SACHSENLANDkurier

Organ des Sächsischen Städte- und Gemeindetages e. V.

Kommunalzeitschrift für die Städte und Gemeinden

DIE THEMEN DER AUSGABE

→ Polizeigesetz
→ Informationssicherheit

Sächsischer Städte- und Gemeindetag

AUSGABE 04|19

Vertrauen 4.0

Wenn aus Big Data Klartext wird.

Die Digitalisierung verändert vieles. Auch in der öffentlichen Verwaltung. Unsere Experten analysieren riesige Datenmengen. Wir verknüpfen Informationen aus verschiedensten Quellen und liefern Ihnen klar verständliche Inhalte. So haben Sie die Koordinaten für effiziente Steuerung jederzeit zur Hand – präziser und aussagekräftiger als je zuvor.

Ihr Ansprechpartner
Rainer Schindler
Tel: +49 341 9856-162
rainer.schindler@de.pwc.com

www.pwc.de/oeffentlicher-sektor

pwc

30. Jahrgang ■ **SLK 04|19**

Inhaltsverzeichnis

SPRUCH DES MONATS

Ohne Sicherheit ist keine Freiheit.

Wilhelm von Humboldt (1767–1835),
Philosoph u. Sprachforscher;
Preußischer Staatsmann

Der »Sachsenlandkurier« (SLK), Kommunalzeitschrift für die Städte und Gemeinden, Organ des Sächsischen Städte- und Gemeindetages (SSG)

VERANTWORTLICH FÜR DEN HERAUSGEBER
Geschäftsführer Mischa Woitscheck
Namentlich gekennzeichnete Artikel geben nicht in jedem Fall die Meinung des Herausgebers wieder. Für die inhaltliche Richtigkeit von Fremdbeiträgen ist der jeweilige Verfasser verantwortlich.

ANSCHRIFT
Sächsischer Städte- und Gemeindetag e. V.
Glacisstraße 3, 01099 Dresden
Telefon: 03 51 81 92 – 0
Telefax: 03 51 8 19 22 22
E-Mail: post@ssg-sachsen.de
Internet: http://www.ssg-sachsen.de

GESAMTHERSTELLUNG
SV SAXONIA VERLAG
für Recht, Wirtschaft und Kultur GmbH
Lingnerallee 3, 01069 Dresden
Telefon: 03 51 48 52 60, Fax: 03 51 4 85 26 61

Der SACHSENLANDKURIER erscheint 6 mal jährlich.

Abonnenten erhalten den SLK als PDF-Datei auf Anfrage unter post@ssg-sachsen.de kostenlos zugesandt.

BEZUGSPREISE
- für Mitgliedsstädte und -gemeinden:
  ein Jahresabonnement: gebührenfrei
  je weiteres Abonnement: 26,00 €
  je Einzelheft: 4,50 €
- für Nichtmitglieder:
  je Jahresabonnement: 30,00 €
  je Einzelheft: 5,00 €
- für Studenten, Referendare und in Ausbildung Stehende sowie gewählte Stadt-, Gemeinde- und Ortschaftsräte und Fraktionen der Gemeinderäte:
  je Jahresabonnement: 26,00 €
  je Einzelheft: 4,50 €

Alle Abonnementspreise einschließlich Versand- und Zustellgebühren. Bei Einzelheftbezug zuzüglich Versand- und Zustellgebühren. In den jeweiligen Bezugsgebühren ist die gesetzliche Mehrwertsteuer enthalten.

BESTELLUNGEN
Schriftlich an die Geschäftsstelle des SSG, Abbestellungen werden nur zum 30. Juni und zum 31. Dezember wirksam.

ANZEIGENVERWALTUNG
SV SAXONIA VERLAG
für Recht, Wirtschaft und Kultur GmbH
Lingnerallee 3, 01069 Dresden
Telefon: 03 51 4 85 26 41, Fax: 03 51 4 85 26 62

TITELBILD: geralt/pixabay.com

POLIZEIGESETZ

INFORMATIONSSICHERHEIT

ALLGEMEINE BEITRÄGE

Sicherheit in Sachsen. Das neue Polizeigesetz

Prof. Dr. Roland Wöller, MdL
Sächsischer Staatsminister des Innern

Sicherheit – ein menschliches Grundbedürfnis

Der Sächsische Landtag hat am 10. April dieses Jahres das neue sächsische Polizeigesetz verabschiedet, das am 1. Januar 2020 in Kraft tritt. Es macht Sachsen sicherer und schützt die Freiheit der Menschen im Freistaat.

Die letzte große Neuerung im Polizeirecht hat es vor 20 Jahren gegeben. Inzwischen befinden wir uns weltweit in einer neuen Sicherheitslage. Die Telekommunikation hat sich rasant weiterentwickelt; sie eröffnet den Kriminellen neue Handlungsräume; die Grenzen zu Polen und Tschechien sind im Zuge der Europäischen Einigung weggefallen; die grenzüberschreitende Kriminalität hat neuen Auftrieb bekommen und der internationale Terrorismus bedroht den Frieden auch im Freistaat Sachsen. Neue Zeiten brauchen neue Antworten.

Sicherheit ist ein hoch aktuelles Thema. Es brennt vielen Menschen unter den Nägeln. 72 Prozent der Bundesbürger machen sich – nach einer Allensbach Umfrage aus diesem Jahr – Sorgen um Kriminalität und Terror – viel mehr als über Arbeitsplätze. Denn Sicherheit ist ein Grundbedürfnis. Jeder von uns will sicher leben. Keiner von uns will beraubt und bestohlen werden, Eindringlinge in der eigenen Wohnung überraschen oder Gewalttaten zum Opfer fallen. Wir wollen uns angstfrei bewegen – auf Straßen und Marktplätzen, in Bahnen und Bussen, Tag und Nacht, in der realen, aber auch in der virtuellen Welt.

Sachsen – ein sicheres Land

Die Zahl der Straftaten hat im Jahr 2018 den niedrigsten Stand der letzten zehn Jahre erreicht. Ca. 7.000 (6.831) Straftaten pro 100.000 Einwohner. Kraftwagen-Diebstähle sind zurückgegangen, auch Wohnungseinbrüche und Gewaltkriminalität, und die Grenzkriminalität ist auf dem niedrigsten Stand seit 10 Jahren. Rauschgiftdelikte nehmen zu, auch politisch motivierte Kriminalität. Statistisch klingt das alles gut. Wir sind insgesamt auf dem richtigen Weg. Gleichwohl braucht es weitere Anstrengungen, um auch das Sicherheitsgefühl der Menschen zu verbessern.

11.000 Polizistinnen und Polizisten – neben 42.000 Feuerwehrfrauen und -männern und 3.000 Helferinnen und Helfern im Katastrophenschutz und Rettungsdienst – tragen die Verantwortung für unsere Sicherheit in Sachsen. Sie sind 365 Tage im Jahr im Einsatz. Rund um die Uhr.

Sie alle sind im wahrsten Sinne des Wortes unsere Helfer und Helden, denen wir großen Dank schulden. Aber zuweilen werden sie im Alltag selber Opfer von Angriffen und Anfeindungen. Deshalb hat die Staatsregierung vor kurzem eine Solidaritätsaktion gestartet, deren Symbol die »Helferschleife« ist. Mit ihr bekunden wir unsere Hochachtung gegenüber diesen tapferen Frauen und Männern und machen deutlich: Wir stehen hinter denen, die sich vor uns stellen.

Neues Gesetz – neue Befugnisse

Mit richterlicher Anordnung können wir jetzt die Telekommunikation verdächtiger Personen überwachen, verdeckte Ermittler einsetzen, die Polizistinnen und Polizisten mit Bodycams ausstatten und Schleierfahndungen durchführen. Wir haben auch früh den Sächsischen Datenschutzbeauftragten eingebunden, um sicher zu stellen, dass das neue Polizeigesetz sich eng an den Vorgaben des Bundesverfassungsgerichtes hält. Denn Sicherheit darf Freiheit nicht einschränken, sondern schützen.

Neben Strafverfolgung und Gefahrenabwehr nimmt im neuen Gesetz die Prävention eine zentrale Stellung ein. Wir müssen handeln, bevor das Kind in den Brunnen gefallen ist. Gerade wo schwerste Straftaten drohen, darf die Polizei nicht warten, bis die Lunte gelegt und die Bombe hochgegangen ist, bis Kriminelle zur Tat geschritten und Opfer zu beklagen sind. Die Polizei muss schon im Vorfeld tätig werden und Straftaten verhindern. Wer präventiv handelt, wehrt Gefahren ab und vermeidet Opfer. Deshalb muss die Polizei mehr dürfen, als die Kriminellen können.

Neu ist im Polizeigesetz auch die Videoüberwachung, um grenzüberschreitende Kriminalität an unseren polnischen und tschechischen Grenzen zu bekämpfen. Diese Regelung ist unerlässlich, weil nach dem Wegfall der innereuropäischen Grenzen Straftaten viel leichter begangen werden können. Kriminelle melden sich bekanntlich nicht an der Grenze oder beantragen Visum. Der Wegfall von Grenzen darf aber nicht heißen Wegfall von Sicherheit. Zu Recht hat das Bundesverfassungsgericht festgestellt, dass die Bundesrepublik Deutschland den Verzicht auf Grenzkontrollen durch Erweiterung von Befugnissen ausgleichen darf, um Gefahren abzuwehren. Und das tun wir in Sachsen mit unserem neuen Gesetz.

Die Polizei kann fortan auch Bodycams einsetzen, also Körperkameras, um Straftäter abzuschrecken und Konflikte zu deeskalieren. Dieser Punkt war im Parlament sehr umstritten. Ich bin froh, dass die Vernunft sich hier durchgesetzt hat. Denn wir müssen die schützen, die uns schützen.

Gesetze – und darüber hinaus

Über dieses Gesetz hinaus tun wir viel für die Polizei und unsere Sicherheit. Wir haben bereits 1.000 neue Stellen in der Polizei geschaffen, und wir investieren viel in Ausbildung und Ausrüstung.

»Mobile Polizeiarbeit« ist das neueste Stichwort. Mit neuen digitalen Instrumenten versetzen wir die Polizei in den Stand, digitale Spuren zu verfolgen und fortan auch unterwegs das zu erledigen, was sie früher nur vom Büro aus konnte.

Polizei gehört vor allem auf die Straße, nicht an den Schreibtisch. Denn sichtbare Polizei heißt mehr Sicherheit – sowohl tatsächliche als auch gefühlte.

Prävention – Schlüssel zu mehr Sicherheit

Aber Sicherheit ist nicht nur eine Angelegenheit der Polizei oder der Sicherheitsbehörden. Der Ort, an dem Bürger Sicherheit erleben, ist die Kommune, in der die Menschen ihren Lebensmittelpunkt haben und sozialisiert werden. Dort entstehen die Probleme. Dort entstehen die Lösungen. Dort entsteht auch das Sicherheitsgefühl.

Kommunen sind wie Seismografen. Sie spüren Verschiebungen und Tendenzen in der Gesellschaft, sie wittern, was richtig läuft und was aus dem Ruder gerät. Hier ist die gesamte Gesellschaft aufgefordert, mitzuwirken. Prävention wirkt. Deshalb stärkt die Staatsregierung die kommunale Kriminal-Prävention. Gefahren vorzubeugen ist günstiger und wirksamer, als Straftaten zu ermitteln und Straftäter zu verfolgen. Auch hier gilt: Wir müssen handeln, bevor das Kind in den Brunnen gefallen ist, zumal es keinen Beleg dafür gibt, dass Strafverfolgung allein durch Polizei die Kriminalitätsrate senkt oder das Sicherheitsgefühl der Bürger erhöht.

Deshalb haben wir vor einigen Monaten die *»Allianz Sichere Sächsische Kommunen«,* abgekürzt ASSKomm, gegründet, um die Sicherheit vor Ort zu stärken. Dabei ist die Polizei ebenso ein Akteur wie es die Kommunalverwaltungen, Schulen, Vereine, kirchlichen Einrichtungen, die Feuerwehr und die gesamte Zivilgesellschaft sind. Es ist ein Irrtum zu glauben, dass Menschen nur gieren und raffen. Menschen sind auch bereit zu geben – Kraft und Lebenszeit. Das ist eine menschliche Seite, die wir stärker fördern sollten.

Der kriminalpräventive Rat von Leipzig hat sich u.a. der Sicherheit für Kleingartenanlagen angenommen, der kriminalpräventive Rat von Dresden widmet sich der Graffitiprävention. Auch die Landkreise Görlitz, Bautzen und Leipzig haben sich seit einigen Jahren auf den »Präventions-Weg« gemacht. Ostsachsen ist vor allem vorbildlich im Bereich der Schulen, und Wurzen und Pirna haben mit Gewalt- und Extremismusprävention ebenso Erfahrungen gesammelt wie mit dem Aufbau von kommunalen Präventionsstrukturen.

Zwei Maßstäbe – tatsächliche und gefühlte Sicherheit

Wir merken aber, dass oft eine Lücke zwischen der tatsächlichen Sicherheit in Sachsen und der gefühlten Sicherheit der Menschen klafft. Die tatsächliche Sicherheit ist hoch, aber die gefühlte Sicherheit niedriger. Nicht nur mit stärkerer Polizeipräsenz, sondern auch mit der kommunalen Prävention können wir über die tatsächliche Sicherheit hinaus auch die gefühlte Sicherheit der Bürger stärken.

Ein anderer, wirksamer Hebel für unsere Sicherheit ist der Städte- und Wohnungsbau. Es ist keine neue Entdeckung, dass verlassene und verwahrloste Gassen, dunkle und schmutzige Straßen den Nährboden für Gewalt und Kriminalität bereiten. Aber neu ist es, dass die Staatsregierung dieser Selbstverständlichkeit mit besonderem Augenmerk Rechnung trägt. Gerade Stadtplanung, Architektur und Bebauung sind Elemente, die für das Sicherheitsgefühl der Bürger entscheidend sind. Wenn man also Städte aus dieser Perspektive gleichsam »einrichtet«, dann stärkt der Städtebau nicht nur das Sicherheitsgefühl der Bürger, sondern auch ihre Identifikation mit der Heimat, in der sie weiterhin gerne leben wollen.

Cyber Kriminalität – die neue Gefahr

Sicherheit gilt nicht nur für die reale Welt, sondern auch für die virtuelle Welt des Internets. Cyber-Kriminalität ist eine wachsende Gefahr. Hier hat sich inzwischen eine sogenannte *»underground economy«* (Untergrund-Wirtschaft) etabliert. Gewöhnliche Kriminelle kaufen im Internet entsprechende »Dienste« ein, die sie für ihre Straftaten benötigen, und begehen so Straftaten. Kriminalität als Dienstleistung ist der Trend.

Davon sind Einzelpersonen, aber auch Unternehmen betroffen. Auch die kleinen, mittelständischen und großen Unternehmen wollen im Freistaat in Sicherheit ihren Geschäften nachgehen. Internet-Kriminalität bedroht auch sie. Mitarbeiterdaten werden gestohlen, Kundendaten an Dritte weitergeleitet, Innovationen geklaut und kopiert. Das schadet nicht nur den Unternehmen, sondern auch unserer Volkswirtschaft. Deshalb ist Sicherheit ein Wirtschaftsfaktor für den Standort Sachsen und Deutschland.

Wir Deutschen sind weltweit berühmt für unsere Ideen und Innovationen. Ein britischer Mathematiker und Philosoph hat einmal gesagt: *»Wenn man einen Deutschen mit ein paar Konservendosen in den Urwald jagt, kommt er mit einer Lokomotive wieder hinaus!«* (Alfred North Whitehead/1861–1947). Deshalb müssen wir die Innovationen unserer Forscher und Unternehmen schützen.

Sachsen hat fast 20 *»Hidden Champions«* (»Verborgene Weltmeister«), also Marktführer weltweit, die nicht jedem und überall bekannt sind. Es müssen aber nicht immer »verborgene Weltmeister« sein, die sich gegen Diebstahl und Kriminalität zur Wehr setzen müssen. Auch gute Unternehmen, die bemüht sind, neue Wege zu gehen und interessante Produkte bzw. Dienstleistungen zu bieten, brauchen Sicherheit.

Nach einer Studie der Allianz für Cybersicherheit wurden 2017 ca. 70 % aller Klein- und Mittelständischer Unternehmen (KMU) Opfer von Cyberangriffen. In der gleichen Studie sehen 48 % der befragten KMU Cyberangriffe als relevante Bedrohung ihrer Firma an. Das ist wenig. Deshalb müssen wir Unternehmen für diese Fragen im Vorfeld sensibilisieren, zumal mehr als 90 % aller erfolgreichen Angriffe auf das Fehlverhalten von IT-Nutzern zurückgehen. Strafverfolgung ist die eine Seite der Medaille, Prävention die andere. Beide gehören zusammen. Beide müssen zusammen gedacht werden.

Die Staatsregierung nimmt die Gefahr in der virtuellen Welt sehr ernst. Technologisch, aber auch in der Ausbildung der Polizei und in der Zusammenarbeit mit Verbraucherzentralen, Volkshochschulen, Industrie- und Handelskammern sowie Handwerkskammern unternehmen wir viel, um den Kriminellen voraus zu sein und unsere Bürger und Unternehmen für Cyber-Gefahren zu sensibilisieren und ihnen beratend zur Seite zu stehen.

Gemeinwohl – Freiheit durch Sicherheit

Die Aufgabe des Staates ist es, das Gemeinwohl zu verteidigen. In einer freiheitlichen Demokratie kann er diese Aufgabe nur erfüllen, wenn er Recht und Ordnung durchsetzt und dadurch die Freiheit der Bürgerinnen und Bürger schützt. Nur so fassen die Bürger Vertrauen in den Rechtsstaat und wissen, dass sie sich auf den Staat verlassen können.

Freiheit ist ein hohes Gut, aber sie ist zerbrechlich. Sie ist auch nicht selbstverständlich. Wir müssen sie immer wieder von neuem erkämpfen. Damit sie gedeihen kann und wir als Bürgerinnen und Bürger in einem demokratischen Rechtsstaat in Frieden und Freiheit leben können, brauchen wir eine robuste Sicherheit. Genau dazu dient das neue sächsische Polizeigesetz.

Polizeigesetz 2019
CDU modernisiert Polizei- und Ordnungsrecht für Sachsen

Rico Anton, MdL
Innenpolitischer Sprecher der CDU-Fraktion

Foto: Ines Escherich

Sicherheit ist Grundvoraussetzung unserer Freiheit und zentrales Versprechen des Staates gegenüber seinen Bürgern. Dieses Versprechen politisch einzulösen und mit den notwendigen Gesetzen zu untermauern, ist eine Aufgabe, die die sächsische CDU als zentral ansieht. Sachsens neues Polizeigesetz trägt diesem Ansinnen Rechnung. Es wird mehr Sicherheit vor Ort schaffen und unser aller Freiheit besser schützen.

Sachsens Städte und Gemeinden sind elementar abhängig von einem guten Sicherheitsgefühl! Es entscheidet im Wesentlichen, wie sie sich entwickeln können. Niemand investiert guten Gewissens in eine Stadt oder Gemeinde, in der er um die Sicherheit seines Eigentums fürchten muss. An dieser Stelle merkt man, dass es sich um einen subjektiven Sicherheitsbegriff handelt – und nicht um reine Fakten oder schnöde Statistiken! Auch wenn diese für die politische Analyse wichtig sind, gilt es dennoch diese emotionale Lage nicht zu vernachlässigen. Der Staat muss seinen Bürgern das berechtigte Gefühl geben, dass sie geschützt werden.

Dies wird durch das staatliche Gewaltmonopol gewährleistet, welches Freistaat und Kommunen im Polizei- und Ordnungsrecht ausüben. Es herrscht hier eine arbeitsteilige Aufgabenwahrnehmung, die in einer engen Verzahnung erfolgt, um erfolgreich zu sein. Auf der Ebene des Freistaates gibt es die Landespolizei, welche den Polizeivollzugsdienst stellt. Auf kommunaler Ebene gibt es die Oberbürgermeister und Bürgermeister, die mit ihren Ortspolizeibehörden und der Verwaltung Aufgaben zur Gewährleistung von Ordnung und Sicherheit vor Ort wahrnehmen. Sicherheit aber allein ist kein Selbstzweck. Sie ist in unserem demokratischen Rechtsstaat Garant für Freiheit.

Freiheit vs. Sicherheit

Eines der sichersten Länder der Welt ist Nordkorea. Aber für die Mehrheit der Deutschen wäre das kein erstrebenswerter Lebensmittelpunkt. Sicherheit allein ist also nichts – aber eine Grundlage! Auf ihr baut alles andere auf. Und in einer demokratischen Gesellschaft paart sich die Frage nach der Sicherheit automatisch mit dem Begriff Freiheit. Das ist der Spannungsbogen, der automatisch entsteht, wenn wir über Sicherheit reden. Es geht um das Entfaltungsrecht des Einzelnen und die Rechte anderer. Das unterscheidet die Demokratie vom Anarchismus. Hier geht es nicht, dass jeder nach seinen eigenen Regeln lebt. Sondern wir haben Leitplanken, zwischen denen man sich bewegen und frei entfalten kann. Aber das findet dort seine Grenzen, wo jemand die Rechte anderer beschränkt oder verletzt. Freiheit und Sicherheit müssen also in Balance gehalten werden. Nur so kann Gesellschaft funktionieren!

Das heißt, den Freiheitsrechten des Einzelnen sind Schranken gesetzt, damit die Freiheitsrechte anderer gewährleistet werden können. Nur so ist langfristig ein friedliches Zusammenleben aller Bürger zu erreichen. Die Schranken sind in unserem Rechtsstaat durch Gesetze bestimmt, vor denen jeder gleich ist. Der Staat hat mittels seines Gewaltmonopols dafür zu sorgen, dass die Bürger sicher leben können und sich an die vorgegebenen Regeln des Zusammenlebens halten und dass ihre Ansprüche, die in den Gesetzen auch verankert sind, durchgesetzt werden. Der Staat muss tätig werden, wenn Einzelne oder auch eine ganze Anzahl von Menschen diese Schranken überschreiten wollen oder überschreiten.

Allerdings: Freiheit und Sicherheit sollen und müssen in einem demokratischen Rechtsstaat immer fein austariert werden. Nur in Diktaturen kann Sicherheit die Freiheit verdrängen. Freiheit birgt in sich also automatisch Sicherheitsrisiken, denn es gibt keinen Vollkasko-Staat. Es gibt in der Literatur einen einzelnen Menschen, der keine Regeln und Gesetze brauchte, da er absolut frei war, weil er allein auf einer einsamen Insel strandete: Robinson Crusoe. Seine Freiheit endete, als er die Fußspuren von Freitag im Sand entdeckte – ab dem Moment musste er seine Freiheit einschränken.

In unserer modernen Demokratie muss die Einschränkung der Freiheit des Einzelnen per Gesetz und verbindlich für alle erfolgen. Und es muss geregelt sein, wie die Staatsgewalt ausgeübt wird. Das heißt, auf welche Weise, mit welchen Mitteln, in welchen Fällen und in welcher Form der Staat den Erhalt und die Schaffung von Sicherheit zur Gewährleistung der Freiheit erreichen soll. Der Ausübung der Staatsgewalt sind klare Schranken zu setzen, damit diese keinem Selbstzweck dient. Diese

klaren Schranken für die Ausübung der Staatsgewalt beinhalten auch eine ständige Überprüfung, ob sie dafür geeignet sind, die Sicherheit der Bürger noch gewährleisten können.

Das gilt insbesondere auch für ein Polizeigesetz. Das Sächsische war 20 Jahre alt. Es stammt noch aus einer Zeit, in der Faxe zwischen Polizeidienststellen verschickt wurden und Kriminelle von der Telefonzelle aus mit ihren Ganovenkollegen über ihren nächsten Coup plauderten – der analog geplant und ausgeführt wurde. In dieser Zeit entstand das bis zum 31. Dezember noch gültige Polizeigesetz. Und es leistete gute Dienste. Es wurde am Ende durch die Polizeibeamten so verantwortungsvoll umgesetzt, dass es bis heute überaus positive Wirkung entfalten konnte. Es war aber nun Zeit für eine Anpassung an die neue und vor allem digitale Lebenswirklichkeit der Menschen. Denn auch Kriminalität geht mit der Zeit und setzt auf moderne Mittel. Landespolizei und kommunale Polizeibehörden brauchten deshalb neue gesetzliche Regelungen, um mit zeitgemäßen Mitteln entgegen zu halten.

Zur Neuregelung ihrer Aufgaben und Befugnisse beschloss der Sächsische Landtag am 10. April dieses Jahres mit der Mehrheit der Regierungskoalition von CDU und SPD das »Gesetz zur Neustrukturierung des Polizeirechtes des Freistaates Sachsen«, welches mit Wirkung zum 1. Januar 2020 in Kraft treten wird. Dem ging ein harter und durch zwei Sachverständigenanhörungen fachlich sehr tiefgreifender Diskussionsprozess voraus. Das zeigt, wie verantwortungsvoll sich die CDU-Fraktion der Herausforderung gestellt hat. Es ging schließlich um neue wirksame Regelungen zur Gefahrenabwehr und ein ausbalanciertes System von Freiheits- und Bürgerrechten.

Die CDU-Fraktion machte deshalb im Gesetzgebungsprozess von der Möglichkeit der Änderung des Regierungsentwurfes umfangreich Gebrauch. So war es beispielweise möglich, die zeitlich parallel ergangene Entscheidung des Bundesverfassungsgerichts zur Rechtmäßigkeit der automatisierten Erfassung von Kfz-Kennzeichen durch einen Änderungsantrag zu berücksichtigen und damit auf der einen Seite die Wahrung der verfassungsmäßigen Bürgerrechte rechtssicher zu gestalten. Auf der anderen Seite konnte aber im Hinblick auf die Verknüpfung von neuen technischen Möglichkeiten und deren Einsatz durch die Polizei die verfassungsrechtlich zulässigen Eingriffsbefugnisse auch gesetzlich gewährleistet werden.

Zu Recht wurde in der Öffentlichkeit eine intensive Diskussion um das Für und Wider des neuen Sächsischen Polizeirechtes geführt. Für die CDU ist es nachvollziehbar, dass es in der Opposition und in der Bürgerschaft Stimmen gibt, die sich kritisch mit dem neuen Polizeirecht in Sachsen auseinandersetzen. In diesem Spannungsfeld der politischen Meinungen und der Sicht auf das Verhältnis von Freiheit und Sicherheit musste eine verfassungsgemäße, dem Datenschutzrecht entsprechende, umfassende und vor allem praktikable gesetzliche Neuregelung her.

Was ist neu am sächsischen Polizei- und Ordnungsrecht?

Zukünftig wird es zwei Gesetze geben, die das Polizeirecht regeln: Einerseits das Polizeibehördengesetz (SächsPBG), das die Stellung der Ordnungsämter der Kommunen und Kreise (Polizeibehörden) bestimmt. Andererseits das Polizeivollzugsdienstgesetz (SächsPVDG) für die Landespolizei in Uniform und die Kriminalpolizei. Durch diese Trennung werden die Rechtssicherheit und vor allem Rechtsklarheit sowohl für die Landespolizei und die Polizeibehörden wie auch die Bürger erhöht. Ordnungsbehördliche Aufgaben werden mit einem eigenen Gesetz klar und verständlich bei den Polizeibehörden der Kommunen angesiedelt. Diese sollen dabei keine neuen Aufgaben übertragen bekommen. Aber die zugewiesenen Befugnisse werden vielmehr konkretisiert, sodass beispielsweise zu der bisher auch schon bestehenden Befugnis der Polizeibehörden zur Videographie sinnvolle Instrumente zur Seite gestellt werden, wie das zur Einrichtung von Alkoholverbotszonen in der Nähe von Kinder- und Jugendeinrichtungen.

