Informationssicherheit in Kommunalverwaltungen

34

Bei den Kommunen und Zweckverbänden bestehen insbesondere hinsichtlich der Ernennung von Beauftragten für die Informationssicherheit und der Aufstellung von Sicherheitskonzepten erhebliche Defizite bei der Umsetzung des Sächsischen Informationssicherheitsgesetzes.

Regelungen für den IT-Notfall bestanden nur in jeder zweiten befragten Kommune. Teilweise fehlten einfache Schutzmaßnahmen.

Die Warnungen und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik hinsichtlich der Verwendung einer russischen Virenschutzsoftware wurden teilweise nicht beachtet.

1 Hintergrund und Gegenstand der Prüfung

1 „Schlecht gesichert - Nach dem Hack auf eine Verwaltung stehen private Daten von Bürgerinnen, Mitarbeitern und Geflüchteten online"[1], „Hackerangriff auf Stadtverwaltung [...]: Systemausfall"[2], „Cyberattacke: Etliche Schulen im [...] betroffen - Hacker fordern Lösegeld"[3], „Hacker verschickt 200.000 Spam-Mails vom Landratsamt"[4], „Wenn ein Hacker einen ganzen Landkreis lahmlegt"[5], „75 Schulen fehlt Zugriff auf Daten"[6], „Cyberangriff auf [...] ein Jahr danach immer noch spürbar"[7].

2 Diese Schlagzeilen zeigen, dass mit der zunehmenden Digitalisierung der Kommunalverwaltung zugleich die Möglichkeiten für Angriffe auf die Informationstechnik wachsen. Datensicherheit muss auch bei fortschreitender Digitalisierung der Kommunalverwaltungen gewährleistet sein. Unberechtigte Datenabflüsse können das Recht auf informationelle Selbstbestimmung gefährden und schwächen das Vertrauen von Bürgern und Unternehmen in die öffentliche Verwaltung.

3 Informationssicherheit ist auf die Sicherheit der gesamten IT-Infrastruktur unter dem Gesichtspunkt der bedarfsabhängigen und zugriffssicheren Verfügbarkeit, Vertraulichkeit und Integrität aller Daten gerichtet und umfasst auch die Möglichkeiten zu deren Wiederherstellung im Notfall. Die Gewährleistung der Informationssicherheit erfordert einen umfassenden Ansatz, der es ermöglicht, technische und organisatorische Maßnahmen innerhalb eines bestehenden Rechtsrahmens zu verbinden.

4 Die Kommunen unterliegen nach § 2 Abs. 1 Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (Sächsisches Informationssicherheitsgesetz - SächsISichG) vom 2. August 2019 als nichtstaatliche Stellen dem Geltungsbereich des Gesetzes. Gemäß § 4 Abs. 2 Satz 1 i. V. m. Abs. 1 Satz 1 bis 3 SächsISichG treffen sie angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zur Gewährleistung der Informationssicherheit. Für technische Maßnahmen soll der Stand der Technik maßgeblich sein. Die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden den Kommunen nach § 4 Abs. 2 Satz 2 SächsISichG zur Anwendung empfohlen.

5 Prüfungsgegenstand war die Gewährleistung der Informationssicherheit, insbesondere nach Maßgabe des SächsISichG. Hierzu führten die StRPrÄ begleitend zu den Turnusprüfungen im Zeitraum von Oktober 2022 bis April 2023 auf Grundlage eines strukturierten Fragebogens örtliche Erhebungen durch. Insgesamt wurden die Ergebnisse von 52 Körperschaften berücksichtigt (47 kreisangehörige Kommunen und 5 Zweckverbände).

[1] ZEIT ONLINE vom 15. November 2022, zuletzt geöffnet am 24. Oktober 2023.
[2] ZEIT ONLINE vom 24. Februar 2023, zuletzt geöffnet am 24. Oktober 2023.
[3] Merkur.de vom 25. Oktober 2022, zuletzt geöffnet am 24. Oktober 2023.
[4] csoonline.com vom 22. Februar 2023, zuletzt geöffnet am 24. Oktober 2023.
[5] Süddeutsche Zeitung vom 23. November 2022, zuletzt geöffnet am 24. Oktober 2023.
[6] Bayerischer Rundfunk vom 24. Oktober 2022, zuletzt geöffnet am 24. Oktober 2023.
[7] MDR.DE vom 6. Juli 2022, zuletzt geöffnet am 24. Oktober 2023.

