SÄCHSISCHE STAATSKANZLEI | Freistaat SACHSEN

Jahresbericht Informationssicherheit 2020

des Beauftragten für Informationssicherheit des Landes

Berichtszeitraum: August 2019 – Juli 2020

Inhalt

1. Einführung 4
2. Gefährdungslage 5
2.1. Gefährdungslage der Landesverwaltung 5
2.2. Angriffsmethoden und -mittel 6
2.2.1. Erpressungstrojaner 6
2.2.2. Schwachstellen in ungepatchter Software 8
2.2.3. Informationssicherheit in der Corona-Pandemie 9
3. Tätigkeitsbericht des Beauftragten für Informationssicherheit des Landes 10
3.1. Anordnungen und Empfehlungen 10
3.1.1. Sperrung Empfang alter Office-Formate 10
3.1.2. Nutzung des Extended Security Updates 10
3.1.3. Rahmenvorgabe zum Einsatz von Soft-Token auf privaten Geräten 11
3.1.4. Erinnerung Meldepflichten der Behörden 11
3.1.5. Sicherheitsempfehlungen Home-Office 12
3.2. Gremienarbeit 12
3.2.1. AG Informationssicherheit Land Sachsen (AG IS) 12
3.2.2. AK ITEG 13
3.2.3. LA ITEG 13
3.2.4. Weitere Gremien 13
3.3. Sensibilisierung und Fortbildung 13
3.3.1. Sensibilisierung durch die INFOSIC 14
3.3.2. E-Learning „Informationssicherheit am Arbeitsplatz“ 14
3.4. Zusammenarbeit mit dem BSI 16
3.4.1. Nutzung MW Scan 16
3.4.2. Verbindungsperson 16
3.4.3. Hospitation 17
4. Sicherheitsangebote des SAX.CERT für Landesverwaltung und Kommunen 17
4.1. Schwachstellenwarndienst 17
4.2. Sicherheitsprüfung Webseiten 17
4.3. Identity Leak Checker 17
4.4. HoneySens – Einbruchssensor 18
5. Bericht zu den ergriffenen Maßnahmen laut SächsISichG 19
5.1. Berichtspflichten nach § 5 Abs. 8 19
5.2. Maßnahmen des SAX.CERT gemäß § 6 Absatz 3 20
5.3. Verarbeitung personenbezogener Daten durch das SAX.CERT gemäß § 6 Abs. 4 20
5.4. Maßnahmen zur Gefahrenabwehr nach § 12 20
5.5. Umgang mit unzulässig erlangten Daten gemäß § 13 Absatz 8 21
5.6. Sicherheitsmeldungen gemäß §§ 16 und 17 21

6. Umsetzungsstand des SächsISichG 22
6.1. Informationssicherheitsorganisation 22
6.1.1. Beauftragter für Informationssicherheit des Landes 22
6.1.2. Beauftragte für Informationssicherheit in den Staatsbehörden 23
6.1.3. Beauftragte für Informationssicherheit in den nicht-staatlichen Stellen 24
6.1.4. Sicherheitsnotfallteam SAX.CERT 24
6.2. Verpflichtungen aus der Leitlinie Informationssicherheit des IT-Planungsrates 25
6.3. Ausblick 26

1. Einführung

Laut dem Risikobarometer der Allianz Versicherungsgruppe sind Cybervorfälle 2020 erstmals das wichtigste Geschäftsrisiko für Unternehmen weltweit. Auch der Staat und seine Verwaltung müssen sich diesen stark zunehmenden Gefahren stellen. Nur wenn ihre Computersysteme sicher bleiben, sind Reaktionsstärke und Handlungsfähigkeit des Staates gewährleistet.

Der Freistaat Sachsen hat diese Herausforderungen mit einem eigenen Gesetz zur Informationssicherheit angenommen. Am 31. August 2019 ist nach dem Beschluss im Sächsischen Landtag das Sächsische Informationssicherheitsgesetz (SächsISichG) in Kraft getreten. Der vorliegende Bericht für den Zeitraum August 2019 bis Juli 2020 erfüllt die damit verbundenen Berichtspflichten zu den nach dem Gesetz ergriffenen Maßnahmen. Darüber hinaus gibt er einen Überblick über die konkrete Gefährdungslage, die vom Beauftragten für Informationssicherheit der Landesverwaltung und vom Sicherheitsnotfallteam SAX.CERT eingeleiteten Maßnahmen sowie zum allgemeinen Umsetzungsstand der Informationssicherheit in der Landesverwaltung Sachsen.

Insgesamt ist dabei festzuhalten, dass die IT- Strukturen immer komplexer und vernetzter werden und sowohl die Zahl der Nutzer als auch die verarbeiteten Datenmengen ständig stark ansteigen. Damit einher geht eine höhere Verwundbarkeit der IT-Systeme, gerade auch in der öffentlichen Verwaltung. 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 es die moderne Verwaltung schaffen, für die Bürger der Vertrauensanker in der digitalen Welt zu sein.

Mit dem Sächsischen Informationssicherheitsgesetz wurde eine neue rechtliche Grundlage geschaffen, um unsere Verwaltungen vor den Cybergefahren besser zu wappnen und zu schützen. Durch das Gesetz werden die bisherigen Vorschriften zur Informationssicherheit zusammengefasst und erheblich erweitert. Demnach gehört es zu den allgemeinen behördenübergreifenden Pflichten, die Sicherheit der informationstechnischen Systeme nach dem Stand der Technik sowie im Rahmen der Verhältnismäßigkeit sicherzustellen. Mit dem neuen Gesetz wurden zudem Grundlagen dafür geschaffen, dass neben den staatlichen Stellen im Freistaat auch alle nicht-staatlichen Stellen ihr Datennetz und damit verbundene Systeme adäquat gegen Angriffe verteidigen dürfen. Der Bedeutung der Grundrechtsrelevanz entsprechend ist dabei ein mehrstufiges Verfahren vorgesehen.

Zur Verteidigung gehört auch, dass das zentrale Sicherheitsnotfallteam, das SAX.CERT im Staatsbetrieb Sächsische Informatik Dienste, personell aufgestockt wird, um beispielsweise Angriffswellen analysieren und die Abwehrmaßnahmen noch genauer ausrichten zu können. Dazu kommt, dass das SAX.CERT nunmehr auch eine Servicestelle für den kommunalen Bereich wird, um ihn in der Informationssicherheit zu unterstützen. Das Gesetz und die daraus abgeleiteten Sicherheitsmaßnahmen fokussieren auf die Lebensader der IT, also das Sächsische Verwaltungsnetz (SVN) und das Kommunale Datennetz (KDN). Sprich: Priorität unserer Schutzmaßnahmen haben alle Behörden, die im gemeinsamen Netz zusammengeschlossen sind.

Neben solchen technischen Vorteilen verbleiben die notwendigen organisatorischen Anstrengungen bei jeder Behörde selbst. Das wird auch im Gesetz deutlich. Dem Behördenleiter kommt dabei eine hohe Verantwortung für die Informationssicherheit zu. Die Leitungsebene trägt die Verantwortung dafür, dass gesetzliche Regelungen eingehalten werden und dass wichtige Geschäftsprozesse störungsfrei ablaufen. Außerdem wird mit dem Gesetz dem jeweiligen Beauftragten für Informationssicherheit (BfIS) eine Mitwirkungsbefugnis in Form des Benehmens bei wesentlichen Änderungen an informationstechnischen Systemen eingeräumt.

Weiterhin legt das Gesetz fest, dass in allen staatlichen und nicht-staatlichen Stellen ein BfIS und ein Vertreter ernannt werden sollen. In den besonders herausragenden Behörden sind die Stellen der Beauftragten dabei hauptamtlich zu besetzen. Für den Aufbau der beschriebenen Organisationsstruktur sieht das Gesetz im Rahmen der zur Verfügung stehenden Haushaltsmittel eine Übergangsregelung bis zum 31. Dezember 2020 vor, damit diese organisatorischen Vorgaben umgesetzt werden können. Der aktuelle Jahresbericht Informationssicherheit 2020 gibt also auch eine Auskunft darüber, ob die Behörden sich bereits auf einem guten Weg zur Umsetzung der gesetzlichen Verpflichtungen befinden.

2. Gefährdungslage

Das Sicherheitsnotfallteam SAX.CERT beobachtet die Gefährdungslage der IT-Sicherheit in der Landesverwaltung mit besonderem Fokus auf das Landesnetz SVN kontinuierlich und stellt in diesem Bericht die Erkenntnisse aus dem Zeitraum August 2019 bis Juli 2020 zusammen. Nach einer Zusammenfassung der Bedrohungslage werden die Methoden und Mittel der Angreifer anhand einiger Beispiele aufgezeigt.

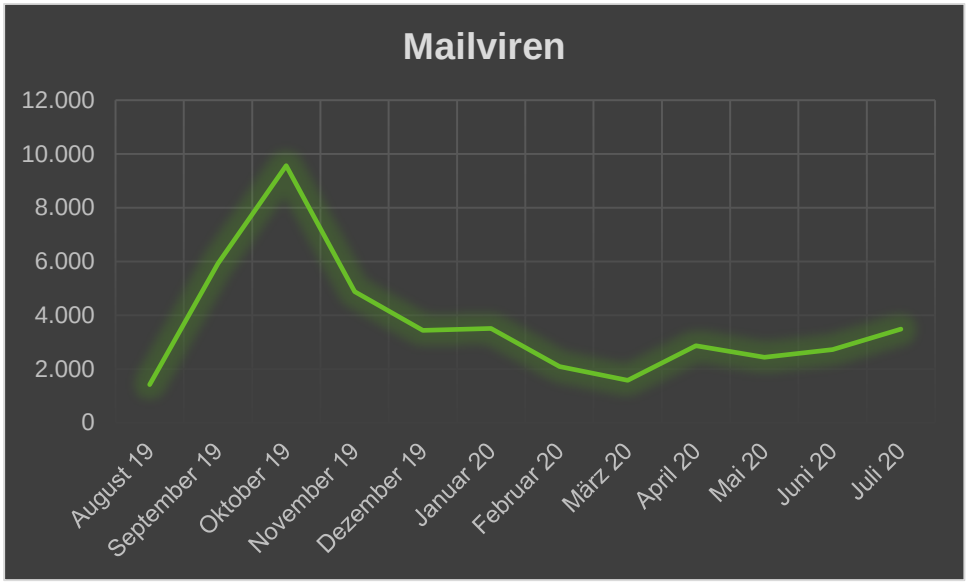
2.1. Gefährdungslage der Landesverwaltung

Das SVN als vom Internet abgekoppeltes internes Netz der Landesbehörden hat durch seine Struktur bereits ein sehr hohes Niveau der Informationssicherheit, da die bei weitem größte Gefährdung von IT-Infrastrukturen durch Cyberangriffe aus Richtung Internet besteht. Hier kommen die Schutzsysteme der zentralen Dienste des SVN zum Tragen, die die Übergänge aus dem internen Netz der Landesverwaltung von und zum Internet zeitgemäß absichern.

