SÄCHSISCHE STAATSKANZLEI | Freistaat SACHSEN

Jahresbericht Informationssicherheit 2021

des Beauftragten für Informationssicherheit des Landes

Berichtszeitraum: August 2020 – Juli 2021

Inhalt

1. Einführung

In den vergangenen Jahren hat sich die Gefahr von Cyberattacken nicht nur auf die Wirtschaft, sondern auch auf die öffentliche Verwaltung erheblich verstärkt. Dabei hat auch die Qualität vieler Cyberangriffe zugenommen. Gleichzeitig wird die IT-Abhängigkeit der Unternehmen, des Staates und der Bürger immer größer, wodurch das Schadenspotenzial wächst.

Die Digitalisierung der Verwaltung muss sicher gestaltet werden. Insbesondere mit Bezug auf das Online-Zugangsgesetz und dem damit verbundenen massiven Ausbau der digitalen Angebote der Verwaltungsleistungen kommt der Informationssicherheit eine Schlüsselrolle zu. Wollen wir mit all unseren digitalen Angeboten Erfolg haben, dann muss die Verwaltung für die Bürgerinnen und Bürger der Vertrauensanker in der digitalen Welt sein.

Der vorliegende Bericht für den Zeitraum August 2020 bis Juli 2021 erfüllt die mit dem Sächsischen Informationssicherheitsgesetz vom 2. August 2019 (SächsGVBl. S. 630, SächsISichG) verbundenen Berichtspflichten. Darüber hinaus gibt er einen Überblick über die konkrete Gefährdungslage, die vom Beauftragten für Informationssicherheit des Landes (BfIS Land) und vom Sicherheitsnotfallteam SAX.CERT eingeleiteten Maßnahmen sowie zum allgemeinen Umsetzungsstand der Informationssicherheit in der Landesverwaltung.

Die COVID-19 Pandemie hat deutlich vor Augen geführt, welche Bedeutung funktionierende und sichere IT-Infrastrukturen haben. Das Home-Office, Homeschooling oder das Abhalten von Videokonferenzen können in diesem Kontext eine spezielle Angriffsfläche bieten.

Im Berichtszeitraum ging eine große Bedrohung für Staat, Wirtschaft und Gesellschaft vom zunehmenden Einsatz von Ransomware als Schadsoftware bei Cyber-Angriffen aus. Dabei werden die IT-Systeme der Betroffenen durch eine Verschlüsselung beeinträchtigt, ihre Verfügbarkeit erheblich eingeschränkt und versucht, die Besitzer mit einer Aufforderung zur Zahlung eines Lösegelds für die Entschlüsselung der Daten zu erpressen. Diese Methode ist durch die Sichtbarkeit und unmittelbare Wirksamkeit besonders effektiv. Weiterhin war der Berichtszeitraum von Schwachstellen in Software-Produkten geprägt, die Angriffswege überhaupt erst ermöglichten. Diese Schwachstellen waren sehr schwerwiegend, da es sich um Produkte mit großer Verbreitung und hoher Marktdurchdringung handelt.

Der Freistaat Sachsen muss auf die stetig wechselnden Gefahrenlagen vorbereitet sein. Mit dem Sächsischen Informationssicherheitsgesetz wurde die rechtliche Grundlage geschaffen, um unsere Verwaltungen zu wappnen und vor den Cybergefahren besser zu schützen. Das Gesetz ermöglicht organisatorische, personelle und technische Sicherheitsmaßnahmen. Insbesondere müssen die Fähigkeiten des Sicherheitsnotfallteams SAX.CERT weiter ausgebaut und personell aufgestockt werden, um beispielsweise Angriffswellen analysieren und die Abwehrmaßnahmen noch genauer ausrichten zu können. Außerdem muss dessen Rolle als IT-Sicherheitsdienstleister auch für den kommunalen Bereich gestärkt werden.

2. Gefährdungslage

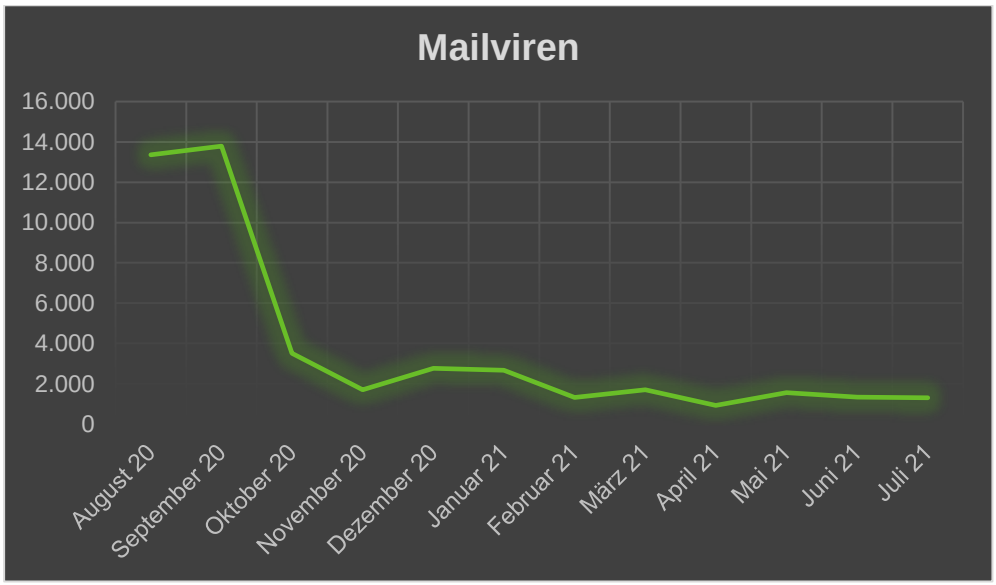
Das Sicherheitsnotfallteam SAX.CERT des Staatsbetriebs Sächsische Informatik Dienste (SID) beobachtet kontinuierlich die Gefährdungslage der IT-Sicherheit in der Landesverwaltung mit besonderem Fokus auf das Sächsische Verwaltungsnetz (SVN). In diesem Bericht sind die Erkenntnisse aus dem Zeitraum August 2020 bis Juli 2021 zusammengestellt. Nach der Zusammenfassung der Bedrohungslage werden die Methoden und Mittel der Angreifer, die im Berichtszeitraum die größte Rolle spielten, anhand einiger Beispiele aufgezeigt.

2.1. Gefährdungslage in der Landesverwaltung

Das SVN ist prinzipiell ein vom Internet unabhängiges internes Netz der Landesbehörden und hat durch diese Struktur ein vergleichsweise hohes Niveau der Informationssicherheit aufzuweisen. Jedoch ist dieses Netz natürlich auch mit dem Internet verbunden, um z. B. die Kommunikation zwischen Behörden und Bürgern oder auch Unternehmen und anderen Institutionen zu gewährleisten. Gerade vor dem Hintergrund, dass nach Onlinezugangsgesetz (OZG) bis 2022 alle wesentlichen Behördenleistungen auch online abrufbar sein sollen, öffnet sich die Verwaltung zunehmend in das Internet. Da aber gerade aus dem Internet Cyberangriffe auf die IT-Infrastruktur der Verwaltung drohen, kommen leistungsfähige Schutzsysteme in den zentralen Diensten des SVN zum Einsatz, die die Übergänge aus dem internen Netz der Landesverwaltung von und zum Internet zeitgemäß auch gegen komplexe und zielgerichtete Bedrohungen absichern und im Berichtszeitraum sowohl kapazitiv als auch technisch erweitert wurden. Ergänzt werden diese zentralen, vielschichtig verschachtelten Schutzsysteme durch dezentrale Virenscanner in den Rechenzentren der Behörden und des zentralen staatlichen IT-Dienstleisters sowie auf den Endgeräten der Bediensteten.

So wurden zwischen August 2020 und Juli 2021 von den über 137 Millionen ankommenden E-Mails bereits über 97 Millionen an der Internetübergangsstelle des SVN als sehr wahrscheinlich Malware enthaltend direkt abgewiesen. Weitere knapp 7 Millionen E-Mails wurden von den dezentralen Systemen als Spam-Mail erkannt und entsprechend markiert. Damit lag der Anteil von unerwünschten Nachrichten am Mail-Aufkommen bei über 76 % (Vorjahreszeitraum: 85 %). Im Vergleich zum Vorjahreszeitraum ging sowohl die Gesamtzahl der eingehenden E-Mails um 47 Millionen als auch die Gesamtzahl der als Spam/Malware abgewiesenen E-Mails um 53 Millionen deutlich zurück.

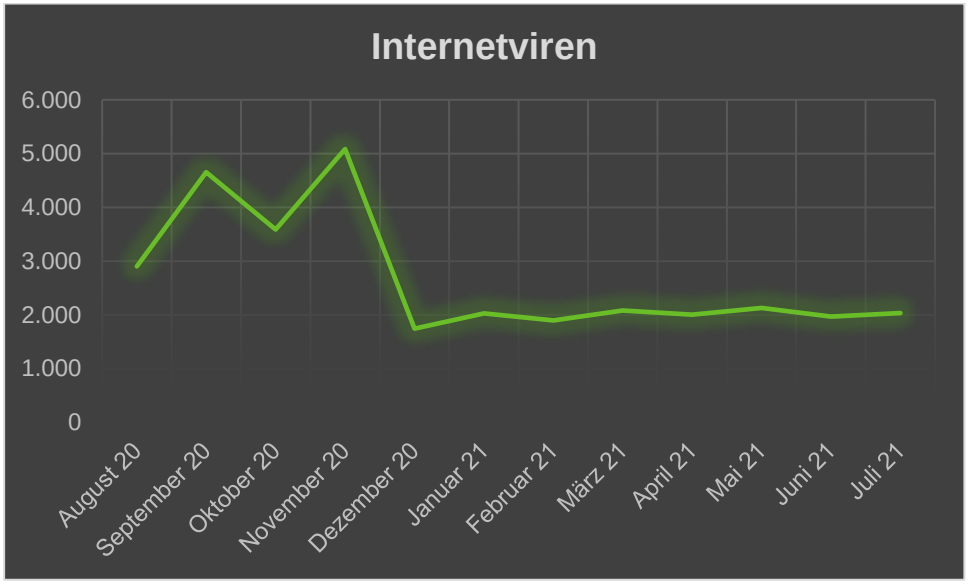
Abbildung 1: Entdeckte Schadprogramme im SVN-Mailverkehr



Daneben wurden knapp 46.000 Viren im Mailverkehr abgefangen. Das ist ein leichter Anstieg zu den 12 Monaten davor, in denen 44.000 Viren abgefangen wurden.

