Freistaat
SACHSEN

Jahresbericht Informationssicherheit 2023

des Beauftragten für Informationssicherheit des Landes
Berichtszeitraum: **August 2022 – Juli 2023**

INHALT

1
EINFÜHRUNG

Der aktuelle Berichtszeitraum ist, genauso wie auch der vorherige, geprägt von der abstrakten Gefahr aus dem Cyberraum in Folge des russischen Angriffskrieges auf die Ukraine. Konkrete Attacken konnten allerdings vorrangig in diesen beiden Ländern beobachtet werden. Deutschland war nur unterschwellig betroffen, insbesondere mit DDoS-Attacken auf verschiedene Behörden und Unternehmen. Das Sächsische Verwaltungsnetz (SVN) wiederum tangierte das nur am Rande. Die im Vorzeitraum begonnen Aktivitäten zur Ablösung der Antivirensoftware Kaspersky wurden fortgesetzt und sind mittlerweile auch vollständig umgesetzt.

Weltweit bleibt Ransomware – also die Verschlüsselung von Daten und nachfolgende Lösegelderpressung – die gefährlichste Form der Cyberkriminalität. Über den Jahreswechsel 2022/ 2023 waren sehr viele Angriffe auf Hochschulen in Deutschland zu verzeichnen. Mit der Westsächsischen Hochschule Zwickau und der TU Bergakademie Freiberg traf es auch zwei sächsische Einrichtungen. Beide konnten noch vor Verschlüsselungsbeginn den Eindringling entdecken und damit den Schaden begrenzen.

Auswirkungen auch für Sachsen hatte der Ransomware-Angriff auf den nordrhein-westfälischen IT-Dienstleister der Industrie- und Handelskammern Deutschlands im August 2022. Obwohl der IT-Dienstleister ebenfalls die Angreifer noch vor dem Beginn der Verschlüsselung entdeckte, waren alle 79 Kammern, auch die sächsischen, über Monate hin nur eingeschränkt arbeitsfähig.

Obgleich das SVN von den vorgenannten Fällen nicht betroffen war, bleibt auch hierfür die Gefahr aus dem Cyberraum sehr groß. Dies zeigen die vielen Angriffsversuche, die von den Schutzsystemen des SVN abgewehrt wurden. Deshalb wurden im Berichtszeitraum die Anstrengungen zur Etablierung eines leistungsfähigen IT-Notfallmanagements verstärkt. In der Staatskanzlei, allen Ministerien und weiteren für den IT-Betrieb der staatlichen Verwaltung wesentlichen Behörden wurden IT-Notfallbeauftragte benannt, von Experten geschult und miteinander vernetzt.

Um mit allen relevanten Partnern noch stärker vernetzt der Bedrohungslage begegnen zu können, wurden mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) intensive Verhandlungen aufgenommen. Die bisherige Absichtserklärung zur Zusammenarbeit wird in eine verbindliche Kooperationsvereinbarung überführt. Aber auch länderübergreifend wurde die Zusammenarbeit gefördert. So hospitierten Bedienstete aus dem sächsischen Sicherheitsnotfallteam SAX.CERT im Bayerischen Landesamt für Sicherheit in der Informationstechnik. Der Informationsaustausch war hier für beide Seiten fruchtbar.

Bereits gute Tradition hat der IT-Sicherheitstag in Dresden, den die Staatskanzlei (SK) gemeinsam mit dem Behördenspiegel im Juni 2023 veranstaltete. Mit einer Rekordbeteiligung von über 220 Bediensteten staatlicher und kommunaler Behörden, Vertreterinnen und Vertretern von Hochschulen sowie Expertenvorträgen aus Verwaltung, Wirtschaft und Forschung war der Kongress ein voller Erfolg.

Generell gilt für Sachsen, dass die Kommunen stark in das IT-Sicherheitskonzept der Staatsverwaltung eingebunden sind. Dazu dienen Veranstaltungen wie der IT-Sicherheitstag genauso wie die Schärfung der IT-Schutzsysteme, die das Kommunale Datennetz (KDN) gemeinsam mit dem SVN nutzt. Vertreterinnen und Vertreter der kommunalen Spitzenverbände profitieren vom Austausch in der Arbeitsgruppe Informationssicherheit (AG IS) und können dort erarbeitete Mindeststandards/ Richtlinien zur Informationssicherheit für die Kommunen übernehmen. Zudem bietet das Sächsische Informationssicherheitsgesetz (SächsISichG) weiterhin einen stabilen Rahmen für die sächsischen Kommunen. Dass sich die Bundesländer bei der Umsetzung der Europäischen Richtlinie NIS2 in nationales Recht nicht darauf einigen konnten, die kommunale Ebene künftig in die Landesgesetzgebung verbindlich mit einzubeziehen, hat für die Sicherheit der sächsischen Kommunen daher keine negative Auswirkung.

Kernbotschaften des Jahresberichts Informationssicherheit

Sicherheitsgefährdungen für die IT der öffentlichen Verwaltung in Sachsen bleiben auf konstantem Niveau

Die Schutzsysteme filterten auch im aktuellen Berichtszeitraum eine hohe Zahl von Angriffen, wenngleich etwas geringer als im Vorjahr: Von den über 110 Millionen eingehenden E-Mails wurden bereits über 67 Millionen direkt am Internet-Gateway des SVN abgewiesen, da der Verdacht bestand, dass sie Schadsoftware enthalten. Von den übrigen Schutzsystemen wurden knapp sechs Millionen E-Mails als Spam und 682.000 E-Mails vom neuen Reputationsdienst als unseriös markiert. Darüber hinaus wurden gut 30.000 Viren im Mailverkehr und 12.000 Viren im Internetverkehr erkannt und blockiert.

Typische Cyber-Angriffe auch auf die öffentliche Verwaltung: Die weltweit angespannte Lage in Bezug auf Ransomware spiegelte sich auch in Sicherheitsvorfällen in Sachsen wieder, allerdings bisher immer außerhalb des Verwaltungsnetzes. So wurden die Westsächsische Hochschule Zwickau und die TU Bergakademie Freiberg Opfer von solchen Attacken, konnten allerdings die Verschlüsselung der Daten erfolgreich verhindern. Darüber hinaus wurden weiterhin Wellen von Phishing-Mails registriert, deren Ziel es war, Nutzerdaten aus dienstlichen E-Mail-Accounts abzufischen. Auch Überlastangriffe mittels Botnetzen, bei denen versucht wurde, Internetseiten und Dienste der Landesverwaltung sowie kommunaler Behörden durch hohe Verkehrslasten zu blockieren, wurden registriert.

Social Engineering mit hohem Schadenspotenzial:
Über den Berichtszeitraum verteilt gab es immer wieder Fälle von Social Engineering, d. h. Betrugsversuchen mit Mitteln der Beeinflussung von Mitarbeitern in sächsischen Behörden per E-Mail und/ oder Telefonanruf, um z. B. finanzielle Transaktionen zu veranlassen. Im schwerwiegendsten Fall entstand dem Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt ein Schaden von ca. 225.000 Euro.

Schutzmechanismen erweitern, Schnittstellen zum Internet einschränken: Zur Erhöhung der Sicherheit der IT-Systeme wurde mit der Link-Reputation ein neues Schutzsystem eingeführt, das alle E-Mails aus dem Internet auf schädliche Links überprüft und diese bei negativer Bewertung technisch als „nicht klickbar" verändert. Nachdem im letzten Berichtszeitraum die wichtigsten aus dem Internet erreichbaren Webdienste der Landesverwaltung separat abgesichert wurden, wurde in den letzten Monaten die Abschaltung weiterer Schnittstellen bzw. die Harmonisierung auf eine zentrale geschützte Schnittstelle vorbereitet.

Sächsisches Informationssicherheitsgesetz wird noch nicht ausreichend umgesetzt

Erweiterte Schutzmechanismen noch nicht flächendeckend im Einsatz: Das SächsISichG lässt in den §§ 12 und 13 erweiterte Maßnahmen zur Gefahrenabwehr zu. Die Möglichkeiten intensiverer Abwehrmechanismen werden nach Angaben der Ressorts kaum genutzt. Das einzige derartige Überwachungssystem zur Erkennung von Anomalien in Datenströmen läuft beim SAX.CERT.

ISMS Land im Aufbau: Mit entsprechender personeller Ausstattung sowohl beim Beauftragten für Informationssicherheit des Freistaats Sachsen (BfIS Land) als auch in den Ressorts hat die Entwicklung des Niveaus der Informationssicherheitsmanagementsysteme (ISMS) in den Behörden und des übergeordneten ISMS der Landesverwaltung spürbar an Fahrt gewonnen. Zahlreiche neue Richtlinien wurden verabschiedet. Dennoch bleibt noch viel zu tun, zudem werden die landesweiten Leitlinien von den Behörden, die sie verbindlich umsetzen müssen, oft als zu starke Reglementierung empfunden. Da mit eigenen personellen Ressourcen eine Unterstützung der jeweiligen Beauftragten für Informationssicherheit (BfIS) nicht ausreichend geleistet werden kann, wird den staatlichen Stellen ein Rahmenvertrag zum Abruf externer Expertise zur Verfügung gestellt.

Es fehlen weiterhin Informationssicherheitsbeauftragte: Nach §§ 7 und 8 SächsISichG haben alle staatlichen und nicht-staatlichen Stellen einen BfIS und einen Stellvertreter zu bestellen. Die Umsetzung sollte bis Ende 2020 erfolgen (§ 20 SächsISichG). Zum Zeitpunkt der Erstellung dieses Berichtes im August 2023 sind zwar erstmals alle Ministerien dieser Verpflichtung nachgekommen, jedoch haben noch nicht alle staatlichen Behörden die Stelle besetzt. Bei den Kommunen ist der Nachholbedarf noch größer: Hier waren zwar für alle Landkreise, aber nur für etwa die Hälfte der Kommunen BfIS benannt. Dieser Anteil hat sich in den letzten zwei Jahren kaum verändert.

Sächsisches Informationssicherheitsgesetz bleibt ein stabiler Rahmen

Das SächsISichG ist ein dauerhaftes Regelwerk: Die Anforderungen an die Informationssicherheit ändern sich regelmäßig, auch durch neue gesetzliche Vorgaben wie die Anfang 2023 in Kraft tretende NIS-2-Richtlinie der EU. Das bestehende SächsISichG bietet eine solide Grundlage zur Umsetzung dieser Anforderungen und enthält eine Regelungstiefe, die noch lange nicht an ihre Grenzen stößt. Es gilt, die mit dem Gesetz verbundenen Anforderungen umzusetzen.