Von den über 184 Millionen ankommenden E-Mails wurden über 151 Mio. bereits im Vorfeld durch die Kopfstelle des SVN als Spam direkt abgewiesen und weitere knapp 6 Mio. von den internen Scannern als Spam-Mail erkannt und entsprechend markiert. Damit lag der Anteil von unerwünschten Nachrichten am Mail-Aufkommen bei über 85 Prozent.

Daneben wurden knapp 44.000 Viren im Mailverkehr abgefangen. Das sind deutlich weniger als in den 12 Monaten davor, in denen Rekordwellen registriert und infolgedessen insgesamt mehr als dreimal so viele Virenmails entdeckt worden waren. Auf der anderen Seite ist der Rückgang auch Folge von veränderten Methoden der Angreifer: So wurden und werden neben immer dynamischeren und damit immer schwerer erkennbaren Schadprogrammen in E-Mail-Anhängen seit einiger Zeit verstärkt Links auf bösartige Webseiten im E-Mail-Text versteckt. Solche Textinhalte werden von den Schutzsystemen oft nicht als Schadsoftware identifiziert. Insgesamt stieg so im Berichtszeitraum die Anzahl von gefährlichen Sicherheitsvorfällen trotz gesunkener Erkennungszahlen deutlich an.

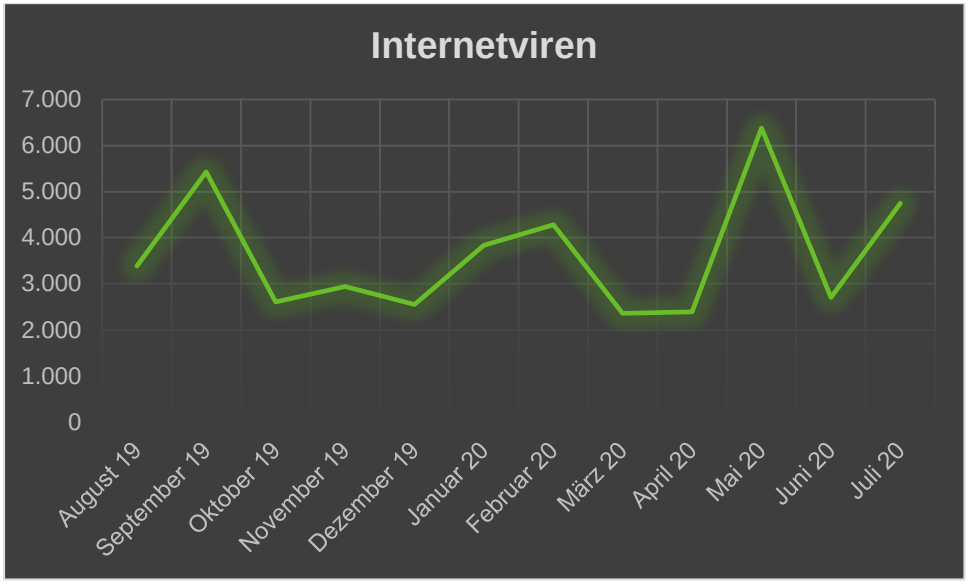
Grafik: Entdeckte Schadprogramme im SVN-Mailverkehr



Um diesem Trend entgegenzuwirken, muss einerseits schon am Eingang des SVN versucht werden, die Erkennung und direkte Abweisung unerwünschter Nachrichten durch eine Verbesserung der Spam-Filter zu erhöhen. Weiterhin ist eine umfassendere Analyse der vorhandenen Virenscannerlogs notwendig, um die Abwehrmaßnahmen u. a. auch gegen Links auf Schadsoftware passend weiterzuentwickeln. Hier hat das SächsISichG wichtige gesetzliche Grundlagen geschaffen, die nun anzuwenden sind.

Neben verseuchten E-Mails ist auch ein in Webseiten versteckter Schadcode eine der wesentlichsten Gefahren für die IT der Verwaltungen. So wurden im Internetverkehr über 43.000 Viren erkannt. In den 12 Monaten zuvor waren es noch knapp 51.000. Der Rückgang hat jedoch nicht mit einer Abnahme der Gefährdung zu tun, sondern steht auch mit der stark zunehmenden Verschlüsselung der Internetverbindungen in Zusammenhang. So sind mittlerweile über 95 % des Internetverkehrs im SVN verschlüsselt und damit für die zentralen Virenscanner nicht mehr einsehbar. Die lokalen Virenscanner auf den einzelnen Rechnern der Mitarbeiter bilden dann den einzigen Schutz beim Aufruf verschlüsselter „HTTPS"-Internetseiten. Diese lokalen Scanner haben aber bei weitem nicht die Möglichkeiten und Erkennungsraten der mächtigen zentralen Scanner mit ihren Sandboxen zur virtuellen Ausführung und Untersuchung mutmaßlicher Schadprogramme und werden diese auch nie bieten können.

Grafik: Entdeckte Schadprogramme im SVN-Internetverkehr



Eine Infektion eines lokalen Rechners kann sich aber durch die hohe Vernetzung innerhalb des SVN behördenübergreifend ausbreiten. Dass dieses Szenario nicht nur hypothetisch ist, zeigen zahlreiche aktuelle Beispiele auch aus Verwaltungen in Deutschland, wo ganze Netzwerke teils monatelang lahmgelegt wurden und massive Datenmengen abgeflossen sind. Deshalb sind weitere Maßnahmen unter Beachtung der datenschutz- und personalvertretungsrechtlichen Vorgaben notwendig, um auch gegen Schadprogramme in verschlüsselten Verbindungen vorgehen zu können. Das SächsISichG verbessert hier die gesetzlichen Grundlagen zum Einsatz entsprechender Schutzsysteme in den zentralen Diensten des SVN.

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. Erpressungstrojaner

Einer der größten Trends im Bereich Cyberkriminalität im Berichtszeitraum waren die sogenannten Erpressungstrojaner (englisch „Ransomware").

Im Mai 2019 war bereits eine neue Version der besonders gefährlichen Schadsoftware „Emotet" bekannt geworden, die anhand gestohlener E-Mails täuschend echte, aber virenverseuchte Nachrich-

ten verschickte. Nach einem Klick auf den Anhang einer solchen E-Mail wurden durch die nachgeladene Schadsoftware einerseits Daten von dem infizierten Rechner gestohlen. Weiterhin wurden der Rechner und teils das ganze zugehörige Netzwerk verschlüsselt und ein Lösegeld („Ransom“) für die Entsperrung verlangt. Allein im Mai 2019 wurden 18 infizierte Einrichtungen (Gemeinde, Städte, Schulen, Firmen) in Sachsen bekannt, bei denen so Landesdaten abgeflossen sind. Im SVN selbst konnte die Ausbreitung der Schadsoftware mehrere Mal nur knapp gestoppt werden.

Der Berichtszeitraum begann bezüglich dieser Gefährdungen erst einmal mit einer mehrmonatigen Pause der Schadsoftwarewellen und einem ungewöhnlich niedrigen Virenaufkommen an den Schutzsystemen des SVN. Diese Pause endete jedoch abrupt im September 2019 mit einer neuen Welle an zwischenzeitlich weiterentwickelten, noch gefährlicheren Erpressungstrojanern. Ein erstes prominentes Opfer in Deutschland war das Kammergericht Berlin. Nach einem flächendeckenden Schadsoftwarebefall in Folge eines unbedachten Klicks auf eine Emotet-E-Mail musste das oberste Straf- und Zivilgerichts des Landes Berlin sein IT-Netzwerk komplett abschalten und in der Folge alle Rechner austauschen. Ein späteres Gutachten wies darauf hin, dass mit hoher Wahrscheinlichkeit auch interne Daten des Gerichts, wie z. B. Passwörter, abgeflossen sind. Auch 9 Monate später ist die Funktionsfähigkeit des Netzes des Gerichts noch nicht wieder vollständig hergestellt.

Kurz vor Weihnachten 2019 erreichte die Schadsoftwarewelle ihren Höhepunkt mit zahlreichen großen Vorfällen. Bundesweit gingen aufgrund der Auswirkungen der Vireninfektionen ganze Städte vom Netz, so z. B. Frankfurt am Main oder Bad Homburg. In vielen Universitäten mussten zehntausende Rechner neu eingerichtet werden. Bis dahin wurden dem SAX.CERT 32 Einrichtungen aus Sachsen (außerhalb des SVN/KDN) bekannt, aus denen Daten mit Bezug zur Landesverwaltung abgeflossen sind. Im SVN selbst wurden nur kleinere Infektionen gemeldet oder durch das SAX.CERT festgestellt, die sich aufgrund der getroffenen Maßnahmen, wie z. B. die vom SAX.CERT tagesaktuell gepflegten zentralen Sperrlisten bekannter Schadsoftwareserver, nicht ausbreiten konnten.

Technisch wurden bei den Schadsoftwaremails meist tatsächliche Kommunikationspartner der Empfänger verwendet. Um die Glaubwürdigkeit weiter zu erhöhen, wurden oft auch im Betreff und im Mailtext Zitate aus tatsächlichen E-Mail-Kommunikationen verwendet, die im Rahmen anderer Infektionen gestohlen wurden. Die verseuchten Anhänge trugen oft zeitlich passende Namen zu den Themen Weihnachtsfeier, Weihnachtsgrüße oder in verschiedenen Varianten von angeblichen Rechnungen oder Antwortschreiben. Zumeist wurden dafür veraltete Office-Formate (*.doc, *.xls und *.ppt) benutzt, da sich darin gut Makros (ausführbare Programmcodes) verstecken lassen. Werden diese Makros beim Öffnen des Dokuments ausgeführt, wird dadurch weiterer Schadcode auf den Rechner heruntergeladen und ausgeführt.