Im Polizeivollzugsdienstgesetz werden die neuen und modernen Befugnisse es ermöglichen, Straftaten und Gefahren, die in der heutigen Zeit in immer stärkerem Maße von Mobilität, unbegrenzter und grenzenloser Kommunikation und virtuellen Netzwerken aber auch Terrorismus geprägt sind, aufzuklären und zu verhindern. Für besondere Gefahrenlagen erhält die Polizei eine erweiterte Bewaffnung; diese soll für die Spezialeinheiten in den besonderen Einsatzlagen die erforderliche Reichweite und Durchschlagskraft sicherstellen.

Den Eingriffsbefugnissen im Bereich der Telekommunikation kommt eine Schlüsselrolle zu. Zulässig sind nun die Ermittlung von Standort- und Gerätedaten von Mobiltelefonen durch den Einsatz von sogenannten »IMSI-Catchern«. Die Polizei darf außerdem auf Grundlage des neuen Polizeivollzugsdienstgesetzes die Telekommunikation von Personen überwachen und aufzeichnen – unter engen Voraussetzungen und auf richterliche Anordnung. Auch können nunmehr nicht nur von den »Telekommunikationsanbietern«, also den klassischen Telefongesellschaften, Daten abgefragt werden. Erstmals sind auch Auskünfte von sogenannten »Telemedienanbietern«, also aus dem Bereich der sozialen Netzwerke, möglich.

Es können Auskünfte über sogenannte »Verkehrsdaten der Kommunikation«, also wer mit wem kommuniziert, abgefragt werden. Und es dürfen die Inhalte im Rahmen der Telekommunikationsüberwachung aufgeklärt werden. Allerdings mit Einschränkung! Die sogenannte Quellentelekommunikationsüberwachung ist nicht erlaubt. Diese Erfassung von Nachrichten bevor diese auf dem Weg vom Sende- zum Empfängergerät verschlüsselt werden, wie zum Beispiel bei WhatsApp-Nachrichten, ist nicht möglich. Auch die Online-Durchsuchung war im aktuellen Gesetz mit dem Koalitionspartner nicht mehrheitsfähig. Deshalb wird die CDU beide Themen nach der Landtagswahl erneut aufgreifen.

Daneben gibt auch das bisherige Polizeigesetz bereits die Befugnis, im Zusammenhang mit Personen, von denen Straftaten drohen, Gefahren aufzuklären und Gefahren durch Unterbindungsmaßnahmen im Vorfeld zu begegnen. Neu wurde dazu aber beispielsweise die Möglichkeit geschaffen, die Kommunikation solcher Personen durch den Einsatz von Störsendern, sogenannten »Jammern«, zu unterbinden. Gefährder können künftig mittels elektronischer Fußfesseln überwacht und Personen, von denen schwere Straftaten drohen, einer Durchsuchung unterzogen werden. Weiterhin wurden Möglichkeiten zum Ausspruch längerfristiger polizeilicher Meldeauflagen, Regelungen zu orts- und gebietsbezogenen Aufenthaltsanordnungen und zur Verhängung von Kontaktverboten geschaffen.

Gerade die letztgenannten beiden Regelungen dienen auch dem Opferschutz. Es kann beispielsweise verhindert werden, dass Gewalttäter sich in die Nähe ihrer Familie begeben oder sich zum Beispiel von Kinderspielplätzen fernhalten müssen. Dabei ist die Zusammenarbeit zwischen der Polizei und den kommunalen Behörden im Bereich der Jugend- und

Sozialarbeit im Sinne der Kriminalitätsprävention seit jeher besonders wichtig und geübte Praxis. Hier sollte auf Grundlage der neuen polizeilichen Befugnisse in Abstimmung zwischen den jeweils vor Ort verantwortlichen Polizeidienststellen und den Ortspolizeibehörden darauf abzielen, dass die neuen Möglichkeiten der Gefahrenabwehr durch die Polizei sinnvoll und wirkungsvoll zur Abwehr von Gefahren eingesetzt werden können.

Die Umsetzung des neuen Polizeirechts löst einen entsprechenden Schulungsbedarf sowohl auf Seiten der Landespolizei als auch bei den kommunalen Polizeibehörden aus. Diesen abzudecken und die Zusammenarbeit zu stärken, ist dann auch Teil der Strategie »Allianz Sichere Sächsische Kommunen« (ASSKomm).

Die Bürger erwarten von der Polizei auch ein wirksames Vorgehen gegen die sogenannte Alltagskriminalität. In diesem Zusammenhang sind zum Beispiel Maßnahmen zur Bekämpfung grenzüberschreitender Kriminalität von Bedeutung. Durch seine lange Außengrenze ist Sachsen dabei ein Bundesland, durch welches Verbindungsrouten für die Verbringung von Diebesgut ins Ausland verlaufen. Die Bekämpfung der grenzüberschreitenden Kriminalität ist deshalb ein Thema für ganz Sachsen. Im neuen Polizeivollzugsdienstgesetz wird, neben der bereits erwähnten automatisierten Kennzeichenerfassung, die Befugnis geschaffen, auch biometrische Daten von Personen gezielt im Hinblick auf die Übereinstimmung mit bereits auffällig gewordenen Täterkreisen, die bandenmäßig oder sonst organisiert handeln, zu filtern und so Täterkreise zu beobachten und dadurch Straftaten bereits im Vorfeld zu verhindern.

Weiterhin wird es nunmehr gesetzlich erlaubt, an Kriminalitätsschwerpunkten Videokameras aufzustellen. Dies hat eine abschreckende Wirkung auf potentielle Straftäter, wie zahlreiche Studien belegen. Diese Befugnis ist insbesondere für die kommunalen Polizeibehörden von Bedeutung.

Aber auch der Schutz der Polizisten, die Beweissicherung und Deeskalation sollen durch eine wichtige neue Befugnis im Bereich der Videographie wesentlich verbessert werden. Durch eine sehr detaillierte Regelung wird der flächendeckende Einsatz von körpernahen Kameras bei der Polizei, den sogenannten »BodyCams«, datenschutzkonform und rechtssicher geregelt.

Aus Sicht der CDU sind im Gesetz nunmehr starke Mechanismen zum Schutz der Grundrechte eingearbeitet. Dies war uns wichtig, denn die gerade in Sachsen lebendige Erinnerung an die Zeit bis zur Friedlichen Revolution 1989 gebietet es, hier besonders sensibel zu sein. Gleichwohl ist es nicht nur verfassungskonform, sondern auch durch das Grundgesetz geboten, unsere Polizei mit dem Handwerkszeug auszustatten, das sie technisch auf Augenhöhe mit den Straftätern und Terroristen agieren kann. Nur so ist das Gewaltmonopol des Staates durchsetzbar!

Damit kann zusammenfassend festgestellt werden:
Auf der Grundlage der neuen, zeitgemäßen Befugnisse wird die Polizei in die Lage versetzt, künftig noch effizienter im Vorfeld von Straftaten erfolgreich tätig zu werden. Die neuen Regelungen des sächsischen Polizeirechts sind wesentlich transparenter und im Verbund mit der Einstellung von 1000 neuen Polizisten bis 2024 sowie einem gemeinsamen Handeln der kommunalen Familie und des Freistaates im Sinne der Strategie der »Allianz Sichere Sächsische Kommunen« wird die Sicherheit vor Ort in unseren Städten und Gemeinden nachhaltig weiter verbessert.

Ein neues Polizeirecht für Sachsen: Stärkung von Transparenz und Bürgerrechten und solide Handlungsgrundlage für Polizeivollzugsdienst und Polizeibehörden

Albrecht Pallas, MdL
Innenpolitischer Sprecher der SPD-Fraktion

Foto: ©Götz Schleser

Vor fast fünf Jahren hat die SPD Regierungsverantwortung in Sachsen übernommen. Wir konnten in dieser Zeit viele unserer zentralen Forderungen umsetzen und im Vergleich zur schwarz-gelben Vorgängerregierung eine 180-Grad-Wende hinlegen. Dank uns ist der Personalabbau gestoppt und das sächsische Spardiktat durchbrochen worden. Es wird wiedereingestellt. Für die SPD waren dabei drei Bereiche sehr wichtig: Schule, Kitas und die Innere Sicherheit in all ihren Facetten. Diese Themen wurden auch von Bürgerinnen und Bürgern, Kommunen, Verbänden und Vereinen immer wieder in Gesprächen an uns herangetragen.

Ein erster großer Schritt war der Stopp des Stellenabbaus bei der Polizei, den wir der CDU schon in den Koalitionsverhandlungen abringen konnten. In einem zweiten Schritt hatten wir durchgesetzt, dass eine Expertenkommission den Personalbedarf bei der Polizei ermittelt und in der Folge 1.000 zusätzliche Stellen geschaffen wurden. Die Ausbildung wurde hochgefahren, mittlerweile werden jährlich bis zu 700 neue Beamtinnen und Beamte eingestellt. Schwarz-gelb wollte ursprünglich die Zahl der Polizeistellen bis 2024 auf rund 12.000 reduzieren. Nach unserer Kurskorrektur werden in fünf Jahren stattdessen rund 14.000 Polizisten in ganz Sachsen für Sicherheit sorgen.

Mehr sichtbare Sicherheit durch alle verantwortlichen Stellen

Aber auch die gesetzlichen Grundlagen sind wichtig, denn um die Innere Sicherheit kümmern sich mehrere Akteure. Auf der einen Seite sind das die Polizei und Sicherheitsbehörden des Freistaats. Dazu kommen unsere Kommunen mit ihren Ordnungsämtern und ihrem gemeindlichen

Vollzugsdienst, die eine wichtige Rolle spielen. Nur wenn alle Akteure und Stellen Hand in Hand vertrauensvoll zusammenarbeiten können, werden die Innere Sicherheit und das Sicherheitsgefühl der Menschen im Freistaat Sachsen bewahrt und weiter gestärkt. Kurz gesagt: Sicherheit muss »sichtbar« sein.

Gute Gesetze sind die Basis erfolgreicher Zusammenarbeit. Denn durch sie wird klar definiert, welche Stelle wann zuständig ist, welche Rechte und Befugnisse sie zur Erfüllung ihrer Aufgaben hat und welche Rolle anderen Behörden hierbei zukommt. Das Polizeigesetz des Freistaates Sachsen von 1991 war auch unter diesem Aspekt dringend zu überarbeiten.

Novellierung war überfällig

Es sprach eine Reihe von Gründen dafür, das derzeit noch geltende Polizeigesetz im Jahr 2019 umfassend weiterzuentwickeln. Die letzte größere Novellierung war 1999. Seither hat sich die Welt weitergedreht. Dank des technischen Fortschritts sind wir alle – und damit auch Straftäter – mobiler geworden. So gibt es neue Kriminalitätsphänomene wie beispielsweise Cyberkriminalität. Auch haben sich die Gefährdungslagen verändert, Stichwort Terrorismus und politisch motivierte Kriminalität. Deswegen galt es, dem Polizeivollzugsdienst zur Gefahrenabwehr und vorbeugenden Verbrechensbekämpfung zeitgemäße Instrumente an die Hand zu geben und in der Praxis festgestellte Regelungslücken zu schließen. Aber auch ein neues europäisches Datenschutzrecht und die Harmonisierung des sächsischen Polizeigesetzes mit den Polizeigesetzen der anderen Bundesländer machten eine grundsätzliche Novellierung notwendig.

Zudem sollte das sächsische Polizeirecht im Sinne einer gemeinsamen Verantwortung des Freistaates und der Kommunen eine neue Struktur erhalten. Nach dem Vorbild anderer Bundesländer wird es künftig in Sachsen für den Polizeivollzugsdienst und die allgemeinen Polizeibehörden jeweils eigenständige Gesetze geben, nämlich das Sächsische Polizeivollzugsdienstgesetz und das Sächsische Polizeibehördengesetz. Dadurch werden für beide Bereiche transparente und anwenderfreundliche Gesetze geschaffen, in denen jeweils Aufgaben, Befugnisse, Organisation und die Regeln der Datenverarbeitung maßgeschneidert für die jeweiligen Behörden bestimmt werden. Damit werden die jeweiligen Aufgabenkreise klar und praxisgerecht voneinander abgegrenzt und Parallelzuständigkeiten nur in sachlich begründeten Fällen beibehalten.

Beteiligung von Anfang an

Für die SPD-Fraktion stand von Anfang an fest, dass die Diskussion um ein modernes und praxisorientiertes Polizeirecht nicht vom grünen Tisch aus geführt werden durfte. Mir als innenpolitischem Sprecher war es sehr wichtig, mit Vertreterinnen und Vertretern aus den verschiedensten Bereichen ins Gespräch zu kommen, um deren vielfältige – und sich mitunter auch deutlich widersprechenden – Perspektiven kennen zu lernen. Polizeivollzugsbedienstete haben uns aus ihrer tagtäglichen Arbeit berichtet und davon, welche Verbesserungen sie sich von einem neuen Polizeigesetz erhoffen. Ich konnte in die Diskussion auch eigene Erfahrungen einbringen, denn als Kriminaloberkommissar weiß ich, wie wichtig klare gesetzliche Grundlagen für die Polizeiarbeit sind.

Wir haben aber auch mit vielen Bürgerinnen und Bürgern sowie Akteuren der Zivilgesellschaft gesprochen, sowohl über deren Sorgen um die Sicherheit als auch über deren Bedenken zu neuen bzw. weitergehenden Befugnissen für Polizei und Polizeibehörden. Zudem hat die SPD-Landtagsfraktion auf zwei »Blaulichtkonferenzen« mit vielen Praktikern unter anderem darüber diskutiert, welche Rolle die Polizei in einer demokratischen Bürgergesellschaft hat und wie es um die Zusammenarbeit von Behörden mit Sicherheitsaufgaben steht. Mit Abgeordneten aus anderen Landtagen und dem Bundestag habe ich über deren Erfahrungen mit ihren eigenen Polizeigesetzen diskutiert, mit dem Sächsischen Landesdatenschutzbeauftragten darüber, wie eine effektive und gleichzeitig für die Polizeibehörden handhabbare datenschutzrechtliche Kontrolle aussehen sollte.

Und natürlich war uns das Wort, waren uns die Vorschläge, Anregungen und Forderungen unserer Kommunen sehr wichtig. Besonders in Erinnerung geblieben sind mir hierbei zwei Vor-Ort-Termine in der Stadt Wurzen, wo ich mit Oberbürgermeister Jörg Röglin und einem Vertreter des Ordnungsamts unter anderem bei einer Stadtbegehung über Sicherheitsthemen und Handlungsbedarfe gesprochen habe. Eine große Rolle haben hier beispielsweise die Voraussetzungen für kommunale Videoüberwachung, die Zusammenarbeit zwischen Landespolizei und dem Ordnungsamt sowie die Rolle von Bürgerpolizisten gespielt.

In der Rückschau auf diese vielen Gespräche bin ich der Ansicht, dass das am 10. April 2019 vom Landtag verabschiedete Gesetz zur Neustrukturierung des Polizeirechts eine sehr gute Basis für die künftige Arbeit der sächsischen Polizeibehörden ist. Denn das Gesetz bringt die Sicherheitsinteressen in ein ausgewogenes Verhältnis zu den Freiheitsrechten der Bürgerinnen und Bürger.

Adressatengerecht: Die Gesetze im Einzelnen

Durch das Gesetz zur Neustrukturierung des sächsischen Polizeirechts wurden zahlreiche Landesgesetze geändert. Neben dem neuen Sächsischen Datenschutz-Umsetzungsgesetz (SächsDSUG) sind für die Sicherheitsbehörden des Landes und die Polizeibehörden vor allem folgende beiden Gesetze von Relevanz: Das Sächsische Polizeivollzugsdienstgesetz (SächsPVDG) und das Sächsische Polizeibehördengesetz (SächsPBG).

Für die Landespolizei: Das Polizeivollzugsdienstgesetz

Das neue Polizeivollzugsdienstgesetz liefert eine moderne Handlungsgrundlage für die sächsische Landespolizei, das die Balance zwischen Freiheit und Sicherheit wahrt. Einerseits gibt es dem Polizeivollzugsdienst angesichts neuer technischer Herausforderungen sowie neuer bzw. sich verändernder Kriminalitätsphänomene angemessene und effektive Eingriffsbefugnisse. Gleichzeitig stellt das Gesetz sicher, dass das polizeiliche Handeln einer gesellschaftlichen Transparenz und wirksamen Kontrolle unterliegt. Der Staat muss in begründeten Fällen in die Grundrechte seiner Bürgerinnen und Bürger eingreifen dürfen. Aber dies muss mit möglichst offenem Visier geschehen und gerichtlich überprüfbar sein.

So wird im neuen Polizeivollzugsdienstgesetz die 2016 auf Forderung der SPD hin eingeführte Vertrauens- und Beschwerdestelle erstmals im

Gesetz verankert. Die Stelle ist unabhängig und wird künftig – außerhalb der Polizeistrukturen – bei der Staatskanzlei angesiedelt. Polizeibediensteten wird es zudem künftig erleichtert, sich an die Beschwerdestelle zu wenden: Die Verpflichtung, den Dienstweg einzuhalten, wird aufgehoben.

Außerdem wird die parlamentarische Kontrolle der Polizeiarbeit erweitert: Landespolizei und Staatsregierung müssen häufiger dem Landtag berichten. Und die mit dem Gesetz neu eingeführten Befugnisse müssen von externen Stellen evaluiert werden. Zudem sind die Speicherfristen für personenbezogene Daten vereinheitlicht und verkürzt worden. Der Sächsische Datenschutzbeauftragte erhält überdies mehr Kontrollrechte.

Nicht durchsetzen konnte sich die SPD mit der Einführung einer anonymisierten Kennzeichnungspflicht für Polizeivollzugsbeamte. Unserer Auffassung nach könnte eine solche Kennzeichnungspflicht entscheidend dazu beitragen, das Vertrauen in die Polizei zu stärken. Denn das mögliche Fehlverhalten einiger weniger Polizeivollzugsbediensteter wäre konkret zuzuordnen und könnte aufgearbeitet werden – ohne die Polizei unter Generalverdacht zu stellen.

Für die Kommunen: Das Polizeibehördengesetz

Die Polizeibehörden haben nach dem Polizeibehördengesetz ebenfalls die Aufgabe, für Sicherheit und Ordnung im Rahmen ihrer Zuständigkeit zu sorgen. Die vorbeugende Bekämpfung von Straftaten wird durch die Novelle aber allein dem Polizeivollzugsdienst zugewiesen. Bei der Aufgabe der Gefahrenabwehr wird der Schwerpunkt auf die Verhütung von Ordnungswidrigkeiten gelegt.

Abschnitt 1 des Polizeibehördengesetzes enthält Regelungen zu den Aufgaben sowie allgemeine Bestimmungen, wobei beispielsweise mit § 3 SächsPBG eine neue Vorschrift mit polizeirechtlich relevanten Begriffsdefinitionen geschaffen wird, indem dort die betreffende Vorschrift des § 4 SächsPVDG entsprechend anwendbar erklärt wird. Definiert werden unter anderem der Begriff der öffentlichen Sicherheit, der öffentlichen Ordnung sowie diverse Gefahrenstufen. Und es wird erläutert, was unter Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung zu verstehen ist.

Abschnitt 2 enthält Regelungen zu Maßnahmen, während die gesetzlichen Grundlagen für Polizeiverordnungen künftig in Abschnitt 3 geregelt werden. Relevante Änderungen ergeben sich beispielsweise bezüglich der Ermächtigung zum Erlass örtlich und zeitlich begrenzter Alkoholkonsumverbote, deren Voraussetzungen künftig in § 33 SächsPBG geregelt werden. Die Vorschrift des § 9 a SächsPolG wurde in mehreren Punkten überarbeitet, um die in der Vergangenheit aufgetretenen Anwendungsprobleme bei dem Erlass von Alkoholkonsumverboten zu beheben – ein Thema, auf das uns die Kommunen in vielen Gesprächen immer wieder aufmerksam gemacht haben.

So wird im neuen § 33 Absatz 1 SächsPBG eine spezielle Rechtsgrundlage für Alkoholkonsumverbote zum Zwecke des Kinder- und Jugendschutzes eingeführt. Insbesondere in der Nähe von Einrichtungen wie Schulen, Kindertagesstätten und Spielplätzen kann künftig der Konsum von Alkohol verboten werden – wenn dafür auf Grund der örtlichen Situation Bedarf besteht. Das Verbot darf sich örtlich höchstens auf einen Bereich von 100 Metern um die Einrichtung erstrecken, wobei von den Grundstücksecken aus gerechnet wird und keine Bereiche erfasst werden dürfen, die nach Gaststättenrecht konzessioniert sind (»außerhalb zugelassener Außenbewirtschaftungsflächen«).

Auch die Rechtsgrundlage des § 9 a Absatz 1 SächsPolG wurde überarbeitet. Bislang mussten Tatsachen die Annahme rechtfertigen, dass sich im Verordnungsgebiet Personen aufhalten, die bestimmte alkoholbedingte Straftaten (in dem betreffenden Gebiet oder woanders) begangen hatten, und angenommen werden können, dass sie solche Straftaten auch künftig begehen werden. Der neue Absatz 2 bestimmt nunmehr, dass es sich um einen Bereich handeln muss, bei dem eine auf Tatsachen beruhende Bewertung des fraglichen Gebietes dieses im Vergleich zum übrigen Gemeindegebiet als Problemschwerpunkt für alkoholbedingte Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung ausweist (Nummer 1) und bei dem Tatsachen die Annahme rechtfertigen, dass es sich auch künftig um einen örtlichen Problemschwerpunkt für entsprechende alkoholbedingte Verstöße handelt (Nummer 2). Auf die bisherige Vorgabe einer maximalen räumlichen Begrenzung des Verbotsgebiets auf »höchstens zwei Plätze und drei Straßen« wurde verzichtet, da sie sich in der Praxis nicht bewährt hat. Das Verbot soll auf bestimmte Tage innerhalb einer Woche und an diesen zeitlich befristet erlassen werden. Die maximale Geltungsdauer der Polizeiverordnung liegt nunmehr bei zwei Jahren anstatt wie bisher bei einem Jahr. Wie bisher auch werden Ausnahmen für den Einzelfall zugelassen.

Alle diese Änderungen im Bereich der Alkoholkonsumverbotsverordnungen sollen den Kommunen den Umgang mit diesem ordnungspolitisch wichtigen Instrument erleichtern. Die vielen Rückmeldungen aus der Praxis in den letzten Jahren hatten hier eindeutig Handlungsbedarf gezeigt. Ich bin sehr zuversichtlich, dass die neuen Regelungen für die Kommunen besser und einfacher handhabbar sein werden.

Die Kreisebene bleibt beim Vollzugsdienst außen vor

Auch in anderen Bereichen wurden Vorschläge der Kommunen aufgegriffen und der Gesetzentwurf geändert. So war zu einem frühen Zeitpunkt geplant, im Polizeibehördengesetz eine Befugnis für die Kreispolizeibehörden vorzusehen, dass diese zum Vollzug kreispolizeibehördlicher Aufgaben und zur Hilfestellung für kleinere Kommunen eigene Vollzugsbedienstete bestellen können. Die Rückmeldungen der kommunalen Ebene, insbesondere vom Sächsischen Landkreistag, haben jedoch ergeben, dass hierfür kein praktischer Bedarf gesehen wird.

Infolge der Anhörung und auch nach Anregungen der kommunalen Ebene konnten wir auch die Voraussetzungen für die kommunale Videoüberwachung im öffentlichen Raum konkretisieren und damit anwenderfreundlicher gestalten. Gleichzeitig haben wir die Speicherfrist für die erfassten Daten europarechtskonform auf einen Monat verkürzt.

Es gab auch Vorschläge und Anregungen der kommunalen Ebene, die zwar diskutiert wurden, aber dennoch keinen Eingang in die Polizeirechtsnovelle fanden. So war beispielsweise im Bereich der Alkoholkonsumverbotsverordnungen angeregt worden, deren maximale Geltungsdauer auf fünf Jahre auszudehnen. In Gesamtschau aller vorgesehenen Anpassungen in § 33 SächsPBG erschien es jedoch sachgerecht, eine Höchstbefristungsdauer von zwei Jahren vorzusehen. Denn dieser

Zeitraum stellt einen sinnvollen Ausgleich zwischen einer übermäßigen Belastung der Gemeindeverwaltung einerseits und der andererseits in angemessenen Zeiträumen gebotenen Überprüfung dar, ob weiterhin tatsächlicher Bedarf für das Alkoholkonsumverbot besteht.

Vom Weisungsrecht zur Kooperation

In der Debatte zum Gesetz wurde unter anderem kritisch angemerkt, dass das Weisungsrecht der Kreis- und Ortspolizeibehörden gegenüber dem Polizeivollzugsdienst abgeschafft werden sollte (wie es bislang in § 75 SächsPolG enthalten ist). Die an die Stelle des Weisungsrechts tretende Pflicht zur Zusammenarbeit und der gegenseitigen Unterrichtung zwischen den Polizeibehörden und dem Polizeivollzugsdienst wurde von der kommunalen Ebene als Verschlechterung im Vergleich zur gegenwärtigen Rechtslage und damit als unzureichend empfunden.

Die SPD-Fraktion im Sächsischen Landtag und ich als zuständiger Fachsprecher haben uns daher im parlamentarischen Verfahren dafür eingesetzt, das Weisungsrecht beizubehalten. Im Ergebnis der Verhandlungen mit unserem Koalitionspartner haben wir dieses Ziel zwar nicht 1:1 erreichen können. Aber es wurden durch den Änderungsantrag der Koalitionsfraktionen klarstellende Ergänzungen in § 4 SächsPBG vorgenommen. Neben der neuen Überschrift »Zusammenarbeit mit dem Polizeivollzugsdienst« wurde § 4 Absatz 1 um einen weiteren Satz dahingehend ergänzt, dass unbeschadet der Zuständigkeit der Polizei zur vorbeugenden Bekämpfung von Straftaten die Polizei und die Polizeibehörden im Rahmen der Gefahrenabwehr zusammenwirken und zur Vermeidung strafbarer Verhaltensweisen (Kriminalprävention) beitragen sollen. Zudem wurde in § 37 SächsPVDG ein neuer Absatz 2 eingefügt, der klarstellt, dass Vollzugshilfeersuchen der Polizeibehörden den Vollzugshilfeersuchen anderer Behörden grundsätzlich vorgehen und damit eine Priorisierung der betreffenden Vollzugshilfeersuchen erreicht.

Großveranstaltungen bleiben Baustelle

Letztlich nicht umgesetzt werden konnte der Vorschlag des Sächsischen Städte- und Gemeindetags zur Einführung einer Anzeige- bzw. Erlaubnispflicht bei öffentlichen Veranstaltungen mit mehr als 1.000 Besuchern und – damit verbunden – einer Pflicht zur Vorlage eines Sicherheitskonzepts. Auch die SPD-Fraktion teilt diese Ansicht der kommunalen Ebene – im Gegensatz zur CDU, die die Einführung einer praxisgerechten Lösung verhindert hat. Da jedoch davon auszugehen ist, dass das Thema weiter aktuell bleiben wird und andere Bundesländer hier bereits rechtliche Regelungen getroffen haben, die als Diskussionsgrundlage dienen können, wird die SPD dieses Thema weiter verfolgen. Dies gilt genauso in den übrigen Bereichen, in denen wir unsere Vorstellungen nicht vollumfänglich umsetzen konnten.

Unterm Strich

In der Gesamtbetrachtung ist die Polizeirechtsnovelle eines der bedeutendsten Gesetzgebungsvorhaben, das die Koalition im Landtag umgesetzt hat. Es war ein fachlich interessanter und politisch anspruchsvoller Prozess. Wir mussten mit unserem Koalitionspartner um viele Themen und Formulierungen hart ringen. Viele Punkte haben sich ergänzt. An einigen Stellen hat die Koalition Kompromisse geschlossen. Im Ergebnis haben wir das Polizeirecht in Sachsen praxisgerecht modernisiert. Das wird sich dann auch praktisch zeigen, wenn das Gesetz zum 1. Januar 2020 in Kraft tritt.