Europäische Regelungen werden die Anforderungen an die Sicherheitsorganisationen erhöhen: Die NIS-2 Richtlinie der EU beinhaltet eine erhebliche Erweiterung der Mindestsicherheitsmaßnahmen und Meldepflichten im Bereich der Cybersicherheit für weitere Unternehmen in bestehenden und neu erfassten Wirtschaftssektoren. Zusätzlich wird erstmals die öffentliche Verwaltung bis einschließlich der Ebene der Länder in den Anwendungsbereich aufgenommen. Dem BfIS Land wird künftig die Rolle einer Aufsichtsbehörde zukommen, und die Aufgaben des Sicherheitsnotfallteams SAX.CERT werden konkretisiert. Die damit einhergehenden zusätzlichen Bedarfe an Ressourcen werden im Rahmen der Neufassung des Sächsischen Informationssicherheitsgesetzes abzustimmen sein.

2
GEFÄHRDUNGSLAGE

Die Gefährdungslage ergibt sich aus potentiellen, schwer objektiv erfassbaren Bedrohungen einerseits und realen Angriffen andererseits. Daher ist eine kontinuierliche Beobachtung technologischer Entwicklungen, aufgedeckter Schwachstellen sowie des Datenverkehrs im Netz der sächsischen Verwaltung erforderlich. Diese Beobachtung erfolgt durch das Sicherheitsnotfallteam SAX.CERT. Das SAX.CERT legt besonderen Fokus auf das SVN sowie das KDN und stellt in diesem Bericht die Erkenntnisse aus dem Zeitraum August 2022 bis Juli 2023 zusammen. Dabei ist festzustellen, dass sich die Anzahl der versuchten und erfolgreichen Angriffe auf die sächsische Verwaltung im Vergleich zum Vorjahr kaum verändert hat. Nach der Zusammenfassung der Gefährdungslage werden die Methoden und Mittel der Angreifer, die im Berichtszeitraum die größte Rolle spielten, anhand einiger Beispiele aufgezeigt. Dabei ist eine weitere Professionalisierung der Angreifer zu erkennen.

2.1 Lagebild in der Staatsverwaltung

Das SVN ist prinzipiell ein vom Internet unabhängiges internes Netz der Staatsbehörden und hat durch diese Struktur ein vergleichsweise hohes Niveau an Informationssicherheit aufzuweisen. Gleiches gilt für das KDN. Jedoch sind diese Netze natürlich auch mit dem Internet verbunden, um z. B. die Kommunikation zwischen Behörden und Bürgerinnen und Bürgern oder auch Unternehmen und anderen Institutionen zu gewährleisten. Gerade vor dem Hintergrund, dass sich die öffentliche Verwaltung stetig weiter digitalisiert und zunehmend Behördenleistungen auch online abrufbar sind, haben Behörden und ihre IT-Netzwerke immer mehr Verbindungen in das Internet. Da aber gerade aus dem Internet heraus Angriffe auf die IT-Infrastruktur der Verwaltung drohen, kommen leistungsfähige Schutzsysteme in den zentralen Diensten des SVN und KDN zum Einsatz. Diese sichern die Übergänge aus dem internen Netz der Staatsverwaltung von und zum Internet auch gegen komplexe und zielgerichtete Bedrohungen zeitgemäß ab, auch weil diese im Berichtszeitraum kontinuierlich 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.

Zwischen August 2022 und Juli 2023 wurden von über 110 Millionen ankommenden E-Mails (Vorjahreszeitraum: 145 Mio.) rund 67,5 Mio. bzw. 61% (Vorjahreszeitraum: 103 Mio. bzw. 71%) an der Internetübergangsstelle des SVN direkt abgewiesen, weil sie unter dem Verdacht standen, für das SVN schädlich zu sein. Weitere knapp 5,3 Mio. E-Mails (Vorjahreszeitraum: 7 Mio.) wurden von den dezentralen Systemen als Spam-Mail erkannt und entsprechend markiert. Damit lag der Anteil von unerwünschten Nachrichten am Mail-Aufkommen mit gut 66% deutlich unter dem Wert des Vorjahres (76%).

Abbildung 1:
Entdeckte Schadprogramme im Mailverkehr

Ergänzend wurden durch den im November 2022 neu eingeführten Dienst zur Prüfung der Reputation von Links eingehender Mails (Vgl. 3.2.1.) bereits rund 682.000 E-Mails gekennzeichnet und die enthaltenen Links unschädlich gemacht.

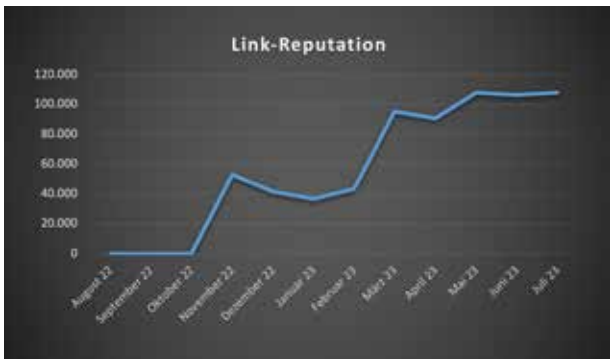


Abbildung 2:
Markierte E-Mails mit verdächtigen Links

Daneben wurden gut 30.000 Viren im Mailverkehr abgefangen. Die intensivsten Angriffe waren im Zeitraum Oktober/ November 2022 (rd. 3.800 Mails p. Monat) sowie im Mai/ Juni 2023 (rd. 4.700 Mails p. Monat) zu beobachten. Ursächlich hierfür waren insbesondere Angriffe mittels der Malware Formbook und Agent Tesla. Im November 2022 konnte zusätzlich eine größere Phishingwelle durch den Emotet Trojaner beobachtet werden, was auf einen Wiederaufbau der im Januar 2021 zerschlagenen Emotet-Infrastruktur schließen lässt. Im Mai/ Juni 2023 führten vermehrt Angriffe durch den Qbot-Trojaner zu den erhöhten Zahlen.

Neben verseuchten E-Mails ist auch ein in Webseiten oder Downloads versteckter Schadcode eine der wesentlichen Gefahren für die IT der Verwaltungen. So wurden im Internetverkehr, wenn z. B. Bedienstete auf ihren dienstlichen Geräten eine Webseite aufrufen, über 12.000 Viren erkannt. In den 12 Monaten zuvor waren es noch knapp 22.000 Viren, was einen grundsätzlich positiven Trend erkennen lässt. Auffällig sind die Monate Oktober 2022 sowie April 2023. Ausschlaggebend hierfür war die Aufnahme von grundsätzlich vertrauenswürdigen, intensiv genutzten Webseiten auf die Liste zu blockierender Downloads durch den Anbieter.

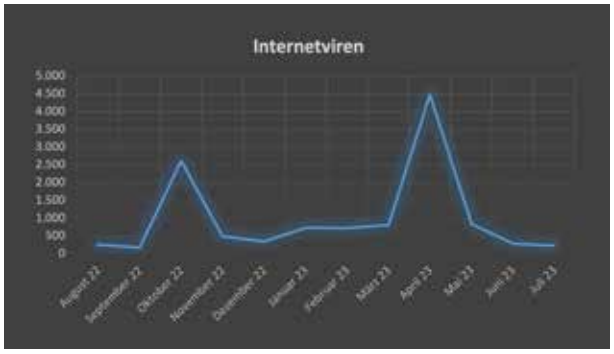


Abbildung 3:
Entdeckte Schadprogramme im Internetverkehr

2.2 Angriffsmethoden und -mittel

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

2.2.1 DDoS-Angriffe

Im aktuellen Berichtszeitraum gab es verschiedene gezielte Überlastangriffe mittels Botnetzen. Dabei wurde von Hackergruppen mit hoher Verkehrslast über einen längeren Zeitraum versucht, die vom Internet aus erreichbaren Server der Staatsverwaltung zu blockieren. Nach voreingestellter Latenzzeit konnten die Schutzsysteme der im SVN genutzten Internet Service Provider (ISP) diese Angriffe zuverlässig abwehren. Es kam nur zu geringen Einschränkungen. Ebenfalls zu beobachten waren sehr kurzzeitige Angriffe, die bereits vor dem Eingreifen des Überlastschutzes wieder endeten. Die Angriffserkennungssysteme des SVN detektierten dabei eine Reihe verschiedener Angriffsmuster und -vektoren, mit denen die aus dem Internet zugänglichen Komponenten und Dienste des SVN auf bekannte Schwachstellen gescannt wurden. Dies ist typisch für Hacker, die diese Schwachstellen dann kommerziell im Darknet als „Cybercrime as a Service" zur Ausnutzung anbieten.

2.2.2 Phishing-Mails

Mittels sogenannter Phishing-Mails versuchen Cyberkriminelle sich als vertrauenswürdige Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es, im weiteren Verlauf an persönliche Daten, wie z.B. Zugangsdaten, eines Bediensteten zu gelangen oder ihn zur Ausführung einer schädlichen Aktion zu bewegen. In der Folge wird dann beispielsweise Identitätsdiebstahl begangen oder eine Schadsoftware (z. B. Ransomware) installiert. Im Berichtszeitraum wurden vom SAX.CERT regelmäßig Wellen von Phishing-Mails registriert, deren Ziel es war, Benutzerdaten von dienstlichen E-Mail-Konten zu erlangen. So gingen u. a. im November 2022 vermehrt Meldungen zu Phishing-Mails des Emotet Trojaners sowie im Mai/ Juni 2023 des Qbot-Trojaners im SAX.CERT ein.

Ransomware – Verschlüsselung und Erpressung

Ransomware sind mit Schadsoftware ausgestattete Trojaner, mit deren Hilfe Cyberkriminelle den Zugriff auf Daten 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 vermehrt auch auf ITSysteme der Hacker kopiert. Die Angreifer drohen mit der Veröffentlichung von sensiblen Daten, bzw. bieten die Daten im Netz zum Verkauf an, sollten die Erpressungsversuche nicht zum Erfolg führen. Ransomware-Angriffe bergen vor allem dann ein enormes Schadpotenzial, wenn sie auf schlecht gesicherte IT-Systeme treffen (z.B. ohne aktuelle Sicherheitsupdates und Schutzmaßnahmen wie eine Mehr-Faktor-Authentisierung) und die Mitarbeiterinnen und Mitarbeiter, z. B. bei der Bearbeitung von E-Mails, angehängte Dokumente oder Links im Text nicht richtig auf Vertrauenswürdigkeit einschätzen können. Verfügt die betroffene Behörde am Ende über keine regelmäßige Datensicherung, sind die Daten ohne Entschlüsselungscode nicht mehr nutzbar. Selbst wenn Backups vorliegen, eingespielt werden und die Verschlüsselung damit umgangen werden kann, droht in solchen Fällen immer noch die Veröffentlichung sensibler Daten durch den vorangegangenen Datendiebstahl. Für die öffentliche Verwaltung gilt es, ein solches Szenario unbedingt zu vermeiden. 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 SVN. Aufgrund eines Hinweises aus dem Landeskriminalamt eines anderen Bundeslandes konnte im November 2022 der bereits durch Cyberkriminelle vorbereite finale Angriff auf ein Segment des Schulnetzes in Leipzig rechtzeitig bemerkt und größerer Schaden verhindert werden. Im Dezember 2022 erhielt das SAX.CERT die Meldung, dass die Westsächsische Hochschu-

le Zwickau von einer Ransomware betroffen ist, im Januar 2023 dann die TU Bergakademie Freiberg. In beiden Fällen wurden die Angriffe so rechtzeitig bemerkt, dass eine Verschlüsselung der Daten verhindert werden konnte. Allerdings mussten über einen längeren Zeitraum Netzwerke wieder neu aufgebaut und kompromittierte Dienste wiederhergestellt werden.