Zur Verschleierung der Schadprogramme vor den Virenscannern versuchen die Absender, die Dateinamen und auch die Dateigröße ständig zu verändern, um eine Erkennung über eine feste Signatur („Fingerabdruck“ bzw. „Hashwert“) zu erschweren. So wurden z. B. im Dezember 2019 Schadprogramme in E-Mails in angeblichen Vertragsdokumenten mit dem Dateinamensformat „Vertrag[123].doc“ versteckt, wobei die laufende Nummer und damit der Dateiname fast immer unterschiedlich waren. Auch der Fingerabdruck der Dateien war immer unterschiedlich. Beides führte in Kombination zu einer Erkennungsrate rein signaturbasierte Scanner von lediglich unter einem Prozent. Scanner auf lokalen Rechnern sind fast ausschließlich signaturbasiert. In den zentralen Diensten sind jedoch weitere Angriffserkennungen wie die bereits erwähnten virtuellen Sandbox-Systeme und ein in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) betriebenes Virenscansystem namens „MWScan“ aktiv, so dass die Virenwellen mit einer Erkennungsrate von über 95 % gut abgewehrt werden konnten.

Als wirkungsvollste Gegenmaßnahme wurde seitens BfIS Land zum 1. Januar 2020 die Sperrung der veralteten Office-Dokumente (*.doc, *.xls und *.ppt) am Eingang des SVN und KDN umgesetzt. Die großen Virenwellen in der ersten Jahreshälfte des Jahres 2020 konnten so deutlich abgemildert werden.

Weitere Erpressungstrojanervorfälle im Berichtszeitraum sind im Folgenden beschrieben:

Gefälschte Bewerbungsmails

Im August 2019 wurden dem SAX.CERT Hinweise auf gefälschte Bewerbungsmails bekannt. Untersuchungen ergaben, dass der Anhang schadhaften Code enthält, der bei Ausführung nicht wie üblich die Dateien einer Festplatte verschlüsselt, um den Betroffenen zu erpressen, sondern der die Festplatten komplett mit Nullen überschreibt. Eine Rekonstruktion der Daten ist damit unmöglich, weshalb die Malware bei Ausführung sehr viel Schaden verursacht. Das SAX.CERT gab unverzüglich eine Warnmeldung an alle Ressorts heraus und informierte zusätzlich im VCV (Verwaltung-CERT-Verbund) über diese neue Bedrohung. Nach Erkenntnissen der Sicherheitsexperten hatten die technischen Systeme diese Schadmails nicht verlässlich erkannt und herausgefiltert, so dass sie bis zum Endnutzer durchkamen. Dem SAX.CERT wurden knapp 30 Fälle dazu in Sachsen bekannt, welche allesamt erfolgreich abgewehrt wurden. Das ist vor allem dem umsichtigen Verhalten der betroffenen Computernutzer zu verdanken, die vorsichtig reagierten und das CERT informierten.

Faxbenachrichtigungen via E-Mail

Im Oktober 2019 wurde bereits die nächste Welle mit Ransomware im SVN beobachtet. Verteilt wurde diese über angebliche e-Faxbenachrichtigungen via E-Mail, die einen Link enthielt, die beim Anklicken eine Worddatei herunterlädt, welche Makros enthält. Falls diese ausgeführt werden, kommt es zum Nachladen einer speziellen Ransomware, die sich Systemrechte auf dem Rechner verschafft und u. a. Backupdateien löscht und diverse Dateitypen verschlüsselt. Unmittelbar nach Bekanntwerden dieser Angriffsvariante durch das SAX.CERT wurden die in den E-Mails enthaltenen Link-Adressen auf eine interne Sperrliste gesetzt, so dass eine Infektion nicht mehr ausgelöst werden konnte. Mit Erfolg: Denn trotz Warnmeldung an die Ressorts wurde in den folgenden Wochen über 100-mal auf den Schadcode-Link geklickt, durch die Sperrung allerdings ohne negative Auswirkung.

Massive Ransomware-Kampagne

Anfang November 2019 wurden innerhalb von gut 24 Stunden knapp 900 angebliche Steuerbescheide als E-Mails mit dem Anhang „steuerbescheid.doc“ von den Mail-Virenscannern erkannt und entfernt. Die Welle war so massiv, dass allein in den ersten drei Minuten des Angriffs über 260 verseuchte Mails erkannt wurden. Einen Tag später wurde bereits der nächste Angriff registriert. Hierbei handelte es sich um gefälschte Rechnungen eines Telekommunikationsanbieters ebenfalls mit einem doc-Anhang. Diese Welle dauerte nur zwei Stunden, in denen 583 Schadmails erkannt wurden. Beide Word-Dokumente enthielten ein Makro welches eine spezielle Ransomware nachlädt und ausführt. In diesen Fällen konnten die technischen Schutzsysteme ein Durchschlagen bis in die E-Mail-Postfächer der Behördenmitarbeiter verhindern.

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 („Patch“). Das SAX.CERT bietet hier allen Behörden der Landes- und Kommunalverwaltung einen kostenlosen Warndienst zu über 2.000 Soft- und Hardwareprodukten an, der per E-Mail gezielt zu den vom Nutzer ausgewählten Produkten warnt, sobald hier neue Lücken bekannt werden (s. 4.2.1. #Schwachstellenwarndienst). Eine breitere Nutzung dieses Dienstes wird ausdrücklich empfohlen. Welche Risiken bei nicht gepatchten Sicherheitslücken auftreten, wird im Folgenden exemplarisch beschrieben.

CITRIX-Lücke

Im Dezember 2019 wurde eine Schwachstelle in CITRIX bekannt. CITRIX ist eine Software, die z. B. zur Einwahl auf Arbeitsplatzrechner aus dem Home-Office benutzt wird. Die entsprechende Warnung und Hinweise für Gegenmaßnahmen wurden am 18. Dezember 2019 über den Schwachstellenwarndienst des SAX.CERT an alle Empfänger verteilt, die das Produkt CITRIX abonniert hatten. Der Staatsbetrieb SID und der IT-Dienstleister T-Systems wurden daraufhin aktiv und schlossen die Lücke für alle staatlichen Behörden, deren Systeme zentral betreut werden. Anfang Januar 2020

informierten dann das BSI und CERT-Bund über den VerwaltungsCERT-Verbund zu einer gestiegenen Gefährdung durch neue Hinweise zur Ausnutzbarkeit der Lücke. Sofort im Anschluss führte das SAX.CERT einen Scan aller im Infoportal enthaltenen Internetseiten und -dienste der Landesverwaltung auf entsprechend verwundbare Server durch und informierte deren Betreiber.

Nachfolgend wurden dann erste Exploits im Internet bekannt und wenige Tage später häuften sich die Berichte zu Schadsoftwareinfektionen auf CITRIX-Servern über die Schwachstelle. So musste z. B. die Stadt Potsdam nach einer solchen Infektion ihre Verbindung zum Internet kappen. Dienste wie die Zulassungsbehörde und das Standesamt waren tagelang geschlossen, eine Erreichbarkeit per E-Mail wochenlang nicht mehr gegeben.

Von den 20 vom SAX.CERT gefundenen CITRIX-Systemen im SVN hatten nur 8 den Patch rechtzeitig installiert. Die anderen 12 Systeme haben den Patch nachgezogen und eine Prüfung auf Vireninfektionen durchgeführt. Dabei musste in einem Fall eine Schadsoftwareinfektion in einer herausgehobenen Einrichtung festgestellt werden, auch wenn zum Glück wohl keine Ausbreitung auf das Netz erfolgt ist.

Kritischere Auswirkungen sind in Sachsen nicht eingetreten, sicher auch wegen der frühzeitigen direkten Ansprache der Betreiber durch das SAX.CERT auf Basis der CERT-Dienste #Sicherheitsprüfung Webseiten, #Infoportal und #Schwachstellenwarndienst. In anderen Bundesländern wurden deutlich mehr Berichte über durch die CITRIX-Lücke infizierte, teils kritische Systeme registriert.

2.2.3. Informationssicherheit in der Corona-Pandemie

Beherrschendes Thema seit März 2020 war in allen Behörden die Corona-Pandemie. Mit der verstärkten Umstellung der Arbeitsweise der Behörden in die Telearbeit bzw. in das Home-Office gerieten mitunter Arbeitsprozesse und -abläufe an Belastungsgrenzen – auch durch teils ungenügend ausgebaute technische Infrastrukturen, die in der Kürze der Zeit nicht mehr auf den notwendigen Stand gebracht werden konnten. In der Anfangszeit gab es so u. a. temporäre Verfügbarkeitsprobleme bestimmter Dienste oder auch mehrere DDoS-(Fehl-)Alarme (ursprünglich eingerichtet zum Zweck der Meldung so genannter Überlastungsangriffe) aufgrund unerwartet vieler Einwahlverbindungen von außen. In einem Fall wurde eine bestehende IT-Infrastruktur kurzerhand für Fernzugriffe von außen freigeschaltet, um die Bedienung aus dem Home-Office zu gewährleisten, was dazu führte, dass auf den schlecht gesicherten Zugriff von weltweit verteilten IPs automatisiert hunderttausende Anmeldeversuche erfolgten. Der Angriff war zwar nicht erfolgreich, wurde aber aufgrund mangelnder Log-Auswertung und fehlender personeller Ressourcen erst nach zwei Monaten bemerkt.

Auf der anderen Seite hatten auch die Cyberkriminellen ihre Angriffsziele auf das neue Thema Corona angepasst. So gab es in Sachsen anfänglich Phishingversuche per E-Mail (angeblich von der WHO oder der Arbeitsagentur mit Corona-Bezug) und in der Hochzeit der Pandemie 1:1-Fälschungen von Corona-Soforthilfe-Antragsseiten. Die auf diesen Phishingseiten eingegebenen Daten wurden von den Kriminellen für die Stellung von Anträgen mit veränderten Kontodaten auf den offiziellen Seiten missbraucht. Es folgten weitere Schadsoftwaremails angeblich vom Gesundheitsministerium oder der Arbeitsagentur mit Corona-Bezug. Die seit 1. Januar 2020 aktive Blockierung von im SVN eingehenden veralteten und unsicheren Office-Dokumenten konnte auch hier mehrfach größeren Schaden abwenden.

3. Tätigkeitsbericht des Beauftragten für Informationssicherheit des Landes

Der Beauftragte für Informationssicherheit des Landes ist laut Sächsischem Informationssicherheitsgesetz u. a. für die Erstellung des Informationssicherheitsmanagementsystems 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 Beauftragte für Informationssicherheit des Landes zur jährlichen Berichterstattung über seine Tätigkeit an den Landtag verpflichtet.

3.1. Anordnungen und Empfehlungen

Gegenüber an das Sächsische Verwaltungsnetz angeschlossenen staatlichen Stellen kann der Beauftragte für Informationssicherheit des Landes Anordnungen treffen oder Maßnahmen ergreifen, um Gefahren für die informationstechnischen Systeme, die mit dem Sächsischen Verwaltungsnetz verbunden sind, abzuwehren. Maßnahmen, die auch die nicht-staatlichen Stellen betreffen, bedürfen hierbei das Benehmen des Beauftragten für Informationssicherheit des Kommunalen Datennetzes (KDN).

