eine für das Inkrafttreten der Cybersicherheitsstrategie Sachsen notwendige Beschlussfassung durch das Kabinett stand zum Ende des Berichtszeitraumes noch aus.

7.1.3 Umsetzung der NIS-2-Richtlinie in Bundesgesetzgebung mit Auswirkung auf Sachsen

Auf Bundesebene soll die NIS-2-Richtlinie mit dem Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des ISMS in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, BR-Drs. 380/24) umgesetzt werden. Entsprechend der unionsrechtlichen Vorgaben wird der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324) und dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122) geschaffene Ordnungsrahmen durch das NIS-2-Umsetzungs-

und Cybersicherheitsstärkungsgesetz auf den Bereich bestimmter Unternehmen erweitert, zusätzlich werden entsprechende Vorgaben für die Bundesverwaltung eingeführt. Im Wesentlichen ändert das geplante Artikelgesetz das BSIG.

Durch die Einführung der in NIS-2 vorgegebenen Einrichtungskategorien „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ und dafür geltender niedriger Schwellwert in Bezug auf Umsatz oder Mitarbeiterzahl erfolgt eine signifikante Ausweitung des bisher auf Betreiber Kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkten Anwendungsbereiches. Durch die Einbeziehung von rechtlich unselbstständigen Organisationseinheiten einer Gebietskörperschaft können auch Eigenbetriebe, Landesbetriebe, aber auch Behörden, soweit sie entsprechende Dienste gemäß der Einrichtungsdefinition erbringen, von dem zukünftigen BSIG erfasst sein.

7.2 IT-Planungsrat: Leitlinie Informationssicherheit

Anfang 2019 verabschiedete der IT-Planungsrat die überarbeitete Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung. Die aktualisierte Fassung konkretisiert die Sicherheitsziele und die dazu umzusetzenden notwendigen Maßnahmen. Der Umsetzungsplan zur Leitlinie schreibt die stufenweise Umsetzung der Vorgaben bis 2025 fest. Ein jährliches Berichtswesen mit 27 Kennzahlen bietet einen Überblick zum Umsetzungsfortschritt. Die Umsetzung des vom IT-Planungsrat beschlossenen CERT-Mindeststandards wird in Sachsen weiter vorangetrieben. Folgende Maßnahme waren für das Jahr 2023 im Umsetzungsplan als Ziele vorgegeben:

Etablierung und Umsetzung zielgruppenbezogener Konzepte zur kontinuierlichen Fortbildung

Diese Maßnahme wurde der AG InfoSic vom Freistaat Sachsen als noch nicht erfüllt gemeldet. Zur Erfüllung dieser Zielvorgabe wurde im Berichtszeitraum eine landesweite Richtlinie inklusive eines dazugehörigen Schulungs- und Sensibilisierungskonzeptes (siehe 3.2) verabschiedet. Dieses muss jedoch in ressort- und behördenspezifischen Konzepten weiter untersetzt werden. Auf Landesebene arbeitet BfIS Land an der Erstellung eines aktualisierten E-Learnings für die verschiedenen Zielgruppen Mitarbeiter, Behördenleitungen und IT-Fachkräfte (siehe 3.4.1). Mit Veröffentlichung der E-Learnings wird diese Zielvorgabe voraussichtlich erfüllt.

Weiterentwicklung der Sicherheitskonzepte ebenenübergreifender Verfahren nach IT-Grundschutz

Diese Zielvorgabe gilt beim Freistaat Sachsen zu 75 % erfüllt. Im Ländervergleich steht Sachsen damit deutlich besser als der Durchschnitt da. Nichtsdestotrotz gilt es, die Vorgaben des IT-Grundschutzes bei der Aufstellung von Sicherheitskonzepten für ebenenübergreifende Verfahren stärker zu berücksichtigen und damit das Sicherheitsniveau der Verfahren weiter anzuheben.

Aufbau des IT-Notfallmanagements

Auch im Bereich des IT-Notfallmanagements wurden für das Jahr 2023 durch die Leitlinie zwei weitere Vorgaben aufgestellt. Dies betrifft zum einen die Erstellung IT-bezogener Notfallkonzepte inkl. der Etablierung von Schnittstellen zum Krisen- und Katastrophenschutz sowie zum anderen die

Durchführung von IT-Notfallübungen. Im Herbst des vergangenen Jahres fand hierzu die länderübergreifende Krisenübung LÜKEX 2023 statt, an welcher der Freistaat Sachsen teilnahm (siehe 3.7). Zudem wurden in Sachsen ein übergreifendes IT-Notfallkonzept sowie ein IT-Notfallvorsorgekonzept initiiert, welche entsprechende Maßnahmen vorsehen. Gleichwohl sind beide Vorgaben aufgrund der geringen Operationalisierung der vorgesehenen Maßnahmen als nicht erfüllt anzusehen.