2 Prüfungsergebnisse

2.1 Beauftragte/r für die Informationssicherheit

6 Fast jede dritte geprüfte Kommune (15 von 47) und einer von 5 Zweckverbänden hatten keine/n Beauftragte/n für die Informationssicherheit (BfIS) und keinen Vertreter ernannt. Für die Beauftragten in 32 Kommunen wurden überwiegend keine Vertreter ernannt (21 Kommunen). Die Aufgaben des BfIS übertrugen die geprüften Kommunen teilweise auf Externe bzw. erfüllten die Aufgaben im Rahmen der interkommunalen Zusammenarbeit.

7 Gemäß § 8 Abs. 1 SächsISichG sollen für die Kommunen als nichtstaatliche Stellen ein BfIS und ein Vertreter ernannt werden. Sie müssen nicht Beschäftigte der Kommune sein und können ihre Tätigkeit für mehrere Kommunen ausüben. Insoweit bestehen flexible Rahmenregelungen, die den Kommunen eigene Handlungsspielräume eröffnen.

8 Gemäß § 4 Abs. 3 SächsISichG trägt der Leiter (der Kommunalverwaltung) die Verantwortung für die Informationssicherheit im Sinne des § 4 Abs. 1 SächsISichG. Er stellt die erforderlichen personellen und finanziellen Ressourcen zur Verfügung. Ihm obliegt die Ernennung des BfIS und des Vertreters.

9 Für die Aufgaben des BfIS in Kommunen gelten gem. § 8 Abs. 2 SächsISichG die Regelungen für die Beauftragten der staatlichen Stellen nach § 7 Abs. 3 SächsISichG. Seine Hauptaufgabe besteht darin, den zuständigen Leiter bei der Aufgabenwahrnehmung hinsichtlich der Informationssicherheit zu beraten und bei der Umsetzung zu unterstützen. Die Aufgaben des BfIS sind im Einzelnen in den Standards des BSI beschrieben und umfassen u. a.:

- die Steuerung des Informationssicherheitsprozesses und die Mitwirkung an allen damit zusammenhängenden Aufgaben,
- die Unterstützung der Leitung der Kommunalverwaltung bei der Erstellung einer Leitlinie,
- die Initiierung und Überprüfung von Sicherheitsmaßnahmen,
- die Koordinierung und Initiierung von sicherheitsrelevanten Projekten und Schulungen,
- die Untersuchung und Meldung von Sicherheitsvorfällen an das CERT (Computer Emergency Response Team) entsprechend den Meldepflichten für nichtstaatliche Stellen nach §§ 15, 17 SächsISichG.[8]

10 **Im Interesse der Gewährleistung der hinreichenden Informationssicherheit haben die Kommunen und Zweckverbände im Regelfall – soweit die Ausnahme rechtfertigende Gründe nicht vorliegen – BfIS und einen Vertreter zu ernennen. Auf die unter Wirtschaftlichkeitsgesichtspunkten positiv zu bewertende Möglichkeit der Beauftragung Externer wird verwiesen.**

2.2 Organisatorische Regelungen

2.2.1 Leitlinien und weitere dienstliche Regelungen

11 60 % der befragten Kommunen verfügten nicht über eine Leitlinie zur Informationssicherheit. Lediglich rund die Hälfte der befragten Kommunen traf einzelne, konkretisierende dienstliche Regelungen zur Informationssicherheit und brachte diese den Beschäftigten nachweislich zur Kenntnis.

12 Die Leitlinie enthält Grundsatzaussagen zur Informationssicherheit, definiert den Geltungsbereich, die Zuständigkeit, die zentrale Strategie und die Ziele für die Etablierung eines ganzheitlichen Informationssicherheitsprozesses. Sie dient als Grundlage für das Sicherheitskonzept und weitere fachspezifische Regelungen.

13 Die in der Leitlinie enthaltenen Grundsatzaussagen bedürfen in Abhängigkeit von den zu ermittelnden Schutzbedürfnissen und bestehenden Sicherheitsrisiken der weiteren Konkretisierung entsprechend der jeweiligen örtlichen Erfordernisse im Einzelfall.

14 Die organisatorische Umsetzung der Maßnahmen und Vorkehrungen zur Gewährleistung der Informationssicherheit obliegt den Kommunen im Rahmen ihrer Organisationshoheit. Gleichwohl empfiehlt sich aus Gründen der

[8] Vgl. LT-Drs. 6/16724, Gesetzesentwurf zur Neuordnung der Informationssicherheit im Freistaat Sachsen, Gesetzesbegründung Teil B. Besonderer Teil zu § 7 Abs. 3.