Emotet und QBot

Bis zu seiner Zerschlagung Anfang des Jahres 2021 war Emotet eine der Hauptbedrohungen, die über bösartige Spam-Kampagnen verbreitet wurde. Emotet war dabei nur der erste Zugang zum Opfer-System und nutzte sogenanntes „Outlook-Harvesting", um sich weiter zu verbreiten. Dazu las Emotet die Kontaktbeziehungen und auch E-Mail-Inhalte aus den Postfächern infizierter Systeme aus. Diese Informationen benutzte es automatisiert zur Weiterverbreitung, sodass die Empfänger fingierte Mails von Absendern erhielten, mit denen sie kürzlich in Kontakt standen. In diesen Mails waren entweder Trojaner angehangen, die weiteren Schadcode enthielten oder Links, die entsprechenden Schadcode geladen haben. Der installierte Schadcode hat seinerseits weitere Programmteile geladen und den Angreifern Zugang zu den Systemen ermöglicht.

Ein vergleichbares Vorgehen ist bei QBot (oder auch Qakbot) zu beobachten. Ursprünglich wurde QBot zur Erlangung von Zugangsdaten, insbesondere im Finanzbereich, entwickelt und fungierte als Backdoor. Mittlerweile wurde QBot so weiterentwickelt, dass es die Funktionalitäten von Emotet erreicht und nach Zerschlagung des Emotet-Netzwerkes zur #1-Bedrohung im Bereich der Trojaner wurde.

Durch das SAX.CERT wurden entsprechende Angriffswellen durch wiederbelebte Emotet-Netzwerke sowie, deutlich ausgeprägter, durch QBot-Netzwerke festgestellt.

2.2.3 Schwachstellen in Software

Beinahe täglich werden neue Sicherheitslücken bekannt, die zu einer Gefährdung ganzer ITNetzwerke führen können. Die wichtigste Gegenmaßnahme ist hier die möglichst zeitnahe Installation der vom Hersteller zur Verfügung gestellten Korrekturen („Patches"). Das SAX.CERT bietet hierzu allen Behörden der Staats- und Kommunalverwaltung einen kostenlosen Warndienst zu über 2.000 Soft- und Hardwareprodukten an, der per E-Mail gezielt zu den vom Nutzer ausgewählten Produkten warnt, sobald hier neue Lücken bekannt werden (Vgl. 4.1.). Welche Risiken bei offenen Sicherheitslücken auftreten, zeigen u. a. folgende Fälle im Berichtszeitraum:

ProxyNotShell (MS Exchange)

Am 11. September 2022 wurde eine Schwachstelle im Microsoft Exchange Server bekannt, die es Angreifern ermöglicht, ihre Berechtigungen zu erhöhen. Um die Schwachstelle auszunutzen, reicht dem Angreifer zunächst der Zugriff auf einen Exchange-Server mit einem einfachen Benutzerkonto. Von diesem kann er mittels manipulierter Anfragen die Schwachstelle ausnutzen und seine Zugriffsberechtigungen ausweiten. Mit den erweiterten Berechtigungen kann der Angreifer Malware oder Schadsoftware installieren sowie Daten ändern bzw. löschen.

Microsoft hatte kurzfristig Workarounds und Patches für alle betroffenen Versionen von Exchange Servern veröffentlicht, die im SVN umgehend eingespielt wurden.

ProxyNotShell (MS Exchange)

VMware ESXi ist eine Software zum Betrieb mehrerer virtueller Maschinen (VM) auf einem einzigen physischen Server. Die Schwachstelle ermöglicht es einem Angreifer, beliebigen Code auf einem anfälligen System auszuführen. Der Angriff basiert auf einer Schwachstelle, die bereits mit einem Patch in 2021 geschlossen wurde.

Das SAX.CERT hatte in einem ersten Schritt in den Ressorts den Einsatz und den aktuellen Versionsstand abgefragt. Der weit überwiegende Teil war auf aktuellem Patchstand. Einzelne, nicht aktuelle Softwareinstallationen wurden umgehend aktualisiert.

2.2.4 Social Engineering

Über den Berichtszeitraum verteilt gab es immer wieder Fälle von Social Engineering, also Betrugsversuchen mit Mitteln der Beeinflussung von Personen mittels E-Mail und/oder Telefonanrufen, um z. B. Finanztransaktionen zu bewirken.

Im Berichtszeitraum ist es Angreifern über diesen Weg geglückt, den Freistaat Sachsen finanziell zu schädigen. So wurde dem Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt im März 2023 eine betrügerische Mail zugeleitet. In dieser Mail wurde um die Überweisung des Betrages einer offenen Rechnung auf ein neues, kürzlich eröffnetes Bankkonto gebeten. Vermeintlicher Absender der Mail war eine Firma, mit welcher tatsächlich ein Vertragsverhältnis besteht. Zudem wurde auf eine tatsächliche Rechnung Bezug genommen, deren Betrag noch nicht überwiesen wurde. Auf Grund der genauen Kenntnis fiel der Betrug anfänglich nicht auf und die Auszahlung wurde auf das Konto der betrügenden Seite veranlasst. Erst auf Nachfrage der tatsächlichen Firma zum Zahlungsstatus wurde der Betrug aufgedeckt. Mit ca. 225.000 Euro entstand hier erheblicher finanzieller Schaden.

Im Kontext des so genannten **CEO-Fraud** waren Angreifer ebenfalls erfolgreich. Geschädigt wurden hierbei Bedienstete einer sächsischen Hochschule. Im Februar 2023 wurde eine Betrugs-Mail an verschiedene Beschäftigte einer Hochschule verschickt. Die Mail täuschte als Absender einen Professor der Hochschule vor und forderte dazu auf, ihm eine Gefälligkeit zu erweisen. Zwei Personen antworteten
und erhielten daraufhin die Aufforderung, Karten für den Google Play Store bzw. Apple iTunes zu kaufen und die Codes per Bild zu übermitteln. Das haben die Personen getan. Ihnen ist dadurch finanzieller Schaden entstanden. Es wurde Strafanzeige erstattet und die Mails und Mail- Protokolle wurden gesichert.

3
TÄTIGKEITSBERICHT DES BEAUFTRAGTEN FÜR INFORMATIONSSICHERHEIT DES LANDES

Der BfIS Land ist laut SächsISichG u. a. für die Erstellung des ISMS der Sächsischen Staatsverwaltung zuständig und erarbeitet verbindliche Mindeststandards zur Informationssicherheit für die staatlichen Stellen. Er initiiert und koordiniert landesweite Sensibilisierungs- und Schulungsmaßnahmen und Projekte zur Informationssicherheit.

Darüber hinaus berät er die Beauftragten der Behörden bei der Erfüllung ihrer Aufgaben. Um dies leisten zu können, stellt er einen Rahmenvertrag zu Beratungsleistungen in der Informationssicherheit zur Verfügung, aus dem die staatlichen Stellen Beratungs- und Unterstützungsleistungen abrufen können. Schwerpunkte des Rahmenvertrags sind Beratungen darauf spezialisierter Firmen zur Erstellung von Informationssicherheitskonzepten, zur Implementierung eines ISMS sowie zu technischen Aspekten der Informationssicherheit.

Zur Gewährleistung hinreichender Transparenz ist der BfIS Land zur jährlichen Berichterstattung über seine Tätigkeit an den Landtag verpflichtet.

3.1 Revisionen und Anordnungen

Zur Prüfung der Wirksamkeit des ISMS und des Stands der Erfüllung der Mindeststandards darf BfIS Land gemäß § 5 Absatz 7 SächsISichG Auskünfte verlangen und eigene Revisionen durchführen. Gegenüber an das SVN angeschlossenen staatlichen Stellen kann er gemäß § 5 Absatz 3 SächsISichG Anordnungen treffen oder Maßnahmen ergreifen, um Gefahren für die informationstechnischen Systeme, die mit dem SVN verbunden sind, abzuwehren. Maßnahmen, die auch die nicht-staatlichen Stellen betreffen, bedürfen hierbei der Herstellung des Benehmens mit dem BfIS des KDN (§ 5 Absatz 4 SächsISichG). Im Berichtszeitraum hat der BfIS Land nachfolgende Prüfungen vorgenommen und Anordnungen im obigen Sinn umgesetzt.

3.1.1 Revisionen

BfIS Land auditierte die Umsetzung technischer Maßnahmen wie die flächendeckende Einführung eines Mobile Device Managements zur Absicherung mobiler Endgeräte sowie die Migration von Altsystemen, für die absehbar keine Sicherheitsupdates mehr geliefert können, auf Systeme, die dem aktuellen Stand der Technik entsprechen. Zudem prüfte er den Umsetzungsstand der beschlossenen Mindeststandards zur Informationssicherheit in den Behörden der Staatsverwaltung.

Weiterhin wurde über eine Abfrage von BfIS Land erfasst, wie hoch der Anteil der dedizierten Kosten für die Informationssicherheit an den gesamten IT-Kosten der staatlichen Stellen im Jahr 2021 war. Hierbei ergab sich ein sehr inhomogenes Bild. Über die gesamte Staatsverwaltung wurden 5 % aller IT-Kosten dediziert für Sicherheit ausgegeben. Zusätzlich wurde bei der Beschaffung neuer Technik auf implizierte Sicherheitsaspekte geachtet – Security by Design.

Im Berichtszeitraum auditierte BfIS Land das Informationssicherheitsmanagement des Landes-ITDienstleisters und prüfte das Audit-Ergebnis der nach dem Standard ISO 27001 vom BSI zertifizierten EU-Zahlstelle des Staatsministeriums für Energie, Klimaschutz, Umwelt und Landwirtschaft. Zudem begleitete BfIS Land die erfolgreiche Re-Zertifizierung des SVN, ebenfalls durch das BSI nach ISO 27001.