Neben verseuchten E-Mails ist auch ein in Webseiten versteckter Schadcode eine der wesentlichsten Gefahren für die IT der Verwaltungen. So wurden im Internetverkehr, wenn z. B. Mitarbeiterinnen und Mitarbeiter auf eine Webseite gehen, über 32.000 Viren erkannt. In den 12 Monaten zuvor waren es knapp 43.000 Viren.

Abbildung 2: Entdeckte Schadprogramme im SVN-Internetverkehr



Eine Infektion eines lokalen Rechners kann sich durch die hohe Vernetzung innerhalb des SVN behördenübergreifend ausbreiten. Dass dieses Szenario nicht nur hypothetisch ist, zeigen zahlreiche aktuelle Beispiele auch in deutschen Behörden. Am prominentesten ist im Berichtszeitraum die Verschlüsselung der IT-Systeme der Verwaltung des Landkreises Anhalt-Bitterfeld in Sachsen-Anhalt durch Cyberkriminelle, bei der Netzwerke lahmgelegt wurden und Datenmengen entwendet und zum Teil sogar veröffentlicht worden sind.

2.2. Angriffsmethoden und -mittel

Cyberangriffe auf das SVN finden quasi täglich statt. Dabei handelt es sich den Erkenntnissen nach zum weit überwiegenden Teil um ungezielte Massenangriffe, die generell im Internet stattfinden. Ungefährlich sind diese deshalb nicht, denn so infizierte Rechner bilden dann regelmäßig den Ausgangspunkt für weitere gezielte Angriffe. Teilweise gibt es auch auf bestimmte Bereiche zugeschnittene Angriffskampagnen, z. B. gegen Universitäten, gegen Hochleistungsrechner oder gegen deutsche Behörden.

2.2.1. Phishing-Mails

Mittels so genannter Phishing-Mails versuchen Cyberkriminelle, sich als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es, im weiteren Verlauf an persönliche Daten eines Internet-Benutzers zu gelangen oder ihn zur Ausführung einer schädlichen Aktion zu bewegen. In der Folge werden dann beispielsweise Kontoplünderung oder Identitätsdiebstahl begangen oder eine Schadsoftware (z. B. Ransomware) installiert.

Im Berichtszeitraum wurden vom SAX.CERT regelmäßig Wellen von Phishing-Mails registriert, deren Ziel es war, die Benutzerdaten von dienstlichen E-Mail-Konten abzufischen. Dabei hat sich die

Qualität dieser Mails deutlich verbessert. Neben weitestgehend fehlerfreier Rechtschreibung und Grammatik sowie verständlichen Formulierungen kommen diese Mails auch scheinbar von vertrauenswürdigen Absendern, die nur nach Prüfung des E-Mail-Headers als Fälschung zu erkennen sind.

Emotet-Trojaner

Von August 2020 bis Januar 2021 gingen die gefährlichsten Phishing-Kampagnen auf das Konto von Cyberkriminellen rund um den so genannten Emotet-Trojaner. So wurden im August 2020 an den E-Mail-Virenscannern an mehreren Tagen Spitzenwerte von über 1.000 Emotet-Dokumenten blockiert. Bei Server-Log-Auswertungen wurde festgestellt, dass von Bediensteten teilweise auf E-motet-Links geklickt wurde, der Download aber durch die Schutzsysteme blockiert werden konnte. Erschwerend kam hinzu, dass sich der Trojaner immer wieder veränderte und dadurch bestimmte verwendete Abwehrmechanismen unwirksam wurden und angepasst werden mussten. Im September registrierten die E-Mail-Virenscanner an einem Tag Spitzenwerte von über 4.400 blockierten Emotet-Dokumenten.

Ende Januar 2021 wurde dann die Zerschlagung der Emotet Infrastruktur bekannt. Im Rahmen eines international koordinierten Vorhabens des Bundeskriminalamts und der Generalstaatsanwaltschaft Frankfurt am Main - Zentralstelle zur Bekämpfung der Internetkriminalität - übernahmen die Strafverfolgungsbehörden die Infrastruktur von Emotet. Hierbei wurden alle Bots, also Computer bzw. IT-Infrastrukturen, die einen aktiven Trojaner enthalten, mit einem Update versorgt, dass dafür sorgt, dass sie keine Verbindung mehr zur Command&Control-Infrastruktur der Cyberkriminellen herstellt, so dass die Bots nicht mehr unter der Kontrolle der Akteure stehen. Vielmehr wurden die Bots mit einem anderen Server verbunden, auf den die Strafverfolgungsbehörden Zugriff haben, um mit den hier gesammelten Informationen betroffene Netzbetreiber/-anbieter in Deutschland und Computernotfallteams auf der ganzen Welt über infizierte Bots zu benachrichtigen. Nach der Informationsphase wurde der Trojaner auf allen IT-Systemen automatisch deinstalliert.

Auch wenn die Zerschlagung von Emotet einen großen Erfolg gegen Cyberkriminelle Strukturen darstellt, ist die Gefahr durch Phishing-Kampagnen nach wie vor groß. Die durch Emotet hinterlassene Lücke wurde zügig durch andere Gruppierungen gefüllt, deren Kampagnen ebenso als Türöffner für nachgelagerte Cyberattacken dienen. So zum Beispiel für Ransomware, von der derzeit die größte Gefährdung für die Informationssicherheit ausgeht – auch für die öffentliche Verwaltung.

Ransomware – Verschlüsselung und Erpressung

Ransomware sind mit Schadsoftware ausgestattete Verschlüsselungstrojaner, mit deren Hilfe Cyberkriminelle den Zugriff auf Daten und deren Nutzung oder auf das ganze Computersystem verhindern können. Dabei werden die Daten auf dem Computer verschlüsselt, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Vor der Verschlüsselung werden die Datensätze der gekaperten Systeme häufig auch noch auf IT-Systeme der Hacker kopiert, so dass die Angreifer mit der Veröffentlichung von sensiblen Daten drohen können, was ihr Erpressungspotenzial verstärkt. 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 Zwei-Faktor-Authentisierung) und die Mitarbeiter z. B. bei der Bearbeitung von E-Mails angehängte Dokumente oder Links im Text nicht richtig auf Vertrauenswürdigkeit einschätzen können. Hat der Betroffene dann auch keine Sicherungskopien, sogenannte Backups, von seinen Daten, sind diese ohne Entschlüsselungscode nicht mehr nutzbar. Aber 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. Insbesondere für die öffentliche Verwaltung, gilt es, ein solches „Worst Case“-Szenario unbedingt zu vermeiden.

Die Sicherheitsexperten des SAX.CERT registrierten im Berichtszeitraum eine allgemein angespannte Lage in Bezug auf Ransomware, durchaus auch mit Sicherheitsvorfällen in Sachsen, allerdings immer außerhalb des Sächsischen Verwaltungsnetzes. Für bundesweites Aufsehen sorgte der Ransomware-Vorfall in der Landkreisverwaltung Anhalt-Bitterfeld. Nicht zuletzt, weil die Landkreisverwaltung aufgrund der schweren Betroffenheit den Katastrophenfall ausgerufen hatte. Hier wurden Anfang Juli die ersten Verschlüsselungen festgestellt und im weiteren Verlauf daraufhin alle IT-Systeme heruntergefahren. Den Angaben zufolge wurden bei dem Angriff Daten ausgeleitet und sämtliche Daten verschlüsselt, die auf dem Server gespeichert sind. Damit war die Landkreisverwaltung nicht in der Lage, den rund 158.000 Einwohnern des Landkreises, Dienstleistungen wie die Auszahlung von Sozialleistungen, KFZ-Zulassungen und dergleichen anzubieten. Die Hacker forderten für die Entschlüsselung ein Lösegeld und drohten in der Folge auch mit der Veröffentlichung von Daten. Da kein Lösegeld bezahlt wurde, veröffentlichten sie einen ersten Datensatz im so genannten Darknet, einem Teilbereich des Internets, der nur durch bestimmte Zugangssoftware erreichbar ist. Für die vollständige Wiederherstellung der IT-Systeme wurden mehrere Monate veranschlagt. Neben dem öffentlichen Vertrauensverlust sind durch Notfallmaßnahmen als auch den Neuaufbau von IT-Systemen enorme Kosten für die Behörde zu erwarten.

2.2.2. Schwachstellen in ungepatchter Software

Beinahe täglich werden neue Sicherheitslücken bekannt, die zu einer Gefährdung ganzer IT-Netzwerke 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 Landes- und Kommunalverwaltung einen kostenlosen Warndienst zu über 1.200 Soft- und Hardwareprodukten an, der per E-Mail gezielt zu den vom Nutzer ausgewählten Produkten warnt, sobald hier neue Lücken bekannt werden. Eine breitere Nutzung dieses Dienstes wird ausdrücklich empfohlen. Welche Risiken bei nicht gepatchten Sicherheitslücken auftreten, zeigten deutlich mehrere Lücken in der Software Microsoft Exchange Server, die im März 2021 bekannt wurden.