Für die SPD war die politische Hauptaufgabe, Transparenz und Kontrolle der Arbeit der Sicherheitsbehörden durch die Öffentlichkeit und den Landtag zu stärken sowie die Bürgerrechte in ein gutes Verhältnis zu den Sicherheitsinteressen zu bringen. Gleichzeitig wollten wir nach den gelösten Personal- und Ausstattungsfragen bei der Polizei den Sicherheitsbehörden moderne und wirksame Instrumente zur polizeilichen und ordnungsbehördlichen Gefahrenabwehr an die Hand geben. Somit ist das Gesetz zur Neustrukturierung des Polizeirechts im Freistaat Sachsen aus Sicht der SPD ein weiterer wichtiger Baustein für handlungsfähigere Sicherheitsbehörden und eine verbesserte Innere Sicherheit in allen Regionen des Freistaates Sachsen.

Herausforderungen bei der Cyber-Abwehr und der Informationssicherheit in Staat und Verwaltung

Thomas Popp
Amtschef der Sächsischen Staatskanzlei
und CIO des Freistaats Sachsen

Foto: ©Matthias Rietschel

Zu Beginn dieses Jahres war Cybersicherheit wieder einmal in aller Munde, nachdem personenbezogene Daten von Politikern und Mandatsträgern unrechtmäßig ins Netz gelangten. Experten, die sich tagtäglich mit der Informationssicherheit in Staat und Verwaltung beschäftigen, wissen, dass die Bedrohungslage im Cyberraum schon seit mehreren Jahren angespannt ist. Und dies permanent und mit Attacken, die weit weniger öffentlichkeitswirksam, aber keinen Deut weniger bedrohlich sind.

Bezogen auf das Sächsische Verwaltungsnetz untermauern Zahlen aus dem Jahr 2018 diese Situation eindrucksvoll: Unsere Sicherheitssysteme haben knapp 80 Millionen Spam-Mails abgewiesen. Gegenüber 2017 bedeutet dies eine Steigerung von über 60 Prozent. Im Internetverkehr wurden über 35.000 Viren erkannt, was einer Steigerung um 44 Prozent im Vergleich zum Vorjahr entspricht. Rund 100.000 Viren haben unsere Sicherheitssysteme im behördlichen E-Mail-Verkehr erkannt. Allein im November sahen wir uns mit so vielen Schadcodes in E-Mails konfrontiert wie im gesamten Vorjahr. Am Ende des Jahres hatten wir 170 Prozent mehr Aufkommen als noch im Jahr 2017.

Die Bedrohungslage hat sich also noch einmal verschärft. Dabei stehen wir nicht einmal im besonderen Fokus der Angreifer. Attacken, die zielgerichtet nur uns galten, haben wir bislang nicht registriert. Und so stellt sich nicht nur die Öffentlichkeit berechtigterweise die Frage: Was können wir dagegen tun? Schließlich sollen die Bürger der Verwaltung ihre Daten mitteilen. Un wenn ein Bürger die Pflicht hat, der Verwaltung seine Daten mitzuteilen, dann hat die Verwaltung die Pflicht, diese Daten zu schützen.

Das unberechtigte Abfließen von staatlichen oder kommunalen Informationen stellt neben der Verletzung des Rechts auf informationelle Selbstbestimmung einer Person auch ein Risiko für die administrative Grundordnung des Staates dar. Daraus erwachsen grundrechtliche Schutzpflichten des Staates, die mit konkreten Maßnahmen zu gewährleisten sind. Mit dem Gesetz zur Neuordnung der Informationssicherheit in Sachsen, das noch vor der Sommerpause vom Sächsischen Landtag beschlossen wurde, reagiert der Freistaat auf diese Herausforderungen.

Das Sächsische Informationssicherheitsgesetz verbindet technische und organisatorische Umsetzungsmaßnahmen und rechtliche Regelungen. Das erste Ziel, das erreicht werden soll: Wir müssen einen viel umfassenderen Einblick erhalten, was in den IT-Systemen der Verwaltungen passiert. So ist vorgesehen, dass die zentralen Stellen der IT-Sicherheit genauer und umfassender als bisher die Datenströme in den Verwaltungen auf gefährliche Inhalte untersuchen und auswerten. Nur so lassen sich die Schutzmaßnahmen wirkungsvoller ausrichten. Hierfür braucht es eine Rechtsgrundlage, weil z. B. E-Mails auch personenbezogene Daten enthalten können bzw. nur noch verschlüsselt ausgetauscht werden. Wir müssen aber unter Wahrung der informationellen Selbstbestimmung des Einzelnen dennoch die Erlaubnis haben E-Mails zu analysieren, um einen wirkungsvollen Schutz aufrecht zu erhalten. Das Gesetz schafft daher Ermächtigungen für alle Behörden im Freistaat, moderne Erkennungs- und Abwehrtechnologien einzusetzen, damit zu jedem Zeitpunkt ein hochaktuelles Gefahrenabwehrsystem besteht.

Das zweite Ziel ist die Stärkung der Sicherheitsorganisation, die strategisch und operativ mit ausreichenden Handlungskompetenzen ausgestattet wird. Wir haben in Sachsen ein zentrales Computernotfallteam, das SAX.CERT im Sächsischen Staatsbetrieb für Informatikdienste. Das ist als IT-Dienstleister direkt der Staatskanzlei unterstellt. Wir werden das SAX.CERT nicht nur mit den notwendigen Kompetenzen, sondern auch dem Personal ausstatten, damit es die wachsende Zahl an Aufgaben bewältigen kann. Zudem wird das SAX.CERT eine Servicestelle auch für den kommunalen Bereich darstellen, der dringend Unterstützung benötigt.

Das Gesetz erleichtert den personellen Aufwuchs im Bereich der Informationssicherheit. Wir wollen in allen Ressorts und den IT-Behörden einen festen Sicherheitsbeauftragten installieren, damit wir in der obersten Landesverwaltung ein einheitliches Sicherheitsniveau erreichen. Zugleich stellt das Gesetz heraus, dass jeder einzelne Mitarbeiter jeder Behörde zu sensibilisieren und zu schulen ist. Dafür haben wir seit langem Angebote, wie z. B. Hacker-Shows, an denen seit 2012 über 12.000 Mitarbeiter teilgenommen haben. Ein weiterer Baustein ist ein E-Learning-Angebot zur Informationssicherheit.

Mit dem Gesetz zur Gewährleistung der Informationssicherheit in Sachsen haben wir aus meiner Sicht im Vergleich zu anderen Ländern einen umfassenderen Ansatz gewählt, der auch noch in fünf Jahren eine hohe Wirkkraft haben wird. Davon bin ich überzeugt. Diese Wirkkraft brauchen wir, brauchen Staat und Verwaltung auch, wenn wir gestalten wollen statt getrieben zu werden.

Das neue Sächsische Informationssicherheitsgesetz

Die Zustimmung der Mehrheit der Abgeordneten des Sächsischen Landtags zum Entwurf des Gesetzes zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (SächsISichG) am 3. Juli ist nichts weniger als ein Meilenstein für die IT-Sicherheit in der öffentlichen Verwaltung. Mit Inkrafttreten wird das neue Gesetz die dann fast auf den Tag genau acht Jahre gültige Verwaltungsvorschrift zur Gewährleistung der Informationssicherheit ersetzen.

Das regelt das neue Sächsische Informationssicherheitsgesetz

Mit dem Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (SächsISichG) werden

- die bisherigen Verwaltungsvorschriften zur Informationssicherheit sowie die entsprechenden Regelungen im Sächsischen E-Government-Gesetz (SächsEGovG) zusammengefasst und erheblich erweitert,
- u.a. die Gerichte, Hochschulen und die Kommunen in den Anwendungsbereich einbezogen, die Befugnisse der Beauftragten für Informationssicherheit (BfIS) und des Sicherheitsnotfallteams (SAX.CERT) ausgeweitet,
- Rechtsgrundlagen für den zulässigen Einsatz moderner Erkennungs- und Abwehrtechnologien geschaffen und
- verschiedene Meldepflichten über Sicherheitsvorfälle eingeführt.

Was regelt das Gesetz im Detail? Abschnitt 1: Allgemeine Vorschriften (§§ 1–4)

Unter den Anwendungsbereich (§ 2) fallen die Behörden und Gerichte des Freistaates Sachsen als staatliche Stellen sowie die seiner Aufsicht unterliegenden Körperschaften (sprich: die Kommunen), Anstalten und Stiftungen des öffentlichen Rechts als nicht-staatliche Stellen. Für Beliehene gilt das Gesetz nur, soweit sie an das Sächsische Verwaltungsnetz oder Kommunale Datennetz angeschlossen sind. Durch die Einbeziehung der Gerichte ist der Anwendungsbereich weiter als im SächsEGovG. Bezogen auf die Grundsätze der Informationssicherheit (§ 4) wurden im Wesentlichen die bestehenden Regelungen aus dem SächsEGovG übernommen. Danach müssen die staatlichen Stellen angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zur Einhaltung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit für die in ihren informationstechnischen Systemen verarbeiteten Daten treffen. Die BSI-Standards in Verbindung mit dem BSI-Grundschutz sind zu berücksichtigen. Neu ist hingegen, dass für technische Maßnahmen der Stand der Technik maßgeblich sein soll. Außerdem sollen die staatlichen Stellen ein Informationssicherheitsmanagementsystem (ISMS) erstellen. Die Absicherung eines angemessenen Informationssicherheitsniveaus wird auch für die nicht-staatlichen Stellen, also auch kommunalen Träger der Selbstverwaltung vorgeschrieben. Das entspricht jedoch den Regelungen im derzeit gültigen SächsEGovG und beinhaltet keine neuen Verpflichtungen.

Abschnitt 2: Organisation der Informationssicherheit (§§ 5–10)

Die Informationssicherheitsorganisation hat sich im staatlichen Bereich bereits etabliert und wird beibehalten. Sie wird durch das SächsISichG nunmehr auf eine gesetzliche Grundlage gestellt. Der Freistaat Sachsen hat bereits seit 2011 entsprechend den Vorgaben des IT-Planungsrates einen Beauftragten für Informationssicherheit des Landes, der weiterhin die zentrale Stelle für die Informationssicherheit im Freistaat Sachsen inne hat. Das Sicherheitsnotfallteam (SAX.CERT) wird die zentrale Stelle für operative Fragen der Informationssicherheit aller staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen. Sein Aufgabenbereich wird erweitert u.a. um die Erfassung und Analyse von Sicherheitsgefährdungen, um ein aktuelles Bild der Sicherheitslage im Freistaat zu erstellen. Das SAX.CERT wird außerdem zentrale Meldestelle nach dem BSI-Gesetz und im Verwaltungs-CERT-Verbund, aber auch für Sicherheitsvorfälle in den staatlichen oder nicht-staatlichen Stellen. Außerdem stehen sowohl das SAX.CERT und der BfIS Land den nicht-staatlichen Stellen, wie u.a. den Kommunen, beratend zur Verfügung. Neben dem BfIS Land erhält auch das SAX.CERT Befugnisse, nötige Anordnungen zu treffen oder erforderliche Maßnahmen zur Abwehr von Gefahren für die Informationssicherheit zu ergreifen. In den staatlichen Stellen sind Beauftragte für Informationssicherheit verpflichtend zu ernennen. Aufgrund der besonderen Stellung in der Landesverwaltung sollen in bestimmten staatlichen Stellen wie Staatsministerien, oder dem Staatsbetrieb Sächsische Informatik Dienste, ein hauptamtlicher BfIS eingesetzt werden. Nicht-staatliche Stellen sollen ebenfalls eine Informationssicherheitsorganisation aufbauen. Dabei können kleine nicht-staatliche Stellen flexibel agieren: Sie dürfen einen gemeinsamen Beauftragten ernennen oder die Aufgabe an Externe übertragen. Die Arbeitsgruppe Informationssicherheit (AG IS) hat sich als beratendes Gremium bewährt. Daher berät es den BfIS Land weiterhin und empfiehlt Maßnahmen zur Sicherstellung angemessener Informationssicherheit. Dabei sichern zwei Vertreter der Kommunen in der AG IS die Vertretung der nicht-staatlichen Behörden.

Abschnitt 3: Maßnahmen zur Sicherstellung der Informationssicherheit (§§ 11–14)

Für den Schutz der Verwaltungsnetze bedarf es u.a. einer Analyse des Datenverkehrs insbesondere am Übergang zum Internet. Das Gesetz schafft Rechtsgrundlagen, wonach Daten, die beim Betrieb von informationstechnischen Systemen der staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen anfallen, durch diese erhoben und automatisiert ausgewertet werden dürfen, soweit dies zur Verhinderung oder Abwehr von Angriffen auf die informationstechnischen Systeme erforderlich ist. Auch werden Rechtsgrundlagen geschaffen, die es ermöglichen, Datenströme nachzuverfolgen, wenn Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung festgestellt wird. Dabei orientieren sich die Regelungen an vorhandenen Vorschriften im BSI-Gesetz und an Gesetzen bzw. -entwürfen zum Thema Informationssicherheit anderer Bundesländer.

Abschnitt 4: Meldepflichten (§§ 15–17)

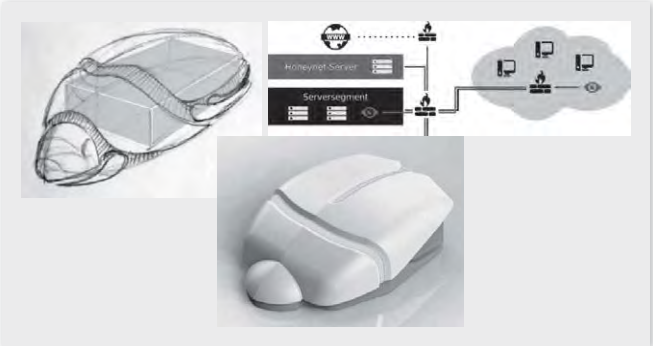
Ein wirksamer Schutz vor Angriffen ist nur möglich, wenn allgemeine Gefährdungen sowie die eigene konkrete Gefährdungslage im Überblick bekannt sind. Daher werden in Abschnitt 4 behördenübergreifende Meldepflichten sowie Meldepflichten der staatlichen und nicht-staatlichen Stellen geregelt.

Abschnitt 5: Schlussvorschriften (§§ 18–21)

Die Schlussvorschriften enthalten den notwendigen Hinweis auf die Einschränkung von Grundrechten gemäß dem Zitiergebot, eine Experimentierklausel und eine Vorschrift zur Evaluierung. Das Gesetz enthält zudem Übergangsfristen bis zur vollständigen Wirksamkeit des Gesetzes, um erforderliche technische und organisatorische Umsetzungsschritte zu gewährleisten.

SAX.CERT – Das gemeinsame Sicherheitsnotfallteam für Land und Kommunen

Christoph Damm
Leiter des Fachbereichs »CERT, Informationssicherheit« im Staatsbetrieb Sächsische Informatik Dienste (SID)



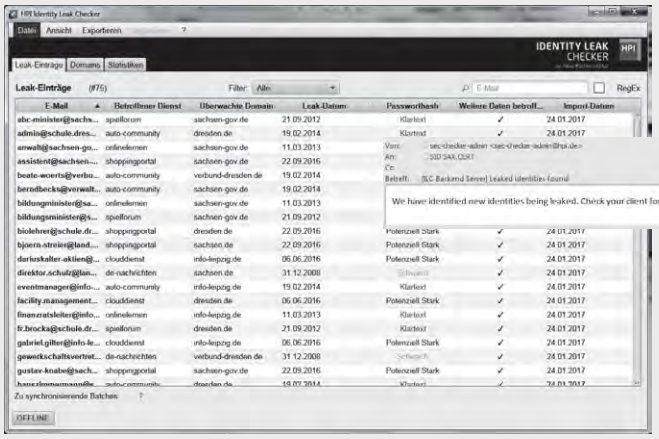
Mit der Verabschiedung der VwV Informationssicherheit im September 2011 als verbindliche Leitlinie für die Landesverwaltung Sachsen wurde neben anderen wichtigen Grundlagen auch erstmals der Aufbau eines zentralen Sicherheitsnotfallteams festgelegt. Dieses Sicherheitsnotfallteam – auf Englisch »Computer Emergency Response Team« oder kurz SAX.CERT – bekam damals die Aufgabe, das allgemeine Sicherheitsniveau in der Landesverwaltung zu erhöhen. Insbesondere sollte das SAX.CERT dazu beitragen, Schäden durch oder an IT-Systemen gar nicht erst entstehen zu lassen bzw. durch eine schnelle und kompetente Beratung den Schaden zu minimieren. Es ist seitdem die zentrale Anlaufstelle Sachsens zu Fragen der technischen Informationssicherheit sowohl für interne als auch für externe Ansprechpartner. Das gilt uneingeschränkt für alle Ressorts und Behörden der Landesverwaltung, aber bisher nur in Ausnahmefällen für kommunale Einrichtungen in Sachsen. Die bisher eingeschränkte Nutzbarkeit des SAX.CERT durch die Kommunen lag neben haushaltrechtlichen Gründen vorrangig an den seit seiner Einrichtung äußerst begrenzten personellen Ressourcen. Derzeit arbeiten im Sachgebiet SAX.CERT des SID insgesamt 3,5 Mitarbeiter (inkl. befristete und externe Stellen) in der Außenstelle Dresden-Glacisstraße. Trotz dieser Einschränkungen wurden und werden bereits jetzt zahlreiche Leistungen für die sächsischen Kommunen erbracht. Einige dieser vorhandenen Dienste und Leistungen sollen im Folgenden näher dargestellt werden. Anschließend soll auf die anstehenden Änderungen durch das neue Sächsische Informationssicherheitsgesetz eingegangen werden.

Hackerfalle HoneySens

Über dieses Projekt findet sich eine nähere Abhandlung in der vorliegenden aktuellen Ausgabe des Sachsenlandkuriers, so dass hier nur kurz darauf eingegangen werden soll. Wesentlich ist dabei das Verständnis der HoneySens-Sensoren als rein passive elektronische »Stolperdrähte« im inneren Netz, die zuverlässig unbekannte und ungewollte Datenverbindungen z. B. durch Schadsoftware und Hacker alarmieren. Die Sensoren benötigen dazu nur eine Netzwerkanbindung und einen Zugriff auf die zentrale Managementoberfläche, auf der die Alarme aller Sensoren zusammengefasst dargestellt werden und die die Sensoren mit notwendigen Konfigurationen und Updates versorgt. Für die Kommunen im KDN übernimmt das SAX.CERT den Betrieb von HoneySens kostenfrei, außerhalb des KDN ist unser Industriepartner T-Systems MMS dafür zuständig. Derzeit sind im kommunalen Bereich 10 Sensoren bei der KDN GmbH, der SAKD sowie in den Städten Radebeul, Freital und Markranstädt, aber auch in den Landratsämtern Meißen, Bautzen, Vogtlandkreis und Zwickau aktiv.

Identity Leak Checker

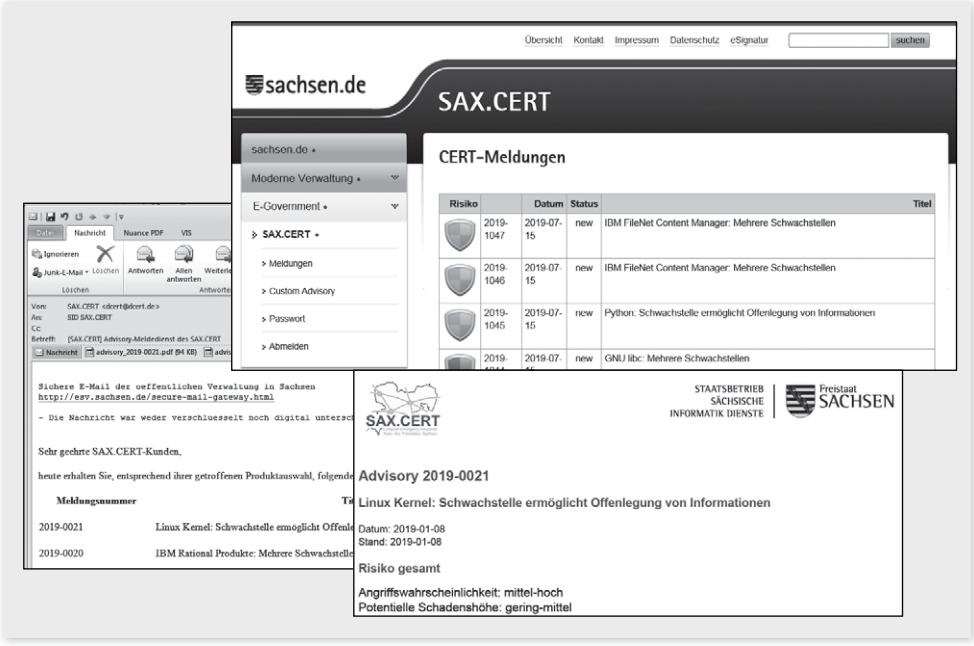
Nach einem aufsehenerregenden Fund von 18 Millionen gestohlenen Nutzernamen mit zugehörigen Passwörtern zahlreicher Internetdienste im Jahr 2014 startete der Freistaat Sachsen eine Zusammenarbeit mit dem Hasso Plattner Institut in Potsdam. Ziel war zukünftig schneller informiert zu werden, wenn gestohlene Identitätsdaten (»Leaks«) aus



dem Freistaat Sachsen im Internet zirkulieren. Im Ergebnis entstand der Identity Leak Checker Client mit derzeit über 9,5 Milliarden Datensätzen, der vom Hasso Plattner Institut gepflegt wird und das SAX.CERT warnt, wenn neue Leaks veröffentlicht werden. Inzwischen nutzen auch erste andere Bundesländer diesen Client, da es immer öfter zu solchen Leaks kommt und es in diesen Fällen wichtig ist, die eigene Betroffenheit schnell abschätzen zu können. In Sachsen nutzen auch erste kommunale Einrichtungen bereits diesen Dienst, z. B. die Stadtverwaltungen Leipzig, Dresden und Makranstädt sowie die Lecos, aber auch das Uniklinikum Dresden und die Landratsämter Meißen, Bautzen und Vogtlandkreis.

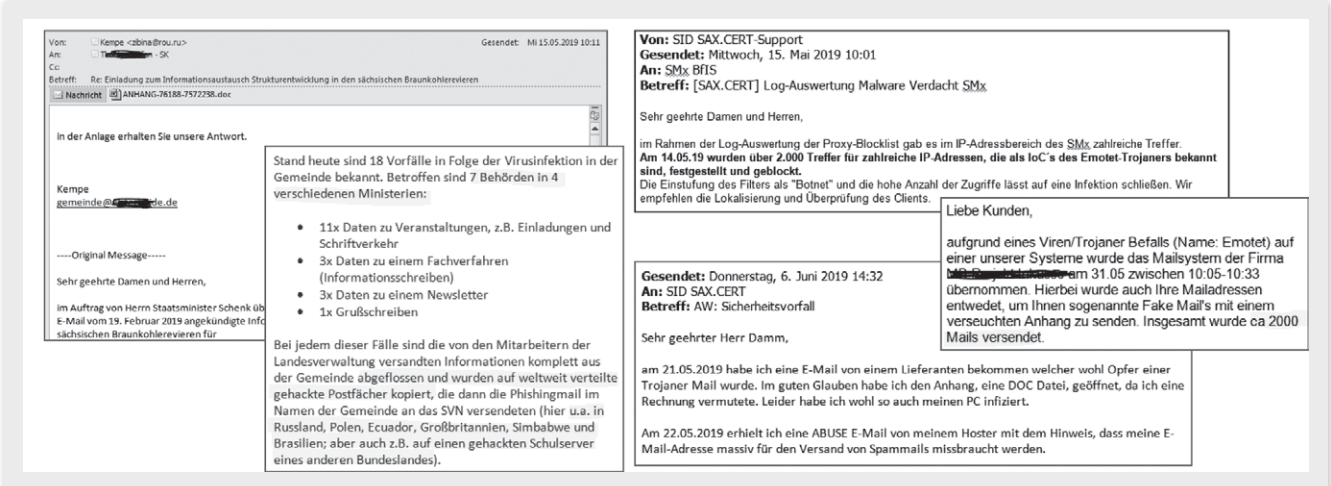
Webseitenscans

Nach einer aufwendigen Zusammenstellung von Listen der Internetseiten und -dienste des Landes Sachsens aus zahlreichen Quellen wie dem Behördenfinder von Amt24 wurden seit ca. 2014 in unregelmäßigen Abständen mehrfach Sicherheitsbewertungen (»Scans«) dieser Webseiten durchgeführt. Im Ergebnis der anfangs erschreckenden Zahlen – so mussten bei den ersten Erhebungen mehr als 75 % aller Landeswebseiten mit der schlechtesten Sicherheitsnote »F« bewertet werden – konnte inzwischen eine deutliche Verbesserung der Lage erreicht werden. Grundlage waren u. a. die nach 2014 erarbeiteten Beschlüsse und Handlungsempfehlungen zur Verbesserung der Webseitensicherheit, die auch Einzug in das Sächsische E-Government-Gesetz fanden. Seit Anfang 2018 finden diese Sicherheitserhebungen zu allen ca. 2.500 Landeswebseiten regelmäßig zweimal monatlich statt (Bewertung Integrität und Softwareaktualität der Webseiten). In den letzten Jahren wurden auch anlassbezogene Scans von kommunalen Webseiten durchgeführt, so z. B. der Scan aller Schulwebseiten Sachsens im Jahr 2015. Insgesamt wurde dabei jeweils noch deutlicher Nachholbedarf gegenüber den Landesseiten festgestellt. Das deckt sich auch mit den in den letzten Jahren bekannt gewordenen Sicherheitsvorfällen, wo Webseiten durch Hacker übernommen und entweder mit virtuellen »Graffities« überschrieben oder mit Schadsoftware und Hintertüren verseucht wurden. Fast alle dem SAX.CERT bisher bekannten gehackten Webseiten stammten dabei aus dem kommunalen Bereich. Das SAX.CERT bietet hier interessierten Kommunen an, deren Webseiten kostenfrei in das monatliche Monitoring der Landeswebseiten mit aufzunehmen. Erste Aufträge z. B. aus den Landratsämtern Meißen, Bautzen und Vogtlandkreis liegen vor.



Informationsdienst

Ein weiterer vom SAX.CERT für die Landesbehörden aufgebauter und angebotener Dienst ist der Warn- und Informationsdienst in Zusammenarbeit mit dem dCERT der Deutschen Telekom. Hier kann durch das SAX.CERT auch für mehrere Nutzer pro Behörde jeweils ein eigenes Nutzerkonto auf dem zentralen Warn- und Informations-Portal angelegt werden. Über das Portal kann dann jeder angelegte Nutzer für sich aus über 2.000 Hard- und Softwareprodukten von 185 Herstellern die ihn betreffenden Produkte auswählen. Wird zu einem von diesen Produkten eine neue Sicherheitslücke bekannt, versendet das Portal automatisch



eine Warn-E-Mail mit ausführlichen Details und Maßnahmenempfehlungen zu dieser Schwachstelle an den betreffenden Nutzer. Auch dieser Dienst ist kostenfrei und wird bereits von mehreren Kommunen genutzt, z. B. durch die Städte Chemnitz und Markranstädt sowie durch die Landratsämter Meißen, Erzgebirgskreis, Nordsachsen und Pirna.