3.1.2 Anordnungen

BfIS Land traf mehrere Anordnungen zum Umgang mit den bei einem Audit erfassten Altsystemen, für die der Lieferant zeitlich absehbar die Auslieferung von Sicherheitsupdates einstellen wird. So wurden Zugriffsrechte darauf stark reglementiert und eine gesonderte Sicherheitsüberwachung veranlasst.

Nachdem im Berichtszeitraum 2021/ 2022 die wichtigsten aus dem Internet erreichbaren Webdienste der Landesverwaltung mit einem zusätzlichen Authentisierungsfaktor separat abgesichert wurden, erfolgte im März 2023 eine Anordnung zur Absicherung des letzten noch verbliebenen Webdienstes.

3.2 Gremienarbeit

Auf Landesebene hält der BfIS Land den Vorsitz der Arbeitsgruppe 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 (AK SVN) teil. Auf Einladung sowie zur Beschlussfassung verbindlicher Mindeststandards zur Informationssicherheit trägt er zudem im Lenkungsausschuss IT- und E-Government (LA ITEG), dem Koordinierungsgremium für ressortübergreifende Entscheidungen zu Fragen der IT und zum E-Government der obersten Staatsbehörden, vor.

Darüber hinaus informiert er im IT-Kooperationsrat regelmäßig auch die kommunalen Spitzenverbände Sächsischer Städte- und Gemeindebund und Sächsischer Landkreistag über die Bedrohungslage in Sachsen.

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. Dieses landesweite ISMS verzahnt die ISMS auf Ebene der staatlichen Behörden. Die AG IS ist Austausch- und Beratungsgremium bei der Erarbeitung von landesweiten Richtlinien und Standards. Im Berichtszeitraum trafen sich die BfIS der Ressorts und die weiteren Teilnehmer der AG zu insgesamt sieben Sitzungen. Dabei wurde folgende landesweite Regelung bzw. technische Umsetzung beschlossen:

Link Reputation
Seit dem 1. November 2022 wurden die zentralen Schutzsysteme des SVN und KDN um die Funktion „Link Reputation" erweitert. Dadurch können sowohl in E-Mails eingebettete Links als auch Links in text-basierten Anhängen auf ihre Reputation geprüft werden. Besteht das Risiko, dass es sich um maliziöse Links handelt, werden die E-Mails mit einem Hinweis für den Empfänger versehen. Zusätzlich werden in E-Mails eingebettete Links, bei denen das Risiko besteht, dass diese auf schädliche Ziele leiten, technisch als „unklickbar" verändert.

Zudem befasste sich die AG IS mit verschiedenen landesweiten Richtlinien (siehe 6.1.2) und bildete Unterarbeitsgruppen zur fachlichen Erstellung.

3.2.2 Lenkungsausschuss IT- und E-Government

Die im Kapitel 6.1.2 genannten Richtlinien wurden gemäß § 5 Abs. 6 SächsISichG von BfIS Land in den LA ITEG als Beschlussvorlage eingereicht und durch das Gremium als ressortübergreifende Mindeststandards beschlossen. Darüber hinaus informierte BfIS Land in den jeweiligen Sitzungen zur allgemeinen Lage der Informationssicherheit und zu ausgewählten Sicherheitsereignissen.

3.3 Sensibilisierung und Fortbildung

Viele der im Kapitel 2.2. dargestellten Angriffsmethoden und -mittel benötigen für ihren Erfolg neben unsicheren Systemen immer auch die ungewollte Mitwirkung des Menschen als Nutzer der Informationstechnik. In diesem Bewusstsein konzentrieren sich Cyberkriminelle stark auf den Faktor Mensch und nicht nur auf technische Schwachstellen. Solange ein unbedachter Klick auf einen EMail- Anhang oder auch die Verwendung dienstlicher Passwörter für die private IT-Nutzung einen ITSicherheitsvorfall begünstigen kann, sind und bleiben Sensibilisierung und Schulung wesentliche Maßnahmen zur Erhöhung der Informationssicherheit. Dies gilt auch für die öffentliche Verwaltung.

Sowohl das SächsISichG als auch das IT-Grundschutz-Kompendium des BSI beschreiben, dass die Sensibilisierung der IT-Anwenderinnen und -Anwender eine elementar wichtige Sicherheitsmaßnahme für den täglichen Umgang mit IT-Systemen darstellt. Dies bedeutet zunächst, dass ein Problembewusstsein für die Bedrohungslage und die Risiken für die Informationssicherheit geschaffen werden muss. Darauf aufbauend ist es dann Ziel und Herausforderung zugleich, eine Verhaltensänderung hin zu einem sicheren Umgang mit IT zu erreichen. Da die wenigsten Verwaltungsmitarbeiterinnen und -mitarbeiter IT-Experten sind, kann das notwendige Wissen am besten über einfache Regeln und nachvollziehbare Sicherheitsmaßnahmen vermittelt werden.

3.3.1 E-Learning zur Informationssicherheit

Das E-Learning-Angebot zur Informationssicherheit am Arbeitsplatz, das seit nunmehr fast sechs Jahren zur Verfügung steht, konnte auch im Berichtszeitraum einen weiteren Anstieg der Teilnehmerzahlen verzeichnen, wenn auch nicht mehr ganz so stark wie im Vorjahr. Dies betrifft sowohl die Absolventinnen und Absolventen des verpflichtenden Teilnahmescheins als auch diejenigen, die den freiwilligen Online-Test zum Sächsischen Informationssicherheits-Schein (SISS) absolviert haben. Bis Ende Juli 2023 haben über 26.000 Nutzerinnen und Nutzer die Teilnahmebescheinigung erworben (bis Juli 2022 waren es über 20.000) und über 22.000 Nutzerinnen und Nutzer den Test zum SISS erfolgreich absolviert (bis Juli 2022 waren es über 18.000).

Betrachtet man die Verteilung der Teilnehmenden auf die Behörden im Freistaat, so weisen die Behörden der Staatsverwaltung gut 3.000 Teilnehmer mehr auf als die Kommunen. Bei den Absolventinnen und Absolventen des Online-Tests zeigt sich jedoch ein anderes Bild: Hier liegen die Kommunen leicht vorn. Dies ist in erster Linie auf die Landeshauptstadt Dresden zurückzuführen, die nach ausführlicher Vorbereitung das E-Learning zur Pflichtschulung für ihre Mitarbeiterinnen und Mitarbeiter erklärt hat und nun gut 8.000 der insgesamt knapp 10.000 Absolventen aus dem kommunalen Bereich beisteuert. Das Vorgehen bei der Einführung und Förderung von E-Learning in Dresden zeigt beispielhaft, wie es einer Kommune gelingen kann, die Informationssicherheit in der eigenen Verwaltung zu erhöhen, indem möglichst viele Mitarbeiterinnen und Mitarbeiter zu diesem Thema geschult werden. Auf staatlicher Seite hat sich im Berichtszeitraum das Justizressort ähnlich engagiert und über 7.500 Teilnehmerinnen und Teilnehmern und gut 4.000 Absolventinnen und Absolventen erreicht.

3.3.2 IT-Sicherheitstag Sachsen: Fortbildung und Vernetzung für IT-Fachkräfte

Am 28. Juni 2023 richtete BfIS Land in Zusammenarbeit mit dem Behördenspiegel den nunmehr vierten IT-Sicherheitstag Sachsen in Dresden aus. Unter dem Motto: „Informationssicherheit weiterentwickeln – Organisationen gestalten, Notfälle vordenken, Netzwerke schaffen" gab es dabei u.a. Fachforen zum Thema IT-Notfall-Übungen, zur Informationssicherheit in kleinen Organisationen und einen Workshop für Kommunen zu Cybersicherheitsübungen. Das Tagungsprogramm richtete sich dabei zuvorderst an IT-Sicherheitsbeauftragte und andere IT-Verantwortliche aus der Staatsverwaltung und den Kommunen. Mit gut 220 Anmeldenden verzeichnete die Tagung ein neues Allzeithoch an interessierten Fachkräften, v.a. aus dem öffentlichen Sektor.

Veranstaltung „IT Sicherheitstag Sachsen" im Deutschen Hygienemuseum in Dresden

3.4 Unterstützung für die Kommunen

Die Gewährleistung der Informationssicherheit stellt für die Kommunen nach wie vor eine besondere Herausforderung dar. So hat fast die Hälfte der sächsischen Kommunen, wie in Kapitel 6.4 beschrieben, trotz gesetzlicher Aufforderung keinen BfIS bestellt. Hier zeigt sich am deutlichsten ein Grundproblem: Ohne eine personelle und organisatorische Anbindung kann kein einheitliches und ausreichend hohes Niveau der Informationssicherheit dokumentiert werden und damit auch nicht vorhanden sein. Einige Kommunen sind hier schon relativ weit und haben zum Teil vorbildliche Initiativen vorzuweisen, die meisten verharren aber noch in einem unbefriedigenden Status.

Grundsätzlich ist in Deutschland jede Verwaltung für ihre Informationssicherheit selbst verantwortlich. Diese Eigenverantwortung der Kommunen beruht nicht zuletzt auf dem verfassungsrechtlichen Grundsatz der kommunalen Selbstverwaltung. Allerdings lässt das Kommunalverfassungsrecht den Kommunen keine unbegrenzte Gestaltungsfreiheit. Denn aus der Eigenverantwortung der Kommunen und ihrer Verpflichtung zur Erfüllung bestimmter öffentlicher Aufgaben ergeben sich auch kommunale Sorgfaltspflichten im Bereich der Informationssicherheit.

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

Der Freistaat Sachsen stellt den Kommunen deshalb zur Verbesserung ihrer Informationssicherheit im Rahmen seiner rechtlichen und finanziellen Möglichkeiten verschiedene Unterstützungen und Anreize zur Verfügung, die auf einer zentralen Webseite zum Thema „Informationssicherheit in Kommunen" dargestellt werden.[1] Hierzu zählen in erster Linie verschiedene technische Unterstützungsleistungen des SAX.CERT, wie in Kapitel 4 beschrieben. Aber auch BfIS Land unterstützt die Kommunen seit mehreren Jahren z.B. bei der Fortbildung von Informationssicherheitsexperten. So finanzierte BfIS Land im Zeitraum Oktober 2022 bis März 2023 die Durchführung von fünf mehrtägigen Fortbildungsveranstaltungen zum IT-Sicherheitsbeauftragten. An den Veranstaltungen, von denen drei online und zwei als Präsenzveranstaltungen in Chemnitz und Leipzig stattfanden, nahmen 59 Bedienstete aus 41 verschiedenen Kommunen teil. Fast alle schlossen die Fortbildung mit der Qualifizierung zum „IT-Grundschutz-Praktiker" nach den Prüfungskriterien des BSI ab.