Exchange-Lücke

In der Nacht zum 3. März 2021 veröffentlichte Microsoft Updates für Microsoft Exchange Server. Damit sollten vier Schwachstellen geschlossen werden, die in Kombination bereits für Angriffe ausgenutzt wurden und es den Angreifern ermöglichten, Daten abzugreifen oder weitere Schadsoftware nachzuladen und auszuführen. Das SAX.CERT verteilte sofort eine Warnmeldung zu diesem Thema. Am selben Tage waren nahezu alle Exchange-Systeme der Staatsverwaltung gepatcht, was vor allem auf die weitgehende Zentralisierung des Betriebes der Exchange-Server beim Staatsbetrieb SID zurückzuführen ist.

Das SAX.CERT begann unmittelbar mit Netz-Scans zur Ermittlung potentiell gefährdeter Systeme und informierte die zuständigen BfIS der Ressorts über die Betroffenheit in deren Geschäftsbereich. Auch das CERT-Bund übermittelte eine Liste mit vermeintlich verwundbaren Systemen in Sachsen, mit der das SAX.CERT weitere Einrichtungen im kommunalen Bereich informierte.

Mit zunehmendem Erkenntnisgewinn über die Ausnutzung der Schwachstelle bundesweit und den darauf ausgerichteten Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Microsoft zur Abwehr von Angriffen, wurden in der Folge durch das SAX.CERT weitere Updates zur Warnmeldung an die Behörden ausgegeben. Für Sachsen erhielt das SAX.CERT fünf Vorfallmeldungen sowohl von staatlichen als auch nicht-staatlichen Stellen zu betroffenen Systemen, ein weiterer Fall wurde durch die Medien bekannt. Die Polizei registrierte allein vom 8. bis 18. März 2021 zehn Anzeigen zu diesem Thema.

Das SAX.CERT scannte in den folgenden Wochen mehrfach die bekannten Systeme, um den Update-Verlauf der verwundbaren Systeme zu verfolgen. In Einzelfällen war das SAX.CERT auch beratend bei der Prüfung auf Kompromittierung tätig.

Kritischere Auswirkungen sind in Sachsen nicht eingetreten, sicher auch wegen der frühzeitigen direkten Ansprache der Betreiber durch das SAX.CERT. In Deutschland insgesamt waren auch zwei Wochen nach der Warnmeldung zu den Schwachstellen bei Exchange noch rund 20.000 Exchange-Installationen verwundbar. 11.000 erfolgreich angegriffene Systeme wurden allein in diesem Zeitraum gezählt. Aufgrund der vom BSI ausgerufenen höchsten Warnstufe Rot informierte der Beauftragte für Informationstechnologie des Freistaats Sachsen (Chief Information Officer - CIO), Herr Staatssekretär Thomas Popp, am 16. März 2021 das Kabinett über die Sicherheitslage und die vollzogenen Sicherheitsmaßnahmen.

2.3. Informationssicherheit in der Corona-Pandemie

Die Corona-Pandemie blieb für die Informationssicherheit der sächsischen Behörden auch im Zeitraum dieses Jahresberichts weiterhin sehr herausfordernd. Auch Monate nach dem Beginn der Pandemie und dem damit verbundenen starken Anstieg der Nutzung des Homeoffices gerieten Arbeitsprozesse und -abläufe immer wieder an Belastungsgrenzen. IT-Kapazitäten wie verfügbare Bandbreite an Netzschnittstellen, parallel mögliche Netzzugriffe von außen aber auch die maximalen Nutzerzahlen für Web- und Videokonferenzen mussten überwacht und bedarfsgerecht angepasst und erweitert werden.

Im Fokus von IT-Vorfällen stand dabei besonders der Bereich Schule. Egal ob kommunal oder staatlich verantwortet, zeigen einige Beispiele, dass die Corona-Pandemie einen Digitalisierungsgrad des Schulbetriebs erzwang, der die Sicherheit und Verfügbarkeit von pädagogisch genutzten IT-Anwendungen mit den physisch darunterliegenden IT-Plattformen vor große Herausforderungen stellte.

LernSAX

Seit dem Start der häuslichen Lernzeit für Schülerinnen und Schüler in Sachsen kam es teilweise zu erheblichen Zugriffs- bzw. Erreichbarkeitseinschränkungen der sächsischen Lernplattform LernSax. Grund dafür war nach Darstellung des Staatsministeriums für Kultus ein Cyberangriff auf die extern, nicht in der Landesverwaltung betriebene Lernplattform LernSax am 9. Dezember 2020, sowie weitere Cyberangriffe seit dem 16. Dezember 2020 in mehreren Wellen auf Angebote anderer Bildungsanbieter, welche im selben Rechenzentrum betrieben werden wie LernSax. Durch diese so genannten DDoS-Angriffe (Distributed Denial of Service – Überlastungsangriff), die mit ihren massenhaften Daten-Anfragen die Dienste funktionsunfähig gemacht haben, sei LernSax kollateral ebenfalls in seiner Funktionsweise stark beeinträchtigt gewesen. Reguläre Anfragen (Lehrer stellen Daten auf die Plattform, Schüler rufen sie ab etc.) seien in der Folge nur sehr langsam bzw. gar nicht bearbeitet worden. Anfang Januar 2021 kamen zu den DDoS-Angriffen auch noch Konfigurationsfehler durch das IT-Personal des externen Betreibers hinzu, die zum Ausfall der Plattform führten. Jedoch hatten auch Schulplattformen anderer Bundesländer mit solchen Ausfällen zu kämpfen. Auch hier wurde häufig von DDoS-Angriffen berichtet. Da es sich um ein Rechenzentrum eines privaten Betreibers handelt, war das SVN nicht berührt. Generell haben DDoS-Angriffe nicht das Ziel, in Computer einzudringen, sondern werden durchgeführt, um Systeme zu blockieren. Damit wird, bezogen auf die Informationssicherheit, das Schutzziel der Verfügbarkeit berührt.

Schulen im Fokus von Cyberkriminellen

Nicht nur das landesweite Lernportal des Freistaats, sondern auch Schulen selbst waren im selben Zeitraum von Cyberangriffen betroffen. So nutzten Hacker in einem Fall die Weihnachtsfeiertage, um die Homepage einer Schule zu kompromittieren. Dabei wurden die Inhalte auf der Schul-Webseite manipuliert und LernSax-E-Mail-Adressen von Lehrerinnen und Lehrern missbraucht. Der IT-Dienstleister setzte den Server zurück und die Schulhomepage wurde komplett neu erstellt.

Über einen weiteren Hackerangriff auf eine andere Schule informierte einige Wochen später das Landesamt für Schule und Bildung. Der Fall wurde bei der Polizei angezeigt und externe Unterstützung beauftragt.

Im Zusammenhang mit der Pandemie-Lage lässt sich auch mit dem Verweis auf andere Infrastrukturen, wie z. B. Impfmittelhersteller, feststellen, dass es vermehrt Cyberangriffe auf Infrastrukturen mit einer besonderen Rolle in dieser Situation gibt. Daher sollte aus staatlicher Sicht besonderer Wert auf einen möglichst hohen Informationssicherheitsschutz der genutzten IT-Systeme gelegt werden, da es sich im hohen Maße um eine Aufgabe im Bereich der Daseinsvorsorge handelt.

3. Tätigkeitsbericht des Beauftragten für Informationssicherheit des Landes

Der BfIS Land ist laut SächsISichG u. a. für die Erstellung des Informationssicherheitsmanagementsystems (ISMS) für die sächsische Staatsverwaltung zuständig und erstellt 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. Zur Gewährleistung hinreichender Transparenz ist der BfIS Land zur jährlichen Berichterstattung über seine Tätigkeit an den Landtag verpflichtet.

3.1. Anordnungen und Empfehlungen

Gegenüber an das SVN angeschlossenen staatlichen Stellen kann der BfIS Land 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 Kommunalen Datennetzes (KDN). Im Berichtszeitraum hat der BfIS Land keine Anordnungen oder Maßnahmen im obigen Sinn umsetzen müssen.

3.2. Gremienarbeit

Auf Landesebene hält der BfIS Land den Vorsitz der Arbeitsgemeinschaft Informationssicherheit (AG IS) und nimmt darüber hinaus als ständiger Vertreter an den Gremiensitzungen verschiedener Fachgremien, u. a. des Arbeitskreises IT und E-Government (AK ITEG) und des Arbeitskreises SVN teil. Auf Einladung bzw. sofern verbindliche Mindeststandards zur Informationssicherheit zu beschließen sind, nimmt er zudem am Lenkungsausschuss IT und E-Government (LA ITEG) teil.

3.2.1. AG Informationssicherheit Land Sachsen

Um eine angemessene Informationssicherheit in den staatlichen Behörden zu realisieren, ist ein landesweites ISMS auf Basis der jeweils geltenden BSI-Standards aufzubauen. Das landesweite ISMS verzahnt das ISMS auf Ebene der staatlichen Behörden. Zentral für den hierfür notwendigen Austausch der Behörden untereinander und das Erarbeiten von landesweiten Richtlinien und Standards ist die AG IS. Im Berichtszeitraum trafen sich die BfIS der Ressorts und die weiteren Teilnehmer der AG zu insgesamt sechs Sitzungen (bis auf eine Sitzung allesamt als Online-Meeting).