3.1.1. Sperrung Empfang alter Office-Formate

Nach längeren Vorarbeiten wurde zum Jahresbeginn 2020 die Sperrung der alten Office2003-Formate im gesamten SVN/KDN aktiviert. Hintergrund war vor allem die Erkenntnis, dass die alten Officeformate wie *.doc eine überproportional große Rolle in den massiven „Emotet“-Virenwellen des letzten Jahres gespielt hatten. Im Gegensatz zu den neuen Formaten gab es bei Office2003 noch keine Trennung in Dokumente ohne Makrofunktionen (jetzt: *.docx) und solche mit Makrofunktionen (jetzt: *.docm). Damit lassen sich bösartige Makros grundsätzlich besser in Office2003-Formaten verstecken.

Die Sperrung alter Office-Formate wird in der Praxis wie folgt umgesetzt: Findet das zentrale Schutzsystem im Anhang einer E-Mail ein altes Office-Format, wird dieser Anhang aus der E-Mail entfernt. Die restliche E-Mail wird mit einem Hinweis auf den entfernten Anhang zugestellt. Der Empfänger wird zusätzlich gebeten, gegebenenfalls den Absender zu bitten, den Anhang in einem aktuellen Office-Format erneut zu senden. Der Absender erhält zeitgleich automatisch die Information, dass alte Office-Formate aus Sicherheitsgründen von der Staatsverwaltung nicht weiter entgegengenommen werden und er darum gebeten wird, den Anhang in einem zulässigen aktuellen Format zu versenden. Die E-Mail enthält einen Link auf eine flankierende Veröffentlichung auf www.sachsen.de.

Im Schnitt wurden seit der Aktivierung des Office2003-Filters mehrere hundert Anhänge täglich in diesem Format aus dem eingehenden Mailstrom im SVN gefiltert. So wurden in den ersten drei Wochen nach Aktivierung des Filters, in dem eine halbe Million E-Mails mit Anhängen an die Behörden zugestellt wurden, bei gut 10.000 E-Mails alte Office-Dokumente gesperrt. Analysen über die Beschaffenheit dieser Anhänge ergaben, dass allein in einer Woche über 800 Dateien bösartig waren. Diese Dateien wären ohne Sperrung bis zum Endnutzer durchgedrungen – so gab es im Januar wieder massive Virenwellen mit *.doc-Anhängen, die so erstmals komplett abgewehrt werden konnten. Sowohl von Seite der Landesbehörden als auch der Kommunen wurden keine nennenswerten Beschwerden über diese Sicherheitsmaßnahme geäußert. Insofern kann diese Maßnahme als ein gemeinsamer Erfolg gewertet werden.

3.1.2. Nutzung des Extended Security Updates

Ende 2019 hatte BfIS Land die Ressorts in einem Schreiben darum gebeten, darüber zu informieren, in welchen Behörden welche der Microsoft-Produkte Windows 7, Windows Server 2008 bzw. 2008 R2 über das Ende des erweiterten Supports am 14. Januar 2020 hinaus verwendet werden. In diesem Fall sollten die Ressorts zudem angeben, ob sie den von Microsoft angebotenen zusätzlichen erweiterten Sicherheitsschutz (Extended Security Update – ESU) nutzen werden.

Bis Ende Januar 2020 wurden von den Ressorts allein für das Betriebssystem Windows 7 über 10.000 Installationen gemeldet, die über das Support-Ende hinaus im Einsatz sein sollten. Dabei sollte nur bei gut 4.500 Installationen auf das ESU zurückgegriffen werden, so dass mindestens 6.000 Windows 7 Installationen ab dem 11. Februar 2020 ohne turnusgemäßen Patch, also ohne aktuelles Sicherheitsupdate, in den Behörden im Einsatz sein würden. Die AG Informationssicherheit empfahl in Kenntnis dieser Zahlen den BfIS Land in der Sitzung am 21. Januar 2020, nach § 5 Absatz 3 SächsISichG die Anordnung an die Ressorts auszusprechen, dass für alle Installationen von Microsoft Produkten, die über das Ende des erweiterten Supports genutzt werden, das ESU zu verwenden ist.

Nicht zuletzt die schwerwiegende Citrix-Lücke Anfang 2020 hatte gerade erst bewiesen, dass ungepflegte Software ein hohes Sicherheitsrisiko darstellt. Eine mögliche Sicherheitslücke in einem massenhaft genutzten Betriebssystem wie Windows 7, welches standardmäßig nicht mehr aktualisiert wird, stellt ein nicht verantwortbares Sicherheitsrisiko dar. Deswegen forderte BfIS Land im Rahmen seiner Befugnis durch das SächsISichG die Ressorts am 30. Januar 2020 per Anordnung auf, das von Microsoft angebotene ESU bis zum 11. Februar 2020 für alle Installationen von Microsoft Produkten einzusetzen, die das bisherige Support-Ende erreicht haben und mit dem SVN verbunden sind. Sollten Ressorts den Einsatz des ESU ablehnen, war dies dem BfIS Land anzuzeigen und zu begründen. In Antwort auf das Schreiben zeigte lediglich ein Ressort beim BfIS Land an, abgekündigte Microsoft-Software ohne den erweiterten Sicherheitsschutz zu betreiben, da mit zeitlicher Verzögerung die Umstellung auf aktuelle Software in Bälde zu erwarten sei.

Der Freistaat Sachsen stand zum damaligen Zeitpunkt mit den Mängeln bei der rechtzeitigen Migration in aktuelle Betriebssysteme nicht alleine dar. Pressemeldungen und parlamentarische Anfragen in anderen Bundesländern wie auch beim Bund legten in der Quantität sogar weitaus kritischere Fälle offen. Aus Sicht des BfIS Land sind Versäumnisse in diesem Bereich jedoch sehr kritisch zu sehen, weil hier Gefahren für die Informationssicherheit entstehen, die sich die Verwaltung selbst anzulasten hat.

3.1.3. Rahmenvorgabe zum Einsatz von Soft-Token auf privaten Geräten

Nach der Verwaltungsvorschrift Dienstordnung hat der Beauftragte für Informationssicherheit des Landes das Recht, ressortübergreifende Rahmenvorgaben als Ausnahme von dem Leitmotiv zu erstellen, dass zur Erledigung dienstlicher Aufgaben grundsätzlich nur dienstlich bereitgestellte Geräte und Datenträger sowie freigegebene Programme (Ausstattung) benutzt werden dürfen (VII. 32 e) Satz 1-3). Da im Rahmen der Corona-Pandemie die Nutzung von Telearbeit/Home-Offices rapide anstieg, aber von den IuK-Bereichen der Behörden aufgrund von Lieferengpässen keine so genannten Hard-Token als Mittel der Zwei-Faktor-Authentifizierung ausgereicht werden konnten, erstellte BfIS Land folgende Ausnahme von der oben genannten Rahmenvorgabe:

„Die Nutzung privater Geräte zum Aufspielen einer Software für die Generierung sicherer Einmalpasswörter (so genannter Soft-Token) oder zum Empfang eines Codes per SMS zur Verwendung als zweiter Faktor bei der Anmeldung mit dienstlichen Geräten in die Infrastruktur des SVN ist erlaubt.“

Hintergrund dieser Regelung ist der Gedanke, dass der Einsatz eines zweiten Faktors in jedem Fall die Sicherheit des Einwahlverfahrens deutlich erhöht, auch wenn „nur“ Soft-Token oder Codes per SMS zum Einsatz kommen. Diese Rahmenvorgabe nach VwV Dienstordnung VII. 32 e) wurde den Behörden der Landesverwaltung übermittelt. Unberührt davon sind personalrechtliche Erwägungen und Haftungsfragen.

3.1.4. Erinnerung Meldepflichten der Behörden

Nachdem im ersten Quartal 2020 trotz bekannter Schadsoftwarewellen dem Sicherheitsnotfallteam keine Sicherheitsereignisse oder Sicherheitsvorfälle, weder von den staatlichen noch den nichtstaatlichen Stellen, gemeldet worden waren, forderte BfIS Land die Ressorts in einem Schreiben dazu auf, gemäß § 16 SächsISichG Sicherheitsereignisse und Sicherheitsvorfälle ihrer informationstechnischen Systeme oder Prozesse an das Sicherheitsnotfallteam zu melden. Schließlich sind sowohl das Sicherheitsnotfallteam als auch BfIS Land auf eine konsistente Datenlage angewiesen.

Nicht zuletzt dienen solche Zahlen auch dazu, die Sicherheitslage belastbar bewerten zu können und die Ressourcenbedarfe für den Bereich der Informationssicherheit des Freistaates zu definieren.

Nach dem Schreiben wuchsen die Meldeaktivitäten für einige Monate spürbar an (#Gemeldete Sicherheitsereignisse und -Vorfälle). Zur weiteren Verbesserung der Informationslage wird BfIS Land nunmehr die im SächsISichG vorgesehene Rechtsverordnung zum Meldewesen erstellen, um hier für eine größere Rechtsverbindlichkeit zu sorgen. Damit werden gleichzeitig auch die Regelungen des AK ITEG-Beschlusses zum Meldewesen aus dem Jahr 2016 und die Beschlusslage des IT-Planungsrates aufgegriffen.

3.1.5. Sicherheitsempfehlungen Home-Office

Die Ausweitung der Corona-Pandemie auf die Bundesrepublik ab März 2020 hatte nicht nur das Leben allgemein, sondern auch das Arbeitsleben im Speziellen in vorher kaum für möglich gehaltene Bahnen gelenkt. Das galt natürlich auch für die Landesverwaltung: immer mehr Behörden schickten ihre Mitarbeiter zumindest in Teilen in das Home-Office. In der Kürze der Zeit stand damit die Informationssicherheitsorganisation und zuvorderst der BfIS Land vor der Herausforderung, pragmatische, weil an der aktuellen Situation ausgerichtete Regelungen mitzutragen, um die Arbeitsfähigkeit der Verwaltung aufrecht zu erhalten. Mitunter mussten hierbei grundsätzliche Standpunkte der Informationssicherheit hintenangestellt werden. Um zumindest ein einigermaßen einheitliches Vorgehen zu gewährleisten, wurde vom BfIS Land ein Merkblatt zu Sicherheitsvorkehrungen und Verhaltensweisen im Home-Office für die BfIS der Behörden erstellt. Dieses stützte sich auf Standards des BSI, wich aber auch in manchen Punkten von Standpunkten der Bundesbehörde ab, weil ein zu rigoroses Reglement die Arbeitsfähigkeit mancher Behörden zu sehr eingeschränkt hätte. Es wird jedoch Aufgabe des BfIS Land und seiner Ressortkollegen sein, darauf hinzuwirken, dass die IT-Infrastruktur künftig so aufgestellt sein wird, dass Home-Office nicht nur technisch möglich ist, sondern dabei auch alle Erfordernisse für Informationssicherheit vollumfänglich erfüllt.