Transparenz und Nachvollziehbarkeit der Erlass von Dienstanweisungen, zumindest soweit einheitliche Regelungen für grundsätzliche Sicherheitsmaßnahmen, wie bspw. das Sperren von Arbeitsplatzrechnern oder der Umgang mit externen Datenträgern, getroffen werden. Abweichend davon kommen insbesondere für Informationen bezüglich aktueller Sicherheitsrisiken auch andere, kurzfristig wirksame Informationskanäle in Betracht (Hausmitteilungen, E-Mails u. a.).

15 **Es empfiehlt sich, Leitlinien aufzustellen und weitere organisatorische Regelungen für die Gewährleistung der Informationssicherheit zu treffen.**

16 Um das Anliegen zu unterstützen, in Kommunen ein angemessenes Niveau der Informationssicherheit herzustellen, haben gemäß Stellungnahme der SAKD die kommunalen Spitzenverbände eine Handreichung[9] entwickelt. Damit kann die Musterleitlinie der SAKD[10] den speziellen Gegebenheiten einer konkreten Organisation angepasst werden. Darüber hinaus stellt die SAKD weitere Informationen und Vorlagen zur Verfügung. Zur systematischen Einführung eines Informations-Sicherheits-Management – Systems (ISMS) wurde ein IT-Grund-Schutz-Profil „Basis-Absicherung-Kommunalverwaltung" erarbeitet.[11] Der Einstieg in die Informationssicherheit für kleine Kommunen soll durch die Initiative „Weg in die Basisabsicherung" (WiBA) erleichtert werden.[12]

2.2.2 Sicherheitskonzepte und Ermittlung von Schutzbedarfen

17 38 der befragten kreisangehörigen Kommunen (80 %) und zwei Zweckverbände haben kein Sicherheitskonzept aufgestellt. Nur rd. jede dritte Kommune hat Schutzbedarfe in Bezug auf Vertraulichkeit, Integrität oder Verfügbarkeit der Daten ermittelt.

18 Kommunen und Zweckverbände haben gem. § 14 SächsISichG vor Aufnahme der Datenverarbeitung nach §§ 12,13 SächsISichG ein für diesen Gebrauch erarbeitetes Sicherheitskonzept zu erstellen sowie die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen aktenkundig zu machen. §§ 12, 13 SächsISichG beziehen sich auf die Verarbeitung von Protokoll- und Inhaltsdaten zur Gefahrenabwehr mit dem Schwerpunkt der automatisierten Verarbeitung.

19 Darüber hinaus sollte ein übergreifendes Sicherheitskonzept aufgestellt werden, das sich an den anerkannten Standards des BSI ausrichtet. Es dient der Ermittlung und Analyse von Risiken beim Betrieb informationstechnischer Systeme und der Bestimmung von Maßnahmen zur Risikobehandlung mit dem Ziel der Risikominimierung (Erreichen eines Sicherheitsniveaus mit vertretbarem Restrisiko). Die Konzepte enthalten technische und organisatorische Maßnahmen, die geeignet sind, die in der Leitlinie festgelegten Sicherheitsziele zu erreichen.

20 Die Ermittlung von Schutzbedarfen ist (neben der Struktur- und der Risikoanalyse) eine wesentliche Voraussetzung für ein Sicherheitskonzept. Nur auf Grundlage der für alle Verwaltungsbereiche ermittelten Schutzbedarfe können zielgerichtet geeignete, erforderliche und angemessene Sicherheitsmaßnahmen festgelegt werden.

21 **Die Kommunen und Zweckverbände haben für den Teilbereich der Verarbeitung von Protokoll- und Inhaltsdaten nach §§ 12,13 SächISichG ein Sicherheitskonzept aufzustellen. Darüber hinaus empfiehlt es sich, ein übergreifendes Sicherheitskonzept unter Berücksichtigung der Standards des BSI zu erstellen und umzusetzen; dies setzt die Ermittlung von Schutzbedarfen voraus.**

2.3 Notfallmanagement

22 Regelungen für den Notfall wurden nicht einmal von der Hälfte der Gemeinden getroffen. Getestet wurde das Funktionieren der Notfallregelungen nicht einmal bei jeder 10. Gemeinde.