Zwei-Faktor-Authentisierung (2FA) für MS Outlook Web App (OWA)

Durch die Ausweitung des Home-Office in der Corona-Pandemie - aber auch ganz generell durch die Zunahme mobilen Arbeitens mit Smartphones und Laptops - werden verstärkt dienstliche Anwendungen genutzt, die aus dem Internet erreichbar sind. Dazu gehört in erster Linie die als OWA bekannte Anwendung, mit der von allen internetfähigen Geräten auf die dienstlichen Outlook-Funktionen wie Mail und Kalender zugegriffen werden kann. Um die Sicherheit der auf diesem Weg erreichbaren Daten zu erhöhen, wurde ausgehend von einem Beschluss der AG IS im November 2020 die Einführung der 2FA für OWA vorbereitet. Nach Aktivierung der 2FA werden die Nutzerinnen und Nutzer mit einer E-Mail-Adresse im sachsen.de-Adressraum künftig nur noch unter der Verwendung eines persönlichen OTP-Tokens (Hardware) bzw. einer Authenticator App (Software auf Smartphone) Zugang zu OWA erhalten. In der Staatsverwaltung sind bereits viele Bedienstete mit Soft- oder Hard-Token ausgestattet, da nur so ein Zugriff aus dem Home-Office auf dienstliche IT-Infrastrukturen möglich ist.

Abschaltung OWA offline

Ebenfalls wurde von der AG IS beschlossen, den Offlinezugriff als Option der OWA-Nutzung zentral deaktivieren zu lassen. Die Deaktivierung wurde am 31. Mai 2021 vollzogen. Der Offlinezugriff ist aus Sicht der Informationssicherheit deshalb problematisch, weil bei dieser Verwendung regelmäßig viele Daten aus dem Mailprogramm auf den Rechner heruntergeladen werden, um das Mailprogramm auch ohne Internetzugriff nutzen zu können. Der Rechner kann dabei auch privat genutzt sein, womit eine Vermischung von privaten und dienstlichen Daten auf einem privat administrierten, potenziell unsicheren, Gerät stattfindet.

3.2.2. Lenkungsausschuss IT- und E-Government

Der Beschluss der AG IS aus dem Januar 2020 zur Richtlinie Schutzbedarfe wurde gemäß § 5 Absatz 6 SächsISichG in den LA ITEG als Beschlussvorlage eingereicht. Die Richtlinie definiert verbindlich für alle staatlichen Stellen die für ein Sicherheitskonzept nach BSI-Standard 200-2 notwendigen Schutzbedarfe. In der Sitzung wurde erläutert, dass sich die Angaben zu Schäden in den Kategorien auf mittelbare und unmittelbare Schadereignisse beziehen. Eine weitergehende Festlegung ist aus Sicht des BfIS Land nicht möglich. Die Richtlinie wurde vom Gremium im Juni 2021 beschlossen und ist dadurch ein ressortübergreifender Standard.

3.3. Sensibilisierung und Fortbildung

Sowohl das SächsISichG (§ 5 Absatz 1 Satz 3) als auch die Datenschutzgrundverordnung beschreiben, wie wichtig die Sensibilisierung und das Training von Mitarbeiterinnen und Mitarbeitern zum Thema Informationssicherheit sind. Dabei geht es zum einen darum, vor Gefahren bei der alltäglichen Nutzung von PC, Smartphone und Internet zu sensibilisieren, und andererseits Kompetenzen zur Gefahrenabwehr zu vermitteln. Da nur die wenigsten Mitarbeiterinnen und Mitarbeiter in der Verwaltung IT-Experten sind, kann das benötigte Wissen am besten über einfache Regeln und verständliche Sicherheitsmaßnahmen vermittelt werden.

Sensibilisierung und Fortbildung sind dabei kein Selbstzweck. Der größte Teil der Cyberangriffe benötigt neben unsicheren Systemen den Menschen als Nutzer der Informationstechnik als unfreiwilligen Komplizen. So sind die im Kapitel 2.2. Angriffsmethoden und -mittel beschriebenen Szenarien zumeist nur möglich, wenn der IT-Nutzer z. B. durch einen unbedachten Klick auf einen Mail-Anhang oder einen Link Schadcode aktiviert. Auch personenbezogene Anmeldedaten werden häufig durch fahrlässiges Handeln der Computernutzer von Hackern abgegriffen. In diesen Fällen können selbst beste Technik und durchdachte Sicherheitsvorkehrungen kaum die Informationssicherheit bewahren. Dies wissend, fokussieren sich Cyberkriminelle stark auf den menschlichen Faktor anstatt nur auf technische Schwachstellen. Solange der einzelne Nutzer Defizite im Umgang mit technischen Mitteln wie seinem Arbeitsplatzrechner zeigt, führt der Weg zu einer nachhaltigen Erhöhung der Informationssicherheit nur über die Sensibilisierung und Fortbildung eines jeden Einzelnen. Das gilt gerade auch für die öffentliche Verwaltung.

E-Learning zur Informationssicherheit – Starker Anstieg der Teilnehmerzahlen

Die Corona-Pandemie hat nicht nur für die IT-Systeme einen Stresstest bedeutet, sondern auch die Sensibilisierung und Fortbildung der Mitarbeiter erschwert. Ein bis auf den letzten Platz gefülltes Rundkino mit seinen knapp 900 Sitzen oder gar über 1.200 Teilnehmern im Kulturpalast Dresden, wie in den Vorjahren bei den Sensibilisierungsveranstaltungen zur Informationssicherheit erreicht, sind seit dem Ausbruch der Corona-Pandemie nicht mehr möglich. Daher hat der BfIS Land in Zusammenwirken mit seinen Kolleginnen und Kollegen in den Verwaltungen auf Landesebene und in

den Kommunen die Werbung für das E-Learning-Angebot zur „Informationssicherheit am Arbeitsplatz“ massiv verstärkt.

Dieses Angebot wurde seit 2018 anfänglich auf einer kleinen Plattform an der Hochschule Meißen (FH) und Fortbildungszentrum angeboten, und ermöglicht es Mitarbeiterinnen und Mitarbeitern von Behörden, sich mit dem kostenfreien Online-Lernangebot selbstständig zum sicheren Umgang mit Informationstechnik fortzubilden. Unterstützt werden sie dabei von den Protagonisten des digitalen Rätsels in Comic-Optik, Herrn Sibe und dem Hund „@gar“, die die Teilnehmer durch die Kapitel „Sichere Passwörter“, „E-Mails sicher machen“, „Viren die rote Karte zeigen“, „Augen auf beim Surfen“, „Sorgfalt bei Sticks & Co.“, „Mobile Geräte nutzen“, „Vorsicht vor Daten-Dieben“ sowie „Social Engineering“ mit wertvollem Hintergrundwissen führen. So beansprucht das Lernangebot je nach Vorwissen drei bis fünf Stunden, wobei jederzeit unterbrochen und zu einem späteren Zeitpunkt fortgesetzt werden kann.

Noch vor dem Beginn der Corona-Pandemie wurde die Plattform technisch ausgebaut, so dass sich deutlich mehr Nutzer für das Angebot registrieren konnten. Und als in den ersten Wochen und Monaten der Corona-Pandemie die Nutzung der Telearbeit bzw. die Wahrnehmung des Home-Office in den Behörden stark anstieg, wurde auch die Erreichbarkeit der E-Learning-Plattform erweitert. So war die Plattform nunmehr auch aus dem Internet erreichbar, so dass ein Anschluss des Computers an das Behördennetz keine zwingende Voraussetzung für die Teilnahme mehr ist.

Ende August 2020 startete in den sächsischen Behörden dann eine groß angelegte Werbekampagne zum E-Learning-Angebot. Ziel war es, noch mehr Mitarbeiterinnen und Mitarbeiter der Behörden dazu zu bewegen, den Online-Kurs zur „Informationssicherheit am Arbeitsplatz“ zu absolvieren – und das mit Erfolg. Seit dem Start der Werbekampagne mit verschiedenen Plakatmotiven [s. Bild] kamen monatlich im Schnitt gut 400 neue Teilnehmer hinzu, mehr als 600 Plakate wurden verteilt.

Abbildung 3: Plakate zum E-Learning

Das E-Learning-Modul wird mittlerweile mit einem verpflichtenden Teilnahmeschein und einem freiwilligen Online-Test zum Sächsischen Informationssicherheits-Schein (SISS) abgeschlossen. Seit der Migration des Angebots von der HSF Meißen in den Staatsbetrieb SID im Oktober 2019 und den damit erweiterten Funktionalitäten (Selbstregistrierung der Teilnehmer, Erweiterung der Kapazität auf 5.000 gleichzeitige Nutzer) haben 6.322 Nutzer den Teilnahmeschein erworben (bis Juli 2020 waren es 946 Nutzer) und 6.686 Nutzer den Test zum Sächsischen Informationssicherheitsschein (SISS) erfolgreich absolviert (bis Juli 2020 waren es 1.222 Nutzer). Mit den vorherigen gut 1.700 Absolventen des E-Learnings an der HSF Meißen haben damit insgesamt fast 8.400 Nutzer den Kurs zur „Informationssicherheit am Arbeitsplatz“ belegt und mit einem Schein abgeschlossen. Beide Zertifikate erhalten die Teilnehmer komfortabel per Download auf der Online-Plattform.