Als neues Angebot für die Kommunen wird nach der erfolgreichen „Roadshow Kommunen" des BSI in Zusammenarbeit mit der SK (siehe Jahresbericht 2022) seit Oktober 2022 an jedem ersten Freitag im Monat eine Online-Sprechstunde von BfIS Land und SAX.CERT zu IT-Sicherheitsthemen für Kommunen angeboten, die dazu dient, aktuelle Themen der Informationssicherheit und die Dienstleistungen vom SAX.CERT näher zu erläutern sowie Fragen und Bedarfe der Kommunen aufzunehmen. Darüber hinaus soll die Sprechstunde den Verantwortlichen aus den Kommunen, die häufig als Einzelkämpfer in ihren jeweiligen Verwaltungen agieren, die Möglichkeit geben, sich untereinander zu vernetzen und ggf. von bereits vorhandenen Erfahrungen oder konkreten Hilfestellungen anderer zu profitieren. An den acht Sprechstunden im Berichtszeitraum nahmen durchschnittlich jeweils gut 30 Vertreterinnen und Vertreter der Kommunen teil.

3.5 Kooperationen mit dem BSI

Seit Beginn des Jahres 2023 befinden sich BfIS Land, federführend für den Freistaat Sachsen, und das BSI in Abstimmungen über eine Kooperationsvereinbarung zwischen beiden Seiten. Sie wird die im November 2018 geschlossene Absichtserklärung zur vertieften Zusammenarbeit ablösen. Die Vereinbarung basiert auf einer Liste möglicher Kooperationsfelder, die seitens des BSI vorgeschlagen und um landesspezifische Themen ergänzt wurden. Ziel ist es, die für Sachsen relevanten Themenfelder mit konkreten Kooperationsthemen zu identifizieren und mit hoher Verbindlichkeit festzulegen, um die Zusammenarbeit mit dem BSI auf eine noch breitere Basis zu stellen.

Auf Grundlage der bisherigen Absichtserklärung und der über Jahre gewachsenen guten Kontakte zum BSI konnten in der Vergangenheit bereits einige Projekte gemeinsam umgesetzt werden. So wurden in der Vergangenheit u. a. Hospitationen von CERT-Mitarbeitenden beim BSI, der Betrieb eines speziellen BSI-Schutzsystems im SVN und anlassbezogene Beratungsleistungen durch Expertinnen und Experten des BSI durchgeführt. Die erste Roadshow des BSI für Kommunen konnte nach Sachsen geholt werden. Vertreterinnen und Vertreter des BSI nehmen regelmäßig an Tagungen zu Themen der Informationssicherheit in Sachsen teil.

[1] https://www.egovernment.sachsen.de/informationssicherheit-in-den-kommunen-5657.html

4
SICHERHEITSANGEBOTE DES SAX.CERT

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

Das Sicherheitsnotfallteam SAX.CERT sitzt beim Sächsischen Staatsbetrieb Informatik Dienste in Radebeul

4.1 Schwachstellenwarndienst

Mit dem Schwachstellenwarndienst (Vulnerability Advisory Service „dCERT") stellt das SAX.CERT in Zusammenarbeit mit einem technischen Dienstleister tagesaktuelle Informationen zu Schwachstellen und Sicherheitslücken in IT-Systemen zur Verfügung. Über das SAX.CERT kann kostenfrei ein eigenes Nutzerkonto angelegt werden, mit dem sich der Kunde aus aktuell mehr als 2.000 Hard- und Softwareprodukten eine individuelle Zusammenstellung auswählen kann. Wird für eines der ausgewählten Produkte eine neue Sicherheitslücke bekannt, versendet das Portal automatisch eine Warn-E-Mail mit ausführlichen Details und Maßnahmenempfehlungen zu dieser Schwachstelle an den betreffenden Nutzer. Der Warndienst wurde Stand Juli 2023 von 280 Abonnenten im Freistaat Sachsen aktiv genutzt und damit von 46 Abonnenten mehr als im Vorjahreszeitraum.

4.2 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. Im Juli 2023 waren insgesamt 40 Sensoren (+8) im produktiven Einsatz. Ein verifiziertes Eindringen in IT-Systeme wurde durch das System nicht detektiert.

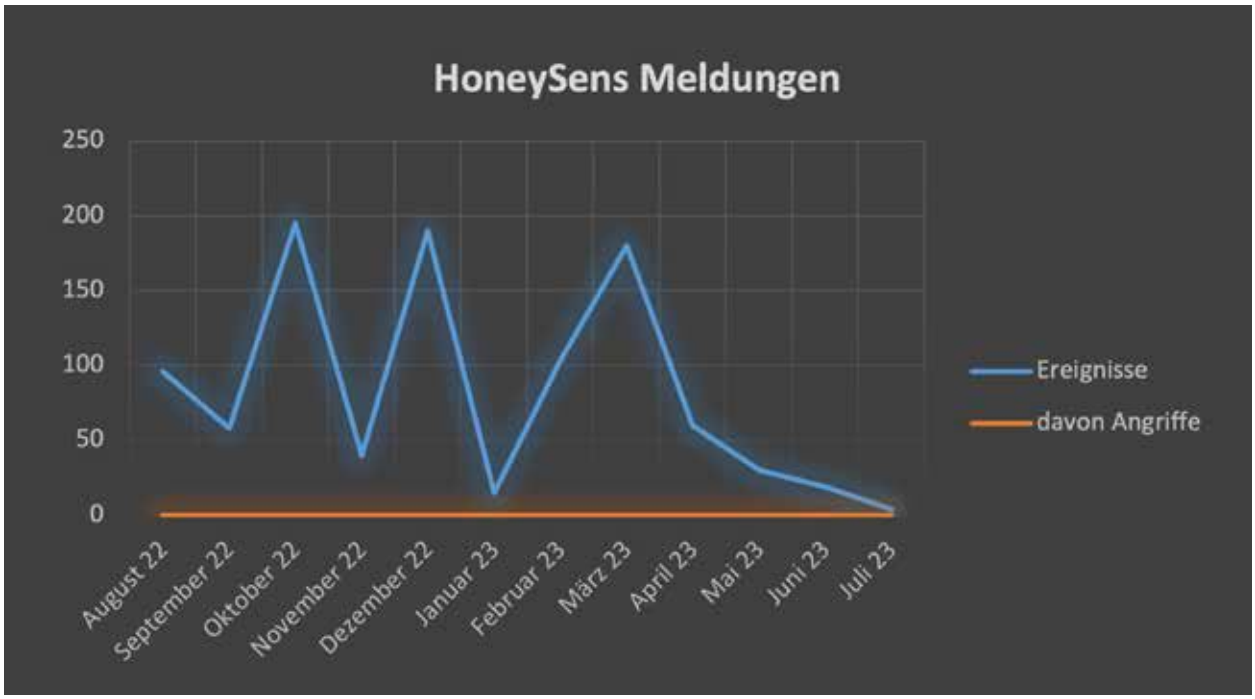


Abbildung 4:
Zugriffe auf den Sensor HoneySens

4.3 Identity Leak Checker

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet, z.B. bei Newsletterbetreibern, Online-Shops und Reisedienstleistern. Ein Großteil der gestohlenen Angaben wird anschließend in Darknet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen. Mit dem Identity Leak Checker bietet das SAX.CERT in Zusammenarbeit mit dem Hasso-Plattner-Institut einen individuellen Dienst zur Überprüfung von E-Mail-Adressen des Freistaates Sachsen auf die Betroffenheit derartiger Leaks an, mit dem alle Maildomains der Staatsverwaltung ständig überwacht werden. Auf Antrag können über das SAX.CERT weitere Mail-Domains in den Dienst aufgenommen werden, was im Berichtszeitraum von 35 Nutzern (+12 zum Vorjahr) außerhalb der Staatsverwaltung wahrgenommen wurde.

4.4 Sicherheitsprüfung Webseiten

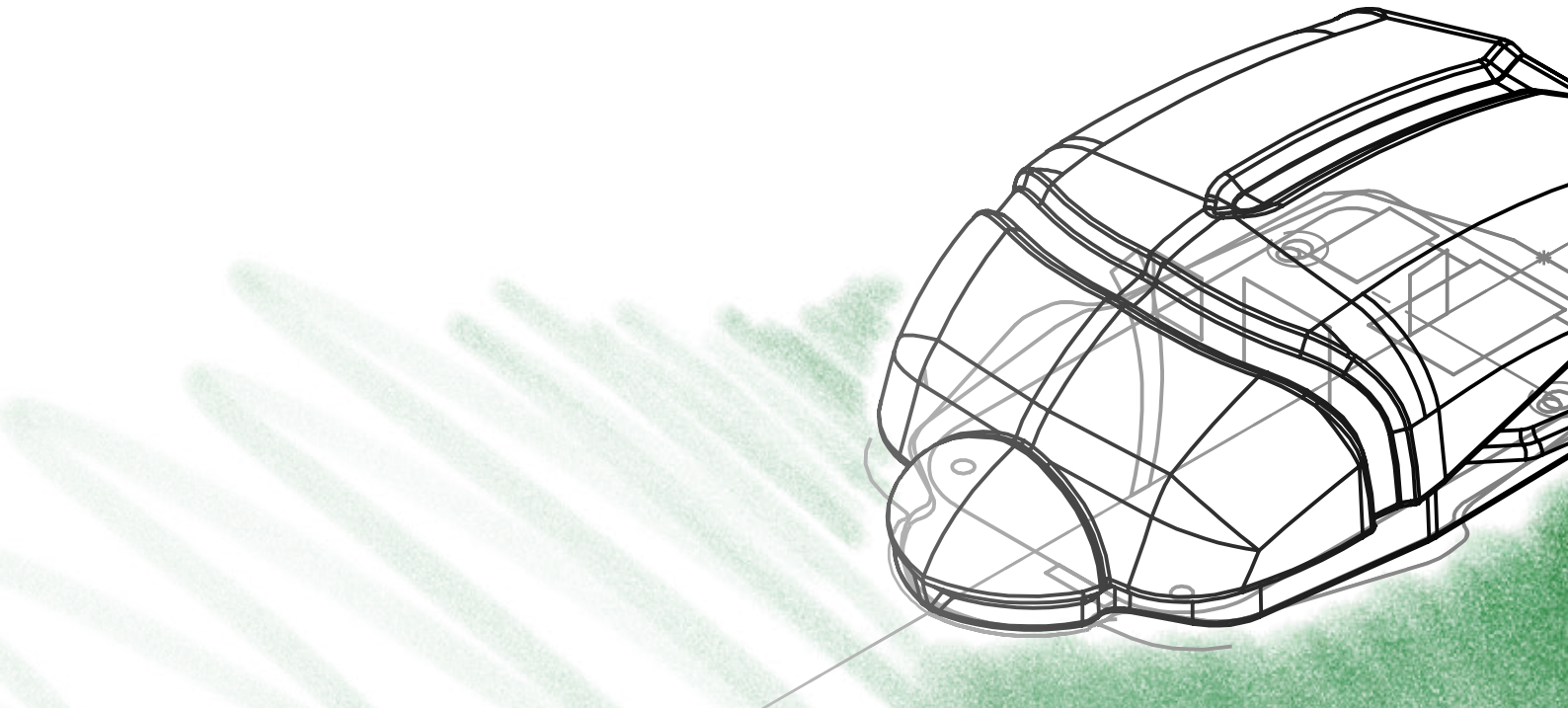
Auf Grundlage des AK ITEG Beschlusses „Automatische Scandienste und Erhöhung der Webseitensicherheit" werden bereits seit 2017 regelmäßig mittlerweile gut 7.400 Internetseiten der Staats- und Kommunalverwaltung durch das SAX.CERT auf veraltete Software und bekannte Schwachstellen getestet (Vorjahreszeitraum: 7.200). 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.