Ausschließlich vom Umsetzungsstand der Leitlinie auf den generellen Stand der Informationssicherheit in den Ländern zu schließen, wäre jedoch zu kurz gegriffen: Die Leitlinie des IT-Planungsrates ist eine von vielen Indikatoren für das Niveau der Informationssicherheit in der öffentlichen Verwaltung, sie bildet das Niveau jedoch nicht ganzheitlich ab. Vielmehr sind Leitlinie und der damit verbundene Umsetzungsplan als ein Plan zu verstehen, mit dem in speziellen Themenfeldern aus Sicht des IT-Planungsrates und dessen Fachgremium AG Infosic besondere Anstrengungen forciert werden sollen.

8 Abbildungs- und Tabellenverzeichnis

9 Glossar

Applikation/App
Eine Applikation, kurz App, ist eine Anwendungssoftware. Der Begriff App wird oft im Zusammenhang mit Anwendungen für Smartphones oder Tablets verwendet.

Advanced Persistent Threats (APT)
Bei Advanced Persistent Threats handelt es sich um zielgerichtete Cyberangriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifender persistenten (dauerhaften) Zugriff auf ein Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifenden aus und sind in der Regel schwierig zu detektieren.

Authentifizierung
Authentifizierung bezeichnet den Vorgang, die Identität einer Person oder eines Rechnersystems anhand eines bestimmten Merkmales zu überprüfen. Dies kann unter anderem durch Passworteingabe, Chipkarte oder Biometrie erfolgen.

Authentisierung
Authentisierung bezeichnet den Nachweis der Authentizität. Die Authentisierung einer Identität kann u. a. durch Passworteingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptografische Signaturen.

Backdoor
Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (Hintertür) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen.

Backup
Unter Backup versteht man das Kopieren von Dateien oder Datenbanken auf physischen oder virtuellen Systemen an einen sekundären Speicherort, um diese im Falle eines Geräteausfalles oder einer Katastrophe für eine Wiederherstellung zu nutzen und bis dahin sicher vorzuhalten.

Bot/Botnetz
Als Botnetz wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.

Brute-Force-Angriff
Bei einem Brute-Force-Angriff wird versucht, ein Passwort zu knacken, indem man nach dem Prinzip des Erratens – also ohne ausgeklügelte Methoden – durch möglichst viele Versuche, ermöglicht durch hohe Rechenleistung, in kurzer Zeit die richtige Phrase herausbekommt.

Command-and-Control-Server (C&C-Server)
Server-Infrastruktur, mit der Angreifende die in ein Botnetz integrierten infizierten Computersysteme (Bots) steuern. Bots (infizierte Systeme) melden sich in der Regel nach der Infektion bei dem C&C-Server des Angreifenden, um dessen Befehle entgegenzunehmen.

DoS/DDoS-Angriffe
Denial-of-Service (Dos, auch Distributed Denial of Service (DDoS)) sind Angriffe, die sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen richten. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff. DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.

Informationssicherheitsmanagementsystem (ISMS)
Ein Informationssicherheitsmanagementsystem ist die Aufstellung von verbindlichen Prozessen und Regeln, die die Informationssicherheit in einer staatlichen oder nicht-staatlichen Stelle dauerhaft steuern, kontrollieren, aufrechterhalten und fortlaufend verbessern.

Malware
Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus Malicious Software und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computerviren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Open-Source
Open-Source-Software ist Software, deren Quelltext öffentlich ist und von Dritten eingesehen, geändert und genutzt werden kann.

Patch
Ein Patch (Flicken) ist ein Software-Paket, mit dem Software-Hersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren. Das Einspielen dieser Updates erleichtern viele Programme durch automatische Update-Funktionen. Als Patch-Management bezeichnet man Prozesse und Verfahren, die helfen, verfügbare Patches für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.

Phishing
Das Wort setzt sich aus Password und fishing zusammen, zu Deutsch: Nach Passwörtern angeln. Der Angreifende versucht dabei, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetnutzenden zu gelangen und diese für seine Zwecke meist zulasten des Opfers zu missbrauchen.

Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (Ransom) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

Security Operations Center / Security Information and Event Management

Das Security Operations Center (SOC) ist eine zentrale Leitstelle, in der Bedrohungen rund um die Uhr überwacht, qualifiziert und abgewehrt werden. Sie nutzen für ihre Arbeit dabei u. a. ein als Security Information and Event Management (SIEM) bezeichnetes Tool im SOC, welches bei der Überwachung von Infrastrukturen als eine Art Radarsystem hilft, das in Echtzeit nach ungewöhnlichem Verhalten, Systemanomalien und anderen Anzeichen für einen Hackerangriff sucht.

Social Engineering

Social Engineering ist der Versuch von Kriminellen, ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyberkriminalität als auch bei der Spionage gehen die Angreifenden geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Spam

Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthalten Spam-Nachrichten jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder sie werden für Phishing-Angriffe genutzt.

Zwei- bzw. Mehr-Faktor-Authentisierung

Bei der Zwei- bzw. Multifaktor-Authentifizierung erfolgt die Authentifizierung einer Identität anhand verschiedener Authentifizierungsfaktoren aus getrennten Kategorien (Wissen, Besitz oder biometrische Merkmale).

Herausgeber:

Sächsische Staatskanzlei

Redaktion sowie Gestaltung und Satz:

Referat 45: Informations- und Cybersicherheit, Kritische Infrastrukturen

Redaktionsschluss:

September 2024