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:

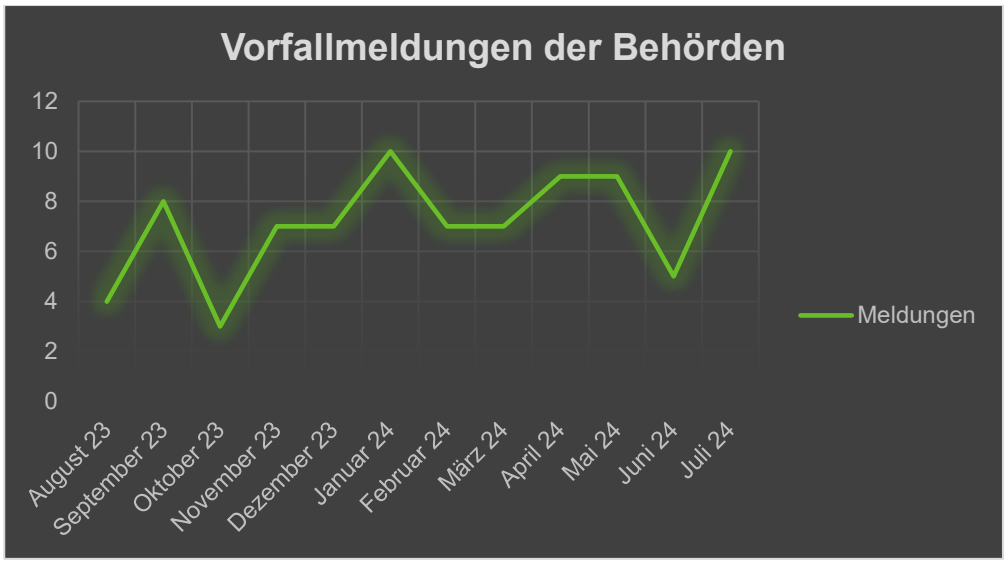
- zu einer erheblichen Beeinträchtigung der Schutzziele geführt haben oder
- behördenübergreifend zu einer erheblichen Beeinträchtigung der Schutzziele führen können.

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).