4.5 Passwort-Checker

Als Sensibilisierung für die Mitarbeiterinnen und Mitarbeiter der Staatsverwaltung bietet das SAX.CERT 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.

4.6 Sprechstunde „Kommunen"

Nach der erfolgreichen „Roadshow Kommunen" des BSI in Zusammenarbeit mit der SK wird seit Oktober 2022 monatlich eine Online-Sprechstunde des SAX.CERT zu Themen der IT-Sicherheit für die Kommunen angeboten. Die Sprechstunde soll dazu dienen, aktuelle Themen und Services des SAX.CERT genauer zu erläutern und Fragen und Bedarfe aus den Kommunen aufzunehmen.



5
BERICHT
Ergriffene Maßnahmen laut SächsISichG

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

5.1 Berichtspflichten nach § 5 Absatz 8

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

Der deutliche Anstieg der Wiederherstellung des Personenbezugs bei Protokolldaten ist darauf zurückzuführen, dass im Berichtszeitraum eine größere Anzahl von technischen Systemen in die automatisierte Überwachung von sicherheitsrelevanten Ereignissen eingebunden wurde.

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	365	0	1
Anzahl von Fällen der Speicherung und der Auswertung von Inhaltsdaten und Wiederherstellung des Personenbezugs pseudonymisierter Daten gemäß § 13 Absatz 3	0	0	1
Anzahl von Fällen der nicht automatisierten Verarbeitung von Daten gemäß § 13 Absatz 4	0	1	1
Anzahl der durchgeführten, unterbliebenen sowie nachgeholten Benachrichtigungen gemäß § 13 Absatz 5	0	1	1
Anzahl von Fällen der Übermittlung von Daten gemäß § 13 Absatz 6 und 7	0	0	0
Umgang mit unzulässig erlangten Daten, die den Kernbereich privater Lebensgestaltung betreffen, gemäß § 13 Absatz 8	0	0	0
Anzahl von gemäß §§ 15 bis 17 gemeldeten Sicherheitsereignissen und Sicherheitsvorfällen	0	51	14

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

5.2 Maßnahmen des SAX.CERT gemäß § 6 Absatz 3

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

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

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

Das SAX.CERT hat im Berichtszeitraum in 5.996 Fällen personenbezogene Daten gemäß § 6 Absatz 4 SächsISichG verarbeitet. Das bedeutet einen Rückgang um 3.198 Fälle (- 35%) 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 Staatsverwaltung sowie für Lageberichte verwendet.

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

5.4 Maßnahmen zur Gefahrenabwehr nach §§ 12 und 13

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

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

Daneben ist seit Januar 2021 ein sogenanntes Security Information and Event Management (SIEM) für das SVN im Einsatz, welches vom SAX.CERT betreut wird. Das operative Vorgehen sieht vor, dass der SIEM-Dienst die Log-Daten aus angebundenen kritischen Netzsegmenten überwacht, verschiedene Ereignisse miteinander korreliert und nach konfigurierten Regeln Alarme auslöst. Die konfigurierten Regeln werden als „Use Cases" (deutsch: Anwendungsfall) bezeichnet. Ein klassischer „Use Case" könnte z. B. ein „Brute Force"-Angriff auf einen Server mithilfe eines Admin-Accounts sein.

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

5.5 Sicherheitsmeldungen gemäß §§ 16 und 17

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

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

Beispiele für derartige Sicherheitsvorfälle sind:

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

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 65 Sicherheitsereignisse gemeldet (51 von den staatlichen Behörden, 14 von den nicht-staatlichen Behörden). Das ist ein Anstieg von einer Meldung zum Vorjahreszeitraum. Die Meldungen für sich genommen lassen keine Rückschlüsse auf eine gestiegene Gefährdungslage durch spezielle Angriffsarten o.ä. erkennen.

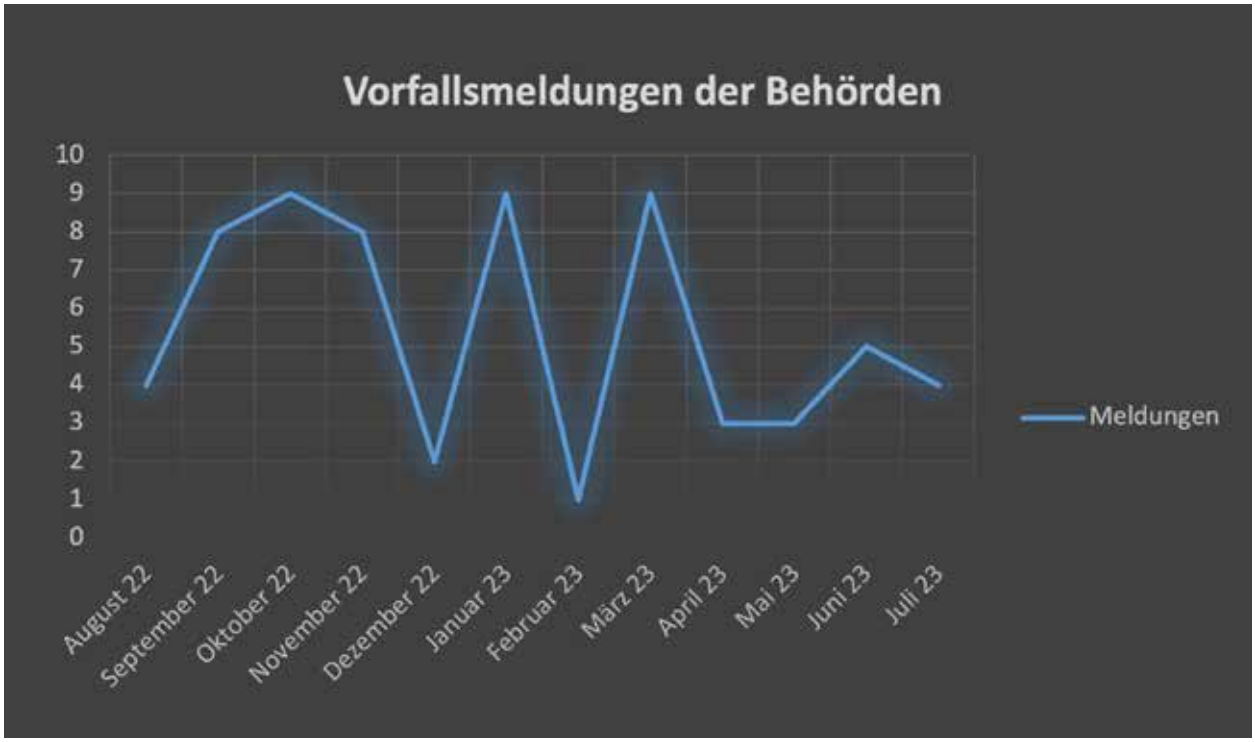


Abbildung 5:
Gemeldete Vorfälle durch Staats- und Kommunalbehörden

6
UMSETZUNGSSTAND SächsISichG

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

6.1 Informationssicherheitsmanagementsystem

§ 5 Absatz 5 SächsISichG verpflichtet den BfIS Land zur Erstellung eines ISMS für die Sächsische Staatsverwaltung. Zur Implementierung und Aufrechterhaltung eines landesweiten ISMS im Freistaat Sachsen wurde ein Rahmendokument zum übergreifenden ISMS Land geschaffen. Im Rahmendokument sind die Strategien und Maßnahmen beschrieben, die der Gewährleistung der Informationssicherheit im Freistaat Sachsen dienen. Ein wesentliches Steuerungsinstrument sind dabei landesweit geltende Richtlinien. Diese Richtlinien werden ausgehend vom BfIS Land in der AG IS erarbeitet, um anschließend, nach Beschlussfassung im LA ITEG, verbindliche Wirkung in den Behörden der Staatsverwaltung zu entfalten. Zusätzlich werden die Richtlinien durch nachgelagerte Konzepte und Dokumente ergänzt, die konkrete Vorschläge zur Umsetzung der in den Richtlinien beschriebenen Vorgaben enthalten.

6.1.1 Leitlinie zur Informationssicherheit

Eine wesentliche Grundlage für die Ausgestaltung des Sicherheitsprozesses ist die Leitlinie zur Informationssicherheit. Sie beschreibt, welche Sicherheitsziele und welches Sicherheitsniveau die Institution anstrebt und mit welchen Maßnahmen bzw. mit welchen Strukturen dies erreicht werden soll. Die Fassung der Leitlinie als Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen entspricht dem Stellenwert der Informationssicherheit im Freistaat Sachsen. Das SächsISichG bildet das übergeordnete strategische Basisdokument zur Sicherstellung der Informationssicherheit und dient der Einrichtung, Aufrechterhaltung und Weiterentwicklung des landesweiten ISMS sowie der ISMS in den Ressorts.

Zudem sind die Anforderungen aus der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-PLR (Leitlinie IT-PLR) umzusetzen. Die Leitlinie IT-PLR beschreibt das Vorgehen bei der Etablierung eines einheitlichen und einvernehmlichen Mindestsicherheitsniveaus unter Berücksichtigung des Grundsatzes der Wirtschaftlichkeit. Um die Ziele der Leitlinie IT-PLR zu erreichen, entwickelte die Arbeitsgruppe Informationssicherheit des IT-Planungsrates (AG InfoSic) einen Umsetzungsplan, der die Sicherheitsziele konkretisiert und die Umsetzung der Sicherheitsmaßnahmen mittels Kennzahlen messbar macht.

6.1.2 Organisation der Informationssicherheit

Zur Planung und Durchsetzung des Informationssicherheitsprozesses ist die Definition von Rollen und Aufgaben erforderlich. Diese sind wesentlich für die Verzahnung des übergreifenden Informationssicherheitsprozesses des ISMS Land und der ISMS der Ressorts und damit für das Funktionieren der Managementsysteme. Die jeweiligen Aufgaben sind im Rahmendokument zum übergreifenden ISMS beschrieben.