Alle diese Dienste wurden bisher jedoch nur im Rahmen der begrenzten personellen Möglichkeiten des SAX.CERT angeboten, soweit sie keinen größeren Zusatzaufwand verursachten oder sich in den Rahmen von zeitlich befristeten Sicherheitsprojekten wie dem Schulseitenscan einordnen ließen. Eine Bekanntmachung im größeren Kreis war im bisherigen Rahmen nicht möglich. Mit dem neuen Sächsischen Informationssicherheitsgesetz soll sich das nun ändern.

Das neue Sächsische Informationssicherheitsgesetz

Nach dem Beschluss des Sächsischen Informationssicherheitsgesetzes am 3. Juli 2019 durch den Sächsischen Landtag werden die Verkündung und damit das In-Kraft-Treten des Gesetzes für August 2019 erwartet. Mit dem In-Kraft-Treten des Gesetzes werden durch viele Betroffene gerade auch aus dem kommunalen Bereich erhebliche Mehraufwände befürchtet. Dazu kommen teilweise noch Sorgen über zu weit gehende Eingriffsrechte durch das SAX.CERT in die internen Daten der einzelnen Einrichtungen sowie über intransparente Weitergabe dieser Daten an andere staatliche Organe. Diese Befürchtungen decken sich jedoch nicht mit den praktischen Erfahrungen des SAX.CERT aus den letzten Jahren. Im Gegenteil muss festgestellt werden, dass die Abwehr der bisherigen Bedrohungen ohne das neue Sächsische Informationssicherheitsgesetz leider zu oft aufgrund mangelnder gesetzlicher Grundlagen im Versuch steckenblieb und letztendlich nur mit viel Glück bisher wohl keine größeren Hackereinbrüche in das gemeinsame Netz des SVN und KDN erfolgt sind. Zur Verdeutlichung der bisherigen Lage vor dem neuen Sächsischen Informationssicherheitsgesetz soll im Folgenden ein aktuelles Beispiel aus der täglichen Arbeit des SAX.CERT beschrieben werden.

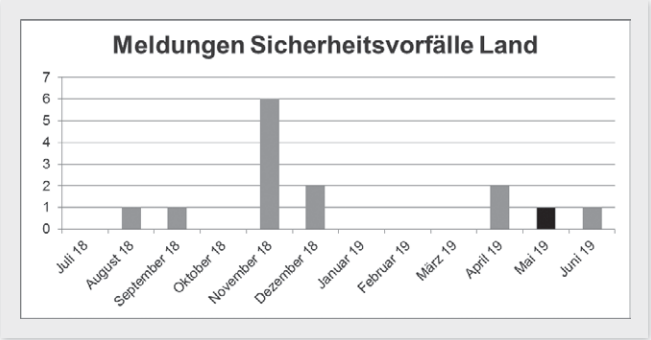
Datenabflüsse von Verwaltungsdaten

Seit längerem ist bekannt, dass das sehr weit verbreitete Schadprogramm Emotet (früher Feodo/Geodo) auf von ihm infizierten Computern das Mailpostfach bez. der Kommunikationspartner auswertet und die Ergebnisse der Analyse an seine Kontrollserver sendet. Im Ergebnis werden dann die Absendeadressen der nächsten Schad-E-Mails so gefälscht, dass der Empfänger einen jeweils zu ihm passenden Absender vorfindet und so leichter das mitgesandte Schadprogramm aktiviert. Solche E-Mails sind auch im SVN schon lange bekannt, meist aber wegen der eher unpassenden Texte doch als Fälschung zu erkennen. Etwa im Herbst 2018 wurde dann erstmals berichtet, dass das Emotet-Schadprogramm dazu übergegangen ist, nicht nur die Kommunikationsbeziehungen, sondern auch die E-Mail-Inhalte in den Postfächern der infizierten Computer auszuwerten und an seine Kontrollserver zu senden. Mitte April 2018 wurde das SAX.CERT erstmals aus dem kommunalen Bereich gewarnt, dass eine neuartige Schad-E-Mail im KDN beobachtet wurde. Diese enthielt nicht nur einen dem Empfänger bekannten (aber gefälschten) Absender, sondern bezog sich im Betreff und im Mailtext auf eine echte E-Mail des Empfängers, die in der Schad-E-Mail zitiert wurde. Ab Anfang Mai 2019 trafen dann auch aus dem Bereich des SVN täglich mehrere Anfragen bzgl. solcher Schad-E-Mails beim SAX.CERT ein.

Im Ergebnis der intensiven Auswertung von insgesamt 73 solcher E-Mails durch das SAX.CERT steht nun fest, dass jede einzelne dieser E-Mails auf eine Schadprogramminfektion des gefälschten Absenders zurückzuführen ist und dass in jedem einzelnen dieser 73 Fälle echte E-Mail-Inhalte der Landesverwaltung von dem Computer des gefälschten Absenders auf weltweit verteilte Schadsoftwareserver abgeflossen sind. Insgesamt sind in diesem Rahmen 25 gehackte Einrichtungen bekannt geworden, davon 16 KMUs, Kommunen und Einrichtungen in Sachsen. Alle diese Einrichtungen sind Kommunikationspartner der Landesverwaltung Sachsen und haben u. a. Daten aus der Kommunikation mit der Landesverwaltung verloren.

Ungenügende Meldungen von Sicherheitsvorfällen

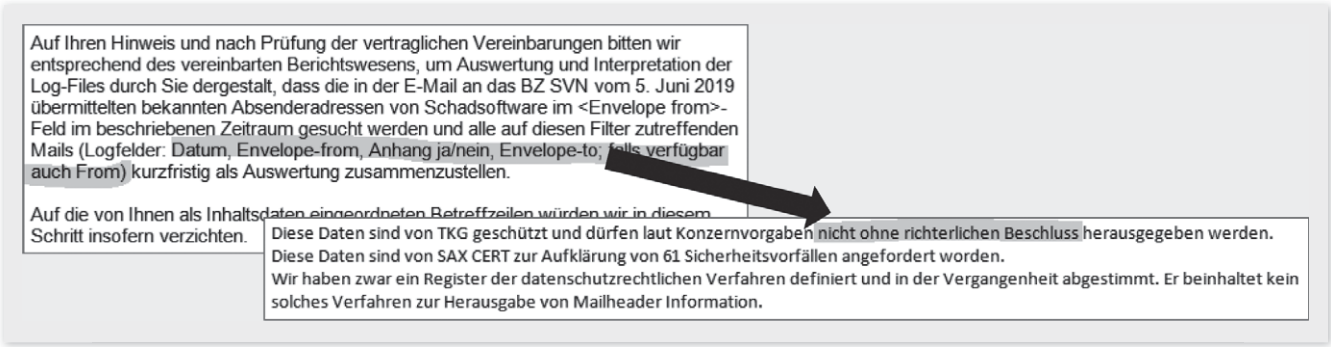
In der gesamten Zeit der beschriebenen Viruswelle im Mai 2019 wurde nur genau ein Sicherheitsvorfall über das offizielle Meldeformular des SAX.CERT gemeldet. Alle anderen Vorfälle sind erst durch Auswertung von E-Mails mit Virenverdacht durch das SAX.CERT festgestellt worden, wobei die Meldung seitens der Mitarbeiter in den Ressorts teilweise erst Wochen nach Eintreffen der Mail erfolgte.



Hier setzt die erste Neuerung des Sächsischen Informationssicherheitsgesetzes an: Die zeitnahe Meldung solcher Vorfälle an das SAX.CERT ist nun gesetzlich geregelt und vorgeschrieben – auch für die Kommunen. Damit kann das SAX.CERT viel schneller und besser als bisher den tatsächlichen Umfang solcher gefährlichen Virenausbrüche erkennen und Gegenmaßnahmen kurzfristig einleiten. Der (Mehr-)Aufwand für das Melden echter Sicherheitsvorfälle für den Einzelnen ist gering gegenüber der zukünftig auch für alle Kommunen verfügbaren dauerhaften Bereitstellung eines aktuellen – und realistischen! – Lagebilds und entsprechender Warnmeldungen durch das SAX.CERT.

Hindernisse bei der Log-Datei-Auswertung

Ein weiterer Ansatz für das Erkennen von Virenausbrüchen ist die Auswertung der Logdateien der Schutzsysteme in den zentralen Diensten des SVN. Aus diesen lässt sich z. B. einfach herauslesen, an welche Postfächer im SVN die gleichen Schad-E-Mails versandt wurden wie die an das SAX.CERT gemeldeten. Mit Hilfe der Eingangszeit der so identifizierten nicht gemeldeten Schad-E-Mails sowie deren Absender und Empfänger ließen sich dann die betroffenen Behörden warnen und die betroffenen Postfächer auf Schadsoftwarebefall prüfen. Eine entsprechende Nachfrage des SAX.CERT während der oben beschriebenen Virenwelle an den Betreiber der Schutzsysteme wurde aus Datenschutzgründen abgelehnt.



Letztendlich wurde nur übermittelt, dass 159 Schad-E-Mails mit gestohlenen echten Mail-Inhalten der Landesverwaltung von den gleichen bösartigen Absendern im SVN eingingen. Davon hatten 145 Mails eine Schadsoftware im Anhang, die nur in 36 Fällen von den zentralen Schutzsystemen erkannt wurde. Hier herrscht also nachweislich eine große Erkenntnislücke zwischen den Meldungen aus den Behörden und der tatsächlichen Lage bez. Informationssicherheits- und Datenschutzvorfällen. Zusätzlich zeigt sich die nachweislich hohe Gefährdung durch sehr dynamische Schadprogramme, die die zentralen Schutzsysteme oft umgehen können. Das Sächsische Informationssicherheitsgesetz schafft hier endlich die gesetzlichen Grundlagen, damit das SAX.CERT erstmals überhaupt ein realistisches, auf aussagekräftige Zahlen aus Log-Dateien gestütztes Lagebild erstellen kann. Auch bekommt das SAX.CERT durch die Auswertung der Log-Dateien erstmals überhaupt die Möglichkeit aktive Schadprogramme im SVN selbst zu identifizieren und bekämpfen zu können. Insofern ist die Vorstellung, die angeblich jetzt schon umfangreichen Überwachungsmöglichkeiten des SAX.CERT würden nun vollends in Richtung einer anlasslosen Totalüberwachung des Netzes ausgebaut, sehr weit von den praktischen Erfahrungen der CERT-Arbeit entfernt. Dennoch wurde im Rahmen der Gesetzesabstimmung auch auf solche Bedenken eingegangen, in dem das Sächsische Informationssicherheitsgesetz sehr weitgehende Berichtspflichten unter anderem zur Log-Datei-Auswertung regelt.

Ausblick

Insgesamt blickt das SAX.CERT dem In-Kraft-Treten des Sächsischen Informationssicherheitsgesetzes deshalb sehr positiv entgegen. Sobald die mit dem Gesetz verbundene Verstärkung des SAX.CERT um 3,5 zusätzliche Mitarbeiter auf dann insgesamt 7 Beschäftige umgesetzt ist, wird das Team dann endlich auch als zentrale Ansprechstelle für alle sächsischen Kommunen mit zur Verfügung stehen können. Weiterhin wird das SAX.CERT dann auch die zentrale Meldestelle für KRITIS-Unternehmen in Sachsen, von denen ja auch einige in kommunaler Hand sind. Aber auch schon jetzt steht das SAX.CERT gern im Rahmen seiner Möglichkeiten allen Kommunen in Sachsen zur Verfügung und bietet seine Dienste gern für diese an. Interessiert? Dann wenden Sie sich bitte mit einer kurzen Beschreibung Ihres Anliegens an die E-Mail sax.cert@cert.sachsen.de.

Projekt HoneySens – den Hackern auf der Spur

Karl-Otto Feger
Referatsleiter 44 der Sächsischen Staatskanzlei und Beauftragter für Informationssicherheit des Landes

Die IT-Systeme der Sächsischen Landesverwaltung unterliegen nicht nur Bedrohungen aus dem Internet, sondern können ebenso zum Ziel von Angriffen aus dem internen Netzwerk selbst werden. Ausgangspunkt solcher Angriffe sind typischerweise mit Schadsoftware befallene Rechner. Aber auch unbemerkt in das Netzwerk vorgedrungene Angreifer oder gegen ihre Weisungen handelnde Mitarbeiter stellen potentielle Bedrohungsszenarien dar, die durch klassische Sicherheitsmaßnahmen wie zentrale Firewalls und Antivirussysteme nicht oder nur sehr eingeschränkt abgedeckt werden können.

Um auf derartige Gefahren zeitnah reagieren zu können, gibt es eine Reihe technischer Lösungen wie Intrusion Detection Systeme (IDS), Intrusion Prevention Systeme (IPS) oder Security Information and Event Management (SIEM)-Systeme. All diesen Systemen und Technologien ist eins gemeinsam: Sie erfordern einen hohen finanziellen und vor allem personellen Aufwand bei Beschaffung, Einrichtung und Betrieb. Dies war der Grund, warum vom Beauftragten für Informationssicherheit der Landesverwaltung Sachsen in Zusammenarbeit mit der Professur für Datenschutz und Datensicherheit der Technischen Universität Dresden im Rahmen einer Diplomarbeit das Projekt »HoneySens« entwickelt wurde. Es sieht eine unter Berücksichtigung der personellen und finanziellen Rahmenbedingungen und der Anforderungen des Sächsischen Verwaltungsnetzes (SVN) gestaltete Architektur vor. In dieser zeichnet der innerhalb gefährdeter Teilnetze platzierte Sensor entsprechende Informationen über alle ankommenden verdächtigen Datenpakete auf und leiten sie an eine zentrale Serverkomponente zur Verarbeitung weiter. Zuständige Administratoren können anschließend

mit Hilfe einer komfortablen Web-Anwendung die aggregierten Daten auswerten und bei Bedarf entsprechende Gegenmaßnahmen einleiten.

Automatisierte Erkennung von Angriffen aus dem Inneren

Zur Erkennung potentieller Angriffe kommt auf den Sensoren die Honeypot-Software zum Einsatz. Deren Zweck ist die Simulation typischer Netzwerkdienste und zugehöriger Sicherheitslücken. Je intensiver ein Eindringling mit diesen »Hackerfallen« kommuniziert, desto mehr Informationen können über dessen Motivation und Vorgehensweise gewonnen werden. Um ein möglichst umfassendes Bild über die Vorgänge innerhalb des Netzwerks zu gewinnen, können die Sensoren auch weitere Datenpakete aufzeichnen. Eine Erkennungsroutine für die von Angreifern häufig zur Informationsgewinnung genutzten Portscans erleichtert zudem die automatische Klassifikation der gesammelten Datenmengen.

Konzeption und Implementierung

Für die Spezifikation der Anforderungen an das HoneySens-System, die insbesondere aus den spezifischen Gegebenheiten des Sächsischen Verwaltungsnetzes und dem Wunsch nach einer wartungsarmen, benutzerfreundlichen Lösung resultierten, wurde eine ausführliche Analyse des zu erwartenden Datenverkehrs in ausgewählten Teilnetzen der Landesverwaltung durchgeführt. Die dabei gewonnenen Daten waren maßgebend für den Entwurf des autonomen Sensornetzwerks und die Auswahl der eingesetzten Hardwareplattform.

Bei der prototypischen Implementierung des Systems wurde besonders auf eine hohe Skalierbarkeit durch den Einsatz kostengünstiger Ein-Platinen-Computer als Sensoren, Standardkonformität, leichte Installation und Wartbarkeit, sowie die vollständig verschlüsselte Kommunikation zwischen allen beteiligten Komponenten geachtet. Ein weiterer wichtiger Teilaspekt war zudem die transparente Integration des Sensornetzwerkes in die bestehenden Strukturen der Landesverwaltung, um den Betrieb der bestehenden IT-Infrastruktur nicht zu beeinträchtigten.

Effiziente Abläufe

Damit auch Administratoren mit dem HoneySens-System arbeiten können, die nicht speziell im Bereich der Informationssicherheit geschult sind, wurde bei der Entwicklung des Prototypen besonders viel Wert auf eine moderne, leicht verständliche grafische Benutzeroberfläche gelegt. Die resultierende Web-Anwendung unterstützt die Benutzer bei allen anfallenden Arbeitsschritten: darunter die komfortable Integration zusätzlicher Sensoren, die Bereitstellung automatischer Updates der Sensor-Software und die Auswertung aller bereits gesammelten Daten. Eine flexible Benutzerverwaltung stellt zudem sicher, dass nur berechtigte Personen Zugang zum System erhalten. Techniken des »Responsive Web Design« stellen weiterhin sicher, dass die Benutzerschnittstelle auch auf Mobilgeräten wie Smartphones und Tablets komfortabel und uneingeschränkt genutzt werden kann.

Auch bei der Konzeption der zentralen Serverkomponente wurden Möglichkeiten zur unkomplizierten Installation berücksichtigt: Die Bereitstellung der Software in Form von virtualisierbaren Containern assistiert beim flexiblen, transparenten Betrieb der Anwendung und vereinfacht zukünftige Updates.

Drei Wege zu HoneySens

HoneySens kann über drei Wege »beschafft« werden. Da es vollständig auf Open Source-Software basiert, stehen die Quellcodes einer sogenannten Community Edition, also einer frei verfügbaren, nicht-kommerziellen Version, auf der Plattform Github bereit. Mit dieser Software kann das System mit den entsprechenden Kenntnissen selbst eingerichtet werden. Weiter ist HoneySens mittlerweile auch als käufliches Produkt durch einen renommierten, industriellen Partner verfügbar, was besonders kleine und mittelständische Unternehmen ansprechen soll. Der dritte Weg der Beschaffung ist gerade für Behörden auf kommunaler Ebene in Sachsen interessant: Für sie ist HoneySens weitgehend kostenfrei verfügbar. Interessierte wenden sich bitte an den Beauftragten für Informationssicherheit des Landes, z. B. per E-Mail: bfis-land@sk.sachsen.de

Das Kommunale DatenNetz III schneller – leistungsfähiger – sicherer

Informationssicherheit im KDN III

Frank Schlosser
Geschäftsführer KDN GmbH

Im Sachsenlandkurier September 2018 berichteten wir über das neue KDN III unter dem Motto »schneller – leistungsfähiger – sicherer« »Migration abgeschlossen«. Damals stellten wir den neuen Leistungsumfang in aller Ausführlichkeit dar und berichteten vom Abschluss der Migration.

Am 3. Juli 2019 wurde vom Sächsischen Landtag das Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen (SächsISichG) beschlossen. Es wird mit seiner Veröffentlichung im August 2019 in Kraft treten. Das neue Gesetz wird auch das Kommunale Datennetz (KDN) und seine Nutzer berühren und zur Sicherheit des KDN beitragen.

Vorab möchten wir jedoch die Gelegenheit nutzen, nochmals auf den Leistungsumfang des KDN III einzugehen.

Die Neukonzeption

In enger Abstimmung mit den kommunalen Spitzenverbänden und der SAKD wurde von der KDN GmbH ein neues Mengengerüst für das KDN III erarbeitet. Wesentliche Argumente dabei waren:

- Zukunftssicherheit auf Grund steigender Bandbreitenanforderung
- kontinuierlich steigende, zu übertragende Datenmengen in den Verwaltungen aufgrund steigender Berichtspflichten der Kommunen wegen gesetzlicher Vorgaben
- progressiv steigender Datenverkehr bei der Nutzung von IT-Verfahren

Auf der kommunalen Seite bestand Einigkeit, dass ein technologisches Treten auf der Stelle oder gar ein Rückschritt auf Grund der Notwendigkeit einer leistungsfähigen Kommunikationstechnologie nicht akzeptabel ist. Weiterhin war zwingend geboten, auf ein sicheres Netz hohen Wert zu legen, um gegenüber der aktuellen Bedrohungslage auch im kommunalen Netz gewappnet zu sein.

Im KDN III sollte Voice over IP (VoIP) verfügbar sein, um der All-IP-Strategie der Telekommunikationsdienstleister zu begegnen, und dies zu wirtschaftlich attraktiven Konditionen.

Bei der Vergabe des SVN 2.0/KDN III wurden diese Ziele erreicht. Mit der Nutzung des KDN III ist die Voraussetzung für die erfolgreiche Umsetzung der Vorgaben des Sächsischen E-Governmentgesetzes (SächsEGovG) gegeben.

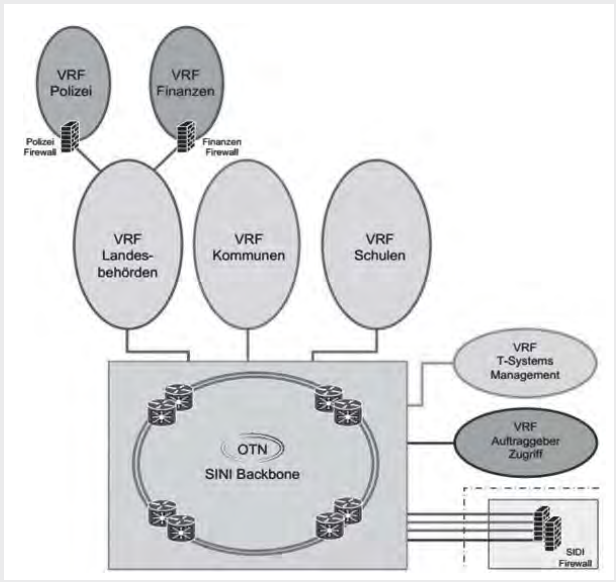
Das KDN III

Das SVN 2.0/KDN III besteht aus folgenden Teilen:

- SVN-integrierte Netzwerkinfrastruktur (SINI)
- SVN-integrierte Diensteinfrastruktur (SIDI) (ehemals Plattform zentrale Dienste)
- SVN-integrierte Mobilfunkanbindung (SIMA), nicht Teil des KDN III
- SVN-integrierte Telefonanbindung (SITA)
- SVN-integrierte redundante Internetanbindung (SIRIA)

Das neue KDN III, Teil SINI

Im Teil SINI sind das Zugangsnetz und der sogenannte Backbone (Rückgrat) zusammengefasst. SINI wird vom Dienstleister T-Systems betrieben. Das SINI-Rechenzentrum, an welchem die Leitungen zusammengeführt werden, ist redundant ausgelegt.



Struktur Netzwerk SINI
Quelle: T-Systems

Für die Kommunen bedeutet das KDN III einen Technologiesprung, mit der eine Zukunftssicherheit auf Grund steigender Bandbreitenanforderung erreicht wird.

Neben den deutlich erhöhten FAG-finanzierten Basis-Bandbreiten im KDN III wurden auch die Leistungsmerkmale im KDN III insbesondere im Bereich IT-Sicherheit der aktuellen Bedrohungslage angepasst. Die erhöhten Sicherheitsanforderungen wurden bei der Definition der Leistungsanforderungen mit dem Sächsischen Datenschutzbeauftragten (SächsDSB) und dem Beauftragten für Informationssicherheit des Freistaates Sachsen abgestimmt.

Gemäß §2, Abs. 1 SächsEGovG müssen *»Die staatlichen Behörden und die Träger der Selbstverwaltung … auch die elektronische Kommunikation ermöglichen. Beliehene sind von dieser Verpflichtung ausgenommen, soweit die elektronische Kommunikation für die ordnungsgemäße Wahrnehmung ihrer Verwaltungsaufgaben nicht erforderlich ist. Für die elektronische Kommunikation sind Verschlüsselungsverfahren anzubieten und grundsätzlich anzuwenden.«*

Um dieser Anforderung gerecht zu werden, wird die Leitungsverbindung ab dem Router in der Verwaltung bis zum SINI-Rechenzentrum und zurück verschlüsselt. Gleiches gilt auch für die Kommunikation der Verwaltungen untereinander. Das Schlüsselmanagement übernimmt eine Komponente im SINI-RZ. Anzumerken bleibt aber, dass das SVN 2.0/ KDN III in seiner Gesamtheit nach dem BSI-Schutzbedarf »normal« eingestuft ist. Dies bedeutet, dass IT-Verfahren, welche für ihre Kommunikation einen höheren Schutzbedarf benötigen, diesen selbst gewährleisten müssen, z. B. durch zusätzliche SSL-Verschlüsselung.

In das Netzabschlussgerät (SVNT, Router) wurde eine Firewallfunktionalität integriert. Die zugehörigen Access Control Listen werden in der Regel von der KDN GmbH gemanagt.

Der Standard Router für VDSL Quelle: CISCO

Die FAG-finanzierten Bandbreiten

Die Finanzierung des KDN III für einen sogenannten Basisanschluss erfolgt weiterhin über das Sächsische Finanzausgleichsgesetz (FAG). Im Vergleich zum KDN II wurde in Abstimmung mit dem Sächsischen Städte- und Gemeindetag die Abstufung zwischen den Gemeindegrößen verändert und weniger Gruppen gebildet. Maßgeblich für die Eingruppierung sind dabei die Verwaltungsaufgaben.

Gruppe 1: Beteiligte Gemeinden in Verwaltungsgemeinschaften bzw. Mitgliedsgemeinden in Verwaltungsverbänden
Gruppe 2: Kreisangehörige Städte und Gemeinden mit eigener Verwaltungskompetenz
Gruppe 3: Kreisfreie Städte und Landkreise

Gruppe	Basisanschluss in der Migrations-/Betriebsphase	Alternative bei VDSL-Nichtverfügbarkeit	Basisanschluss in der Endausbauphase	Alternative bei VDSL Nichtverfügbarkeit in der Endausbauphase
1	VDSL 16 Mbit/s SK 4	LTE oder ADSL bis zu 16 Mbit/s SK 4	VDSL 16 Mbit/s SK 4	LTE oder ADSL bis zu 16 Mbit/s SK 4
2	VDSL 50 Mbit/s SK 4	EthC 10 Mbit/s SK 4	EthC 50 Mbit/s SK 4 (zzgl. 10 % Eigenanteil)	Entfällt
3	EthC 100 Mbit/s SK 1	Entfällt	EthC 100 Mbit/s SK 1	Entfällt

Wie o. a. ist nach der Migration vom KDN II auf das KDN III ein weiterer Technologiesprung geplant, der alle Verwaltungen mit eigenen Verwaltungsaufgaben mit synchroner und hoch skalierbarer Glasfaseranbindung versorgen soll, soweit dies technisch möglich ist. Da diese Technologie im Vergleich mit der VDSL-Technologie finanziell aufwändiger ist, wurde von den Kommunalen Spitzenverbänden und der KDN GmbH beschlossen, den Basisanschluss über EthernetConnect mit 50 Mbit/s unter Beteiligung der Kommunen aus dem FAG zu fördern. Dieser Eigenanteil der Verwaltung beträgt 10 v. H. des Preises der Anbindung und liegt bei einem absoluten Betrag von knapp EUR 100,00 brutto monatlich.

Mit dem Sprung in die Glasfasertechnologie wird es den Kommunen möglich, auch höhere Bandbreiten zu vergleichsweise niedrigen Zusatzkosten zu beauftragen. Dabei wächst die Bandbreite nichtlinear im Verhältnis zu den Kosten.

Dort, wo es möglich war, wurden bereits in der Migrationsphase Glasfaseranschlüsse gelegt. Aktuell werden sukzessive die kupferbasierten EthC-10-Verbindungen auf Glasfaser EthC 50 umgerüstet.

Das neue KDN III, Teil SIDI

Beim Teil SIDI handelt es sich um das Dienste-Rechenzentrum (ehemals Plattform zentrale Dienste). Im Zuge der Migration auf das SVN 2.0 wird auch die Plattform der E-Government-Basiskomponenten in die zentralen Dienste integriert. Das SIDI-Rechenzentrum ist ebenfalls redundant ausgelegt.

Informationssicherheit im KDN III

Wie bereits eingangs erwähnt, wurde auf Grund der gestiegenen Bedrohungslage im Internet sehr viel Wert auf Schutzsysteme und erhöhte Informationssicherheit gelegt.