Schaut man sich die Verteilung der Teilnehmer auf die Behörden im Freistaat an, liegen die Behörden der Landesverwaltung derzeit deutlich vor den Kommunen. Fast 75 % der Teilnehmer kommen aus den Ministerien und ihren nachgeordneten Behörden, doch die Kommunen holen auf. Im Jahr 2020 wurde nicht einmal jeder sechste Sächsische Informationssicherheitsschein von einer Mitarbeiterin bzw. einem Mitarbeiter aus den Kommunen abgelegt, in diesem Jahr hingegen bereits jeder zweite. Nachdem im Jahr 2020 noch Limbach-Oberfrohna die Kommune mit den meisten Teilnehmern war, ist seit Beginn des Jahres 2021 die Landeshauptstadt Dresden mit weitem Abstand davongezogen. Die Landeshauptstadt hatte nach einer detaillierten Vorbereitung das E-Learning zur Informationssicherheit zu einer verpflichtenden Schulung ihrer über 15.000 Mitarbeiterinnen und Mitarbeiter erklärt. Das Vorgehen zur Einführung und Bewerbung des E-Learnings in Dresden zeigt dabei exemplarisch, wie es einer Kommune gelingen kann, die Informationssicherheit der eigenen Behörde zu erhöhen, indem man möglichst viele Mitarbeiterinnen und Mitarbeiter in diesem Thema fortbildet.

Tabelle 1: Teilnehmer am E-Learning ausgewählter staatlicher und nicht-staatlicher Stellen

(Stand: 2. Juli 2021)

ausgewählte staatliche Stellen	Teilnahmeschein	Test bestanden
justiz.sachsen.de	468	432
polizei.sachsen.de	56	84
dresden.de	1520	1911
smf.sachsen.de	179	163
smi.sachsen.de	196	141
smk.sachsen.de	83	74
sms.sachsen.de	29	32
smul.sachsen.de	1369	1091
kv-sachsen.de	120	120
smwk.sachsen.de	21	16
statistik.sachsen.de	39	329
lds.sachsen.de	838	977
ltv.sachsen.de	566	603

Hinweis: Teilnehmer seit Start im Jahr 2018; reine Teilnahmebescheinigungen werden seit Februar 2020 ausgestellt, davor war nur der Abschluss mittels Test möglich.

3.4. Zusammenarbeit mit den Kommunen

Nicht nur beim E-Learning, sondern auch bei der Fortbildung von Informationssicherheits-Experten half der BfIS Land den Kommunen im Berichtszeitraum. So unterstützte der Landesbeauftragte den Sächsischen Städte- und Gemeindebund (SSG) finanziell bei der Ausrichtung von Fortbildungsseminaren zum IT-Sicherheitsbeauftragten (IT-SiBe), die mit der Qualifizierung zum IT-Grundschutz-Praktiker nach Prüfungskriterien des BSI abschließen. An den vier Lehrgängen, die aufgrund der Corona-Pandemie allesamt online stattfinden mussten, nahmen nach Angaben des SSG 82 Mitarbeiterinnen und Mitarbeiter teil, die als Informationssicherheitsbeauftragte in ihrer Behörde fungieren.

Gemeinsam mit den bereits benannten kommunalen BfIS bilden diese neu zertifizierten Sicherheitsbeauftragten den Grundstock für das kommunale Netzwerk im Bereich Informationssicherheit. Das Sicherheitsnotfallteam SAX. CERT bot diesem Netzwerk im Auftrag des BfIS Land im Berichtszeitraum weitere Sicherheitsdienstleistungen an, die in Kapitel 4 im Detail dargestellt werden.

3.5. Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik

Der BfIS Land setzt sich seit jeher für eine enge Zusammenarbeit der Bundesländer mit dem BSI ein. Zwischen der Staatskanzlei und dem BSI existiert seit November 2018 eine Absichtserklärung zu einer engeren Zusammenarbeit.

Im Berichtszeitraum standen vor allem folgende Bereiche im Mittelpunkt:

- Austausch zu Prozessen der Prävention von Cyber-Angriffen und des IT-Krisenmanagements mit dem CERT-Bund des BSI,
- Informationsaustausch zum Aufbau einer leistungsfähigen Cyber-Abwehr im Bereich der Detektion und der Reaktion,
- Austausch zur Stärkung der Resilienz bestehender IT-Lösungen (z. B. Web-Checks, Penetrationstests),

Einen zusätzlichen positiven Effekt auf die Zusammenarbeit wird dabei auch der Außenstelle des BSI in Sachsen zukommen, die am 1. Juli 2021 offiziell eröffnet wurde. Ziel des BSI ist es, mit dem Dienstsitz Freital von der Nähe zum Innovationscluster in der Region Dresden und den daraus entstehenden Synergieeffekten zu profitieren. Mit ca. 200 Stellen bis Ende 2022 werden in Freital insbesondere die Themen Sicherheit in Chiptechnologien und von 5G-und 6G-Netzen sowie der Digitale Verbraucherschutz angesiedelt.

4. Sicherheitsangebote des SAX.CERT für Landesverwaltung und Kommunen

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 staatlichen und nicht-staatlichen 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 dem 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 der Kunde aus aktuell mehr als 1.200 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 Nutzer. Der Warndienst wurde Stand August 2021 von 204 Abonnenten im Freistaat Sachsen aktiv genutzt (112 im Bereich Land, 92 im Bereich Kommunen). Das stellt nahezu eine Verdopplung der Nutzerzahlen im Vergleich zum Vorjahreszeitraum dar, der vor allem auf hohe Zuwächse bei den Kommunen zurückgeht.

4.2. Sicherheitsprüfung Webseiten

Auf Grundlage des Beschlusses 3/2017 "Automatische Scandienste und Erhöhung der Webseitensicherheit" des AK ITEG werden zweimal monatlich knapp 7.200 Internetseiten der Landes- und Kommunalverwaltung durch das SAX.CERT auf veraltete Software und bekannte Schwachstellen getestet (Vorjahreszeitraum: 6.000). Bei schwerwiegenden Sicherheitslücken werden die Betroffenen informiert. Bei den Kommunen erfolgt das in der Regel über die KDN GmbH, soweit dem SAX.CERT kein direkter Ansprechpartner bekannt ist.

Um die Kommunikation und den Informationsaustausch entscheidend zu verbessern, wurde vom SAX.CERT im November 2020 ein Informationsportal ins Leben gerufen. In der aktuellen Version dient das Infoportal dem Abgleich der durch die Ressorts betriebenen Webseiten. Dabei wird das Ziel verfolgt, bei Bekanntwerden von Schwachstellen diese kritischen Gefahren zeitnah an die betroffenen Behörden weiterzuleiten. Ein schnelles und zielgerichtetes Vorgehen ist dabei von besonderer Bedeutung, denn Zeit spielt in diesem Zusammenhang oftmals eine wesentliche Rolle. Zum jetzigen Zeitpunkt stellt das Infoportal eine Liste mit den im jeweiligen Ressort betriebenen Webseiten bereit. Die BfIS der Ressorts haben darüber hinaus die Möglichkeit, eine Kontaktliste zu verwalten, mit deren Hilfe dem Team vom SAX.CERT ermöglicht werden soll, bei erkennbaren Gefahren den jeweils Zuständigen schnell und zielgerichtet erreichen zu können. Zudem erhalten Nutzer Kenntnis über den derzeitigen Status jeder ressortbezogenen Webseite, sowie den aktuellen Status einer möglichen Abschaltung einer Webseite, sofern diese sicherheitskritische Lücken aufweist.

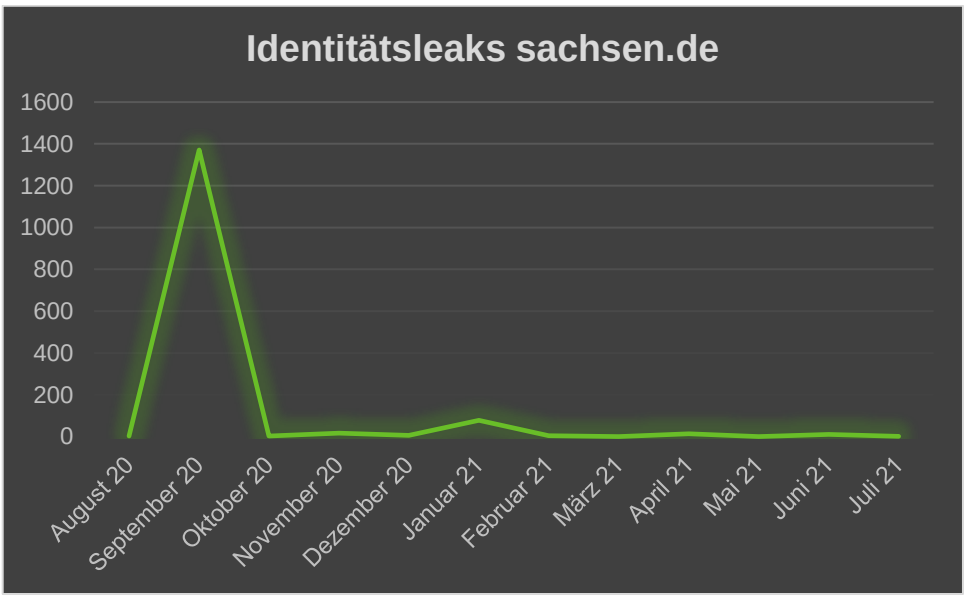
Im weiteren Verlauf soll auf dieser Basis das Infoportal um weitere Funktionalitäten erweitert werden. Vorgesehen sind hier eine detaillierte Auswertung und Gefahreneinstufung durch die von den monatlich durchgeführten Webseitenscans gefundenen Schwachstellen, sowie die Möglichkeit einen Sicherheitsvorfall melden zu können. Die Anzeige der an den Schutzsystemen vorhandenen Sperrlisten soll Nutzern darüber hinaus die notwendigen Kenntnisse liefern, wenn Zugriffe auf das Internet blockiert werden.

4.3. Identity Leak Checker

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-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 (HPI) einen individuellen Dienst zur Überprüfung von E-Mail-Adressen des Freistaates Sachsen auf die Betroffenheit von derartigen Leaks an, mit dem alle Maildomains der Landesverwaltung ständig überwacht werden. Auf Antrag können über das SAX.CERT weitere Mail-Domains in den Dienst aufgenommen werden, was im Berichtszeitraum von 20 Nutzern außerhalb der Landesverwaltung und zwei Hochschulen genutzt wurde.