Der landesweite Informationssicherheitsprozess hat zum Ziel, ein ressortübergreifendes ISMS zu etablieren, aufrechtzuhalten und bereits bestehende ISMS der Ressorts in das ISMS Land zu integrieren. Dafür werden die Teilprozesse Dokumentenmanagement, Aufrechterhaltung und Verbesserung, Kompetenzmanagement und Incident Management benötigt. Übergreifende Leitlinien, Richtlinien und Konzepte legen die Rahmenbedingungen bzw. Mindestanforderungen für diese Teilprozesse fest:

Darüber hinaus wurden und werden nach Bedarf und in Abstimmung mit der AG IS weitere landesweite Leitlinien, Richtlinien (sog. Mindeststandards) und Konzepte zur Gewährleistung und Verbesserung der Informationssicherheit durch BfIS Land entwickelt. Dazu gehörten im Berichtszeitraum die:

- Richtlinie zur Authentifizierung im Nutzerkonto,
- Richtlinie zur sicheren Grundkonfiguration mobiler Endgeräte,
- Richtlinie zur Löschung und Vernichtung von Daten.

Teilprozess	Leitlinien, Richtlinien, Konzepte
Dokumentenmanagement	- Richtlinie zur ISMS-Dokumentation (in Anhörung) - Richtlinie zum ISMS-Berichtswesen (ausstehend)
Aufrechterhaltung und Verbesserung	- Richtlinie zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen (ausstehend) - Richtlinie zur internen ISMS-Auditierung (ausstehend)
Kompetenzmanagement	- Richtlinie zur Schulung und Sensibilisierung (in Anhörung) - Schulungs- und Sensibilisierungskonzept (im Entwurf)
Incident Management	- Leitlinie zum IT-Notfallmanagement (freigegeben) - Richtlinie zur Behandlung von Sicherheitsvorfällen (in Erstellung) - Richtlinie zum IT-Notfallstab Land (im Entwurf) - Übergreifendes IT-Notfallkonzept (in Erstellung)
Sicherheitskonzept	- Richtlinie zur Definition von Schutzbedarfskategorien (freigegeben) - Richtlinie zur Durchführung von Risikoanalysen (in Anhörung)

Tabelle 2: Leitlinien, Richtlinien, Konzepte des ISMS Land (Umsetzungsstand in Klammern)

6.1.3 Sicherheitskonzept

Das landesweite Sicherheitskonzept zur Informationssicherheit ergibt sich aus den Sicherheitskonzepten der Ressorts und den übergreifenden Richtlinien des ISMS Land, welche die Mindeststandards in Bezug auf die Umsetzung der ISMS in den Ressorts vorgeben, um ein angemessenes Sicherheitsniveau innerhalb der Ressorts zu gewährleisten.

Sicherheitskonzepte sind neben der Organisation der Informationssicherheit ein weiteres Hilfsmittel, um die Sicherheitsstrategie umzusetzen und die Sicherheitsziele zu erreichen. Die Inhalte der Richtlinien bilden dabei den Rahmen für die Maßnahmen in den Sicherheitskonzepten, der staatlichen Stellen nach § 7 Abs. 1 SächsISichG und der nachgeordneten Behörden. Die Prüfung der Sicherheitskonzepte, sowohl auf Angemessenheit und Wirksamkeit der Maßnahmen als auch hinsichtlich der Umsetzung der Maßnahmen, erfolgt im Rahmen interner Audits. Der BfIS Land hat bzgl. aller durchgeführten Audits/Revisionen ein Informationsrecht und überwacht die Umsetzung der Anforderungen an die Informationssicherheit.

6.2 Beauftragter für Informationssicherheit des Landes

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

- beratende Unterstützung der staatlichen BfIS (§ 5 Absatz 1 Satz 2 und Satz 3 SächsISichG)

- Maßnahmenanordnung zur Gefahrenabwehr (§ 5 Absatz 3 und Absatz 4 SächsISichG)

- Festlegung von verbindlichen Mindeststandards (§ 5 Absatz 6 SächsISichG)

- Durchführung von Revisionen (§ 5 Absatz 7 Satz 2 SächsISichG).

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

Im Referat 45 der SK, dem BfIS Land als Referatsleiter vorsteht, sind neben dem in diesem Bericht adressierten Themenbereich Informationssicherheit auch die Themengebiete Cybersicherheit und KRITIS angesiedelt. Hierunter fällt u. a. die Koordinierung von Cybersicherheitsthemen im Austausch mit weiteren staatlichen Akteuren wie dem Cybercrime Competence Center Sachsen des Landeskriminalamtes Sachsen, dem Landesamt für Verfassungsschutz, der Zentralstelle Cybercrime der Generalstaatsanwaltschaft Dresden und der Abteilung Katastrophenschutz im Staatsministerium des Innern.

2022 hatte Sachsen den Vorsitz der AG Infosic des IT-Planungsrats inne. BfIS Land koordinierte somit in 2022 zusätzlich die verschiedenen Aktivitäten der Mitglieder der AG Infosic, übte die Berichtspflicht an den IT-Planungsrat aus und nahm dessen Aufträge zur Informationssicherheit in der Bund-Länder-Zusammenarbeit entgegen. Sachsen war damit auch Mitveranstalter der Jahrestagung der Informationssicherheitsbeauftragten von Ländern und Kommunen am 24. und 25. Oktober 2022 in Nürnberg. Zum Jahreswechsel 2022/ 2023 übergab BfIS Land den Vorsitz der AG Infosic an das Saarland.

Um die wachsende Aufgabenlast zu bewältigen, wurden BfIS Land im Doppelhaushalt 2023/ 2024 weitere Stellen zugeführt. Damit konnte insbesondere der Teilbereich IT-Notfallmanagement personell untersetzt und fachlich stark aufgestellt werden.

6.3 Beauftragte für Informationssicherheit in den staatlichen Stellen

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 mögliche Einsichtnahme in sensible Protokolldaten zur Erkennung und Begrenzung von sicherheitsrelevanten Ereignissen erfordert eine organisatorisch unabhängige Ausgestaltung der BfIS-Rolle.

Bereits seit der ersten Leitlinie Informationssicherheit des IT-Planungsrates aus dem Jahr 2013 besteht für die Staatsverwaltung 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 Absatz 1 SächsISichG genannten insgesamt 15 Staatsbehörden einen hauptamtlichen BfIS zu bestellen. Die Umsetzung hatte bis zum 31. Dezember 2020 im Rahmen der zur Verfügung stehenden Haushaltsmittel zu erfolgen (§ 20 SächsISichG). Im Berichtszeitraum war es einem Ministerium nicht gelungen, die offene Stelle zu besetzen. Dies erfolgte allerdings unmittelbar darauf am 1. August 2023. Damit erfüllen nun alle der in § 7 Absatz 1 SächsISichG genannten Staatsbehörden diese gesetzliche Anforderung.

Im nachgeordneten Bereich haben im Berichtszeitraum ca. 70 % der Behörden und Einrichtungen offiziell einen BfIS bestellt. Bei den verbleibenden 30 % wurden aber, mit einer Ausnahme, zumindest Bedienstete benannt, die als Schnittstelle für die Belange der Informationssicherheit in die jeweilige staatliche Stelle hinein dienen. Diese decken dann jedoch nicht den kompletten Umfang aller BfIS-Aufgaben ab.

6.4 Beauftragte für Informationssicherheit in den nicht-staatlichen Stellen

Nach Maßgabe des § 8 SächsISichG sollen alle nicht-staatlichen Stellen einen BfIS und einen Stellvertreter ernennen. Über die Ernennung des BfIS und seines Vertreters ist der BfIS Land innerhalb eines Monats zu unterrichten. Allerdings erfolgte die Meldung durch die sächsischen Kommunen auch im aktuellen Berichtszeitraum weiterhin zögerlich. Stand 31. Juli 2023 waren zwar für alle Landkreise, aber nur für 218 (Vorjahr: 212) der 418 (Vorjahr: 419) Kommunen BfIS gemeldet, was etwa 52 % aller Gemeinden in Sachsen entspricht. Die Einwohnerzahl der Kommunen mit einem BfIS entspricht mit 3,1 Millionen allerdings ungefähr Dreiviertel der sächsischen Bevölkerung. Es sind also insbesondere die kleineren Kommunen, die ihrer gesetzlichen Verpflichtung bislang nicht nachgekommen sind.

Die BfIS der Landkreise kommen regelmäßig zum Austausch zusammen und binden BfIS Land dazu ein.