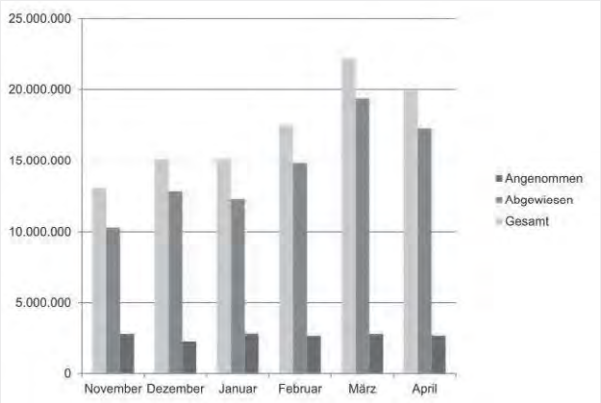
Gerne werden KDN-Anschlüsse mit AGB-Produkten der großen Provider verglichen. Gerade im Bereich Informationssicherheit sind diese Vergleiche aber so nicht zielführend. Der größte finanzielle Posten der SIDI-Dienste sind eben die Schutzsysteme, die man bei einem AGB-Produkt nicht bekommt.

Dies sind u. a. die Unterschiede zu AGB-Produkten:
- exklusive Infrastruktur im Backbone
- exklusive virtuelle Infrastruktur
- Transportverschlüsselung für alle übertragenen Daten
- exklusives Service-Center, das heißt, 7 Tage die Woche 24 Stunden einsatzbereit

- Bündelung in redundantem Rechenzentrum
- Sicherheitsinfrastruktur auf sehr hohem Niveau nach aktuellem Stand der Technik
- Übergang zu befreundeten Netzen (z. B. Netze des Bundes (NdB), welche Voraussetzung für einen sicheren Zugang zum KBA, zur Bundesdruckerei, zum nationalen Waffenregister etc.)
- Abschottung gegenüber »feindlichen Netzen« (z. B. Internet)

Folgende drei Grafiken unterstreichen die Notwendigkeit und Wirksamkeit der Schutzsysteme:

Mailaufkommen SVN und KDN						
Abgewiesene Mails aufgrund						
Monat	von Realtime Blacklists	von DNS-Checks	von ACLs	von Relay-Versuchen	von Greylisting	ungültige Adresse
Apr 19	7.112.676	6.345.770	1.612.263	48.012	1.972.030	161.858
Mrz 19	7.518.154	8.154.786	1.300.347	121.811	2.105.344	181.945
Feb 19	4.909.469	6.401.594	1.034.244	152.648	2.145.195	156.272
Jan 19	3.349.959	4.739.920	1.782.911	104.954	2.214.409	140.233
Dez 19	4.626.925	4.297.862	1.961.132	90.939	1.742.075	142.450
Nov 19	3.507.578	3.662.537	891.712	95.224	2.017.837	115.714

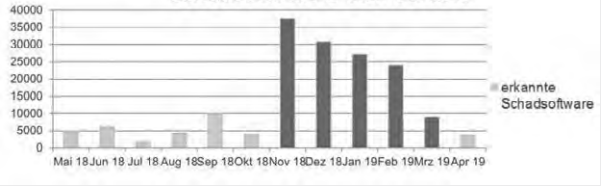


Mailaufkommen SVN und KDN

Die Grafik zeigt, dass aktuell nur etwas weniger als 10 % aller Mails angenommen werden, der Rest ist Spam, Phisching, Malware.

Während die angenommenen Mails nahezu gleichbleiben und damit sozusagen der »normale Verwaltungsverkehr« eine Basislinie bildet, steigt der Anteil der abgewiesen Mails fast permanent.

Schon damit wird die Notwendigkeit der starken Schutzsysteme begründet.



Schadsoftware E-Mail-Verkehr

Neu im SVN 2.0/KDN III ist der Schutz vor »Advanced Persistant Threat« (APT). APT, was übersetzt *»fortgeschrittene, andauernde Bedrohung«* bedeutet, ist ein Begriff für einen komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen aller Branchen, welche aufgrund ihres Technologievorsprungs potenzielle Opfer darstellen oder als Sprungbrett auf solche Opfer dienen können. Gegen diese Art von Bedrohungen, die über »normale« Trojaner, Würmer und Viren hinausgehen, ist das KDN nunmehr auch geschützt.

Das SVN 2.0/KDN III selbst ist in seinen Rechenzentren so ausgestaltet und dokumentiert, dass eine BSI-Zertifizierung jederzeit möglich ist. Bei der Abgrenzung zwischen dem LAN der Kommune und dem WAN (Weitnetz) des KDN III ist die Übergabestelle klar definiert, nämlich der LAN-Port des Netzabschlussgerätes im KDN III. Bis dahin reicht die Verantwortung der KDN GmbH. Das dort eingesteckte Kabel unterliegt bereits der Verantwortung der Kommune. Von Bedeutung ist dies nicht nur für die Betriebsverantwortung der KDN GmbH, sondern auch für die Abgrenzung der sogenannten IT-Verbünde für eine BSI-Zertifizierung. Es wird dabei auf eine klare Abgrenzung der IT-Verbünde und IT-Systeme geachtet und so der Umfang für die BSI-Zertifizierung definiert. Auf KDN-Seite erstreckt sich der verantwortete IT-Verbund bis zum LAN-Port des KDN-Netzabschlussgerätes und ab dort beginnt der IT-Verbund der Kommune..

Bis Ende 2019 werden die SIDI-Rechenzentren nach BSI zertifiziert.

Das SächsISichG und das KDN III

Erstmalig gibt es mit dem Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen (SächsISichG) eine gesetzliche Regelung für Landesbehörden sowie die seiner Aufsicht unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (nicht-staatliche Stellen).

Für den Datenschutz gab und gibt es mit dem Bundesdatenschutzgesetz, dem Sächsischen Datenschutzgesetz und jetzt mit der EU Datenschutzgrundverordnung sowie dem Sächsischen Datenschutz Durchführungsgesetz Rechtssicherheit seit 1991.

Jetzt gibt der Gesetzgeber auch für die Informationssicherheit rechtliche Rahmenbedingungen vor und schafft damit Rechtssicherheit.

Dabei sind folgende Grundsätze vorgegeben:

- angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zur Gewährleistung der Informationssicherheit.
- Berücksichtigung der jeweils geltenden Standards und des jeweils geltenden IT-Grundschutz-Kompendiums des Bundesamtes für Sicherheit in der Informationstechnik durch alle staatlichen Stellen, um ein angemessenes Informationssicherheitsniveaus zu gewährleisten
- Empfehlung zur Anwendung des geltenden IT-Grundschutz-Kompendiums des BSI für die Kommunen
- Um die Erreichung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus zu gewährleisten, haben alle staatlichen Stellen die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.
- Für Kommunen wird die Anwendung empfohlen.

Das IT-Grundschutz-Kompendium ist neben den BSI-Standards die grundlegende Veröffentlichung des IT-Grundschutzes. Das umfangreiche Arbeitsinstrument und Nachschlagewerk zur Informationssicherheit enthält in der 1. Edition 2018 die ersten 80 IT-Grundschutz-Bausteine, die für künftige Editionen kontinuierlich aktualisiert und erweitert werden. Die Bausteine sind in zehn Schichten aufgeteilt und

thematisieren unterschiedlichste Sachverhalte der Informationssicherheit – von Anwendungen (APP) über Industrielle IT (IND) bis hin zum Sicherheitsmanagement (ISMS). Bei der Erstellung der Bausteine wurde bereits eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt. Die Anforderungen in den Bausteinen bilden den aktuellen Stand der Technik ab.

Die 1. Edition des IT-Grundschutz-Kompendiums ersetzt die zur Sicherheitsmesse it-sa im Oktober 2017 veröffentlichte Final-Draft-Version. Seit dem 1. Februar 2018 dient das IT-Grundschutz-Kompendium als Prüfgrundlage für Zertifizierungen nach ISO 27001 auf Basis von IT-Grundschutz.

Weitere Informationen zum neuen IT-Grundschutz-Kompendium finden Sie unter: *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html*

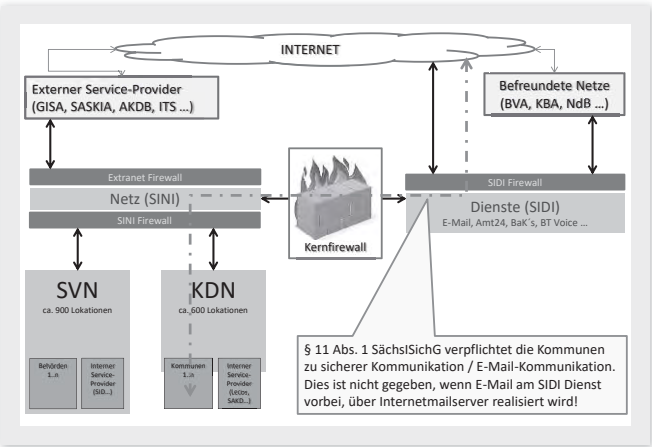
Die Verantwortung für die Informationssicherheit im Sinne des Absatzes 1 trägt der jeweilige Leiter der staatlichen oder nicht-staatlichen Stelle, bei Schulen der jeweilige Schulträger.

Die Informationssicherheit lag schon immer in der Verantwortung des gesetzlichen Vertreters der Kommune (Bürgermeister, Oberbürgermeister, Landrat), nun wird dies auch im Gesetz untermauert.

Bei der Verantwortung im SVN 2.0/KDN III gibt es aber Unterschiede zwischen dem Freistaat und der KDN GmbH. Der Freistaat ist im SVN 2.0 für alle seine Behörden und nachgeordneten Einrichtungen verantwortlich. Die Verantwortung der KDN GmbH endet an der Schnittstelle des KDN-Routers zum LAN der Kommune (kommunale Selbstverwaltung).

Die Verträge zwischen der KDN GmbH und ihren Kunden sehen allerdings einen Passus vor, welche die Netzkunden auf die Informationssicherheit verpflichtet.

»Wir verpflichten uns zudem, sofern nicht bereits vorhanden, ein IT - Sicherheitskonzept zu erstellen und zu aktualisieren sowie übergreifende Maßnahmen zur Sicherheit der Informationstechnik in speziellen Regelungen (Dienstordnung, Dienstvereinbarung für Internet bzw. E-Mail usw.) verbindlich festzulegen. Insbesondere werden Regelungen über Zugangsberechtigungen, Benutzerkontrolle, Zugriffsberechtigungen, Übermittlungskontrolle sowie Weitergabe, Verwendung und Transport von Daten getroffen und die diesbezüglichen Verantwortlichkeiten in entsprechenden Dienstanweisungen festgelegt. Die Vorgaben der DSGVO bzw. SächsDSDVG werden von uns eingehalten.«



Ein weiterer neuer Aspekt ist die gesetzliche Forderung zur Bestellung eines Beauftragten für Informationssicherheit (BfIS) in jeder Kommune. Ein BfIS kann dabei für mehrere Kommunen tätig sein. Die Kommunen können dies im Rahmen des KomZG selbst ausgestalten. Auch diese Aufgabe war schon immer vorhanden, wurde meist aber nur in größeren Kommunalverwaltungen umgesetzt. Der neue gesetzliche Rahmen ist eine wichtige Aufwertung der Informationssicherheit.

An den Sicherheitsbedingungen zum Anschluss an das KDN III ändert sich nichts. Fremdnetzübergänge in andere Netze in den Kommunen sind nach wie vor durch einen durch das Bundesamt für Informationstechnik (BSI) zertifizierten Auditor zu testieren. Im Detail verweise ich auf den Artikel meiner Kollegen Kurth und Lieder in diesem Heft.

WLAN im KDN

Sollen in den Verwaltungen WLAN-Zugriffe für Gäste ermöglicht werden, empfiehlt die KDN GmbH dringend den Einsatz eines getrennten Internetzugangs für die WLAN-Hotspots. Dieser solle eine getrennte Wegeführung innerhalb der Bauten der Verwaltung erhalten, um eine Infizierung des Verwaltungs-LAN durch Schadcode über unsichere infizierte Mobilgeräte zu vermeiden.

Telefonie im KDN

Nicht zu unterschätzen sind Sicherheitsaspekte, welche durch die Ablösung der ISDN-Anschlüsse durch IP-basierte Anschlüsse hinzukommen. Bisher wurde auf den Telefonanschlüssen der Kommunen ISDN (Integriertes Sprach- und Datennetz) verwendet. ISDN ist zwar ein digitaler Standard, unterscheidet sich aber grundsätzlich vom in Netzwerken verwendeten Internet Protokoll (IP, die Vermittlungsschicht im Netzverkehr). Über IP werden Datenpakete im Netzwerk adressiert und versendet.

ISDN ist in einem Computernetzwerk nicht routbar, das heißt, es kann nicht zielgerichtet auf Netzwerkadressen adressiert werden. Damit kann es grundsätzlich auch keinen Schadcode auf Rechnersysteme transportieren. Die Verbindung zu Rechnern und Telefonen wird bei ISDN von der Telefonanlage hergestellt, entweder analog oder per IP. Auch wenn die Telefonanlage per IP mit dem Rechnernetz (LAN) verbunden ist, durch die Wandlung auf ISDN in der Telefonanlage für die Sprachkommunikation kann von außen kein Schadcode eingeschleust werden.

Bei der IP-Telefonie ist dies anders. Schon die Sprachsignale werden in Datenpakete des IP verpackt. Dies nennt man Voice over IP (VoiP). Die Datenverbindung wird im Internet geroutet wie jede andere auch. Wenn nun der IP-Anschluss für VoiP mit einer TK-Anlage verbunden wird, die wiederum per IP mit dem LAN verbunden wird, kann über diese Verbindung das LAN von außen angegriffen werden. Ist dieses LAN dann noch mit dem KDN verbunden, ist die Hintertür des KDN offen. Damit dies nicht geschieht, wird der IP-Telefonanschluss als Fremdnetzzugang definiert und ist als solcher zu schützen und zu auditieren. Auf den Artikel »Der Zertifizierte Netzübergang – ganz praktisch« von Herrn Kurth und Herrn Lieder wird verwiesen.

Das KDN bietet auch dafür eine Lösung. Mit Einführung des KDN III können Telefondienste auch über das KDN bezogen werden. Der Übergang in das öffentliche Telefonnetz findet gesichert im SIDI-Rechenzentrum statt und ist durch die beschriebenen Schutzsysteme geschützt.

Auf den Artikel »IP-Telefonie (VoIP) und Informationssicherheit« von Frau Blume und Herrn Nikol in diesem Heft wird verwiesen.

Ein zertifizierter Fremdnetzzugang ist dann obsolet.

MDM/EMM im KDN

Ein weiterer Faktor der Informationssicherheit ist die schere Nutzung von Smartphones und Tabletts. Die Gefahr, dass durch ungesicherte Mobilgeräte Daten unerlaubt und unbemerkt abfließen oder Schadsoftware sich Zugang zum Handy oder dem Tablett und dann ins LAN der Verwaltung verschafft.

Um sich gegen diese Bedrohung zu schützen, gehört zum Basisschutz gemäß BSI Grundschutzkompendium auch der Einsatz eines Mobile Device Management Systems (Mobilgeräte-Verwaltungssystem).

Dabei werden die angeschlossenen Mobilgeräte zentral von einem Administrator gemanagt. Zum Management gehören u.a. Vorgaben zu den Nutzerrechten, zentrale Sperrung bei Verlust, Vorgabe für Passwörter, Verteilung von Updates und Restriktionen zu eingesetzten Apps.

Im KDN wird ein MDM System bereitgestellt, welches mandantenfähig ist, eine Administration der Geräte auf Kundenebene erlaubt und auch die Festlegung von Profilen je Nutzer/Nutzergruppe in der Verwaltung durch die Verwaltung selbst erlaubt.

Derzeit läuft die Pilotierung im Zweckverband KISA, KISA steht aber auch als Ansprechpartner für das MDM in sächsischen Kommunalverwaltungen bereit.

Fazit:

Mit dem KDN III steht den sächsischen Kommunen eine leistungsfähige und im Rahmen des aktuellen Stands der Technik sichere Kommunikationsinfrastruktur zur Verfügung. Mit Zusatzdiensten wie Telefonie und MDM ist es für die Anforderungen einer fortschrittlichen und sicherheitsbewussten Kommunalverwaltung bestens gerüstet.

Informationssicherheit und Datenschutz

Konrad Biskupski (LL.B.)
Fachbereichsleiter Datenschutz, IfDDS GmbH

Es ist kurz vor 15 Uhr an einem Montag im Mai dieses Jahres, als ein Mitarbeiter eines großen deutschen Verlagshauses für IT-Medien die E-Mail eines vermeintlichen Geschäftspartners öffnet. Die Korrespondenz bezieht sich auf einen tatsächlichen Geschäftsvorgang, verbunden mit der Bitte, die im angehängten Word-Dokument befindlichen Informationen zu prüfen und gegebenenfalls zu korrigieren. Eine angebliche Fehlermeldung fordert dazu auf »Enable Editing« zu klicken. Das Unheil nimmt nun seinen Lauf.

Zwei Tage später entscheiden sich die Verantwortlichen für einen kompletten Lockdown und das Hinzuziehen von spezialisierten Incident-Response-Teams und IT-Forensikern, um der Lage Herr zu werden – das Dynamit-Phishing Schadprogramm ‚Emotet' hatte die Systeme infiziert. Allein die Kosten für die eingesetzten Spezialisten belaufen sich derzeit auf geschätzte 50.000 Euro. Nach Unternehmensangaben wird es einige Wochen in Anspruch nehmen, den Befall endgültig zu beenden. Das gesamte Schadensausmaß kann derzeit noch nicht beziffert werden.

Dieser Fall verdeutlicht, dass Cyber-Resilienz heute wichtiger ist denn je. Staatliche Stellen, als Träger der Daseinsvorsorge, müssen besondere Schutzmaßnahmen ergreifen, um Ihre Handlungsfähigkeit auch in Zeiten zunehmender elektronischer Kommunikation und einer allgemeinen Verwaltungsmodernisierung aufrecht zu erhalten. Das Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (Sächsisches Informationssicherheitsgesetz – Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen) verfolgt eben diesen Zweck.

Im folgenden Artikel wird insbesondere auf die Wechselwirkung des Gesetzes mit den bestehenden Datenschutzregularien eingegangen. Einige Regelungen sind verwandt, andere laufen dem Datenschutz scheinbar zuwider.

Sicherheit der Verarbeitung

Im Vorblatt zum Gesetzesentwurf heißt es: »Mit dem mittlerweile nicht mehr wegzudenkenden Einsatz der Informationstechnik (IT) bei der Erledigung von Verwaltungsaufgaben und Verwaltungsprozessen muss auch der Sicherheit der den Verwaltungen überlassenen oder von ihnen erzeugten Daten angemessen und nachprüfbar Rechnung getragen werden«.

Gelingen soll dies einerseits durch das Etablieren von technischen und organisatorischen Maßnahmen und andererseits durch die Schaffung einer Reihe von Institutionen, wie dem Beauftragten für Informationssicherheit und der Einrichtung sogenannter Sicherheitsnotfallteams.

Obwohl der Begriff Informationssicherheit ein breiteres Schutzspektrum fasst, als der des Datenschutzes (vgl. Abb. 1) – der mithin ausschließlich personenbezogene Daten zu schützen sucht – sind klare Synergien erkennbar: Beide Gesetze verpflichten die verantwortliche Stelle, technische und organisatorische Maßnahmen nach dem Stand der Technik zu ergreifen, um die (personenbezogenen) Daten bezüglich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit abzusichern. Führt man sich vor Augen, dass staatliche Stellen (wie auch nicht-staatliche Stellen im Sinne des Gesetzes) mit der umfangreichen Verarbeitung personenbezogener Daten befasst sind, ist ein hoher

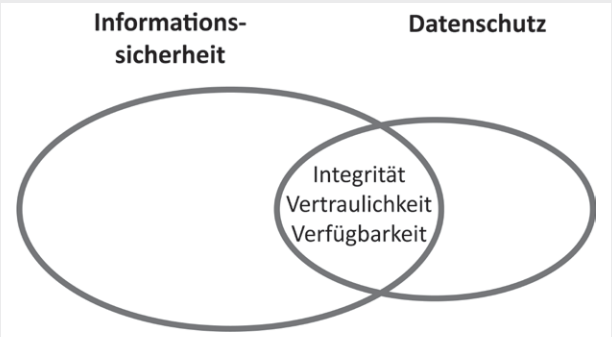


Abbildung 1 – Informationssicherheit und Datenschutz

Schutzbedarf geboten. Besonders begrüßenswert ist die Konkretisierung der Umsetzung vorgenannter organisatorischer und technischer Maßnahmen durch den Gesetzgeber, nach der staatliche Stellen die jeweils geltenden Standards und das jeweils geltende IT Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen haben (vgl. § 4 Abs. 1 Satz 1 Sächsisches Informationssicherheitsgesetz). Derart greifbare Regelungen sucht man in den einschlägigen Normen des Datenschutzes vergeblich.

Beauftragte für Informationssicherheit und Datenschutzbeauftragte

Die Aufgaben der behördlichen Datenschutzbeauftragten ergeben sich aus Art. 39 Datenschutz-Grundverordnung. Die Aufgaben der behördlichen Datenschutzbeauftragten ergeben sich aus Art. 39 Datenschutz-Grundverordnung (entgegen der häufig vertretenen aber irrigen Annahme, gilt das Bundesdatenschutzgesetz für öffentliche Stellen des Freistaats Sachsen nicht). Neben einer unterrichtenden und beratenden Stellung fungieren Datenschutzbeauftragte als Kontrollinstanz für geltende Datenschutzvorgaben.

Das Aufgabenspektrum der Beauftragten für Informationssicherheit differiert hingegen: Das Gesetz spricht von einer Förderung der Informationssicherheit und der Koordinierung entsprechender Maßnahmen. Den Beauftragten für Informationssicherheit werden also gewisse Weisungsspielräume eingeräumt, was sich auch in der Verantwortung für nachstehende Meldepflichten widerspiegelt. Eine datenschutzrechtliche Meldung nach Artt. 33, 34 Datenschutz-Grundverordnung ist hingegen von der verantwortlichen Stelle selbst veranlasst. Datenschutzbeauftragte können jedoch Empfehlungen für oder wider eine solche Meldung hervorbringen. Da Beauftragte für Informationssicherheit im Falle eines Sicherheitsereignisses berechtigt sind, Einsicht in die Protokolldaten ihrer Zuständigkeitsbereiche zu nehmen, sollte ein den Datenschutzbeauftragten analoges Berufsgeheimnis nach § 203 Abs. 4 Strafgesetzbuch angestrebt werden.

Das Recht der Datensichtung ist einem Korrektiv unterworfen, nach dem Daten vom Sächsischen Rechnungshof, des Sächsischen Datenschutzbeauftragten, den Gerichten und Staatsanwaltschaften, den Behörden und Organisationen mit Sicherheitsaufgaben sowie den Hochschulen lediglich im Einvernehmen mit der jeweiligen verantwortlichen Stelle eingesehen werden dürfen (vgl. § 7 Abs. 3 SächsISichG). Für Daten des richterlichen, staatsanwaltschaftlichen oder rechtspflegerischen Arbeitsprozesses gilt zudem § 41c des Sächsischen Justizgesetzes entsprechend.

Die Erforderlichkeit der Benennung eines Datenschutzbeauftragten/einer Datenschutzbeauftragten ergibt sich aus Art. 37 Abs. 1a Datenschutz-Grundverordnung, nach dem öffentliche Stellen automatisch zur Benennung verpflichtet sind. Bei Beauftragten für Informationssicherheit wird zunächst unterschieden, ob es sich um eine staatliche Stelle oder eine nicht-staatliche handelt. Im ersten Fall ist die Benennung obligatorisch, ansonsten fakultativ. Gleichwohl ist eine Berufung vom Gesetzgeber als ratsam bewertet worden (Soll-Vorschrift). In der Praxis wird sich die Erforderlichkeit – wie auch im Datenschutz – jedenfalls häufig an der Frage orientieren, inwieweit die einschlägigen Normen ohne eine entsprechende personelle Stelle realistisch umsetzbar sind. Wie auch im Datenschutz, kann die Position durchaus von externen Dienstleistern besetzt werden und der- oder dieselbe Beauftragte für mehrere Einrichtungen tätig sein. Es besteht jeweils eine Meldepflicht. Weisungsfreiheit und unmittelbares Vortragsrecht beim Verantwortlichen ist darüber hinaus beiden Institutionen immanent.

Im Rahmen der Erforderlichkeitsbeurteilung bei nicht-öffentlichen Stellen sei noch auf das Vorhandensein und den Umfang der Anbindung zum Kommunalen Datennetz respektive zum Sächsischen Verwaltungsnetz hingewiesen, deren Schutz primärer Regelungsinhalt des Sächsischen Informationssicherheitsgesetzes ist.

Inwieweit eine Zulässigkeit der in Rede stehenden Beauftragten in Personalunion gegeben ist, bleibt abzuwarten. Das Spannungsverhältnis zwischen Schutz des Rechts auf informationelle Selbstbestimmung und Schutz der Informationssicherheit (in Form der Auswertung gegebenenfalls personenbezogener Protokolldaten) spricht nach Ansicht des Autors eher für das Vorliegen eines Interessenskonfliktes und mithin gegen die Zulässigkeit. Gleichwohl sollte die Rechtmäßigkeit letztlich anhand tatsächlicher Umstände des Einzelfalls bewertet werden, insbesondere da die erforderliche Fachkunde konkordant ist. Technische und organisatorische Maßnahmen könnten beispielsweise ein probates Mittel darstellen, den etwaigen Interessenskonflikt auf ein Minimum zu reduzieren.

Meldepflichten

Nebst den seit 25. Mai vergangenen Jahres laut der Europäischen Datenschutz-Grundverordnung bestehenden Meldepflichten gegenüber der Datenschutzaufsichtsbehörde bei der Verletzung des Schutzes personenbezogener Daten ergeben sich aus Abschnitt 4 des Sächsischen Informationssicherheitsgesetzes weitere Anzeigepflichten.

Unterschieden wird hierbei in präventive Meldungen sicherheitsrelevanter Informationen, »die zur Abwehr von Gefahren für die informationstechnischen Systeme von Bedeutung sind« und dem Meldeprozess für Sicherheitsereignisse und Sicherheitsvorfälle gegenüber dem Sicherheitsnotfallteam (CERT-Sachsen). Letztgenannte Anzeigen werden in Zukunft wohl regelmäßig mit einer datenschutzrechtlichen Meldung gegenüber dem Sächsischen Datenschutzbeauftragten einhergehen. Die Chance, ein einheitliches Kompetenzzentrum für derartige Meldungen einzurichten, wurde vertan. Es bleibt zu hoffen, dass die Zusammenarbeit zwischen Informationssicherheits- und Datenschutzbehörden verstärkt wird, um Dopplungen im Bewältigungsprozess zu vermeiden.

Die sich aus dem Sächsischen Informationssicherheitsgesetz ergebenden Meldepflichten sollen inhaltlich zukünftig in Form von Rechtsverordnungen der Staatsregierung konkretisiert werden. Hierbei wird ein

gewisses Fingerspitzengefühl von Nöten sein, denn dem Sicherheitsnotfallteam wird die Befugnis eingeräumt, alle für die Abwehr von Gefahren für die Informationssicherheit erforderlichen Informationen zu sammeln und auszuwerten. Dies könnte zu datenschutzrechtlichen Problemen führen, da zu diesen Informationen durchaus (sensible) personenbezogene Daten gehören können. Geäußert wurde diese Sorge unter anderem auch in der Stellungnahme der Liga der Freien Wohlfahrtspflege in Sachsen zum Entwurf des Gesetzes. Von praktischer Bedeutung wird in diesem Zusammenhang auch die Verantwortung für die Übermittlung personenbezogener Daten nach § 6 Sächsischem Datenschutzdurchführungsgesetz sein: Demnach trägt die übermittelnde – also meldende – Stelle die Verantwortung für die Rechtmäßigkeit der Übermittlung. Das Notfallsicherheitsteam repräsentiert im Falle einer proaktiven Meldung der staatlichen Stelle keine anfragende Stelle im Sinne des Gesetzes. Hier ist die Staatsregierung aufgefordert, rasch einheitliche Regelungen in Form vorgenannter Verordnungen zu schaffen, um die öffentlichen Einrichtungen nicht auf das dünne Eis etwaiger Datenschutzverstöße zu führen.