Im September 2020 wurden hier die meisten Abflüsse von Anmeldedaten sächsischer Behörden gemeldet: Insgesamt über 6.100 Anmeldedaten (Vorjahr: 1.000) zu E-Mails-Accounts registrierte der Identity Leak Checker, darunter 1505 E-Mail-Adressen der Domain Sachsen.de mit zugehörigen Klartextpasswörtern. Im Vorjahreszeitraum waren es lediglich 74 E-Mail-Adressen. Die betroffenen Behörden wurden, wie in solchen Fällen üblich, umgehend automatisiert gewarnt, um die Accounts die betroffenen Nutzer zu sperren und neu aufzusetzen.

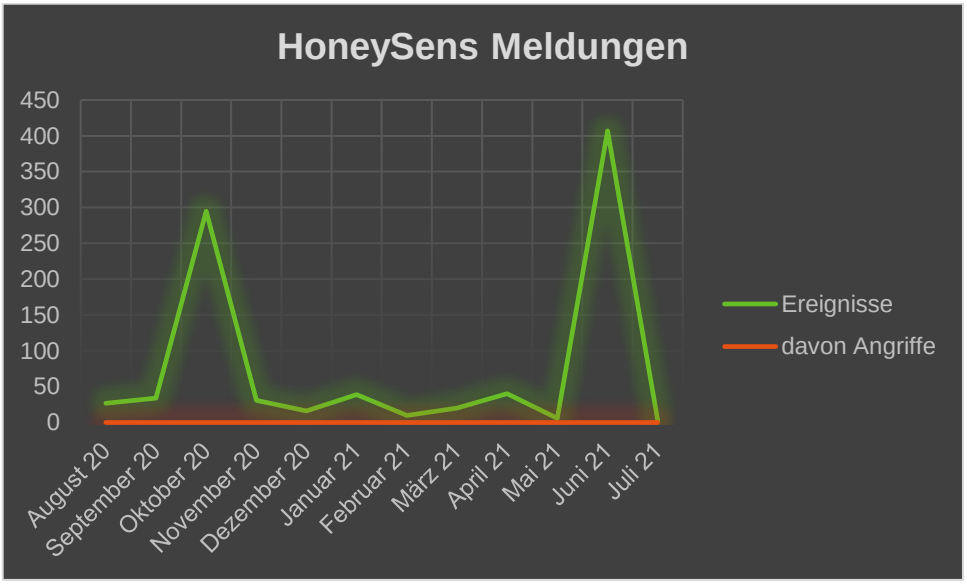
Abbildung 4: Gemeldete Identitätsdatenleaks von E-Mail-Accounts der Domain sachsen.de



4.4. HoneySens – Einbruchssensor

HoneySens ist eine Sicherheitslösung zur Erkennung von Hacker-Angriffen in internen Netzwerken, bestehend aus Sensoren/Clients zur Überwachung des Netzwerks sowie einer zentralen Serverinstanz, an die die Clients verdächtige Zugriffsversuche melden. Interessierte können beim SAX.CERT kostenlos Sensoren beantragen, die anschließend im eigenen Netzwerk betrieben werden können. Bei sicherheitsrelevanten Zugriffen wird 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. Zum Zeitpunkt der Erstellung dieses Berichts (August 2020) waren insgesamt 28 Sensoren im produktiven Einsatz (12 Land, 16 Kommunen).

Abbildung 5: Zugriffe auf den Sensor HoneySens



4.5. Passwort-Checker

Als Sensibilisierung für die Mitarbeiterinnen und Mitarbeiter der Landesverwaltung bietet das SAX.CERT seit Juli 2021 einen Passwort-Checker auf seiner Internetseite https://apps.sachsen.de/cert/passwortcheck 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 Sicherheitsnotfallteam oder durch andere staatliche wie auch nicht-staatliche Stellen, an den 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 als auch der staatlichen und nicht-staatlichen Stellen zum Schutze der Informationssicherheit. Im Rahmen seiner Fachaufsicht über das SAX.CERT hat der BfIS Land die Daten vom Sicherheitsnotfallteam angefordert. Die Übermittlung etwaiger Daten bezogen auf die nachfolgend in der Tabelle aufgelisteten im Gesetz benannten Arten der Datenverarbeitung in den staatlichen und nicht-staatlichen Stellen hat laut Gesetz durch die Behörden selbst 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.

Tabelle 2: Anzahl von Fällen der Bearbeitung von Daten nach § 5 Absatz 8

(Vorjahreszahl in Klammern)

Art der Datenverarbeitung	SAX.CERT	staatliche Stellen	nicht-staatliche Stellen
Anzahl von Fällen der nicht automatisierten Auswertung, der personenbezogenen Verarbeitung und der Wiederherstellung des Personenbezugs pseudonymisierter Daten bei Protokolldaten gemäß § 13 Absatz 2	0	6 (1)	0
Anzahl von Fällen der Speicherung und der Auswertung von Inhaltsdaten und Wiederherstellung des Personenbezugs pseudonymisierter Daten gemäß § 13 Absatz 3	0	1 (0)	0
Anzahl von Fällen der nicht automatisierten Verarbeitung von Daten gemäß § 13 Absatz 4	0	0	0
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
Anzahl von gemäß §§ 15 bis 17 gemeldeten Sicherheitsereignissen und Sicherheitsvorfällen	0	42 (16)	11 (4)

5.2. Maßnahmen des SAX.CERT gemäß § 6 Absatz 3

„Das Sicherheitsnotfallteam kann zur Erfüllung seiner Aufgaben gegenüber staatlichen Stellen und nichtstaatlichen Stellen, soweit sie an das Sächsische Verwaltungsnetz oder das Kommunale Datennetz angeschlossen sind, im Einvernehmen mit dem Beauftragten für Informationssicherheit des Landes und im Benehmen mit dem jeweils zuständigen Beauftragten für Informationssicherheit die erforderlichen 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. Das umfasst insbesondere die dazu erforderliche Datenverarbeitung."

Im Berichtszeitraum wurden keine Anordnungen durch das SAX.CERT veranlasst. Im Rahmen der gefahrenabwehrenden Maßnahmen wurden an die Ressorts 19 Warnmeldungen, 6 Frühwarnungen und 3 weitere sicherheitsrelevante Informationen abgesetzt. Da das SAX.CERT seit April 2021 auch an die ihm von den Kommunen gemeldeten BfIS direkt Warnmeldungen absetzt, wurden seitdem 15 Warnmeldungen, 3 Frühwarnungen und 1 Information an d/iesen Empfängerkreis versandt.

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

Das SAX.CERT hat im Berichtszeitraum in 12.820 Fällen personenbezogene Daten gemäß § 6 Absatz 4 SächsISichG verarbeitet. Das bedeutet einen Anstieg um 2.307 Fälle (+ 21%) 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 Absenders und des Empfängers 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-Anhangs 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 Landesverwaltung 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 schadcodebehafteten E-Mails eingehend analysieren.

5.4. Maßnahmen zur Gefahrenabwehr nach § 12

„Zur Erkennung und Abwehr von Gefahren für die informationstechnischen Systeme im Freistaat Sachsen etwa durch Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung dürfen das Sicherheitsnotfallteam sowie die staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen innerhalb ihres jeweiligen Zuständigkeitsbereichs Protokolldaten erheben und automatisiert auswerten sowie die an den Schnittstellen der informationstechnischen Systeme anfallenden Protokoll- und Inhaltsdaten erheben und automatisiert auswerten, soweit dies zur Verhinderung oder Abwehr von

Angriffen auf informationstechnische Systeme der staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen oder zum Erkennen, Eingrenzen oder Beseitigen dieser Störungen der Informationssicherheit erforderlich ist."

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. Darüber hinaus meldeten einzelne Ressorts bzw. staatliche Behörden, Maßnahmen nach §§ 12, 13 SächsISichG in eigener Zuständigkeit ausgeübt zu haben. Dabei handelte es sich ausnahmslos um eine automatisierte Erhebung und Kontrolle von Daten mittels bestimmter, zumeist kommerzieller Virenscanner.

5.5. Umgang mit unzulässig erlangten Daten gemäß § 13 Absatz 8

„Eine über die [in § 13] Absätze 1 bis 7 hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. Soweit möglich, ist bei der Datenverarbeitung technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese Daten nicht verwendet werden und sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren."

Ein entsprechender Umgang mit unzulässig erlangten Daten wurde dem BfIS Land für den Berichtszeitraum nicht gemeldet.

5.6. 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.