---

[9] https://www.staedtetag.de/files/dst/docs/Publikationen/Weitere-Publikationen/Archiv/informationssicherheitslinie-kommunalverwaltung-handreichung-2017.pdf, zuletzt geöffnet am 24. Oktober 2023.

[10] https://www.sakd.de/fileadmin/leistungsangebote/informationssicherheit/SAKD_Muster-Leitlinie_zur_Informationssicherheit_v1.0.docx, zuletzt geöffnet am 24. Oktober 2023.

[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.pdf, zuletzt geöffnet am 24. Oktober 2023.

[12] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/WIBA/Weg_in_die_Basis_Absicherung_WiBA.html, zuletzt geöffnet am 24. Oktober 2023.

23 Das Einrichten eines Notfallmanagements betrifft u. a. die Festlegung von Verhaltensweisen, Ansprechpartnern und Meldewegen im Notfall. Das ist auch Bestandteil des geltenden IT-Grundschutz-Kompendiums des BSI, das den nichtstaatlichen Stellen gem. § 4 Abs. 2 Satz 2 SächsISichG zur Anwendung empfohlen wird.

24 Nur die Hälfte der befragten Gemeinden und kein Zweckverband nutzen die vom Freistaat angebotenen Sicherheitsdienstleistungen des Sicherheitsnotfallteams SAX.CERT. Es unterstützt die BfIS der nichtstaatlichen Stellen des Freistaates Sachsen in technischen Sicherheitsfragen (§ 6 Abs. 1 SächsISichG) und bietet für Kommunen kostenlose Dienstleistungen an (bspw. HoneySens - Sicherheitslösung zur Erkennung von Hackerangriffen in internen Netzwerken, Sicherheitsscans von Internetseiten).[13]

25 **Die Implementierung von Regelungen zu Notfällen wird dringend empfohlen.** Zudem wird auf die Möglichkeit der Nutzung von Unterstützungsleistungen des Sicherheitsnotfallteams SAX.CERT, das im SID angesiedelt ist, hingewiesen.

26 Das SMI verwies in seiner Stellungnahme auf weitere kostenlose Unterstützungsangebote des Freistaates für die Kommunen[14]. Dazu gehören auch Fortbildungsangebote zum „IT-Grundschutz-Praktiker" und eine monatlich angebotene Sprechstunde des SAX.CERT.

2.4 Einfache Schutzmaßnahmen

27 Festlegungen über einfache Schutzmaßnahmen, bspw. der Sperrung von Arbeitsplatzrechnern beim Verlassen des Arbeitsplatzes, wurden bei 20 der 47 Gemeinden nicht getroffen. Nur reichlich die Hälfte der Kommunen verfügte über Gefahrenmeldeanlagen in ihren Serverräumen. 12 Gemeinden konnten einen ausreichenden Zutrittsschutz zu diesen Räumen nicht gewährleisten. Bei 2 Kommunen war der Zugang zu schützenswerten Ressourcen auf berechtigte Benutzer und IT-Komponenten nicht beschränkt (z. B. Schutz durch Passwörter bzw. Verschlüsselungen).

28 Das Fehlen einfacher Schutzmaßnahmen erleichtert den unberechtigten Zugriff auf Anwendungen und Daten und gefährdet insoweit die Vertraulichkeit und Integrität von Daten.

29 **Den Kommunen wird empfohlen, zumindest einfache Schutzmaßnahmen festzulegen und umzusetzen und in diesem Zusammenhang Gefahrenmeldeanlagen in Serverräumen vorzuhalten und den Zutrittsschutz zu Serverräumen umfassend zu gewährleisten.**

2.5 Empfehlungen des BSI

30 Einige der geprüften Körperschaften nutzten trotz entgegenstehender Empfehlung des BSI noch eine Virenschutzsoftware des russischen Herstellers Kaspersky, darunter auch Zweckverbände, die Aufgaben der Abwasserentsorgung und der Trinkwasserversorgung erfüllen. Diese Zweckverbände werden alle durch dieselbe betriebsführende Gesellschaft betreut.

31 Das BSI hat am 15. März 2022 vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky gewarnt. Virenschutzsoftware hat tiefgehende Eingriffsrechte in PCs, Smartphones, Laptops und andere IT-Infrastrukturen. Vertrauen in die Zuverlässigkeit und den Eigenschutz des jeweiligen Herstellers sowie seine authentische Handlungsfähigkeit ist daher entscheidend für den sicheren Einsatz solcher Systeme. Bestehen Zweifel hieran, birgt Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur.