Einschränkung von Grundrechten

Kritisch begutachtet werden muss die Einschränkung des Fernmeldegeheimnisses sowie des Rechts auf informationelle Selbstbestimmung. Gleichwohl die Schranke für eine Einschränkung der einfache Gesetzesvorbehalt ist, wird sich die Rechtmäßigkeit an verfassungsmäßigen Prinzipien, insbesondere der Verhältnismäßigkeit, messen lassen müssen.

Unstrittig ist die Verfolgung eines legitimen Zwecks, da die Sicherheit der Verwaltungssysteme – insbesondere des Kommunalen Datennetzes und des Sächsischen Verwaltungsnetzes – ein zu schützendes Rechtsgut darstellt. Das Auswerten einschlägiger Daten durch staatliche Expertenteams ist im Ernstfall ferner geeignet, vorgenannten Zweck zu verfolgen. Zudem wäre eine Erforderlichkeit des Eingriffs dann gegeben, wenn kein geringeres Mittel für eine (gleichartige) Erreichung des Zwecks vorläge. Hier könnte man durchaus argumentieren, dass eine Verarbeitung anonymisierter Daten ausreichend wäre (vgl. § 16 Abs. 1ff. Gesetzesbegründung zum Sächsischen Informationssicherheitsgesetz). Diesem Umstand steht jedoch entgegen, dass zum einen Daten im Zuge der Anonymisierung bereits verfälscht und mithin gegebenenfalls forensisch unbrauchbar gemacht werden, zum anderen spielt insbesondere der zeitkritische Faktor eine Rolle: So müssen Systeme im Notfall schnellstmöglich jedenfalls in eine ‚stabile Seitenlage' gebracht werden. Der Gesetzgeber sucht den Kompromiss und verlangt »angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person«, zu denen insbesondere die Anonymisierung zählen kann (vgl. § 6 Abs. 5 Gesetzesbegründung zum Sächsischen Informationssicherheitsgesetz).

Entscheidend ist also das Ergebnis der Abwägung im Zuge der Angemessenheitsprüfung. Den verfassungsmäßig verbürgten Rechten auf informationelle Selbstbestimmung sowie dem Fernmeldegeheimnis steht die Gewährleistung der Informationssicherheit, als eine im öffentlichen Interesse liegende Aufgabe, gegenüber.

Die Handlungsfähigkeit zentraler staatlicher Organe stellt zweifelsohne ein hohes Rechtsgut dar. Es darf von einem gesellschaftlichen Konsens ausgegangen werden, dass gewisse – für genannte Persistenz – unvermeidbare Eingriffe hingenommen werden. In der Begutachtung kann in diesem Zusammenhang auch der Grundsatz der »reasonable expactations« der betroffenen Person dienlich sein: Kann aus Sicht des objektiven Dritten vernünftigerweise davon ausgegangen werden, dass bei einem (vermuteten) Sicherheitsvorfall auch der Inhalt der eigenen E-Mails, sonstiger digitaler Kommunikation und weiterer in den Systemen befindlicher personenbezogener Daten jedenfalls wahrgenommen, mithin aber auch ausgewertet und gespeichert werden?

Bedienstete können beispielsweise im Zuge von Datenschutzschulungen darauf hingewiesen werden, dass eine etwaige Auswertung – auch personenbezogener Daten – statthaft sein kann, um die Sicherheit der Systeme zu gewährleisten. Insbesondere beim Vorliegen eines (ratsamen) Verbots der Privatnutzung von Internet und E-Mail ist eine Auswertung aus datenschutzrechtlicher Sicht weit weniger kritisch zu beurteilen.

Ungleich schwieriger ist die Sachlage bei den Personengruppen, die nicht zu den Beschäftigten zählen. Ein die Verwaltung adressierender Bürger geht nicht zwangsläufig davon aus, dass seine personenbezogenen Daten im Rahmen einer IT-sicherheitsrelevanten Untersuchung ausgewertet und gespeichert werden. Der Gesetzgeber hat zwar den Anwendungsbereich der Datenschutzregelungen für Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten weitgehend aufgeweicht (vgl. u.a. Art. 2 Abs. 2 lit. d Datenschutz-Grundverordnung), das CERT-Sachsen stellt jedoch keine Behörde in diesem Sinne dar und könnte auch in Fällen einer rein technisch bedingten Störung personenbezogene Daten auswerten (müssen). Betroffene könnten im Rahmen einer transparenten Verarbeitung nach Art. 12 Datenschutz-Grundverordnung im Zuge der Übermittlung der Datenschutzbestimmungen bereits über eine etwaige Auswertung Ihrer personenbezogenen Daten durch die entsprechenden Stellen und die einschlägigen Rechtgrundlagen aufgeklärt werden.

Zur Verhältnismäßigkeitsprüfung kann zudem die aus dem Datenschutz bekannte Eingabekontrolle (vgl. Abb. 2) eine hilfreiche Brücke bilden: Auch bei dieser Maßnahme werden personenbezogene Daten verarbeitet, um den Datenschutz (und die Datensicherheit) zu gewährleisten. Die juristische Bewertung orientiert sich dabei an der Zweckgebundenheit (insbesondere im Lichte der Speicherbegrenzung) sowie an der Verhältnismäßigkeit im engeren Sinne (Angemessenheit). So kann beispielsweise ein mehrstufiges Verfahren mit unterschiedlichen

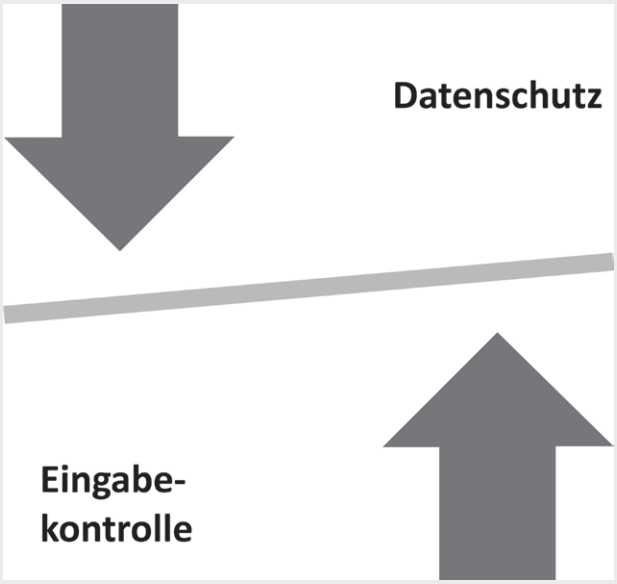


Abbildung 2 – Datenschutz und Eingabekontrolle

Eingriffsintensitäten ein probates Mittel darstellen. Regelmäßig wird die Abwägung wohl mit Recht zugunsten der Informationssicherheit substanzieller öffentlicher IT-Systeme ausfallen.

Letztendlich bleibt abzuwarten, in welcher Form der Gesetzgeber die Konkretisierung der Eingriffe in Form oben genannter Verordnungen vornehmen wird. Dabei sollten auch datenschutzrechtliche Grundprinzipien wie Speicherbegrenzung und Datensparsamkeit Eingang finden (vgl. auch Stellungnahme des Sächsischen Datenschutzbeauftragten zum Gesetzesentwurf).

Fazit

Zu Zeiten hochspezialisierter Schadprogramme wie ‚Emotet' und immer ausgeklügelteren Angriffstechniken ist es konsequent und begrüßenswert, dass der Gesetzgeber öffentliche Stellen in die Pflicht nimmt. Fälle aus Baltimore und Atlanta haben kürzlich deutlich aufgezeigt, dass Kommunen und andere öffentliche Einrichtung zusehends ins Visier der organisierten Cyberkriminalität geraten und die Organisationen mitten ins Mark treffen können. Baltimore kostete ein einzelner Vorfall 4,6 Millionen US-Dollar in den ersten drei Wochen und geschätzte weitere 5,4 Millionen Dollar bis Ende 2019.

Eine ausreichende personelle wie finanzielle Ausstattung des CERT-Sachsen, als zentrale präventive und reaktive Einrichtung im Freistaat, sollte folglich stets gewährleistet sein. Denn wie im Datenschutz wird die Informationssicherheit schließlich am Vorliegen der benötigten Ressourcen zu bewerten sein. Die Bildung von Institutionen für Umsetzung und Überwachung allein wird erfahrungsgemäß nicht zu einer nachhaltigen Verbesserung der Sicherheit führen, wenn benötigte Mittel nicht von oberster Ebene bereitgestellt werden. Es darf sich also dem Tenor des Bundesamtes für Sicherheit in der Informationstechnologie angeschlossen werden: »Informationssicherheit ist Chefsache«.

Der Mensch und die Informationssicherheit: Sensibilisieren, Bewusstsein schaffen, Handeln ändern

Bastian Fermer
Referent, Sächsische Staatskanzlei

Gefährdungen in der Informationssicherheit entstehen nicht nur, indem Schwachstellen aufgrund fehlerhafter Software ausgenutzt werden, die von technischen Sicherheitslösungen nicht oder zumindest erst sehr spät erkannt werden. Gefahren sind auch möglich, weil der Mensch mit unbedachten Mausklicks unfreiwillig zum Komplizen von Hackern werden kann. So wird Schadcode in den überwiegenden Fällen erst durch Menschen aktiviert. Auch personenbezogene Anmeldedaten werden häufig durch fahrlässiges Handeln der Computernutzer an die Hacker überliefert. In diesen Fällen können selbst beste Technik und durchdachte Sicherheitsvorkehrungen kaum die Informationssicherheit bewahren. Insofern verwundert es nicht, dass die Nutzer von Computer, Tablet und Smartphone das größte Fehlerrisiko der Informationstechnik ausmachen. Statistiken zeigen immer wieder, dass ca. 95 Prozent aller Sicherheitsvorfälle in der IT erst durch leichtsinniges oder einfach unwissend riskantes Verhalten der Nutzer möglich wurden. Daher ist zu beobachten, dass sich Cyberkriminelle immer stärker auf menschliches Fehlverhalten anstatt auf technische Fehler fokussieren.So gelangen sie an persönliche Daten oder geistiges Eigentum oder erpressen Unternehmen bzw. Behörden um Geld. Solange der einzelne Nutzer Defizite im Umgang mit technischen Mitteln wie seinem Arbeitsplatzrechner zeigt, führt der Weg zu einer nachhaltigen Erhöhung der Informationssicherheit nur über die Sensibilisierung und Fortbildung eines jeden Einzelnen. Das gilt gerade auch für die öffentliche Verwaltung.

Sensibilisierung durch die INFOSIC

Sowohl das neue Sächsische Informationssicherheitsgesetz als auch die Datenschutzgrundverordnung beschreiben, wie wichtig die Sensibilisierung und das Training von Mitarbeitern ist. Dabei geht es zum einen darum, vor Gefahren bei der alltäglichen Nutzung von PC, Smartphone und Internet zu sensibilisieren und zum anderen Kompetenzen zur Gefahrenabwehr zu vermitteln. Da nur die wenigsten Mitarbeiter in der Verwaltung IT-Experten sind, kann das benötigte Wissen am besten über einfache Regeln und verständliche Sicherheitsmaßnahmen vermittelt werden. Ganz nach diesem Leitmotiv organisiert der Beauftragte für Informationssicherheit des Landes mit der Großveranstaltung INFOSIC seit dem Jahr 2012 so genannte »Live-Hackings«, die sich ausdrücklich an alle Mitarbeiterinnen und Mitarbeiter von Landes- und Kommunalbehörden richten. Mittlerweile ist die INFOSIC die größte Sensibilisierungsveranstaltung für Informationssicherheit im Freistaat Sachsen. Der Zuspruch und das Interesse an einer Teilnahme sind unter den Mitarbeitern der Landes- und Kommunalverwaltung über die Jahre

stark gestiegen. Wurden in den Anfangsjahren in Leipzig und in Chemnitz jährlich knapp 700 Teilnehmer begrüßt, erhöhte sich die Zahl in den Folgejahren schlagartig, so dass mittlerweile jährlich rund 3.000 Mitarbeiter aus den Verwaltungen an diesen Veranstaltungen teilnehmen. Durch diese und andere dezentral vom BfIS Land organisierte bzw. unterstützte Veranstaltungen wurden bislang insgesamt über 12.000 Mitarbeiter aus der öffentlichen Verwaltung in Sachsen direkt erreicht. Mit dieser Teilnehmerzahl belegt der Freistaat Sachsen im Bundesvergleich einen Spitzenplatz. Der IT-Planungsrat unterstützt die Länder bei der Ausrichtung, indem es die erfahrenen Referenten von IT-Beratungsunternehmen vermittelt und finanziert.

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

INFOSIC 2019 in Leipzig, Chemnitz und Dresden

In diesem Jahr werden die landesweiten Sensibilisierungsveranstaltungen zur Informationssicherheit an folgenden Terminen angeboten:

- 26. September – Leipzig, Audimax im Augusteum der Universität
- 1. Oktober – Chemnitz, Audimax der Technischen Universität
- 8. Oktober – Dresden, Rundkino

An allen Orten werden dabei jeweils zwei verschiedene Veranstaltungen angeboten:

- 8:30-12:30 Uhr: INFOSIC – Die Hacker kommen
  In der 4-stündigen Basis-Veranstaltung (inkl. halbstündiger Pause zur Hälfte) bekommen Sie in einer unterhaltsamen Mischung aus Vorträgen und Technikdemonstrationen (»Live-Hacking«) Informationen und Tipps zu folgenden Themengebieten:
  - Gefährdungen durch die Nutzung der modernen Informationstechnik
  - Tücken der Internetnutzung
  - Mobilität mit Sicherheitslücken
  - Der Mensch als Angriffsziel von Hackern
  - Digitale Identitäten

- 13:30-15:30 Uhr: INFOSIC plus – IT-Sicherheit für Fortgeschrittene
  In der 2-stündigen Veranstaltung werden ausgewählte Themen des Basis-Kurses detaillierter erläutert sowie weitere Themen der Informationssicherheit präsentiert, die nicht Teil des Basis-Kurses waren. Der Besuch lohnt sich vor allem für Teilnehmer, die schon eine klassische INFOSIC besucht haben und mehr wissen wollen.

Beide Sensibilisierungsveranstaltungen richten sich ausdrücklich an ALLE Mitarbeiterinnen und Mitarbeiter von Landes- und Kommunalbehörden und sind KEINE IT-Experten-Veranstaltungen.

Anmeldung unter lsnq.de/infosic2019

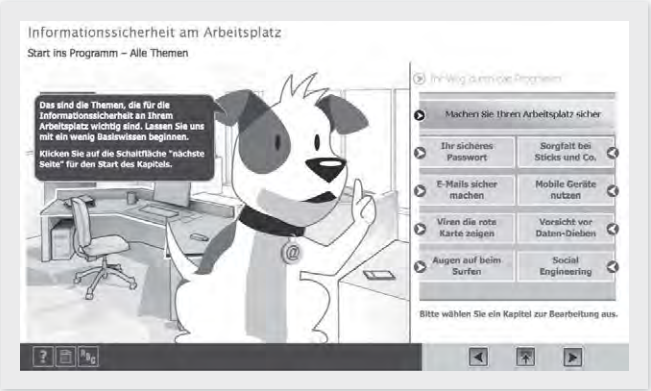
E-Learning zur Wiederholung und Vertiefung

So überaus gut besucht die INFOSIC-Veranstaltungen auch sind: Mit solchen Präsenzveranstaltungen allein kann Sensibilisierung und Fortbildung im Bereich Informationssicherheit nicht umfassend umgesetzt werden. Bei schätzungsweise 80.000 Computerarbeitsplätzen in den sächsischen Behörden auf Landes- und Kommunalebene ist es das Ziel, möglichst allen Bediensteten die Teilnahme an einer Sensibilisierung zu ermöglichen. Aus diesem Grund wird seit gut einem Jahr ein vom Beauftragten für Informationssicherheit des Landes in Zusammenarbeit mit der TU Dresden weiter entwickeltes E-Learning-Angebot zur Informationssicherheit an der HSF Meißen angeboten.

Kernstück des E-Learning-Angebotes ist die Lernwelt »Informationssicherheit am Arbeitsplatz«. Sie zeigt den teilnehmenden Behördenmitarbeitern, wie sie sensible Daten und Informationen sowohl am Arbeitsplatz, als auch im privaten Umfeld vor unberechtigtem Zugriff und Missbrauch schützen können. In der Lernwelt können sich die Bediensteten in insgesamt neun Kapiteln und ihrem eigenen Tempo mit verschiedenen Aspekten der »Informationssicherheit am Arbeitsplatz« beschäftigen. Die Kapitel bilden dabei eine Geschichte im Comic-Stil ab. Protagonisten der Geschichte sind u.a. Florian Sibe, Sicherheitsbeauftragter der Behörde, sein Assistent »@gar«, der immer wieder nützliche Tipps und Zusammenfassungen rund um

das Thema gibt, sowie Susanne, die IT-Spezialistin der Behörde, und die Putzfrau Lisa. Diese beiden wiederum kommen immer wieder zu Aspekten der Informationssicherheit ins Gespräch. Anlass dafür ist ein Sicherheitsvorfall in der Behörde, zu dem es in jüngster Zeit gekommen ist. Aufgabe des Nutzers ist es nun, diesen Sicherheitsvorfall aufzuklären. Um genau dies zu können, müssen die Bediensteten den Ursachen auf den Grund gehen. Dabei werden in den neun Kapiteln der Lernwelt wichtige Inhalte zur Informationssicherheit am Arbeitsplatz vermittelt. Die Bearbeitung aller Kapitel nimmt ca. vier bis fünf Stunden Zeit in Anspruch und kann auch in Etappen erfolgen. Es gibt dabei keine strikt festgelegte Reihenfolge für die Kapitel.

Das E-Learning-Modul wird mit einem Online-Test zum Sächsischen Informationssicherheits-Schein (SISS) abgeschlossen. Über 1.600 Mitarbeiter haben diesen Kurs bislang erfolgreich abgeschlossen.



Anmeldung unter: https://lsnq.de/InfosicAmAP

Der zertifizierte Netzübergang – ganz praktisch

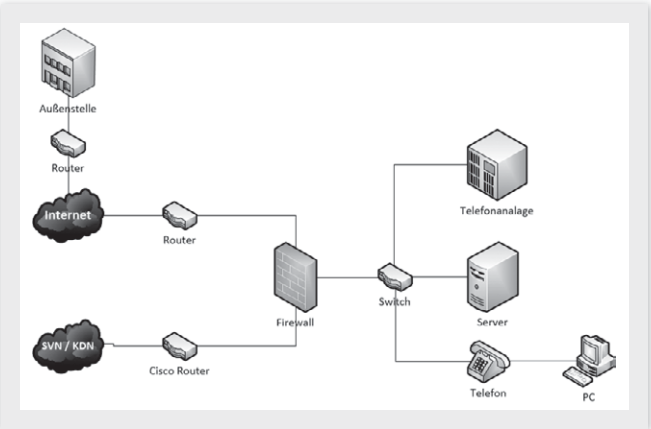
Marcus Kurth
Informationssicherheits-beauftragter KISA

Jan Lieder
Informationssicherheits-beauftragter KDN,
Netzwerkmanager KDN

Die Anbindung und ausschließliche Nutzung des Kommunalen Datennetzes (KDN) bietet für Kommunen ein hohes Maß an Sicherheit, welche durch die zentralen Systeme des KDN/SVN erreicht werden. Dennoch kann der Fall eintreten, dass die exklusive Nutzung des Kommunalen Datennetzes für eine Institution nicht ausreichend ist um spezielle Einsatzszenarien umsetzen zu können. Ein typisches Beispiel ist die Anbindung von vielen Außenstellen an die zentralen Systeme der jeweiligen Institution oder die Bereitstellung von eigenen individuellen Diensten im Internet. Ein Beispiel welches aktuell auf jede Institution zukommt, ist die Umstellung von ISDN-Telefonie auf IP-basierte Telefonie. Auch neue Dienste die im Zuge von Smart Cities zum Einsatz kommen, können eine solche Forderung aufstellen.

Um aus den individuellen Einsatzszenarien immer den bestmöglichen Nutzen zu ziehen und den administrativen Aufwand zu reduzieren, kommt es oftmals unweigerlich zu einer Überschneidung des KDN mit einem anderen Netz, wie beispielsweise einem weiteren DSL-Anschluss. Dieser Umstand ist bei der Nutzung des KDN nicht per se verboten, bedarf aber zwingend der Erfüllung der Bedingungen für den Betrieb eines sogenannten Fremdnetzübergangs. *In der Abbildung ist ein typischer Fremdnetzübergang anhand der Anbindung von Außenstellen und der Telefonie über einen weiteren DSL-Anschluss dargestellt.*

Für den Fall, dass dieser Fremdnetzübergang nicht vermieden werden kann, schreibt die KDN GmbH in seinen Nutzungsbedingungen vor, diesen Übergang von einem BSI-lizenzierten Auditor testieren zu lassen. Dieses



Testat erstreckt sich mindestens auf die beiden Bausteine und vorhandenen technischen Elemente Router/Switches (NET.3.1) und das Sicherheitsgateway/Firewall (NET.3.2) des BSI IT-Grundschutz Kompendiums in der aktuellen Edition. Mindestens diese Bausteine bedeuten in diesem Zusammenhang, dass der Auditor den zu überprüfenden Bereich auch erweitern kann. Dies kann beispielsweise dann notwendig werden, wenn die Institution zum Beispiel eine virtuelle Firewall im Einsatz hat. Somit erweitert sich der Fokus der Testierung um diesen Bereich. Was aber immer in den Audits enthalten ist, ist die Begehung des Serverraums in dem die Technik für den Fremdnetzübergang untergebracht ist. Hierbei wird ebenfalls mit Hilfe der Anforderungen des BSI IT-Grundschutz-Kompendiums die Sicherheit des Serverraums überprüft und bewertet.

Der Weg zu einer erfolgreichen Testierung eines Fremdnetzübergangs ist ein Prozess, welcher nicht in jeder Institution mit dem gleichen Aufwand bewertet werden kann. Die Erteilung eines Testats setzt voraus, dass für den Übergang eine Sicherheitskonzeption für die beiden o.g. Bausteine erstellt wird. Für die Dokumentation dieser Sicherheitskonzeption ist es erforderlich, dass alle Referenzdokumente im Rahmen einer Zertifizierung nach BSI IT-Grundschutz Kompendium (A0 bis A4, ggf. auch A5) vorliegen. Einen großen Anteil macht dabei die Prüfung der einzelnen Anforderungen der beiden Netz-Bausteine NET.3.1 und NET.3.2 aus. Jede

einzelne Anforderung der beiden Bausteine muss analysiert und dokumentiert werden. Exemplarische Anforderungen sind u.a. die Erstellung von Sicherheitsrichtlinien, Regelungen zum Schutz der Technik gegenüber Angriffen oder auch Konfigurationsvorgaben. Die Bewertung, Dokumentation und Umsetzung dieser einzelnen Anforderungen muss von einem, im Umgang mit der jeweils im Einsatz befindlichen Technik, geschulten Personal durchgeführt werden. Dies kann entweder durch den eigenen IT-Administrator selbst erfolgen oder man beauftragt für die Vorbereitung einen externen Dienstleister. Dabei kann dann immer individuell entschieden werden, wie viel Arbeit hausintern verbleibt bzw. wie stark der externe Dienstleister unterstützen soll. Grundsätzlich sollte eine Testierung nur dann angestrebt werden, wenn mindestens ein eigener IT-Administrator bei der Institution angestellt ist.

Wurde in der jeweiligen Institution bereits mit dem Aufbau eines Informationssicherheitsmanagementsystems (ISMS) begonnen, können daraus Vorteile für die Testierung gezogen werden. Dies kann beispielsweise sein, dass die Institution bereits eine Leitlinie zur Informationssicherheit verabschiedet hat oder den Serverraum nach den Anforderungen des BSI IT-Grundschutz Kompendium ertüchtigt hat. Aber auch das Vorhandensein eines klassischen Netzplans ist in der Vorbereitung für ein Testat sehr hilfreich.

Zusätzlich ist für den finanziellen Aufwand einer Testierung noch entscheidend, ob denn bereits die notwendige IT-Technik vorhanden ist. Hat die Institution aktuell keine eigene Firewall-Lösung im Einsatz, muss diese erst beschafft werden. Ist wiederum eigene Technik vorhanden muss die Frage gestellt werden, ob diese denn die Anforderungen des BSI erfüllen kann. Auch bei der Klärung dieser Fragen bietet sich der Kontakt zu externen Dienstleistern an.

Somit sind für den finanziellen Aufwand folgende Faktoren zu benennen:
- Vorhandensein geeigneter Technik oder Neu-/Erstbeschaffung entsprechender Technik
- Umfang der Unterstützungsleistungen durch externe Dienstleister
- aktueller Stand im Aufbau eines ISMS

»Nach dem Testat ist vor dem Testat.«
Der Aufbau eines ISMS ist ein Prozess und auch die Testierung eines Fremdnetzübergangs ist in diesem Zusammenhang ein Teil dessen, welche nicht mit der Erteilung des Auditberichts abgeschlossen ist. Ein ausgestelltes Testat ist maximal 2 Jahre gültig. Im Normalfall ist es auch erst mit Ablauf dieser Zeit notwendig, diesen Testierungsprozess wieder aufzugreifen. Für die erfolgreiche Retestierung müssen die Ergebnisse des Auditberichts bearbeitet und dokumentiert sein, um gegenüber dem Auditor auch die Nacharbeit nachzuweisen. Sollte es aber im Rahmen der 2 Jahre zu Änderungen am vormals testierten Fremdnetzübergang kommen, wie beispielsweise die Beschaffung neuer Technik oder auch der kompletten Änderung des Übergangs, verliert das Testat seine Gültigkeit. In diesem Fall muss der Retestierungsprozess bereits vor Ablauf der 2 Jahre begonnen werden.

Die reine Möglichkeit seitens des KDN, einen Fremdnetzübergang zu betreiben, kann für eine angeschlossene Institution Vorteile bringen, wird aber gleichermaßen auch an hohe Vorgaben zur Informationssicherheit geknüpft. Die Erfüllung dieser Vorgaben und damit der Erhalt eines Testats für den Fremdnetzübergang ist aber ein realistisches Projekt. Dennoch muss die Entscheidung für ein solches Projekt sehr gut überlegt sein, denn die Vorbereitung und die Aufrechterhaltung aller Sicherheitsmaßnahmen fordern personelle und finanzielle Ressourcen. Aus diesem Grund sollte im ersten Schritt immer geprüft werden, ob die geplanten Einsatzszenarien nicht auch ohne einen Fremdnetzübergang umgesetzt werden können.