3.2. Gremienarbeit

Auf Landesebene hält der Beauftragte für Informationssicherheit des Landes den Vorsitz der AG Informationssicherheit und nimmt darüber hinaus als ständiger Vertreter an den Gremiensitzungen des AK ITEG, des AK SVN sowie der AG IBES teil. Auf Einladung bzw. sofern verbindliche Mindeststandards zur Informationssicherheit zu beschließen sind, nimmt er zudem am LA ITEG teil.

3.2.1. AG Informationssicherheit Land Sachsen (AG IS)

Um eine angemessene Informationssicherheit in den staatlichen Behörden zu realisieren, ist ein landesweites Informationssicherheitsmanagementsystem (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 Informationssicherheit. Im Berichtszeitraum trafen sich die Beauftragten für Informationssicherheit der Ressorts und die weiteren Teilnehmer der AG zu Sitzungen am 20. August und 26. November 2019 sowie am 21. Januar und – aufgrund der Corona-Pandemie verschoben – am 26. Mai 2020 (erstmals als Online-Meeting).

Anpassung Geschäftsordnung an SächsISichG

Das Sächsische Informationssicherheitsgesetz regelt die Zuständigkeiten, Aufgaben und den Zuschnitt der AG Informationssicherheit neu (§ 10 SächsISichG) und dadurch z. T. abweichend zur bisher gültigen Geschäftsordnung. Zentrale Änderung ist durch die im Gesetz formulierte Anordnungsbefugnis der BfIS Land, dass die AG Informationssicherheit den BfIS Land nunmehr berät und die Beschlüsse einen rein empfehlenden Charakter haben. Die beschlossenen Empfehlungen werden nicht mehr erst dem AK ITEG, sondern sofort dem LA ITEG vorgelegt. Zudem erhält die kommunale Ebene erstmals Stimmrecht in der AG und wird nunmehr ständig durch Vertreter der beiden Spitzenverbände Sächsischer Städte- und Gemeindetag sowie Sächsischer Landkreistag vertreten sein.

Richtlinie Definition der Schutzbedarfskategorien

Ziel war der Beschluss zu ressortübergreifenden einheitlichen Schutzbedarfskategorien. Die Richtlinie definiert verbindlich für alle staatlichen Stellen die für ein Sicherheitskonzept nach BSI-Standard 200-2 notwendigen Schutzbedarfe. In der Sitzung wird erläutert, dass sich die Angaben zu Schäden in den Kategorien auf mittelbare und unmittelbare Schadereignisse beziehen. Eine weitergehende Festlegung ist aus Sicht BfIS Land nicht möglich. Nach Diskussion der Teilnehmer zu den finanziellen Stellenwerten wird vereinbart, die absoluten Zahlen aus dem Entwurf zu streichen; sie sollten in den Häusern selbst festgelegt werden.

Da der LA ITEG seit dem Beschluss der AG IS nicht mehr getagt hat, konnte darüber bislang nicht entschieden werden.

3.2.2. AK ITEG

In der Sitzungen des AK ITEG am 10. Dezember 2019 informierte BfIS Land die Teilnehmer über die geplante #Sperrung Empfang alter Office-Formate, über das #E-Learning „Informationssicherheit am Arbeitsplatz“ und zu den Teilnahmezahlen der #Sensibilisierung durch die INFOSIC.

In der Sitzung am 4. Februar 2020 informierte BfIS Land über die Auswirkungen der #Sperrung Empfang alter Office-Formate, über die aktuelle Sicherheitslage und hierbei u.a. über #Schwachstellen in ungepatchter Software am Beispiel der CITRIX-Lücke.

3.2.3. LA ITEG

Im Berichtszeitraum August 2019 bis Juli 2020 tagte der LA ITEG nicht.

3.2.4. Weitere Gremien

Im Arbeitskreis Sächsisches Verwaltungsnetz erhielt BfIS Land von einem Ressort den Hinweis, dass eine Beschaffungslücke bei den so genannten Hard-Tokens (als Mittel der Generierung eines zweiten Faktors bei der Einwahl von außen auf den Remote-Desktop) bestünde und die Behörde sich aufgrund der restriktiven VwV Dienstordnung gezwungen sähe, die Anschaffung von dienstlichen Smartphones für die Implementierung eines App-basierten Smart-Tokens in die Wege leiten zu müssen. Nach Sicherheitsprüfung durch BfIS Land erließ dieser eine Ergänzung zur #Rahmenvorgabe zum Einsatz von Soft-Token auf privaten Geräten. Damit haben die Behörden nunmehr auch die Freiheit, ihren Mitarbeitern die Möglichkeit zu eröffnen, den zweiten Faktor zur Anmeldung auf die dienstliche Arbeitsumgebung mit einem privaten Smartphone zu generieren.

3.3. Sensibilisierung und Fortbildung

Gefährdungen in der Informationssicherheit entstehen nicht nur, indem Schwachstellen aufgrund fehlerhafter Software ausgenutzt werden, die von technischen Sicherheitslösungen nicht oder zumindest erst sehr spät erkannt werden. Gefahren sind auch möglich, weil der Mensch als Nutzer der Informationstechnik mit unbedachten Mausklicks unfreiwillig zum Komplizen von Hackern werden kann. So wird Schadcode in den überwiegenden Fällen erst durch einen falschen Klick von Menschen aktiviert. Auch personenbezogene Anmeldedaten werden häufig durch fahrlässiges Handeln der Computernutzer an die Hacker überliefert. In diesen Fällen können selbst beste Technik und durchdachte Sicherheitsvorkehrungen kaum die Informationssicherheit bewahren. Insofern verwundert es nicht, dass die Nutzer von Computer, Tablet und Smartphone das größte Fehlerrisiko der Informationstechnik ausmachen. Statistiken zeigen immer wieder, dass ca. 95 Prozent aller Sicherheitsvorfälle in der IT erst durch leichtsinniges oder einfach unwissend riskantes Verhalten der Nutzer möglich wurden. Daher ist zu beobachten, dass sich Cyberkriminelle immer stärker auf menschliches Fehlverhalten anstatt auf technische Fehler fokussieren. So gelangen sie an persönliche Daten oder geistiges Eigentumoder erpressen Unternehmen bzw. Behörden um Geld. 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.

3.3.1. Sensibilisierung durch die INFOSIC

Sowohl das Sächsische Informationssicherheitsgesetz als auch die Datenschutzgrundverordnung beschreiben, wie wichtig die Sensibilisierung und das Training von Mitarbeitern ist. Dabei geht 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 Mitarbeiter in der Verwaltung IT-Experten sind, kann das benötigte Wissen am besten über einfache Regeln und verständliche Sicherheitsmaßnahmen vermittelt werden. Ganz nach diesem Leitmotiv organisiert der Beauftragte für Informationssicherheit des Landes mit der Großveranstaltung INFOSIC seit dem Jahr 2012 so genannte „Live-Hackings“, die sich ausdrücklich an alle Mitarbeiterinnen und Mitarbeiter von Landes- und Kommunalbehörden richten. Mittlerweile ist die INFOSIC die größte Sensibilisierungsveranstaltung für Informationssicherheit im Freistaat Sachsen. Der Zuspruch und das Interesse an einer Teilnahme sind unter den Mitarbeitern der Landes- und Kommunalverwaltung über die Jahre stark gestiegen. Wurden in den Anfangsjahren in Leipzig und in Chemnitz jährlich knapp 700 Teilnehmer begrüßt, erhöhte sich die Zahl in den Folgejahren schlagartig, so dass mittlerweile jährlich fast 3.000 Mitarbeiter aus den Verwaltungen an diesen Veranstaltungen teilnehmen. Durch diese und andere dezentral vom BfIS Land organisierte bzw. unterstützte Veranstaltungen wurden bislang insgesamt über 15.000 Mitarbeiter aus der öffentlichen Verwaltung in Sachsen direkt erreicht. Mit dieser Teilnehmerzahl belegt der Freistaat Sachsen im Bundesvergleich einen Spitzenplatz. Der IT-Planungsrat unterstützt die Länder bei der Ausrichtung, indem es die erfahrenen Referenten von IT-Bildungsanbietern vermittelt und finanziert.

Die Zielgruppe einbinden und „betroffen machen“ ist seit Jahren Markenzeichen der INFOSIC. Zwei Computerexperten schlüpfen in einer Bühnenshow in die Rollen eines unbescholtenen Computernutzers und eines Hackers. Unter dem Veranstaltungstitel „Die Hacker kommen! – Techniken, Tipps und Tricks für jeden, der Computer nutzt“ zeigen sie in diesem Rollenspiel leicht verständlich einfache Tricks und Handgriffe, damit die Teilnehmer sowohl an ihrem Arbeitsplatz ihre Informationen und Daten vor fremden Zugriff schützen, als auch im privaten Umfeld kein leichtes Opfer für Cyberkriminelle werden. In einer unterhaltsamen Mischung aus Vorträgen und Technikdemonstrationen („Live-Hacking“) gibt es dabei u. a. Informationen zu den Gefahren bei der Nutzung der modernen Informationstechnik, den Tücken bei der Internetnutzung und Tipps für sicheres mobiles Arbeiten. Zudem bekommen die Teilnehmer in kleinen Tests gezeigt, wie Angreifer auch die Psyche des Menschen oder sein Rollenverhalten ausnutzen, um an gewinnbringende Daten zu gelangen.

INFOSIC 2019

Die Veranstaltungen der INFOSIC 2019 am 26. September in Leipzig (zwei Termine im Audimax am Campus Augustusplatz), am 1. Oktober in Chemnitz (zwei Termine im Audimax der Technische Universität) und am 8. Oktober in Dresden (2 Termine im Rundkino) waren wie in den Vorjahren sehr nachgefragt. Zu den kostenlos angebotenen Live-Hacking-Veranstaltungen kamen insgesamt über 2.900 Teilnehmer und damit gut 600 mehr als im Vorjahr.