6.5 Sicherheitsnotfallteam SAX.CERT

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

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

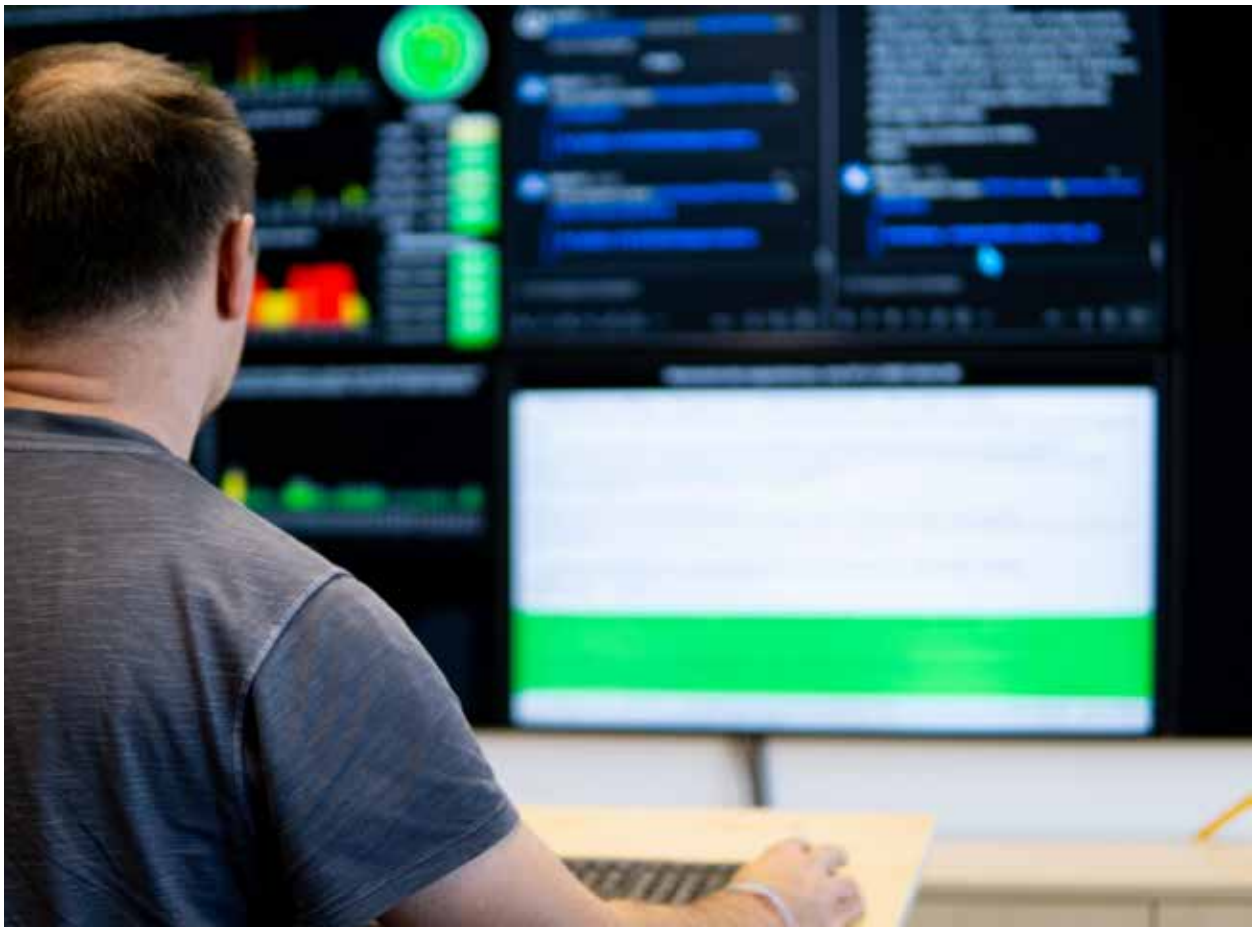
Wie in den Kapiteln 4 und 5 beschrieben, hat das SAX.CERT seine gesetzlichen Aufgaben zu den oben genannten Aufgaben 1 bis 4 sowie 7 und 8 erfüllt. Neu war im Berichtszeitraum die Einführung spezifischer monatlicher Lageberichte zur Informationssicherheit für die Landesbehörden einerseits und die Kommunen andererseits. Nun erhalten beide Ebenen Lageberichte mit auf sie zugeschnittenen Zahlen und Informationen. Der Verteilerkreis der Lageberichte konnte so um ein Vielfaches erweitert werden.

Zu 5: Das SAX.CERT ist weiterhin die zentrale KRITIS-Anlaufstelle für den Freistaat Sachsen, die gemäß § 8b Abs. 2 BSI-Gesetz vom BSI über versuchte oder erfolgte Angriffe auf die Sicherheit der Informationstechnik von Betreibern kritischer Infrastrukturen informiert wird. Zu Beginn des Jahres 2023 wurde auf Grundlage des zwischen den Ländern und dem Bund abgestimmten neuen Meldeprozesses (siehe Jahresbericht 2022) mit den Fachaufsichten der KRITIS-Sektoren und -Branchen in den zuständigen Ressorts ein neuer Meldeprozess eingeführt, in den auch das Lagezentrum des SMI eingebunden ist, um außerhalb der Büroarbeitszeiten der Verwaltung erweitert reagieren zu können. Seit Jahresbeginn wurden jedoch keine für Sachsen relevanten Sicherheitsvorfälle bei Betreibern kritischer Infrastrukturen durch das BSI gemeldet.

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

Erkenntnisreich war die Hospitation von zwei Bediensteten im CERT des Bayerischen Landesamts für Sicherheit in der Informationstechnik im Juli 2023. Für die dem SAX.CERT im Haushaltsjahr 2023 neu zugewiesenen Stellen konnten im Berichtszeitraum anteilig Besetzungsverfahren erfolgreich durchgeführt werden.

Die Stellenbesetzung selbst fällt allerdings erst in den nächsten Berichtszeitraum. Aus europäischer Rechtsetzung (siehe 7.2) wird das SAX.CERT weitere Aufgaben erhalten, die ab Oktober 2024 zu erfüllen sind und einen weiteren personellen Ausbau erfordern werden.



Sicherheitsüberwachung im SAX.CERT

7
WEITERE VERPFLICHTUNGEN FÜR DIE INFORMATIONSSICHERHEIT DER VERWALTUNG

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

7.1 Verpflichtungen aus der Leitlinie Informationssicherheit des IT-Planungsrates

Anfang 2019 verabschiedete der IT-Planungsrat die überarbeitete Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung. Die aktualisierte Fassung konkretisiert die Sicherheitsziele und die dazu umzusetzenden notwendigen Maßnahmen. Der Umsetzungsplan zur Leitlinie schreibt die stufenweise Umsetzung der Vorgaben bis 2025 fest. Ein jährliches Berichtswesen mit 26 Kennzahlen bietet einen Überblick zum Umsetzungsfortschritt. Mit Inkrafttreten der Leitlinie IT-Notfallmanagement (siehe 6.1) konnte mit der Umsetzung der Maßnahmen zum ITNotfallmanagement in Sachsen begonnen werden. Zudem wird die Umsetzung des vom ITPlanungsrat beschlossenen CERT-Mindeststandards in Sachsen vorangetrieben.

Für 2022 waren im Umsetzungsplan außerdem die flächendeckende Erstellung der Sicherheitskonzepte für geschäftskritische oder für OZG-Verfahren (40% erfüllt), die Einhaltung der Anschlussbedingungen an das Verbindungsnetz in Bund und Ländern (erfüllt) sowie die Weiterentwicklung der Zusammenarbeit der CERTs im Verwaltungs-CERT-Verbund durch Hospitation (erfüllt) als Ziele vorgegeben.

Als Zielvorgaben für 2023 sind die Etablierung zielgruppenbezogener Konzepte im Bereich Schulung und Sensibilisierung, die Anwendung des IT-Grundschutzes auf Ebenen übergreifende ITVerfahren, die Erstellung IT-bezogener Notfallkonzepte inkl. der Etablierung von Schnittstellen zum Krisen- und Katastrophenschutz sowie die Durchführung von IT-Notfallübungen vorgesehen.

Parallel dazu wird jährlich die Fortbildung der BfIS und die Durchführung von Sensibilisierungsveranstaltungen für die Beschäftigten durch den IT-Planungsrat gefördert. Auf der anderen Seite gibt es Handlungsfelder, in denen die meisten Bundesländer noch einen Nachholbedarf haben, z. B. beim IT-Notfallmanagement.

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

7.2 Verpflichtungen aus europäischer Rechtsetzung

Die weltweit steigende Anzahl von Cyber-Angriffen, besonders auf Kritische Infrastrukturen, hat zur Einführung der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, der so genannten NIS2-Richtlinie, durch die EU geführt, die bis Oktober 2024 in den Mitgliedstaaten in nationales Recht umgesetzt sein muss. Sie soll ein einheitliches ITSicherheitsniveau für KRITIS-Betreiber in den Mitgliedstaaten etablieren und erweitert unter anderem den Geltungsbereich der bisherigen NIS-Richtlinie. Wesentliche Neuerung ist die Einbeziehung der öffentlichen Verwaltung auf Ebene der Bundesverwaltung und der Landesverwaltungen in den Anwendungsbereich. Im Gegensatz zur Bundesebene müssen die von der NIS2-Richtlinie umfassten Einrichtungen auf Landesebene erst noch nach einem risikobasierten Ansatz erfasst, also identifiziert, werden.

Mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) wird die europäische NIS2-Richtlinie auf Bundesebene umgesetzt. Durch Änderung des bestehenden SächsISichG erfolgt dies auf Landesebene. Sachsen ist mit dem SächsISichG grundsätzlich gut aufgestellt und erfüllt viele Anforderungen der EU-Richtlinie bereits jetzt. Allerdings wird insbesondere die Behandlung von IT-Sicherheitsvorfällen weiter professionalisiert, sowohl durch genauere Anforderungen an das SAX.CERT als auch durch eine verbindliche Meldeverordnung, die das Gesetz ergänzen wird. Vor dem Hintergrund der globalen Veränderungen in der Sicherheits- und Bedrohungslage sollen das Gesetz und die Verordnung weiterhin für alle Einrichtungen der Landesverwaltung Gültigkeit erhalten, um die bisherige Strategie eines ganzheitlichen Sicherheitsniveaus für die Behörden im Freistaat Sachsen weiter zu verfolgen.

8
ABBILDUNGS- UND TABELLENVERZEICHNIS

9
GLOSSAR

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

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

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

Command-and-Control-Server (C&C-Server)
Server-Infrastruktur, mit der Angreifer die in ein Bot-Netz 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.

Indicators of Compromise (IoC)
Indicators of Compromise (IoC, oder im Deutschen auch „Kompromittierungsindikatoren" genannt) sind die digitalen Spuren, die mit hoher Wahrscheinlichkeit auf einen unberechtigten Zugriff auf einen Computer hinweisen.

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.

Mobil Device Management
Zu Deutsch: Mobilgeräteverwaltung, steht für die zentralisierte Verwaltung aller möglichen Arten von Mobilgeräten durch dafür zuständige Administratoren mit Hilfe von Software und Hardware.

Mobil Incident Response Team
Zu Deutsch: Mobiles Vorfallsreaktionsteam, steht für ein Team, welches bei einem Sicherheitsvorfall vor Ort die betroffene Einrichtung bei der Bearbeitung des Vorfalls unterstützt.

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.

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

Social Engineering
Bei Cyberangriffen 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 Cyberkriminalität 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 werden für Phishing-Angriffe genutzt.

Wiper
Wiper ist eine Schadsoftware, die Dateien, Backup-Systeme und Bootsektoren der Betriebssysteme unwiederbringlich zerstört, um maximalen Schaden anzurichten.

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).

Verteilerhinweis

Diese Informationsschrift wird von der Sächsischen Staatsregierung im Rahmen ihrer verfassungsmäßigen Verpflichtung zur Information der Öffentlichkeit herausgegeben. Sie darf weder von Parteien noch von deren Kandidaten oder Helfern im Zeitraum von sechs Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung.

Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme des Herausgebers zu Gunsten einzelner politischer Gruppen verstanden werden könnte. Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist. Erlaubt ist jedoch den Parteien, diese Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.

Herausgeber:
Sächsische Staatskanzlei

Redaktion:
Referat 45: Informations- und Cybersicherheit, Kritische Infrastrukturen

Gestaltung und Satz:
TORUX, Dresden

Druck:
Druckerei WIRmachenDRUCK GmbH

Redaktionsschluss:
Oktober 2023

Bezug: Diese Druckschrift kann kostenfrei bezogen werden bei:
Zentraler Broschürenversand
der Sächsischen Staatsregierung
Adresse: Hammerweg 30, 01127 Dresden
Telefon: +49 351 210367172
Telefax: +49 351 2103681
E-Mail: publikationen@sachsen.de
Internet: www.publikationen.sachsen.de