IP-Telefonie (VoIP) und Informationssicherheit

Uwe Nikol
Fachberater SAKD

Franziska Blume
Netzwerkmanagerin KDN

Als Telefone und ISDN-TK-Anlage noch eine separate Infrastruktur ohne physische Verbindung zum Datennetz einer Verwaltung gebildet haben, hatte der IT- Sicherheitsverantwortliche einige Probleme weniger: Sein Datennetz konnte vom Telefonnetz nur dort angegriffen werden, wo die ISDN- und LAN-Infrastruktur eine Verbindung hatten, zum Beispiel über Multifunktionsdrucker, die sowohl eine LAN-Verbindung als auch einen ISDN-Karte für die Fax-Funktion haben. Bekannt sind über diesen Weg geführte Netzangriffe durch manipulierte Faxe, mit dem Ziel, Schadcode auf dem Betriebssystem des Multifunktionsgerätes zu installieren. Auch direkte ISDN-Angriffe auf TK-Anlagen sind möglich; sie haben meist das Ziel, automatisiert teure Telefonate zu generieren. Die Möglichkeit, im Datennetz Schaden anzurichten, besteht durch die physische Trennung dabei nicht.

Die Zeiten dieser relativen Unabhängigkeit von Telefonie- und Datennetz sind jedoch vorüber. Alle Provider sind aktuell dabei, ihre Netze zu konsolidieren und Telefoniedienste nur noch IP-basiert (Internet Protocol) anzubieten. Das Netzprotokoll für den Aufbau und die Steuerung der Verbindung ist »SIP« (Session Initiation Protocol) für Telefone und »SIP-Trunk« für TK-Anlagen. Für die Aushandlung der Kommunikationsdetails und den eigentlichen Transport der Audio-Daten kommen dann weiter auf IP basierende Netzprotokolle zum Einsatz; diese können auch die Verschlüsselung des Transportkanals übernehmen.

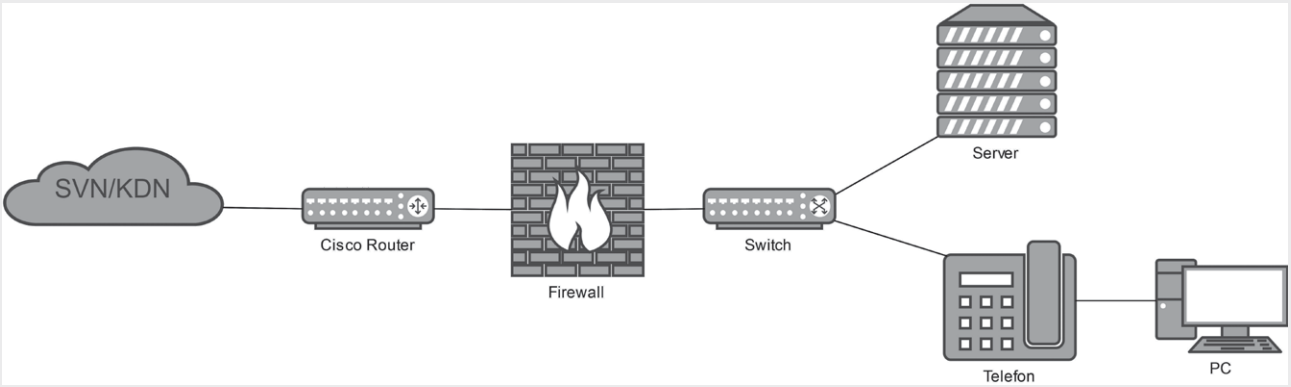
Mit der Umstellung der Technologie auf Providerseite ergibt sich entsprechender Handlungsdruck bei den Nutzern. Viele Kommunalverwaltungen haben diesen Schritt bereits vollzogen und sowohl ihre externe als auch ihre interne Telefonie konsequent auf VoIP (Voice over IP) umgestellt. Gleichzeitig wurden einige notwendige Dienste wie zum Beispiel für EC-Cash Geräte ins Datennetz der KDN III migriert. Je nach vorhandener Netzwerkgröße bzw. Komplexität bedarf die Migration auf IP-Telefonie einer außerordentlich sorgfältigen und langfristen Planung sowie Umsetzung einschließlich Tests. Andere haben sich entschieden bei Umstellung auf Providerseite ihre existierende ISDN-Technik vorerst mit Hilfe von VoIP-Adaptern weiter zu benutzen. Das kann jedoch nur eine Übergangslösung sein. Spätestens am Lebensende der alten TK-Anlage muss gehandelt werden. ISDN-TK-Anlagen und klassische Zweidraht-Telefone werden vom Markt verschwinden.

VoIP-Umstellung bedeutet, dass jedes Endgerät (Telefon) über eine IP-Adresse verfügen und über eine entsprechende Netz-Infrastruktur erreichbar sein muss. Damit sind die Geräte via Internet-Technologie angebunden und können über das Internet-Protocol (IP) angegriffen werden. Das Gleiche gilt für die Dienste einer VoIP-TK-Anlage. Audiodaten sind damit prinzipiell den gleichen Gefährdungen ausgesetzt wie alle Daten in einem Netz und müssen bezüglich ihrer Verfügbarkeit und Vertraulichkeit geschützt werden. Dagegen spielt die Integrität der Audiodaten bei einem Telefonat eher eine untergeordnete Rolle. Hinzu kommen einige Telefonie-spezifische Gefährdungen wie Gebühren- oder Identitätsbetrug oder die prinzipielle Gefährdung, die sich dadurch ergibt, dass ein zusätzlicher TK-Provideranschluss als weiterer Internetanschluss mit entsprechenden Sicherheitsanforderungen zu betrachten ist und dies gegenüber der KDN GmbH angegeben werden muss bzw. in der Erklärung zur Datensicherheit im KDN III aktualisiert werden muss. In jedem Fall müssen die Verwaltungen in ihrem Sicherheitskonzept die Aspekte der VoIP-Telefonie, inklusive eines Notfallkonzeptes, mit betrachten.

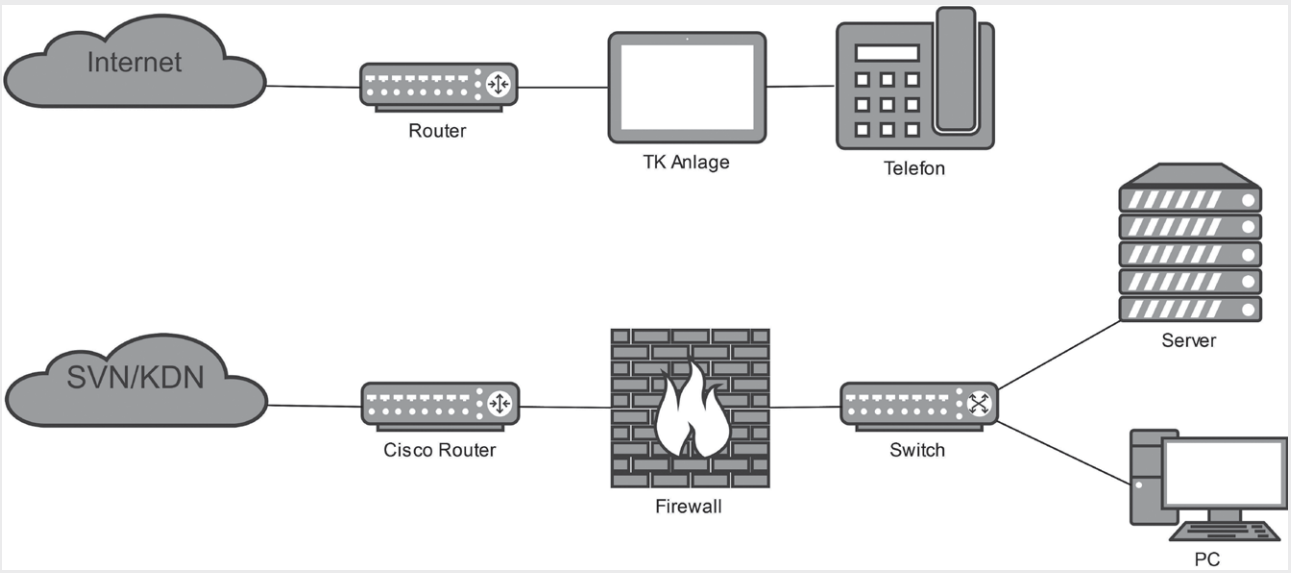
Ein wirksamer Ansatz zur Reduzierung der Sicherheitsprobleme besteht in der Trennung zwischen VoIP-Telefonienetz und Datennetz, wie es zu Zeiten der konventionellen Telefonie üblich war. Tatsächlich entfallen damit alle Angriffsmöglichkeiten auf das Datennetz aus dem Adressbereich der VoIP-Dienste und IP-Telefone. Diese Trennung kann virtuell erfolgen, indem auf gemeinsamer Ethernet-Switch-Infrastruktur getrennte Layer-2-VLANs (Virtual Local Area Network) konfiguriert werden. Dies gilt unter der Voraussetzung, dass das VoIP-Telefonienetz ebenfalls wie das Datennetz ganzheitlich im KDN III betrieben wird. Ist der Verzicht auf einen Drittanbieter nicht möglich oder nicht gewollt, ist eine entsprechende Testierung nach BSI notwendig.

Eine andere Möglichkeit ist die physische Trennung, indem separate Switches für Telefonie- und Datennetz zum Einsatz kommen. Bei Bezug der Telefonie über einen Drittanbieter ist das gesamte Netzwerk einschließlich Router des Providers physisch vom KDN Datennetz zu trennen. Im Fall der physischen Trennung ergibt sich noch der zusätzliche Nachteil, dass die doppelte Anzahl an Verbindungen und Patchmöglichkeiten zum Endplatz benötigt werden, da der in der Regel im IP-Telefon integrierte VLAN-Switch nicht für den Anschluss von PC oder Notebook verwendet werden kann.

Besteht lediglich der Anspruch, den aus der konventionellen Telefonie gewohnten Funktionsumfang auch in der VoIP-Umgebung zu haben und nur zu telefonieren, ist die übergangslose Netztrennung unter den Sicherheitsaspekten eine gute Lösung.



Beispiel: Telefonie- und Datennetz im KDN – Zentrale Lösung



Beispiel: Internetanschluss von Drittanbieter für Telefonie und Datennetz KDN physisch getrennt

Damit sind aber wesentliche funktionale Mehrwerte, die VoIP bietet, nicht mehr nutzbar: Die Verbindung von Computer- und Telefoniediensten (Computer Telephony Integration CTI). Als Beispiele dafür seien hier die unter dem Begriff UC (Unified Communications) zusammengefassten Möglichkeiten der Integration von Audio- oder Video-Informationen in E-Mailsysteme oder andere Kommunikationsdienste genannt oder auch der automatische Aufruf von Datenbankinhalten in Abhängigkeit vom Teilnehmernummer eines eingehenden Anrufes, der als Call-Center-Applikation zum Einsatz kommen kann. Um diese Dienste nutzen zu können ist es zwingend erforderlich, zwischen den Computerdiensten des Datennetzes und dem Telefonienetz eine Verbindung zu schaffen, entweder indem beide Netzbereiche im selben Adressbereich liegen (flache Netzarchitektur) oder indem zwischen den getrennten VLANs eine IR-Routinginstanz etabliert wird. In beiden Fällen sind alle Telefoniedienste und –geräte den gleichen Angriffsszenarien und Risiken ausgesetzt wie PCs, Server oder Dienste im Datennetz.

Telefonie ist für jede Verwaltung eine unternehmenswichtige Anwendung, so dass die VoIP-TK-Anlage, unabhängig davon, ob diese als Hardwaregerät (Appliance), Dienst auf einem Server, oder als Software in Form einer virtuellen Maschine (VM) ausgeführt wird, den Status eines wichtigen Severs bekommen sollte. Damit ergeben sich entsprechende Sicherheitsanforderungen, wie das Absichern eines immer aktuellen Patchlevels, entsprechender Zugangs- und Zugriffsschutz oder die Integration in die Backupmechanismen der Verwaltung. Die Probleme können teilweise entschärft werden, indem man die Verantwortung – sofern möglich – dafür in die Hände eines Providers legt. Er kann die TK-Anlage für seine Kunden als Cloud-Lösung betreiben. Neben wirtschaftlichen Überlegungen (abhängig vom Portpreis pro IP-Telefon) setzt das ein großes Vertrauen in den Provider voraus, da de facto das eigene Telefonbuch außer Haus gegeben wird – mit allen Gefährdungen bezüglich Identitäts- und Vertraulichkeitsschutz. Das gleiche Vertrauen in die Leistungsfähigkeit des Providers ist bei der Leitung für die Audio-Kommunikation erforderlich. Bei Ausfall dieser Leitung ist keine externe Telefonkommunikation mehr möglich; das Weiterfunktionieren der internen Telefonie kann über technische Optionen im Zugangsrouter abgesichert werden. Im Notfallkonzept der Verwaltung sollten diese Fälle betrachtet werden. Neben der Verfügbarkeit der Leitung sind mögliche Netzangriffe darüber zu betrachten. Nicht bei allen TK-Provideranschlüssen kann davon ausgegangen werden, dass nur die für die VoIP-Kommunikation erforderlichen Protokolle darüber transportiert werden. Vielmehr ist davon auszugehen, dass es sich um einen vollwertigen Internetanschluss handelt und entsprechende Absicherungen des eigenen Datennetzes (Firewall) erforderlich sind.

Seit Einführung des KDN III tritt die KDN GmbH auch als Anbieter von VoIP-Diensten auf. Damit haben sächsische Kommunen jetzt die Möglichkeit, Telefoniedienste über das KDN III mit dem dort realisierten hohen Sicherheitsniveau zu beziehen. Je nach vorhandenen bzw. gewünschten Kriterien stehen dabei verschiedene Lösungen zur Verfügung. Es werden ISDN sowie VoIP-fähige Telefonanlagen unterstützt, aber auch eine Zentrale Lösung wird angeboten.

Informationen und Ansprechpartner:

Frank Schlosser – KDN GmbH – schlosser@kdn-gmbh.de
Jan Lieder – KDN GmbH - lieder@kdn-gmbh.de
Franziska Blume – KDN GmbH – blume@kdn-gmbh.de
weitere Informationen: www.kdn-gmbh.de

Uwe Nikol – SAKD – nikol@sakd.de
weitere Informationen: www.sakd.de

Marcus Kurth – KISA – marcus.kurth@kisa.it
weitere Informationen: https://www.kisa.it/de/it-sicherheit.html

Matthias Martin – SSG – matthias.martin@ssg-sachsen.de
weitere Informationen: https://www.ssg-sachsen.de/index.php?id=informationssicherheit

Informationssicherheit in Sachsen
https://www.egovernment.sachsen.de/informationssicherheit.html

BSI - Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de

Wenn guter Rat teuer ist: Richtig reagieren im IT-Sicherheits-Notfall

Christian Kuß, LL.M. (Bristol)
Rechtsanwalt

Die Computersysteme wurden gehackt und Daten abgegriffen. Der Laptop wurde im Taxi vergessen, das Passwort steht auf dem Post-IT auf der Unterseite. Was ist zu tun? Dieser Beitrag gibt einen Überblick über die Handlungspflichten – auch nach dem neuen Sächsischen Informationssicherheitsgesetzes – und Best Practices im Umgang mit IT-Sicherheitsvorfällen.

1. Die Ausgangslage

Angesichts der steigenden Gefahren für die Sicherheit von informationstechnischen Systemen wird es immer bedeutsamer, sich mit den drohenden Risiken und möglichen Gegenmaßnahmen auseinanderzusetzen. 2017 und 2018 führten Cybersecurity-Vorfälle zu einem wirtschaftlichen Schaden in Höhe von insgesamt über 40 Milliarden Euro – allein in der deutschen Wirtschaft. Dass aber nicht nur Unternehmen der Privatwirtschaft gefährdet sind, sondern auch die öffentliche Hand Opfer von Cyberattacken werden kann, zeigte sich, als persönliche Daten von Mitgliedern des Bundestages im Internet veröffentlicht wurden.

Aber auch im Freistaat Sachsen spielt das Thema Informationssicherheit eine Rolle: Nach Angaben des zentralen Computernotfallteams (SAX.CERT), wonach im Jahr 2018 im Staatsbetrieb Sächsische Informatikdienste (SID) etwa 80 Millionen Spam-Mails abgewiesen und im E-Mail-Verkehr fast 100.000 Viren erkannt wurden, wird deutlich, dass die Gefahren für die Sicherheit informationstechnischer Systeme enorm sind. Umso bedeutsamer wird es – gerade auch im Hinblick auf die fortschreitende Digitalisierung der Verwaltung – sich nicht nur der Vorbeugung und Abwehr möglicher Gefahren zuzuwenden, sondern sich auch damit auseinanderzusetzen, wie im Ernstfall richtig zu reagieren ist.

2. Die Gesetzeslage im Überblick

Der Gesetzgeber hat in den letzten Jahren mehrere Gesetze erlassen, um der steigenden Bedrohungslage für die Sicherheit informationstechnischer Systeme Schutzmaßnahmen entgegenzusetzen. Auf EU- und Bundesebene wurden verschiedene Regularien mit dem Ziel erlassen, die Cybersicherheit zu erhöhen. In den Bundesländern haben bisher das Saarland und Bayern entsprechende Gesetzesvorhaben initiiert. Auf europäischer Ebene ist hier der Erlass der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, kurz NIS-Richtlinie, im Jahr 2016 hervorzuheben. Diese war durch den deutschen Gesetzgeber in nationales Recht umzusetzen, was mit dem Informationssicherheitsgesetz auch geschehen ist. Das Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen soll nun die rechtlichen Rahmenbedingungen für die Gewährleistung der Informationssicherheit in der Verwaltung des Freistaates Sachsen schaffen.

Es richtet sich an Behörden und Gerichte als staatliche Stellen sowie an öffentlich-rechtliche Körperschaften, Anstalten und Stiftungen als nicht-staatliche Stellen. Wesentliche Zielsetzungen sind der Erhalt der Leistungsfähigkeit und Effizienz der Verwaltung sowie die Verwaltungsmodernisierung. Das Gesetz soll die Informationssicherheit in den staatlichen und nicht-staatlichen Stellen erhöhen und Gefahren für informationstechnische Systeme abwehren.

3. Gesetzliche Vorgaben im Rahmen eines Sicherheitsvorfalls

Zur Erhöhung der Cybersecurity sieht das Gesetz im Wesentlichen vor, die Befugnisse der Beauftragten für Informationssicherheit und des Sicherheitsnotfallteams auszuweiten. Zentrale Regelung im Zusammenhang mit der Reaktion auf Sicherheits-Notfälle sind insbesondere die vorgesehenen Meldepflichten. Diese sollen dazu dienen, aus vergangenen Vorfällen zu lernen, um in der Zukunft auf ähnlich gelagerte Vorfälle vorbereitet zu sein und diesen mit wirksamen Abwehrstrategien zu begegnen. Das Sammeln, Auswerten und Untersuchen von Informationen über Sicherheitsrisiken oder -vorkehrungen und die gegenseitige Information, Beratung und Warnung sind nach der Begründung wesentliche Bestandteile des Schutzes der Informationssicherheit. Die Meldepflichten werden im vierten Abschnitt geregelt, wobei zwischen stellenübergreifenden Meldepflichten und Pflichten der staatlichen Stellen sowie Pflichten der nicht-staatlichen Stellen unterschieden wird.

Das Gesetz stellt außerdem die grundsätzliche Verpflichtung für staatliche und nicht-staatliche Stellen auf, angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zur Gewährleistung der Informationssicherheit zu treffen und stellt maßgeblich auf den Stand der Technik ab. Für die Verarbeitung personenbezogener Daten ergibt sich diese Verpflichtung aber auch bereits aus der Datenschutzgrundverordnung, so dass sich insofern keine Neuerungen aus dem Sächsischen Informationssicherheitsgesetz ergeben werden, soweit der Schutz personenbezogener Daten im Raum steht.

Kommt es zu einem IT-Sicherheitsvorfall, stehen potentiell verschiedene Meldepflichten im Raum. Das Informationssicherheitsgesetz des Bundes sieht derartige Meldepflichten vor, die sich aber nur an Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste richten. Die Betreiber haben bei einem IT-Sicherheitsvorfall diesen der Aufsichtsbehörde zu melden. Diese Meldungen müssen ausführlich sein, um eine Verfolgung der Attacken und die Entwicklung wirksamer Schutzmaßnahmen zu ermöglichen und unter anderem Angaben zur Störung sowie Auswirkungen, Ursachen und betroffener Informationstechnik enthalten. Die Meldepflicht greift nur ein bei Störungen, die negative Auswirkungen auf die kritische Infrastruktur haben oder bei Störungen, die eine solche negative Auswirkung haben könnten und erheblich sind. Anbieter digitaler Dienste sind nur bei erheblichen Auswirkungen eines Sicherheitsvorfalls zur Meldung verpflichtet. Eine regelmäßige Meldepflicht, wie im Sächsischen Informationssicherheitsgesetz, ist nicht vorgesehen.

3.1. Was ist ein IT-Sicherheits-Notfall?

Ein Notfall beschreibt eine Situation, in der eine Gefahr oder ein Schaden einzutreten droht. Ein IT-Sicherheits-Notfall liegt also vor, wenn die IT-Sicherheit gefährdet oder geschädigt werden kann. Die Informationssicherheit umfasst im Kern die Gewährleistung des Schutzes von Vertraulichkeit, Integrität und Verfügbarkeit von in informationstechnischen Systemen verarbeiteten Daten. Eine Gefährdung oder Schädigung der Vertraulichkeit, Integrität oder Verfügbarkeit kann Folge verschiedener Ereignisse sein, die von der bewussten Ausnutzung einer Sicherheitslücke mittels Hackerangriffs über das Einschleusen von Schadsoftware bis zu einem versehentlich Fehlverhalten eines Mitarbeiters reichen.

Das Sächsische Informationssicherheitsgesetz nennt den Begriff des Sicherheitsnotfalls zwar nicht, unterscheidet aber zwischen einem Sicherheitsvorfall und einem Sicherheitsereignis und knüpft an deren Vorliegen unterschiedliche Meldepflichten. Ein Sicherheitsvorfall liegt vor, wenn die zum Schutz der Informationssicherheit implementierten Maßnahmen versagt haben. Folge des Vorfalls ist eine Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit. Es ist nach einem Sicherheitsvorfall also tatsächlich zu negativen Auswirkungen auf die Informationssicherheit gekommen. Ein Sicherheitsereignis stellt demgegenüber die Vorstufe des Vorfalls dar. Es liegt vor, wenn der Versuch unternommen wurde, die Informationssicherheit zu verletzen.

3.2. Stellenübergreifende Meldepflichten

§ 15 SächsISichG verpflichtet alle an das Sächsische Verwaltungsnetz oder das Kommunale Datennetz angeschlossenen Stellen, unabhängig davon, ob es sich um staatliche oder nicht-staatliche Stellen oder Beliehene handelt. Die Meldung an das Sicherheitsnotfallteam erstreckt sich auf sämtliche für die Abwehr von Gefahren für die Informationssicherheit relevanten Informationen. Hierunter fallen Informationen über Sicherheitslücken in genutzter Software, erkannte Schadprogramme sowie erfolgte oder versuchte Angriffe. Die Meldung muss unverzüglich und unabhängig von der Betroffenheit der jeweiligen Stelle erfolgen. Sie greift also auch dann ein, wenn gar kein Sicherheitsereignis oder Sicherheitsvorfall vorliegt

Die Meldepflicht betrifft Informationen zu Ereignissen, die stellenübergreifend sind oder sein können, also in ihrer Wirkung mehr als nur eine einzelne Behörde treffen könnten. Ziel dieser Meldepflicht ist die umfassende Information des Sicherheitsnotfallteams, so dass es in die Lage versetzt wird, andere Stellen zu warnen. Deshalb sollen in den Fällen, in denen die zu meldenden Informationen einer gesetzlichen Beschränkung zur Weitergabe unterliegen – z. B. aus Gründen des Geheimschutzes – im Zweifel auch diejenigen, der Beschränkung nicht unterliegenden Teile der Information an das CERT übermittelt werden. Unvollständige Informationen sind mit Blick auf die Möglichkeit, andere Behörden warnen zu können, besser als gar keine Informationen.

3.3 Meldepflichten der staatlichen Stellen

Für staatliche Stellen, also Behörden und Gerichte, sieht § 16 SächsISichG eine Meldepflicht für Sicherheitsereignisse und Sicherheitsvorfälle ihrer Systeme vor. Die Pflicht entsteht mit dem Eintreten des Ereignisses bzw. Vorfalls, ohne dass es einer Aufforderung durch das CERT bedarf.

Hat ein Sicherheitsvorfall eine erhebliche Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit der im System verarbeiteten Daten zur Folge oder kann er behördenübergreifend zu einer erheblichen Beeinträchtigung führen, hat die Meldung unverzüglich zu erfolgen. Dies ist der Fall, wenn der Sicherheitsvorfall die erbrachten Dienstleistungen der Behörde oder des Gerichts bedroht oder wenn er nicht automatisch oder mit wenig Aufwand abgewehrt werden kann. Unabhängig davon gelten unerwartete, neuartige oder außergewöhnliche Sicherheitsvorfälle sowie gezielte Angriffe stets als erheblich in dem Sinne, so dass diese unverzüglich zu melden sind. Umgekehrt sind täglich vorkommende Ereignisse wie Spam, vom Virenscanner gestoppte Schadsoftware und Hardwareausfälle im üblichen Rahmen von der unverzüglichen Meldepflicht ausgenommen.

Durch die Meldung kann das CERT Maßnahmen empfehlen, um den Schaden zu minimieren und ein zuverlässiges Lagebild über den Schaden sowie die Lage der Informationssicherheit erhalten. Letzterem dient auch vor allem die Meldepflicht über statistische Angaben und Protokolldaten in Bezug auf Sicherheitsereignisse und nicht unverzüglich zu meldende Sicherheitsvorfälle, also Sachverhalte, die keine akuten Gefahren für die Informationssicherheit mit sich bringen. Die Information hierüber soll in regelmäßigen Abständen erfolgen. Die Staatsregierung wird ermächtigt, die Modalitäten des Meldeverfahrens durch Rechtsverordnung zu regeln.

3.4 Meldepflichten der nicht-staatlichen Stellen

Die öffentlich-rechtlichen Körperschaften, Anstalten und Stiftungen unterliegen den gleichen Meldepflichten wie staatliche Stellen, wenn sie mit dem Sächsischen Verwaltungsnetz oder dem Kommunalen Datennetz verbunden sind. Anderenfalls steht es ihnen frei, Sicherheitsereignisse und -vorfälle an das CERT zu melden.

3.5 Weitere Meldepflichten

Bezieht sich der Sicherheitsvorfall auf personenbezogene Daten einer natürlichen Person, ist auch die Meldepflicht an die Datenschutzaufsichtsbehörde nach der DSGVO zu beachten. Demnach hat im Falle einer Verletzung des Schutzes personenbezogener Daten die Meldung unverzüglich und möglichst innerhalb von 72 Stunden zu erfolgen. Unter Umständen sind auch die von dem Vorfall betroffenen Personen zu benachrichtigen Eine Verletzung der Melde- und Benachrichtigungspflicht kann ein Bußgeld nach sich ziehen.

4. Vorsicht ist besser als Nachsicht

Wenn der Notfall tatsächlich eintritt, ist schnelles Handeln angesagt, um den Schaden zu vermeiden oder zumindest so gering wie möglich zu halten. Ohne ausreichende Vorbereitung ist dies meist nicht möglich. Deshalb ist es wichtig, sich bereits im Vorfeld mit den Grundsätzen der Informationssicherheit auseinanderzusetzen. Unerlässlich ist die Information anhand des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Auch ist ein Notfallmanagementsystem zu etablieren. Dieses sollte neben ausdrücklich geregelten Zuständigkeiten auch Sofortmaßnahmen vorsehen und eine Organisation für die Handhabung des Vorfalls vorsehen. Es sollte ausdrücklich regeln, wer im Fall der Fälle die Verantwortung trägt, also letztendlich die Entscheidungen trifft. Es sollte keine Unklarheiten geben, an wen sich Mitarbeiter mit einem möglichen Verdacht in Bezug auf einen Sicherheitsvorfall wenden können und wer den Vorfall an wen zu melden hat.