Von den Landesbehörden kamen knapp 2.000 Teilnehmer, von den Kommunen gut 700 und 200 von sonstigen Einrichtungen. Knapp zwei Drittel aller Teilnehmer waren dabei Frauen. Die Teilnehmer aus den Landesbehörden und Kommunen des Freistaates zeigten sich sehr zufrieden mit dem Angebot. Eine Teilnehmerbefragung über das Beteiligungsportal Sachsen, an der sich knapp 700 Personen beteiligten, ergab Zufriedenheitswerte ähnlich wie in den Vorjahren (83 % fanden die Veranstaltung insgesamt gut, 14 % sehr gut).

3.3.2. E-Learning „Informationssicherheit am Arbeitsplatz“

So überaus gut besucht die INFOSIC-Veranstaltungen auch sind: Mit solchen Präsenzveranstaltungen allein kann Sensibilisierung und Fortbildung im Bereich Informationssicherheit nicht umfassend umgesetzt werden. Bei schätzungsweise 80.000 Computerarbeitsplätzen in den sächsischen Behörden auf Landes- und Kommunalebene ist es das Ziel, möglichst allen Bediensteten eine Fortbildung im Bereich Informationssicherheit zu ermöglichen. Aus diesem Grund wird vom Beauftragten für Informationssicherheit des Landes ein E-Learning-Angebot bereitgestellt.

Kernstück des E-Learning-Angebotes ist die Lernwelt „Informationssicherheit am Arbeitsplatz“. Sie zeigt den teilnehmenden Behördenmitarbeitern, wie sie sensible Daten und Informationen sowohl am Arbeitsplatz als auch im privaten Umfeld vor unberechtigtem Zugriff und Missbrauch schützen können. In der Lernwelt können sich die Bediensteten in insgesamt neun Kapiteln und ihrem eigenen Tempo mit verschiedenen Aspekten der Informationssicherheit am Arbeitsplatz beschäftigen. Die Kapitel bilden dabei eine Geschichte im Comic-Stil ab. Protagonisten der Geschichte sind u. a. Florian Sibe, Sicherheitsbeauftragter der Behörde, sein Assistent „@gar“, der immer wieder nützliche Tipps und Zusammenfassungen rund um das Thema gibt, sowie Susanne, die IT-Spezialistin der Behörde, und die Putzfrau Lisa. Die beiden Letzteren kommen immer wieder zu Aspekten der Informationssicherheit ins Gespräch. Anlass dafür ist ein Sicherheitsvorfall in der Behörde, zu dem es in jüngster Zeit gekommen ist. Aufgabe des Nutzers ist es, diesen Sicherheitsvorfall aufzuklären. Um genau dies zu können, müssen die Bediensteten den Ursachen auf den Grund zu gehen. Dabei werden in den neun Kapiteln der Lernwelt wichtige Inhalte zur Informationssicherheit am Arbeitsplatz vermittelt. Die Bearbeitung aller Kapitel nimmt ca. vier bis fünf Stunden Zeit in Anspruch und kann auch in Etappen erfolgen. Es gibt dabei keine strikt festgelegte Reihenfolge für die Kapitel.

Tabelle: Teilnehmer am E-Learning ausgewählter staatlicher Stellen (Stand: 2. Juli 2020)

ausgewählte staatliche Stellen	Test erfolgreich	Teilnahmeschein
justiz.sachsen.de	291	87
polizei.sachsen.de	60	31
sk.sachsen.de	37	
smf.sachsen.de	99	39
smi.sachsen.de	236	54
smk.sachsen.de	46	6
sms.sachsen.de	582	3
smul.sachsen.de	826	480
smwa.sachsen.de	80	3
smwk.sachsen.de	101	18
statistik.sachsen.de	306	14
sme.sachsen.de	41	83
smr.sachsen.de		1

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

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 SID im Oktober 2019 und den damit erweiterten Funktionalitäten (Selbstregistrierung der Teilnehmer, Erweiterung der Kapazität auf 5.000 gleichzeitige Nutzer) haben 946 Nutzer den Teilnahmeschein erworben und 1.222 Nutzer den Test zum Sächsischen Informationssicherheitsschein (SISS) erfolgreich absolviert. Mit den vorherigen gut 1.700 Absolventen des E-Learnings an der HSF Meißen haben damit gut 3.900 Nutzer den Kurs zur „Informationssicherheit am Arbeitsplatz“ belegt und mit einem Schein abgeschlossen.

3.4. Zusammenarbeit mit dem BSI

Der Beauftragte für Informationssicherheit des Landes setzt sich seit jeher für eine engere Zusammenarbeit der Bundesländer mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ein. Ein entsprechender Beschluss der Innenministerkonferenz aus dem Jahr 2017 zu einer besseren Koordinierung und Abstimmung von Maßnahmen von Bund und Ländern im Bereich IT-Sicherheit geht u. a. auf hiesige Initiativen während des sächsischen IMK-Vorsitzes im selben Jahr zurück. Danach wurde das Engagement des BSI zur Beratung und Unterstützung der Bundesländer sukzessive ausgebaut. Als Konsequenz daraus vereinbarten das BSI und die Sächsische Staatskanzlei im November 2018 in einer Absichtserklärung eine engere Zusammenarbeit unter anderem in folgenden Bereichen:

- gegenseitiger Austausch von Mitarbeiterinnen und Mitarbeitern im Rahmen von Hospitationen,
- 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,
- Bereitstellung von technischer Expertise des BSI vor Ort,
- Austausch zur Stärkung der Resilienz bestehender IT-Lösungen (z. B. Web-Checks, Penetrationstests),
- Beratung und Unterstützung seitens des BSI beim Aufbau eines landesweiten Informationssicherheitsmanagementsystems in Sachsen.

Im Berichtszeitraum manifestierte sich die Zusammenarbeit vor allem in folgenden Projekten bzw. Maßnahmen:

3.4.1. Nutzung MW Scan

Die Virenscanner des SVN erkennen nicht immer sämtliche Schadsoftware, wie z. B. eine große Anzahl nicht erkannter Viren im Dezember 2018 beweist. Das Bundesamt für Sicherheit in der Informationstechnik entwickelt aus eigenen Erkenntnissen und Zuarbeiten weiterer Behörden eigene Signaturen zur Erkennung fortgeschrittener Schadprogramme. Diese Signaturen werden auch den Bundesländern zur Mitnutzung angeboten. Mit dem Einsatz dieser zusätzlichen Schutzmaßnahme seit August 2019 im SVN konnte die Anzahl nicht erkannter Schadsoftware im E-Mail-Verkehr weiter gesenkt werden. Dementsprechend sank das Risiko für die Teilnehmer im SVN, selbst Opfer von Schadsoftware zu werden.

Mit der Implementierung dieser Software steht dem SAX.CERT zudem erstmals eine zeitnahe Auswertungsmöglichkeit der im Mailstrom gefundenen Schadsoftware zur Verfügung. Die Zahlen werden viertelstündlich vom System übermittelt, was ein zeitnahes Monitoring ermöglicht. Dieses Monitoring und ein darauf basierender automatischer Alarm beim Vorliegen von aktuellen Virenwellen soll nach Abschluss der Testphase allen Ressorts zur Verfügung gestellt werden. Neben dem Monitoring ermöglichen es die neuen Daten, nun auch eine Bewertung der Wirksamkeit der verschiedenen Schutzsysteme vornehmen zu können. Demnach hat die virtuelle Sandbox-Erkennung mit 85 % den bei weitem größten Anteil an den exklusiven Erkennungen (also der Erkennung von Viren die kein anderes Scansystem gefunden hat). Zusätzlich entfallen aber 15 % aller exklusiven Virenfunde auf den Schutz durch das neue MWScan-System, das damit nachweislich eine wertvolle Ergänzung darstellt. Die klassischen signaturbasierten Virenscanner erkannten dagegen im Untersuchungszeitraum keinen einzigen Virus mehr exklusiv.

3.4.2. Verbindungsperson

Seit Mai 2019 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine so genannte Verbindungsperson für die Region Ost in Dresden ernannt. Die Verbindungspersonen sind feste Ansprechpartner vor Ort und ermöglichen eine schnelle und direkte Kontaktaufnahme mit dem BSI. Sie sind bei Veranstaltungen präsent und nehmen Vortragstätigkeiten für das BSI in der Region wahr. Darüber hinaus geben die Verbindungspersonen einen Überblick über die Angebote und Expertise des BSI und vermitteln bei Bedarf Beratung und Unterstützung. Die Verbindungspersonen sind zentrale Anlaufstellen für Länder und Kommunen, Bundes- und EU-Behörden in den jeweiligen

Regionen, Unternehmen jeder Art im Bereich der Wirtschaft, Think-Tanks und Entscheidungsträger im Bereich Gesellschaft.

Die Verbindungsperson ist zum Zeitpunkt der Erstellung des Berichts (August 2020) in den Räumlichkeiten der Außenstelle des BSI in Freital angesiedelt. Im Jahr 2017 und Anfang 2019 hatte das BSI Verbindungspersonen bereits für das Rhein-Main-Gebiet (in Wiesbaden), für Norddeutschland (in Hamburg), für Süddeutschland (in Stuttgart) und für den Großraum Berlin ernannt.

3.4.3. Hospitation

Ende September 2019 konnte ein Mitarbeiter des SAX.CERT im Rahmen einer Hospitation im BSI vertiefte Einblicke in das Wirken und Arbeiten des CERT-Bund und des IT-Lagezentrums des BSI erhalten. Unter anderem wurde der Aufbau und die Wirkungsweise spezieller Schutzsysteme skizziert, das Incident Handling bei Krisen und schweren Vorfällen besprochen und Erfahrungen bei aktuellen Crimeware-Kampagnen, wie z. B. Emotet, ausgetauscht.

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 (nichtstaatliche 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 ca. 2.000 Hard- und Softwareprodukten eine individuelle Zusammenstellung auswählen kann. Wird für eines der ausgewählten Produkte eine neue Sicherheitslücke bekannt, versendet das Portal automatisch eine Warn-E-Mail mit ausführlichen Details und Maßnahmenempfehlungen zu dieser Schwachstelle an den betreffenden Nutzer. Der Warndienst wurde Stand August 2020 von 103 Abonnenten im Freistaat Sachsen aktiv genutzt (83 im Bereich Land, 20 im Bereich Kommunen).