32 Daher empfiehlt das BSI, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.[15]

33 Das SMI führte in seiner Stellungnahme aus, dass mit Schreiben vom 17. März 2022 der CIO des Freistaates die Geschäftsführer der kommunalen Spitzenverbände in der Sache „Kaspersky" angeschrieben und gebeten hatte, die Warnung des BSI zu beachten und eine Sicherheitsbewertung in den Kommunen vorzunehmen.

---

[13] https://www.cert.sachsen.de/dienstleistungen-3967.html, zuletzt geöffnet am 24. Oktober 2023.
[14] https://www.egovernment.sachsen.de/informationssicherheit-in-den-kommunen-5657.html, zuletzt geöffnet am 24. Oktober 2023.
[15] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/Archiv/FAQ-Kaspersky/faq_node.html, zuletzt geöffnet am 24. Oktober 2023.

34 **Es empfiehlt sich, den Warnungen des BSI zu folgen. Die Vorsitzenden der Zweckverbände sind gehalten, bei ihren betriebsführenden Gesellschaften auf die Umsetzung hinzuwirken. Aufgrund der verstärkten Abhängigkeit der Verwaltungen von der Funktionsfähigkeit der eingesetzten Informationstechnik hat sich insbesondere das Risiko für finanzielle Beeinträchtigungen und Nachteile durch Angriffe von außen deutlich erhöht. Durch Einsatz einer sicheren Virenschutzsoftware kann sich das Risiko wirtschaftlicher Nachteile für die Verwaltungen reduzieren.**

3 Stellungnahmen

35 Das SMI, die SAKD und der SSG nahmen zu den Feststellungen des Entwurfes des Jahresberichtsbeitrages Stellung.

36 Das SMI hat die SK als die für das SächsISichG fachlich zuständige oberste Landesbehörde einbezogen. Sie hat mitgeteilt, dass sie die Analysen des SRH insgesamt teile und die Empfehlungen an die Kommunen unterstütze. Ergänzend zu Tz. 6 merkte sie an, dass gem. § 8 Abs. 1 SächsISichG 198 Kommunen per August 2023 einen Beauftragten für Informationssicherheit gemeldet haben. Zu den Ausführungen unter Tz. 11 wurde ergänzt, dass alle in der Arbeitsgruppe Informationssicherheit des Landes beschlossenen Leit- und Richtlinien zur Informationssicherheit in der Landesverwaltung auch den in der Arbeitsgruppe vertretenen kommunalen Spitzenverbänden zur Kenntnis gegeben werden. Das SMI wird die obere RAB bitten, die Feststellungen des SRH mit den unteren RAB auszuwerten und diese zu bitten, in geeigneter Weise entsprechende Auswertungen mit den Kommunen ihres Zuständigkeitsbereiches vorzunehmen.

37 Die SAKD begrüßt die weitere Sensibilisierung für das Thema Informationssicherheit. Die Ergebnisse der Erhebungen stimmen mit den Erfahrungen der SAKD weitgehend überein. Die SAKD unterstützt die Kommunen in Form von Informationsaufbereitung und -vermittlung, der Sensibilisierung weiterer Partner und der Koordinierung der Maßnahmen mit den kommunalen Spitzenverbänden und dem Freistaat Sachsen.

38 Der SSG erachtet die Prüfung der Informationssicherheit in sächsischen Kommunen durch den SRH als einen bedeutsamen Schritt zum weiteren Ausbau einer verantwortungsvollen digitalen Verwaltung. Die Kommunen sind sich der zunehmenden Herausforderungen im Bereich der Informationssicherheit bewusst. Aufbau und Umsetzung von Schutzmaßnahmen ist ein dynamischer Prozess. Der SSG verweist darauf, dass die Informationssicherheit und der Datenschutz unterschiedlich zu betrachten sind und jeweils einen eigenen Beauftragten erfordern.

4 Schlussbemerkungen

39 Der SRH nimmt die konstruktiven Stellungnahmen zur Kenntnis und erkennt die Bemühungen des Freistaates Sachsen, der SAKD und des SSG an, die Gewährleistung der Informationssicherheit durch die Kommunen zu unterstützen.

40 Die kommunalen Körperschaften sind gehalten, die zur Verfügung stehenden Unterstützungsangebote möglichst umfassend zu nutzen und die erforderlichen Ressourcen und Kompetenzen für die Aufgabenerfüllung im Rahmen der Informationssicherheit bereitzustellen.