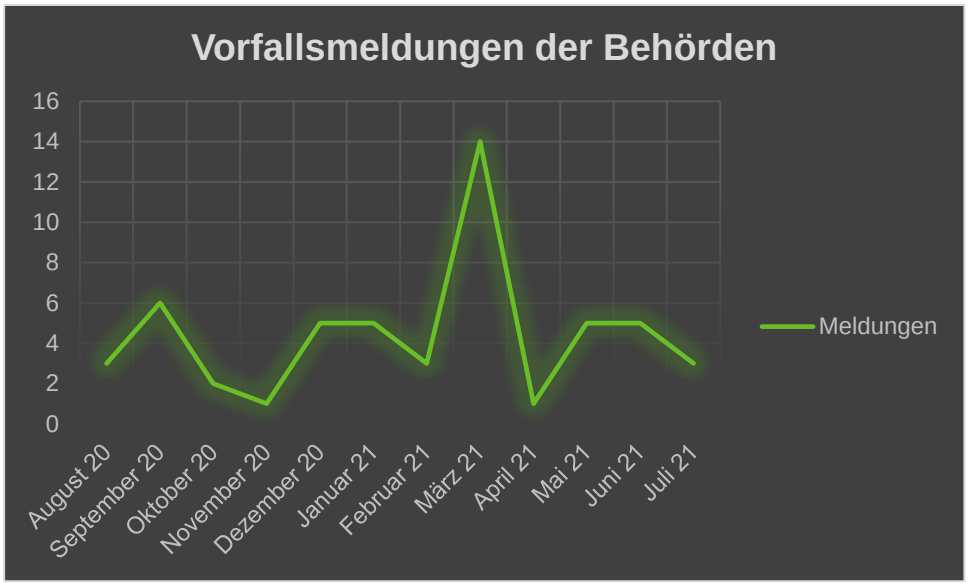
Beispiele für derartige Sicherheitsvorfälle:

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

Darüber hinaus hat der AK ITEG mit dem Beschluss 1/2016 festgelegt, dass Sicherheitsvorfälle in den Ressorts per Meldeformular an das SAX.CERT zu melden sind.

Im Berichtszeitraum wurden dem SAX.CERT über das Meldeformular 53 Sicherheitsereignisse gemeldet (42 von den staatlichen Behörden, 11 von den nicht-staatlichen Behörden). Das ist ein erheblicher Anstieg im Vergleich zu den 20 Meldungen in den 12 Vormonaten. Dieses Allzeithoch ist jedoch weniger einer stark gestiegenen Gefährdungslage als dem verbesserten Meldeverhalten der Behörden zuzuschreiben.

Abbildung 6: Gemeldete Vorfälle durch Landes- und Kommunalbehörden



6. Umsetzungsstand des SächsISichG

Das SächsISichG ist seit 31. August 2019 in Kraft. Die im Gesetz beschriebenen Maßnahmen zur Stärkung der Sicherheitsorganisation (§§ 7 bis 9 SächsISichG) sind dabei bis zum 31. Dezember 2020 im Rahmen der zur Verfügung stehenden Haushaltsmittel umzusetzen. Dazu gehören u. a. die Bestellung eines hauptamtlichen BfIS in den Ressorts und weiteren wichtigen Behörden sowie die Umsetzung eines Informationssicherheitsmanagementsystems.

6.1. Informationssicherheitsorganisation

Um die Informationssicherheitsziele zu erreichen, benötigt jede Behörde, wie auch der Freistaat Sachsen insgesamt, eine Informationssicherheitsorganisation. Hiermit sind die Personen und Prozesse gemeint, die gewährleisten sollen, dass die Ziele durch Entwicklung und Umsetzung von Maßnahmen erreicht werden. Grundlage jeder Informationssicherheitsorganisation ist die Benennung eines Zuständigen für die Informationssicherheit. Die Informationssicherheitsorganisation des Freistaates Sachsen besteht aus den zentralen strategischen und operativen Akteuren der Informationssicherheit sowie den Zuständigen für die Informationssicherheit in den wichtigsten Landesbehörden bzw. -einrichtungen, die wiederum der Kopf ihrer eigenen Informationssicherheitsorganisation sind.

Die im Gesetz benannten Ziele bezogen auf die Informationssicherheitsorganisation konnten im Berichtszeitraum zwar verbessert, allerdings noch nicht vollständig umgesetzt werden. So wurden durch die Staatskanzlei die Bedarfe für eine angemessene Personalausstattung bei den BfIS und im SAX.CERT einschließlich der aus den Ressorts gemeldeten in die Verhandlungen zum Doppelhaushalt 2021/2022 eingebracht. Im Ergebnis wurden sechs Staatsministerien mit Planstellen unterstützt, die in ihrem Ministerium bislang über keinen hauptamtlichen BfIS verfügten und damit die Anforderungen des § 7 Absatz 1 SächsISichG noch nicht erfüllt hatten. Das betrifft das Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung; das Staatsministerium für Wirtschaft, Arbeit und Verkehr; das Staatsministerium für Wissenschaft, Kultur und Tourismus; das Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt; das Staatsministerium für Kultus sowie das Staatsministerium für Regionalentwicklung.

6.1.1. Beauftragter für Informationssicherheit des Landes

Der BfIS Land bildet die zentrale strategische Instanz in der Informationssicherheitsorganisation der Behörden im Freistaat Sachsen. In seiner Zuständigkeit liegt die landesweite Förderung, Koordinierung und Abstimmung aller erforderlichen Belange der Informationssicherheit in den Behörden im Freistaat Sachsen. 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 wurden durch das SächsISichG im Vergleich zur abgelösten VwV Informationssicherheit vom 7. September 2011 erweitert und gestärkt, u. a. durch

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

Im Referat 45 in der Staatskanzlei, dem der BfIS Land als Referatsleiter vorsteht, ist neben dem in diesem Bericht adressierten Themenbereich Informationssicherheit auch die Cybersicherheit und seit dem 1. März 2020 die IT-Sicherheit kritischer Infrastrukturen angesiedelt. Hierunter fällt u. a. die Koordinierung von Cybersicherheitsthemen im Austausch mit weiteren staatlichen Akteuren wie dem

Cybercrime Competence Center des Landeskriminalamtes Sachsen, dem Landesamt für Verfassungsschutz, der Zentralstelle Cybercrime der Generalstaatsanwaltschaft Dresden und der Abteilung Katastrophenschutz im Staatsministerium des Innern.

Die Aufgabenlast aus den mit dem Gesetz verbundenen Pflichten insbesondere zur Beratung der BfIS der staatlichen und nichtstaatlichen Stellen, zur Koordination eines ISMS des Landes sowie zu den Dokumentationspflichten war im Arbeitsbereich des BfIS Land weiterhin sehr hoch und wird weiter steigen. Der Bedeutung des BfIS Land als zentrale strategische Stelle der Informationssicherheit im Freistaat Sachsen wird auch künftig insbesondere im Hinblick auf eine angemessene personelle Ausstattung des Referats Rechnung zu tragen sein.

6.1.2. Beauftragte für Informationssicherheit in den Staatsbehörden

Die BfIS der staatlichen Stellen sind zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb ihres Zuständigkeitsbereiches. Die Hauptaufgabe des BfIS besteht darin, den Leiter der staatlichen Stelle bezüglich der Informationssicherheit zu beraten und bei der Umsetzung zu unterstützen. Seine Aufgaben sind in den Standards des BSI festgelegt. Die Einsicht in sensible Protokolldaten, um sicherheitsrelevante Ereignisse zu erkennen und zu begrenzen, erfordert die Einrichtung der unabhängigen Funktion des BfIS.

Bereits seit der ersten Leitlinie Informationssicherheit des IT-Planungsrates aus dem Jahr 2013 besteht für die Landesverwaltung in Sachsen die Verpflichtung, organisatorische, technische und personelle Maßnahmen für eine angemessene IT-Sicherheit umzusetzen. Mit dem SächsISichG wurden im August 2019 diese Maßnahmen für die staatlichen Stellen unabweisbar 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 zur Verfügung stehende Haushaltsmittel zu erfolgen (§ 20 SächsISichG). Zum Zeitpunkt der Erstellung des vorliegenden Berichts im August 2021 erfüllten 13 von 15 Staatsbehörden diese gesetzliche Anforderung eines hauptamtlich bestellten BfIS. Mit Abschluss der laufenden Besetzungsverfahren der im Doppelhaushalt 21/22 übertragenen Planstellen sollte die Umsetzung der gesetzlichen Verpflichtung auch für die beiden Ministerien ohne hauptamtlichen BfIS bis Jahresende 2021 gelingen.

Tabelle 3: Hauptamtliche BfIS in den staatlichen Stellen nach § 7 Absatz 1

(Stand: 31.Juli 2021)

Hauptamtlicher BfIS	ja	nein
Staatskanzlei	x	
Staatsministerium für Energie, Klimaschutz, Umwelt und Landwirtschaft	x	
Staatsministerium der Finanzen	x	
Staatsministerium des Innern	x	
Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung	x	
Staatsministerium für Kultus		x
Staatsministerium für Regionalentwicklung	x	
Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt		x
Staatsministerium für Wirtschaft, Arbeit und Verkehr	x	
Staatsministerium für Wissenschaft, Kultur und Tourismus	x	
Leitstelle für Informationstechnologie der sächsischen Justiz	x	
Staatsbetrieb Sächsische Informatik Dienste	x	
Sächsischer Rechnungshof	x	
Landespolizeipräsidium	x	
Sächsischer Datenschutzbeauftragter	x	

Des Weiteren werden bei großen Behörden (mit mehr als 1.000 Mitarbeiterinnen und Mitarbeitern) und Behörden mit besonderer Kritikalität hauptamtliche BfIS als zwingend notwendig erachtet, obgleich sie gesetzlich nicht festgeschrieben sind.

Tabelle 4: Hauptamtliche BfIS bei staatlichen großen bzw. KRITIS-Behörden

(Stand: 31. Juli 2021)

Hauptamtlicher BfIS	ja	nein
Landesdirektion Sachsen		x
Landestalsperrenverwaltung	x	
Polizeidirektionen (koordinierend)	x	
Landesamt für Umwelt, Landwirtschaft und Geologie	x	
Staatsbetrieb Immobilien und Baumanagement	x	
Sächsische Krankenhäuser (koordinierend)		x
Landesamt für Steuern und Finanzen	x	
Gerichte (koordinierend)		x

6.1.3. Beauftragte für Informationssicherheit in den nicht-staatlichen Stellen

Nach Maßgabe von § 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 Monats zu unterrichten. Allerdings erfolgte die Meldung durch die sächsischen Kommunen trotz mehrfacher Aufforderungen über den kommunalen Spitzenverband SSG im Berichtszeitraum weiterhin zögerlich. Bis August 2021 waren alle Landkreise, aber lediglich 87 der 419 sächsischen Städte und Gemeinden ihrer gesetzlichen Pflicht zur Unterrichtung nachgekommen. BfIS Land stellt hierfür ein Online-Formular zur Verfügung.