4.2. Sicherheitsprüfung Webseiten

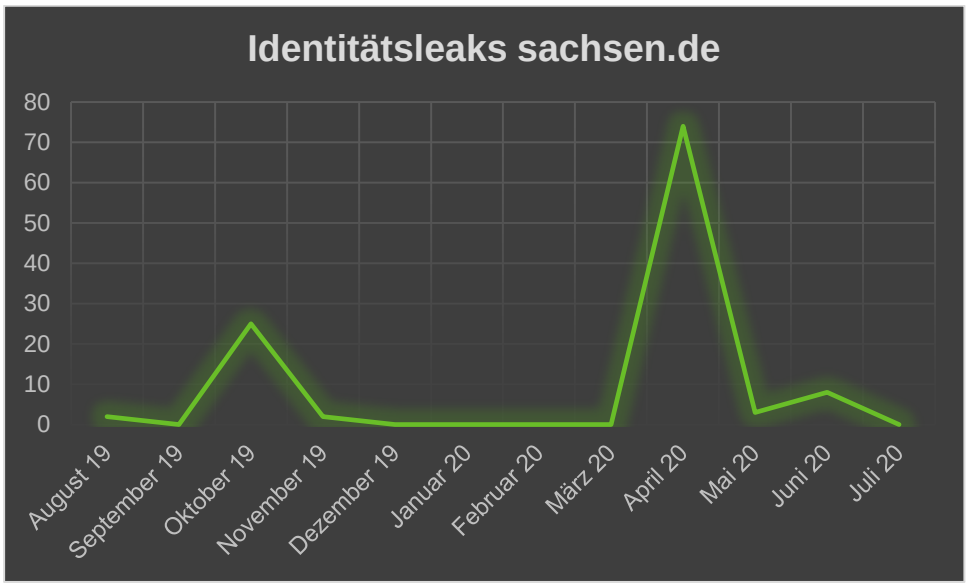
Auf Grundlage des Beschlusses 3/2017 "Automatische Scandienste und Erhöhung der Webseitensicherheit" des AK ITEG werden zweimal monatlich über 6.000 Internetseiten der Landes- und Kommunalverwaltung durch das SAX.CERT auf veraltete Software und bekannte Schwachstellen getestet. Bei schwerwiegenden Sicherheitslücken 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.

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 15 Nutzern außerhalb der Landesverwaltung und zwei Hochschulen genutzt wurde.

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

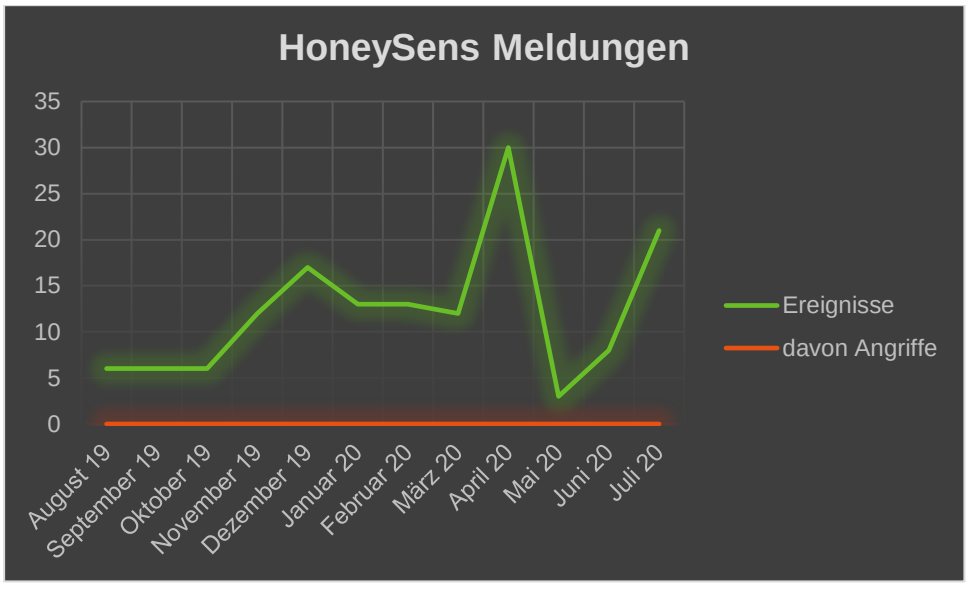
Grafik: Gemeldete Identitätsdatenleaks von E-Mail-Accounts der Domain sachsen.de



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 26 Sensoren im produktiven Einsatz (9 Land, 17 Kommunen).

Grafik: Zugriffe auf den Sensor HoneySens



5. Bericht zu den ergriffenen Maßnahmen laut SächsISichG

Zur Kompensation der Grundrechtseingriffe ist der Beauftragte für Informationssicherheit des Landes 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 Abs. 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 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 daher aus, dass von den Behörden keine solchen datenverarbeitenden Tätigkeiten vorgenommen oder gemeldet wurden.

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

Art der Datenverarbeitung	SAX.CERT	staatliche Stellen	nicht-staatliche Stellen
die Anzahl von Fällen der nicht automatisierten Auswertung, der personenbezogenen Verarbeitung und der Wiederherstellung des Personenbezugs pseudonymisierter Daten bei Protokolldaten gemäß § 13 Absatz 2	0	1	0
die Anzahl von Fällen der Speicherung und der Auswertung von Inhaltsdaten und Wiederherstellung des Personenbezugs pseudonymisierter Daten gemäß § 13 Absatz 3	0	0	0
die Anzahl von Fällen der nicht automatisierten Verarbeitung von Daten gemäß § 13 Absatz 4	0	0	0
die Anzahl der durchgeführten, unterbliebenen sowie nachgeholten Benachrichtigungen gemäß § 13 Absatz 5	0	0	0
die Anzahl von Fällen der Übermittlung von Daten gemäß § 13 Absatz 6 und 7	0	0	0
die Anzahl von gemäß §§ 15 bis 17 gemeldeten Sicherheitsereignissen und Sicherheitsvorfällen	0	16	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 wurde keine Anordnungen durch das SAX.CERT veranlasst. Im Rahmen der gefahrenabwehrenden Maßnahmen wurden an Ressorts 14 Warnmeldungen, 8 Frühwarnungen und 4 weitere sicherheitsrelevante Informationen abgesetzt.

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

Das SAX.CERT hat im Berichtszeitraum in 10.513 Fällen personenbezogene Daten gemäß § 6 Absatz 4 SächsISichG verarbeitet.

Dabei handelt es sich in allen Fällen um E-Mails, in denen von den zentralen Virenscannern des SVN Schadsoftware festgestellt wurde 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 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 daher 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 SächsISichG und 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 Sächsischen Informationssicherheitsgesetzes gelten verschiedene Meldepflichten für die staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen sowie Beliehene, die an das Sächsische Verwaltungsnetz oder das Kommunale Datennetz angeschlossen sind. Diese Stellen sind nach den §§ 16 und 17 SächsISichG dazu verpflichtet, Sicherheitsvorfälle unverzüglich zu melden, wenn diese:

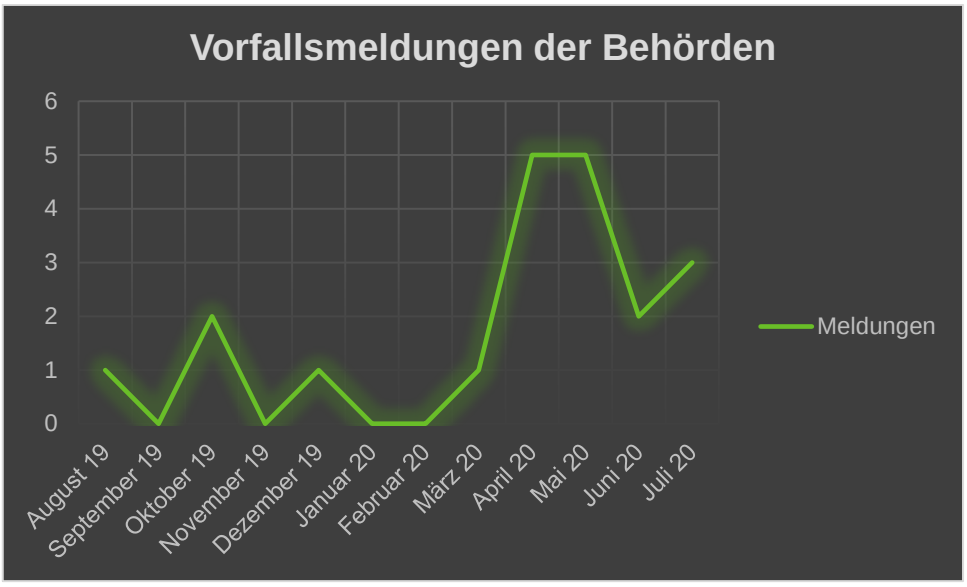
- zu einer erheblichen Beeinträchtigung der Schutzziele geführt haben oder
- behördenübergreifend zu einer erheblichen Beeinträchtigung der Schutzziele führen können.

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.

Grafik: Gemeldete Vorfälle mittels Meldeformular durch Landes- und Kommunalbehörden



Im Berichtszeitraum wurden dem SAX.CERT über das Meldeformular 20 Sicherheitsereignisse gemeldet (16 von den staatlichen Behörden, 4 von den nicht-staatlichen Behörden). Das ist ein Anstieg auf insgesamt niedrigem Niveau im Vergleich zu den 14 Meldungen in den 12 Vormonaten.

Der markante Anstieg im April 2020 ist dabei auf das entsprechende Sensibilisierungsschreiben des BfIS Land an die BfIS der Ressorts zurückzuführen.

6. Umsetzungsstand des SächsISichG

Das Sächsische Informationssicherheitsgesetz 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 Beauftragten für Informationssicherheit in den Ressorts und weiteren wichtigen Behörden sowie die Umsetzung eines Informationssicherheitsmanagementsystems.

6.1. Informationssicherheitsorganisation

Um die Informationssicherheitsziele zu erreichen, benötigen jede Behörde als 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 noch nicht vollständig umgesetzt werden. Zwar sind die strategisch und operativen Institutionen durch das Gesetz mit ausreichenden Handlungskompetenzen ausgestattet worden. Zum Ende des Berichtszeitraums mangelte es jedoch stellenweise noch an personeller Untersetzung.

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 auch die Sensibilisierung der Mitarbeiter in den Behörden. Hierzu gehört auch der Aufbau einer geeigneten Organisationsstruktur. Die Befugnisse des BfIS Land wurden durch das SächsISichG im Vergleich zu früher 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 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 LKA (SN4C), LfV, ZSC der GenStA Dresden und die Abteilung Katastrophenschutz im SMI.

Im Berichtszeitraum war die Stelle des BfIS Land nach der Pensionierung des langjährigen Beauftragten für Informationssicherheit, Herrn Karl-Otto Feger, zweimal über mehrere Monate unbesetzt, nachdem seine Nachfolgerin im Amt, Frau Dr. Kristin Roespel, nach wenigen Monaten in einen anderen Aufgabenbereich versetzt worden war. Seit dem 1. Juli 2020 ist Herr Christoph Damm neuer Beauftragter für Informationssicherheit des Landes.