6.1.4. Sicherheitsnotfallteam SAX.CERT

Das Sicherheitsnotfallteam SAX.CERT ist die zentrale Stelle für operative Fragen der Informationssicherheit der staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen gemäß § 6 Abs. 1 SächsISichG. Das Gesetz regelt zahlreiche Neuerungen und Aufgabenerweiterungen für das SAX.CERT im Vergleich zu vor seinem Inkrafttreten. Um diesen Aufgabenerweiterungen gerecht werden zu können, wurden im Doppelhaushalt 21/22 erste zusätzliche Planstellen ausgebracht, die bis zum Jahresende 2021 besetzt sein sollen. Um das geforderte Leistungsspektrum tatsächlich vollumfänglich abdecken zu können, ist eine weitere Personalzuführung in Folgejahren angezeigt.

So soll neben den Aufgaben als Computernotfallteam der Sächsischen Landesverwaltung das SAX.CERT auch zentraler Ansprechpartner für alle sächsischen Kommunen und für sächsische Unternehmen im KRITIS-Bereich sein und diese bei IT-Sicherheitsereignissen und -Vorfällen unterstützen und beraten. Weiterhin hat das SAX.CERT die Rolle der zentralen Meldestelle im Sinne des BSI-Gesetzes und der Meldestelle für den VerwaltungsCERT-Verbund des IT-Planungsrates wahrzunehmen. Darüber hinaus hat das SAX.CERT die Aufgabe, die Lage der Informationssicherheit im Freistaat Sachsen zu analysieren und regelmäßig darüber zu berichten. Auch der Koalitionsvertrag der Sächsischen Staatsregierung vom 20. Dezember 2019 bekräftigt noch einmal die wachsende Bedeutung des SAX.CERTs, in dem dort der Ausbau des SAX.CERT zu einem IT-Sicherheitszentrum für Land, Kommunen und Betreiber kritischer Infrastrukturen (KRITIS) festgeschrieben ist.

Trotz der Ressourceneinschränkungen in der Vergangenheit bot das SAX.CERT eine Reihe von Dienstleistungen an, die Behörden und Gerichte des Freistaates Sachsen sowie Kommunen kostenfrei in Anspruch nehmen. Diese wurden im Berichtszeitraum sowohl qualitativ als auch quantitativ weiter ausgebaut. Nichtsdestotrotz sind strukturelle Probleme geblieben, die das SAX.CERT an der Erfüllung seiner Aufgaben aus dem Gesetz einschränkt. So wird u. a. im Rahmen des begonnenen Prozesses zur Einführung einer Rechtsverordnung zum Meldeverfahren ein Weg zu finden sein, wie die Behörden die notwendigen Daten zur Erkennung und Abwehr von Gefahren für die informationstechnischen Systeme durch Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung dem SAX.CERT übermitteln können.

6.2. Rechtsverordnung zum Meldeverfahren

Das SächsISichG sieht eine Verordnungsermächtigung in § 16 Absatz 2 zum Erlass näherer Vorgaben zum Meldeverfahren vor. Das Verfahren zum Erlass der Rechtsverordnung wurde 2021 mit dem notwendigen Erforderlichkeitsbericht an die Ressorts eingeleitet.

Gemäß § 16 SächsISichG sind staatliche Stellen, aber auch nicht-staatliche Stellen, soweit deren informationstechnische Systeme mit dem SVN oder dem KDN verbunden sind, nach § 17 SächsISichG verpflichtet, meldepflichtige Ereignisse an das Sicherheitsnotfallteam SAX.CERT zu melden.

Schließlich sind sowohl das Sicherheitsnotfallteam als auch der BfIS Land auf eine konsistente Datenlage angewiesen. Nicht zuletzt dienen solche Zahlen auch dazu, die Sicherheitslage belastbar bewerten zu können, und auch die Ressourcenbedarfe für den Bereich der Informationssicherheit des Freistaates zu definieren. Die Verordnung ist notwendig und erforderlich zur Festlegung der meldepflichtigen Ereignisse und deren Meldeverfahren an das Sicherheitsnotfallteam.

Ein funktionierendes Meldewesen in der Informationssicherheit ist essentiell, um möglichen Gefährdungen wirkungsvoll begegnen zu können. So waren im Fall der Exchange-Lücken aufgrund der sehr kritischen Situation kurzfristige Reaktionszeiten der Behörden gegenüber dem Sicherheitsnotfallteam notwendig. Die geplante Rechtsverordnung sieht daher auch Regelungen vor, die die Verbindlichkeit einer Rückmeldung an das SAX.CERT erhöhen. Zudem werden konsequent eingehaltene Meldewege auch durch die Informationssicherheitsleitlinie des IT-Planungsrates eingefordert, stellen doch die Meldungen innerhalb eines Landes die Basis für den Austausch der Länder-CERTs untereinander dar. Darüber hinaus sind folgende Inhalte vorgesehen:

- eine Bestimmung, die Meldepflichten bei erheblichen Sicherheitsvorfällen entsprechend des AK ITEG-Beschlusses 1/2016 vom 12. Januar 2016 aufnimmt.
- formale Vorgaben der Meldung unter Verwendung des vom Sicherheitsnotfallteam zur Verfügung gestellten Meldeformulars.
- Regelungen zur regelmäßigen automatisierten Übermittlung von bestimmten Daten zur Erfassung und Analyse eines Lagebildes im Freistaat Sachsen durch das Sicherheitsnotfallteam, um so Warnmeldungen an die Behörden und Kommunen im Freistaat zu ermöglichen.

6.3. Verpflichtungen aus der Leitlinie Informationssicherheit des IT-Planungsrates

Anfang 2019 verabschiedete der IT-PLR die überarbeitete Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung. Nach dem dazugehörigen Umsetzungsplan waren im Berichtszeitraum die ersten Einzelmaßnahmen, die bis Ende 2020 umgesetzt sein sollten, in den sächsischen Landesbehörden überwiegend umgesetzt. Die meisten Behörden hatten demnach nach eigener Auskunft die Rollen und deren Aufgaben im Informationssicherheitsmanagement festgelegt und dokumentiert und die Rollen in den Behörden besetzt. Hingegen war in den Behörden oftmals noch kein Prozess zur Erstellung von Richtlinien für die Informationssicherheit für den jeweiligen Zuständigkeitsbereich und auch kein Prozess zur regelmäßigen Überprüfung der Richtlinien etabliert.

Der Umsetzungsplan zur Leitlinie setzt zusätzlich zum SächsISichG weitere Schwerpunkte für die Informationssicherheit, die durch die Verbindlichkeit für die Bundes- und Landesbehörden auch in Sachsen zu beachten sind. So sind bis Ende 2021 in den hiesigen Landesbehörden folgende Maßnahmen umzusetzen:

- Ein kontinuierlicher Verbesserungsprozess zur Gewährleistung von Umsetzung, Wirksamkeit und Beachtung der Informationssicherheitsmaßnahmen ist etabliert und wird angewandt.
- Es sind Konzepte im Bereich Information, Weiterbildung und Sensibilisierung aller Beschäftigten zu Themen der Informationssicherheit für unterschiedliche Mitarbeitergruppen vorhanden
- Der übergreifende Notfallmanagementprozess, z. B. in Form einer Notfallmanagement-Leitlinie, ist initiiert.
- Die Rolle des Notfallbeauftragten und dessen Aufgaben sind festgelegt und dokumentiert
- Die Ansprechpartnerinnen und –partner für das IT-Notfallmanagement (Notfallmanager) sind bei den wesentlichen Behörden benannt.

Eine Sonderrolle spielen die letzten drei Anstriche, die zum Handlungsfeld 5: Teil „IT-Notfallmanagement“ der Leitlinie Informationssicherheit gehören, da diese Thematik nicht durch das SächsISichG geregelt wird. Verschiedene Behörden wie die Polizei und auch der staatseigene IT-

Dienstleister haben bereits entsprechende Konzepte erstellt und Rollen besetzt. Darauf aufbauend gilt es nun, dies auf alle Behörden der Staatsverwaltung auszuweiten. Bereits zu Jahresbeginn 2021 hat BfIS Land einen Prozess zur Erarbeitung einer landesweiten Leitlinie zum IT-Notfallmanagement angestoßen, die als Mindeststandard und Muster-Leitlinie für alle Ressorts beschlossen und auch den Kommunen zur Adaption zur Verfügung gestellt werden soll.

7. Abbildungs- und Tabellenverzeichnis

8. Glossar

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

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.

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 Geräteausfalls 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.

Command-and-Control-Server (C&C-Server)
Server-Infrastruktur, mit der Angreifer 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 Angreifers, um dessen Befehle entgegen zu nehmen.

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

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.

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 Angreifer versucht dabei, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetnutzers zu gelangen und diese für seine Zwecke meist zulasten des Opfers zu missbrauchen.

Ransomware

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

Social Engineering

Bei Cyber-Angriffen durch Social Engineering versuchen Kriminelle, ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Angreifer geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

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. Mehr-Faktor-Authentisierung erfolgt die Authentisierung einer Identität anhand verschiedener Faktoren aus getrennten Kategorien (Wissen, Besitz oder biometrischen Merkmalen).

Herausgeber:

Sächsische Staatskanzlei

Redaktion sowie Gestaltung und Satz:

Referat 45: Informations- und Cybersicherheit, Kritische Infrastrukturen

Redaktionsschluss:

25. Oktober 2021