Mit Blick auf die personelle Ausstattung des Referats als zentrale strategische Stelle der Informationssicherheit im Freistaat Sachsen ist zu konstatieren, dass die Aufgabenlast aus den mit dem Gesetz verbundenen Pflichten insb. zur Beratung der BfIS der staatlichen und nichtstaatlichen Stellen, zur Koordination eines ISMS des Landes sowie zu den Dokumentationspflichten bereits zum Ende des Berichtszeitraums sehr hoch war und weiter steigen wird. Die Ausstattung des Referats muss entsprechend angepasst werden.

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 Beauftragten für Informationssicherheit (BfIS) zu bestellen. Die Umsetzung hat 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 2020 erfüllten 9 von 15 Staatsbehörden diese gesetzliche Anforderung eines hauptamtlich bestellten BfIS.

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

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 Mitarbeitern) und Behörden mit besonderer Kritikalität hauptamtliche BfIS als zwingend notwendig erachtet, sogleich sie gesetzlich nicht festgeschrieben sind.

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

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[1]
Landesamt für Steuern und Finanzen	x	
Gerichte (koordinierend)		x

[1] Bislang ist in keinem der vier Sächsischen Krankenhäuser ein BfIS benannt.

6.1.3. Beauftragte für Informationssicherheit in den nicht-staatlichen Stellen

Stand 7. August 2020 wurden dem BfIS lediglich von acht nicht-staatlichen Stellen die Benennung von Beauftragten für Informationssicherheit mitgeteilt, obwohl das Gesetz eine Unterrichtungspflicht an den BfIS Land regelt, § 8 Absatz 1 Satz 4 SächsISichG. Wenngleich dem BfIS Land z. B. bekannt ist, dass alle Landkreise bereits eigene BfIS ernannt haben, sind durch die Landkreise keine nennenswerten Meldungen erfolgt. Um der Unterrichtungspflicht einfach und bequem nachkommen zu können, wurde hierzu auch ein Online-Formular bereitgestellt (Beauftragte für Informationssicherheit (BfIS) | Beteiligungsportal E-Government) und die Kommunen über ihre Spitzenverbände SSG und SLKT informiert. Eine stärkere Nutzung dieses Formulars durch die nicht-staatlichen Stellen ist angezeigt.

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 (§ 6 Abs. 1 SächsISichG). Im Berichtszeitraum wurde der Ausbau des SAX.CERT am Standort Glacisstraße in unmittelbarer Nähe zum Regierungscampus intensiviert. Im Laufe des Jahres 2019 wuchs das SAX.CERT so von drei auf sechs Mitarbeiter auf, darunter die beiden ersten zwei unbefristeten Stellen. Die personelle Sollstärke des SAX.CERT für die bestehenden Aufgaben aus der Verwaltungsvorschrift Informationssicherheit der Sächsischen Staatsregierung (VwV IS) konnte damit zum Stand Ende 2019 vorläufig abgeschlossen werden.

Mit Inkrafttreten des Sächsischen Informationssicherheitsgesetz (SächsISichG) sind darüber hinaus zahlreiche Neuerungen und Aufgabenerweiterungen für das SAX.CERT geregelt worden. Neben den Aufgaben als Sicherheitsnotfallteam der Sächsischen Landesverwaltung soll das SAX.CERT künftig als zentraler Ansprechpartner für alle sächsischen Kommunen und für sächsische Unternehmen im KRITIS-Bereich diese bei IT-Sicherheitsereignissen und -vorfällen unterstützen und beraten. Weiterhin soll das SAX.CERT die Rolle der zentralen Meldestelle im Sinne des BSI-Gesetzes und der Meldestelle für den VerwaltungsCERT-Verbund des IT-Planungsrates wahrnehmen. Darüber hinaus erhält 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.

Mit dem bestehenden Personal konnten im Berichtszeitraum die bereits vor dem Gesetz in der VwV IS festgelegten Basisaufgaben erfüllt werden. Jedoch ist kritisch anzumerken, dass das Sicherheitsnotfallteam seit der Versetzung seines ehemaligen Leiters in die Position des BfIS Land seit Juli

2020 keinen Leiter mehr hat und es allgemein schwer ist, qualifiziertes Personal im Bereich Informationssicherheit zu gewinnen und vor allem zu halten. Der durch das Gesetz zusätzlich erweiterte Aufgabenbereich sowie durch den Koalitionsvertrag gegebene Auftrag zum Aufbau eines behördenübergreifenden Informationssicherheitszentrums, das sächsische Verwaltungen und Betreiber kritischer Infrastrukturen unterstützt, ist ohne zusätzliche personelle Ausstattung nicht realisierbar.

Trotz der Ressourceneinschränkungen bietet das SAX.CERT bereits jetzt eine Reihe von Dienstleistungen an, die Behörden und Gerichte des Freistaates Sachsen sowie Kommunen kostenfrei in Anspruch nehmen können (#Sicherheitsangebote des SAX.CERT für die Landesverwaltung und die Kommunen). Positiv hervorzuheben ist, dass Anfang Mai 2020 in einem Pilotbetrieb ein Lagezentrum mit der entsprechenden Visualisierung der Gefährdungslage eingerichtet worden ist. Auch ein Informationsportal, über das die Behörden Dienste des SAX.CERT nutzen sollen, wurde aufgebaut und soll mit Veröffentlichung dieses Berichts den Regelbetrieb aufgenommen haben. Nicht unbeachtet darf bleiben, dass das SAX.CERT noch vor strukturellen Problemen zur Erfüllung seiner Aufgaben aus dem Gesetz steht. So bedarf es zusätzlicher Vereinbarungen und technischer Lösungen in Zusammenarbeit mit dem technischen Dienstleister des Sächsischen Verwaltungsnetzes (SVN), damit notwendige Daten zur Erkennung und Abwehr von Gefahren für die informationstechnischen Systeme durch Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung dem SAX.CERT übermittelt werden können.

6.2. Verpflichtungen aus der Leitlinie Informationssicherheit des IT-Planungsrates

Anfang 2019 verabschiedete der IT-PLR die überarbeitete Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung. Die Arbeitsgruppe Informationssicherheit wurde dabei mit der Erstellung einer Umsetzungsplanung und der Erarbeitung und Festlegung von Controlling-Kennzahlen für die Leitlinie beauftragt. Dazu wurden für die fünf Handlungsfelder der Leitlinie insgesamt 26 Umsetzungsschritte identifiziert. Zuständig für die Umsetzung der Maßnahmen sind prioritär die einzelnen Länder, abweichend für einzelne Maßnahmen die AG Infosic des IT-PLR selbst.

Sowohl die Leitlinie Informationssicherheit des IT-PLR als auch der Umsetzungsplan setzen für die Informationssicherheit im Freistaat eher nachrangige Impulse. Entscheidend für die sächsische Staatsverwaltung ist das SächsISichG. So werden die im „Handlungsfeld 1: Informationssicherheitsmanagement“ benannten Mindestanforderungen mit der Umsetzungsfrist 2020 entsprechend auch im SächsISichG adressiert. Laut Umsetzungsplan des IT-Planungsrates sind bis Ende 2020 in den sächsischen Landesbehörden folgende Maßnahmen umzusetzen:

- Die Rollen und deren Aufgaben im Informationssicherheitsmanagement sind festgelegt und dokumentiert.
- Die Rollen sind in den Behörden besetzt.
- Die Leitlinie für Informationssicherheit ist in der jeweiligen Behörde in Kraft gesetzt und regelt den jeweiligen Zuständigkeitsbereich verbindlich.
- In den Behörden ist ein Prozess zur Erstellung von Richtlinien für die Informationssicherheit für den jeweiligen Zuständigkeitsbereich etabliert.
- Der Prozess zur regelmäßigen Überprüfung der Richtlinien ist etabliert.
- Meldepflichtige Ereignisse, Meldestellen und Meldeabläufe sind für alle Behörden und Einrichtungen festgelegt und dokumentiert.
- Ein Aus- und Fortbildungsprogramm der Beauftragten für Informationssicherheit (BfIS) wird regelmäßig angewendet.
- Es findet eine kontinuierliche Fortbildung der BfIS statt.

Die weiteren Handlungsfelder 2 bis 4, u. a. „Gemeinsame Abwehr von IT-Angriffen“, werden durch die AG Infosic des IT-PLR thematisch begleitet und in den Ländern umgesetzt. Gerade bei der Zusammenarbeit der CERTs im Austausch der Länder untereinander und mit dem Bund ist Sachsen über das SAX.CERT in hohem Maße eingebunden. Das SAX.CERT treibt den Austausch über seine engen Verbindungen auf Arbeitsebene mit dem BSI voran.

Eine Sonderrolle spielt hier das Handlungsfeld 5: Teil „IT-Notfallmanagement“, da diese Thematik nicht durch das SächsISichG geregelt wird. Nach Einschätzung des BfIS Land sind hierzu Stand August 2020 kaum Konzepte, Prozesse oder auch notwendige personelle Ressourcen vorhanden.

6.3. Ausblick

Die sächsische Verwaltung nutzt zunehmend die Vorteile der Digitalisierung. Mit fortschreitender Entwicklung bieten sich immer neue Möglichkeiten der Datenverarbeitung, der Kommunikation und des Wissenstransfers. Jedoch geht mit diesen Chancen auch ein stetig wachsendes Risiko der Verletzlichkeit einher, wie zahlreiche kritische Sicherheitsvorfälle auch in der deutschen Verwaltung zeigen. Ein effektives System für die Gewährleistung der Informationssicherheit ist der entscheidende Faktor, diese Risiken zu minimieren und vorausschauend Schutzvorsorge zu betreiben. Hierzu ist eine zeitnahe Befähigung der sächsischen Verwaltungsorganisation dringend geboten.

Die Gewährleistung der Informationssicherheit vor dem Hintergrund einer sich permanent verschärfenden Bedrohungslage und die Umsetzung des Onlinezugangsgesetzes bis Ende 2022 sind die zentralen Herausforderungen bei der Digitalisierung der sächsischen Verwaltung. Doch dem Freistaat fehlen zum Zeitpunkt der Erstellung des vorliegenden Berichts (August 2020) die notwendigen Personalressourcen, um diesen Herausforderungen adäquat begegnen zu können. Eine angemessene Personalausstattung ist jedoch notwendig, wenn die Einhaltung der bundes- und landesrechtlichen Verpflichtungen nicht gefährdet werden soll.

Herausgeber:

Sächsische Staatskanzlei

Redaktion sowie Gestaltung und Satz:

Referat 45: Informations- und Cybersicherheit, Kritische Infrastrukturen

Redaktionsschluss:

27. August 2020