So können Notfälle nicht nur schnell ermittelt werden, sondern auch hinsichtlich der möglichen Folgen und notwendiger Gegen- und Folgemaßnahmen analysiert werden. Dafür ist auch eine Einbindung und entsprechende Schulung der Mitarbeiter für das Verhalten im Notfall notwendig. Ohne entsprechendes Sicherheits- und vor allem auch Problembewusstsein der Mitarbeiter bleiben Ereignisse und Vorfälle möglicherweise längere Zeit unentdeckt, was zu vertieften Schäden führen könnte.

5. Richtig reagieren

Sobald ein Sicherheitsvorfall eintritt, ist dieser entsprechend der Vorgaben des neuen Sächsischen Informationssicherheitsgesetzes bzw. für Betreiber kritischer Infrastrukturen nach dem BSI-G unverzüglich an die entsprechende Stelle zu melden. Mit der Meldung des Vorfalls hat die von dem Vorfall betroffene Stelle aber noch nicht alle Handlungspflichten erfüllt. Vielmehr sind die notwendigen Vorkehrungen zu treffen, um die Risiken für die Rechte und Freiheiten der betroffenen Personen möglichst gering zu halten. Hieraus folgt die Pflicht, den Vorfall zu untersuchen und gegebenenfalls Maßnahmen abzuleiten, die eine Wiederholung des Vorfalls verhindern. Der Verantwortliche muss also Sicherheitslücken schließen und das System vor Hackerangriffen schützen. Möglicherweise ist auch das System vom Netzwerk zu trennen, um eine Weiterverbreitung der Gefährdung zu verhindern. Bei der Aufarbeitung des Vorfalls sollte am besten ein Forensik-Spezialist eingebunden werden. Das Team um das CERT wird gegenüber den Behörden und Gerichten die nötigen Anordnungen treffen oder erforderliche Maßnahmen ergreifen. Für die Selbstverwaltungsträger wird es mit möglichen Handlungsoptionen beratend zur Seite stehen. In Betracht kommt auch eine strafrechtliche Aufarbeitung durch die Staatsanwaltschaft.

6. Fazit

Mit der entsprechenden Vorbereitung ist auch der IT-Sicherheitsnotfall in den Griff zu bekommen. Problembewusstsein und eine stabile

Organisation sind hier das A und O. Die neuen Meldepflichten im Sächsischen Informationssicherheitsgesetz werden es dem CERT insoweit vereinfachen, einen umfassenden Überblick über die Lage der Informationssicherheit im Freistaat Sachsen zu erstellen. Insgesamt leistet das Gesetz einen wichtigen Beitrag zur Erhöhung der Sicherheit informationstechnischer Systeme und folgt den Maßnahmen im Rahmen der Cyberstrategie auf EU- und Bundesebene. So sind Behörden und Gerichte gut gewappnet, um den steigenden Cybergefahren zu trotzen.

7. Checkliste

Sind Sie fit für den IT-Sicherheitsnotfall? Anhand dieser Checkliste können Sie sich einen schnellen Überblick verschaffen.

I. Vorbereitende Maßnahmen:
   - Gibt es ein Notfallmanagementsystem? Enthält dieses:
     - Verantwortlichkeiten?
     - Interne Ansprechpartner?
     - Sofortmaßnahmen?
     - Kontaktdaten der Meldestellen?
   - Sind Mitarbeiter sensibilisiert und geschult?

II. Bei Eintritt des Sicherheits-Vorfalls:
   - Meldung an das CERT notwendig und ggf. erfolgt?
   - Sofortmaßnahmen nach dem Notfallmanagementsystem erfolgt?
   - Maßnahmen zur Beweissicherung und Untersuchung des Vorfalls erfolgt?
   - Maßnahmen zur Verhinderung zukünftiger Vorfälle erfolgt?

Kassensicherheit – Nur eine Aufgabe der IT?

Norbert Fischer
Diplom-Wirtschaftsingenieur (FH)

Welche grundlegenden Anforderungen bestehen an die Kassensicherheit?

Unter dem Schlagwort »Digitale Verwaltung« unterliegt das kommunale Verwaltungshandeln einer dauerhaften Veränderung. Der digitale Wandel betrifft viele Bereiche der Verwaltung und fordert ein Umdenken sowie eine Neuausrichtung der Organisation. Die stetige Weiterentwicklung von Verwaltungsprozessen im Sinne der Digitalisierung ist ein unaufhaltsamer Prozess, von dem alle Beteiligten profitieren werden.

Bereits seit einiger Zeit werden Verwaltungsprozesse durch fachspezifische IT-Lösungen unterstützt. Viele Tätigkeiten in der Kassenverwaltung sind heute schon automatisiert. Die Kasse bedient sich dabei unter anderem elektronischer Kassensysteme, Kassenautomaten, elektronischer Bezahlsysteme und professioneller Finanzsoftware zur Abwicklung von Bankgeschäften, um nur eine Auswahl typischer IT-Lösungen zu nennen. Die Verwaltungsprozesse in der Kasse unterliegen dabei vielen gesetzlichen Normierungen, die sich zum Teil erheblich von denen der Privatwirtschaft unterscheiden und sind daher nur mit großen Hürden in die digitale Welt zu überführen. Damit die Digitalisierung fortschreiten kann, wird zunehmend der Zuschnitt der Verwaltungsprozesse an die Möglichkeiten der IT-Lösungen angepasst. Das stößt dann auf Grenzen, wenn durch die Anpassung der Verwaltungsprozesse die bestehenden Rechtsgrundlagen nicht eingehalten werden. Mit dem verstärkten Einsatz von Soft- und Hardware im Sinne der Digitalisierung besteht sicherlich Anpassungsbedarf an die gesetzlichen Normierungen, um der digitalen Weiterentwicklung den notwendigen Raum zu lassen. Der Automatisierungsgedanke rückt dabei das Thema IT-Sicherheit immer stärker in den Fokus.

Die große Vielfalt von elektronischen Geräten und unterschiedlichen Softwarelösungen erfordert ein immer komplexeres Sicherheitssystem. Die Sicherheit im Kassenbereich wird dabei von den Anforderungen an das bestehende IT-System sowie an die Softwarelösungen geprägt. Das Sicherheitsgefühl nimmt mit dem Einsatz aktueller Soft- und Hardware zu. In unserer Beratungspraxis stellen wir fest, dass vor dem Hintergrund der Dominanz von IT-Sicherheit die Bereiche der Organisation der Aufgabenwahrnehmung, der räumlichen Ausstattung und des Personaleinsatzes nicht die notwendige Beachtung finden. Die IT-Sicherheit deckt nur einen Teil der Sicherheitsanforderungen im Kassenbereich ab. Um den inneren und äußeren Sicherheitsanforderungen gerecht zu werden, bedarf es aus unserer Sicht einer personellen, organisatorischen, räumlichen und sachlichen Betrachtung der Sicherheitsthematik (siehe Abbildung 1).

Dienstanweisung zur Errichtung und zum Geschäftsgang der kommunalen Kasse	**Arbeits- und Datenschutz**
Innere Sicherheit – Sichere und ordnungsgemäße Erledigung von Geschäftsvorfällen der Gemeindekasse und Vermeidung von Manipulationsmöglichkeiten	Äußere Sicherheit – Sichere Verwahrung von Zahlungsmitteln, Wertgegenständen etc. und Verhinderung von Einbruch, Diebstahl und Überfällen
Personell	Räumlich
Organisatorisch	Sachlich

Abbildung 1: Perspektiven der Kassensicherheit (eigene Darstellung)

Der Gesetzgeber hat für das Einrichten und Betreiben einer Kasse besondere Normierungen geschaffen, die über das übliche Maß hinausgehen. Der Grund dafür besteht darin, dass der Kassenbereich eine besondere Stellung in der Verwaltung einnimmt, da in diesem Bereich öffentliche Gelder verwaltet und verwahrt werden. In Sachsen werden die Bestimmungen in der *Sächsischen Kommunalen Kassen- und Buchführungsverordnung* (SächsKomKBVO) geregelt. Nach § 5 SächsKomKBVO ist die Gemeindekasse so einzurichten, dass

1. sie ihre Aufgaben ordnungsmäßig und wirtschaftlich erledigen kann,
2. für die Sicherheit der Beschäftigten gegen Überfälle angemessen gesorgt ist,
3. Datenverarbeitungseinrichtungen oder -systeme, Automaten für den Zahlungsverkehr und andere technische Hilfsmittel nicht unbefugt benutzt werden können und
4. die Zahlungsmittel, die zu verwahrenden Gegenstände, die Bücher, das Inventar und die Belege sicher aufbewahrt werden können.

Neben Sachsen haben auch andere Bundesländer ähnliche Regelungen. Aufgrund der Vielzahl von unterschiedlichen kommunalen Kassen, kann dieser Artikel nicht alle Besonderheiten der erforderlichen Sicherheit aufzeigen. Eine Verbesserung der Sicherheit entsteht bei vielen Kassen bereits durch eine optimierte Gestaltung des Kassenbereiches, durch die Anwendung von sicherheitstechnischen Einrichtungen, einer Anpassung der Ablauforganisation sowie durch die Qualifizierung von Personal. Dieser Artikel beschäftigt sich mit ausgewählten und gängigen Maßnahmen zur Erlangung von Kassensicherheit, die nicht durch ein IT-System allein gewährleistet sind.

1. Personelle Sicherheit

Die personelle Sicherheit beschreibt alle personenbezogenen Maßnahmen zur Gewährleistung der geforderten Sicherheit und ist ein wichtiger Bestandteil des Sicherheitskonzeptes. Die personelle Sicherheit darf nicht losgelöst von den anderen Bestandteilen betrachtet werden. Sämtliche technischen, baulichen oder organisatorischen Maßnahmen entfalten keine Wirkung, wenn das Verhalten und/oder das Bewusstsein der Mitarbeiter nicht der gewünschten Sicherheitskultur in der Verwaltung entsprechen.

Die Sicherheitskultur in einer Verwaltung ist definiert durch Einstellungen, Werte und grundlegende Überzeugungen zu allen sicherheitsrelevanten Fragen. Dabei ist dies nicht ausschließlich eine Aufgabe der Kasse, sondern der gesamten Verwaltung. Die Grundpfeiler einer guten Sicherheitskultur ist die offene und vertrauensvolle Kommunikation innerhalb der Verwaltung.

Zur personellen Sicherheit gehört auch, dass das Personal im Kassenbereich eine adäquate Ausbildung, aktuelle Stellenbeschreibungen und eine darauf aufbauende Stellenbewertung besitzt. Bereits in der Stellenbeschreibung werden dann die sicherheitsrelevanten Tätigkeiten verankert und Stellvertreterregelungen eindeutig geklärt. Die Mitarbeiter der Kasse sind regelmäßig über die Regelungen der Dienstanweisung zur Errichtung und zum Geschäftsgang der kommunalen Kasse und in Bezug auf Datenschutz sowie IT-Sicherheit zu unterrichten. Bereits bei der Einweisung neuer Mitarbeiter erfolgt eine Sensibilisierung zu allen relevanten Sicherheitsmaßnahmen. Auch im Falle eines Abganges von Mitarbeitern ist ein strukturierter Prozess notwendig. Die Mitarbeiter müssen wissen, wie Sie sich in bestimmten Situationen zu verhalten haben.

Zur Erlangung eines anwendungsbereiten Fachwissens müssen die Mitarbeiter aus dem Kassenbereich regelmäßig an Fort- und Weiterbildungen teilnehmen. Die Aufgaben im Kassenbereich werden durch immer neue Rechtsprechungen beeinflusst. Ein rechtssicherer Auftritt der Kassenmitarbeiter unterstützt das Selbstvertrauen und führt zu einer souveränen Außenwirkung. Weiterhin von Bedeutung sind regelmäßige Schulungen zum Umgang mit Besuchern der Kasse. Die Mitarbeiter sollten Sicherheit gerade im Umgang mit schwierigen Besuchern erlangen und den Notfallplan verinnerlicht haben.

In anderen Bundesländern (§ 43 Verwaltungsvorschrift zur Kommunalhaushaltsverordnung Bayern (VVKommHV)) ist darüber hinaus geregelt, dass die Kassenverwalter in geordneten wirtschaftlichen Verhältnissen leben und regelmäßig mindestens die Hälfte des jährlichen Urlaubsanspruches zusammenhängend antreten sollen. Während des Urlaubs sollen die Kassenverwalter keine Aufgaben der Kasse wahrnehmen. In der Urlaubszeit sind zur Absicherung des laufenden Geschäftes die bestehenden Vertretungsregelungen anzuwenden. Regelmäßige Vertretungen über einen längeren Zeitraum dienen der Überprüfung von gelebten Prozessen und sollen mögliche Schwachstellen oder bestehende Unregelmäßigkeiten aufdecken. Gut funktionierende Vertretungsregelungen sind stets die beste Kontrolle vor Betrugsversuchen.

Eine klare Aufgabenstruktur mit Vertretungsregelungen (siehe auch Stellenbeschreibung) muss in jeder Gemeindekasse vorliegen. Wenn die geringe Verwaltungsgröße ein durchgängiges Vertretungskonzept nicht ermöglicht, sind durch die Dienstanweisung zur Errichtung und zum Geschäftsgang der kommunalen Kasse Ausnahmen zu regeln. Diese Ausnahmen sind durch die Kassenaufsicht stärker zu kontrollieren.

2. Organisatorische Sicherheit

Die Kasse ist stets als Einheitskasse zu führen, d. h. sämtliche Ein- und Auszahlungen sind an einer zentralen Stelle in der Verwaltung zu organisieren. Ausnahmen von der Einheitskasse sind beispielsweise Handvorschüsse und Zahlstellen, die ebenfalls nach den Regeln der Einheitskasse zu führen sind. Die Einheitskasse ermöglicht eine ordnungsmäßige und wirtschaftliche Aufgabenwahrnehmung. Zur ordnungsmäßigen Erledigung der Aufgaben gehört auch die organisatorische Sicherheit der Verwaltungsprozesse, vor allem bei Prozessen im Zusammenhang mit dem Zahlungsverkehr. Die Buchführung und der Zahlungsverkehr unterliegen in der öffentlichen Verwaltung besonderen Regelungen, um Manipulationen und Unregelmäßigkeiten zu verhindern. Ein wesentliches Instrument ist das Trennungsprinzip, dass die Haushaltsführung (Anordnung) und die Kassengeschäfte (Vollzug) voneinander trennen. Der Gesetzgeber unterteilt das Trennungsprinzip noch weiter in ein dreifaches Trennungsprinzip (siehe Abbildung 2). Die Trennungsprinzipien sind auch bei dem Einsatz von Vorprogrammen, wie beispielsweise für die Lohn- und Gehaltsbuchhaltung, zu berücksichtigen. Bereits in der Aufbauorganisation ist eine Trennung empfehlenswert.

3-faches Trennungsprinzip		
Buchhaltung vs. Zahlungsverkehr	**Buchhaltung/Zahlungsverkehr vs. Feststellung/Anordnung**	**Feststellung vs. Anordnung**
Mitarbeiter, die Aufgaben des Zahlungsverkehrs wahrnehmen, sollen nicht buchen *(§ 5 Abs. 2 SächsKomKBVO)*	Mitarbeiter der Kasse sollen keine Kassenanordnungen vorbereiten und erteilen *(§ 7 Abs. 3 SächsKomKBVO)*	Mitarbeiter, die die sachliche und rechnerische Feststellung erteilen, dürfen nicht anordnen *(§ 7 Abs. 2 SächsKomKBVO)*

Abbildung 2: Trennungsprinzipien (eigene Darstellung)

Die Kasse wird erst mit dem Vorliegen einer vollständigen Zahlungsanordnung tätig. Nach § 8 Abs. 1 SächsKomKBVO wird der Mindestinhalt einer Zahlungsanordnung geregelt. Folgende Angaben sind pflichtiger Bestandteil der Zahlungsanordnung:

1. den anzunehmenden oder auszuzahlenden Betrag;
2. den Grund der Zahlung;
3. den Zahlungspflichtigen oder Empfangsberechtigten;
4. den Fälligkeitstag;
5. den Buchungssatz, soweit erforderlich die Kostenstelle und das Haushaltsjahr;
6. die Bestätigung, dass die sachliche und rechnerische Feststellung nach § 11 SächsKomKBVO vorliegt;
7. das Datum der Anordnung;
8. die Unterschrift des Anordnungsberechtigten.

Vor allem die den Buchungssatz betreffende Position mit Produkt, Konto und Betrag dürfen nicht im Nachgang geändert werden. Erkennt der Kassenverwalter Fehler in der Anordnung, so ist die Anordnung zurückzugeben und erneut durch den Anordnungsberechtigten zu erstellen. Gibt der Inhalt einer Kassenanordnung zu Bedenken Anlass, darf entsprechend § 7 Abs. 1 Satz 3 SächsKomKBVO diese nur ausgeführt werden, wenn die anordnende Stelle sie nach Beanstandung schriftlich aufrechterhält. Liegen dem Kassenmitarbeiter die vollständige und richtige Zahlungsanordnung sowie die erfolgte Buchung durch die Geschäftsbuchhaltung vor, kann die Zahlung erfolgen.

Bei der Zahlung ist das Vier-Augen-Prinzip zu wahren. Die Zahlung kann erst dann abgeschlossen werden, wenn sich zwei Kassenmitarbeiter davon überzeugt haben, dass die Zahlungsanordnung, der Beleg und die Buchung nachvollziehbar und nicht widersprüchlich sind. Die Freigabe erfolgt mit den von der Bank an die Kassenmitarbeiter übergebenen Bankberechtigungen. Die Bankberechtigungen durch Kennwörter, USB-Sticks oder andere technische Hilfsmittel für die Abwicklung des Zahlungsverkehrs dürfen nicht untereinander geteilt bzw. ausgetauscht werden. Dafür sind ausreichend Bankberechtigungen entsprechend der Vertretungsregelungen zu beantragen, um durchgängig das Vier-Augen-Prinzip zu wahren.

Für eine ausreichende Prozesssicherheit sollte der Prozess erhoben und auf geeignete Art dargestellt bzw. modelliert werden. Sind Prozessschritte anzupassen, muss dies noch vor der Implementierung in einen elektronischen Workflow erfolgen, denn nachträgliche Änderungen des elektronischen Workflows sind regelmäßig schwierig umzusetzen.

Neben der Prozesssicherheit können weitere organisatorische Maßnahmen ergriffen werden. Zahlstellen und Handvorschüsse, aber auch die damit einhergehenden Bargeldbestände sind auf ein notwendiges Minimum zu begrenzen und nicht benötigte Bargeldmittel immer rechtzeitig zur Bank zu bringen. Bei der Bank sollte darüber hinaus ein Tageslimit eingerichtet und Auslandsüberweisungen gesperrt werden. Bei der Festlegung des Tageslimits empfiehlt sich eine Orientierung an der durchschnittlichen Obergrenze aller Auszahlungen im Jahr. Bei der Entscheidung eines Tageslimits sind Abrundungen auf ungerade Zahlen zu empfehlen (z. B. 187.000 EUR statt 200.000 EUR). Um dennoch Zahlungen über dem Limit oder ins Ausland ausführen zu können, ist häufig eine Anmeldung der Zahlung bei der Bank notwendig. Finden regelmäßig Bargeldtransporte eines erheblichen Werts statt, sind externe Sicherheitsdienste mit dem Geldtransport zu beauftragen. Die individuellen Wertgrenzen sind nach den örtlichen Bedürfnissen festzulegen und in der Dienstanweisung zur Errichtung und zum Geschäftsgang der kommunalen Kasse zu hinterlegen.

3. Räumliche Sicherheit

Nach § 5 Arbeitsschutzgesetz hat der Unternehmer respektive der Bürgermeister die Sicherheit und den Gesundheitsschutz der Beschäftigten zu gewährleisten und, wenn nötig, zu verbessern. Der erste wichtige Schritt ist hierbei die Durchführung einer Gefährdungsbeurteilung. In § 3 Deutsche Gesetzliche Unfallversicherung Vorschrift 1 ist festgelegt, dass der Unternehmer die für die Versicherten mit ihrer Arbeit verbundenen Gefährdungen ermitteln und bei Bedarf Maßnahmen einleiten und umsetzen muss.

Bei einem Neubau sind die bestehenden Vorschriften schon bei der Planung zu berücksichtigen und in der Ausführungsphase auch umzusetzen. Dazu sind die Mitarbeiter der Kasse bereits frühzeitig in den Planungsprozess einzubeziehen, da die beauftragten Architekten und Büroraumausstatter regelmäßig nicht mit den hohen Anforderungen an die räumliche Kassensicherheit vertraut sind. Vielfach ist die Verwaltung jedoch in bestehenden Gebäuden untergebracht und muss die unter Berücksichtigung der herrschenden Bedingungen optimale Lösung finden. Die räumliche Sicherheit ist abhängig von der gegebenen Struktur des Gebäudes und den funktionalen Arbeitsbereichen der Kasse. Die räumliche Sicherheit betrifft nicht nur den Kassenbereich als solchen, sondern auch den Standort und die Funktion von Kassenautomaten sowie den verschiedenen Zahlstellen. Für Informationen über die baulichen Anforderungen einer Gemeindekasse können die Kommunen auf die Unfallkasse Sachsen und polizeilichen Beratungsstellen zugehen.

Die räumliche Sicherheit ist anhand einer Gefährdungsbeurteilung bei den folgenden typischen Anlässen immer neu zu bestimmen:
- Erstermittlung
- Erweiterung oder Umbau der Kasse
- Anschaffung neuer Technik bzw. von neuen Ausstattungsgegenständen
- Änderungen von gesetzlichen Vorschriften (auch von Dienstanweisungen)
- wesentlichen Änderungen der Arbeitsorganisation (z. B. Digitalisierung)
- Auftreten von bestimmten Ereignissen, wie beispielsweise Arbeitsunfälle, Betrug, körperliche Übergriffe usw.

Die Kassenbauarten unterteilen sich in geschlossene Kassen, offene Kassen mit und ohne Tresen; der Kassenautomat stellt eine Sonderform dar. Grundsätzlich besteht auch die Möglichkeit, die verschiedenen Kassenbauarten zu kombinieren, um auf die örtlichen Situationen oder die zu erbringenden Leistungen reagieren zu können. Die Unfallkasse Sachsen kann bei Bedarf zu den Anforderungen an die räumliche Kassensicherheit beraten.

Für alle Bauarten gilt, dass für den Kassenkunden keine direkte Sicht auf die Geldbestände möglich ist. Zudem empfiehlt sich auf die Möglichkeit von Blickkontakt zwischen den Kassenmitarbeitern zu achten. Ein Blickkontakt von Kassenmitarbeitern setzt voraus, dass der jeweils andere Kassenmitarbeiter die Sprache, Mimik und Gesten des anderen Mitarbeiters erkennen kann. Darüber hinaus sollte der Mitarbeiter immer die Möglichkeit haben, den Raum verlassen zu können, ohne am Besucher vorbeigehen zu müssen.

Geschlossene Kassen

Bei einem hohen Besucheraufkommen und hohen Tagesumsätzen finden sich geschlossene Kassen häufig wieder. Bei dieser Bauart sitzen die Kassenmitarbeiter in einem separaten Raum, der nur durch befugte

Personen betreten werden kann. Die räumliche Trennung zu den außenstehenden Personen erfolgt über einen zumindest durchbruchhemmenden Glasaufbau.

Diese Bauart widerspricht jedoch mehr und mehr dem Gedanken einer offenen Kommunikation und bürgernahen Betreuung. Daher sind in der Praxis immer häufiger offene Kassen zu finden, zumal der Bargeldbestand aufgrund der elektronischen Bezahlmöglichkeiten weiter sinken wird. Diese Bauart wird auch zukünftig bei ausgewählten Leistungen der Gemeindekasse und im Bedarfsfall Anwendung finden, vor allem um den physischen Schutz von Mitarbeitern zu gewährleisten.

Offene Kassen mit und ohne Tresen

Sind das Besucheraufkommen und die Tagesumsätze gering und besteht kein umfassender Beratungsbedarf, kommt eine offene Kasse mit einem durchgehenden Tresen in Betracht. Der durchgehende Tresen stellt dabei die Übersprungsicherung dar und schafft den notwendigen Sicherheitsabstand. Sämtliche Tätigkeiten an den Geldbeständen (Geldkassette oder Tresor) sollte der am Tresen stehenden Kunde nicht einsehen können.

Offene Kassen ohne Tresen sind nur bei geringen Bargeldbeständen zu empfehlen. Anstelle eines Tresens erfolgt bei umfassendem Beratungsbedarf die Trennung zwischen den Kassenmitarbeiter und dem Kunden durch einen Schreibtisch.

Kassenautomat

Eine weitere Möglichkeit ist der Kassenautomat. Die Kassenautomaten sind in der Lage, nicht nur Geld einzunehmen, sondern auch Auszahlungen zu leisten. Damit können Kassenautomaten gerade auch bei kleinen Kommunen für deutlich mehr Sicherheit sorgen. Die Kassenautomaten sollten immer so eingebaut werden, dass eine Be- und Entleerung über die Rückseite in einem separaten Raum erfolgen kann. Besteht diese Möglichkeit nicht, sind immer mindestens zwei Personen zu unregelmäßigen Zeiten mit der Be- und Entleerung zu beauftragen. Auch der Kassenautomat sollte immer so aufgestellt werden, dass dieser durch einen ständigen Blickkontakt eines Verwaltungsmitarbeiters überwacht werden kann.

4. Sachliche Sicherheit

Zur sachlichen Sicherheit gehört ein Mindestmaß an Sicherheitsausstattung, die von der räumlichen Sicherheit nicht umfasst ist. Zu den erforderlichen Sachmitteln im Kassenbereich gehören aus unserer Sicht eine zeitgemäße IT-Umgebung, Gefahrenmelde- und Überwachungsanlagen sowie sichere und abschließbare Aufbewahrungsmöglichkeiten für Bargeldmittel. Zudem ist in den Kassenräumen die Betriebsanweisung so zu hinterlegen, dass diese jederzeit durch die unterwiesenen Mitarbeiter eingesehen werden kann. In einer Betriebsanweisung für die Kassenarbeitsplätze werden alle organisatorischen und verhaltensbezogenen Maßnahmen zusammengefasst, die den Beschäftigten ein sicherheits- und gesundheitsgerechtes Verhalten am Arbeitsplatz ermöglichen.

Bei der Installation von Fachsoftware sind die Einstellungen individuell auf das vor Ort bestehende System unter Berücksichtigung des örtlichen IT-Sicherheitskonzeptes hin anzupassen. Die Grundkonfiguration reicht häufig allein nicht aus, um die geforderten Sicherheitsstandards zu erfüllen. Die eingesetzte Software sollte zudem die aktuellsten Bedingungen an Datensicherheit erfüllen. Dafür ist es notwendig, regelmäßig die aktuellste Version der eingesetzten Software zu nutzen. Aktuelle Software erfordert auch eine leistungsfähige IT-Infrastruktur. Dafür sind die von den Softwareanbietern empfohlenen Hardwarevoraussetzungen umzusetzen, damit die eingesetzte Software und die IT-Umgebung optimal aufeinander abgestimmt sind. Das IT-Sicherheitskonzept und das daraus resultierende Rechtekonzept sind regelmäßig zu überprüfen und mit dem Kassenbereich abzustimmen. Das Rechtekonzept muss mit den Regelungen in der Dienstanweisung zur Errichtung und zum Geschäftsgang der kommunalen Kasse übereinstimmen. Der Administrator soll bei der Anmeldung immer einen separaten Zugang erhalten und keinen Mitarbeiterzugang. Der Administrator soll keine Rechte zur Nutzung von Fachanwendungen erhalten, d. h. beispielsweise Buchungen oder Zahlungen veranlassen können. Das IT-Sicherheitskonzept sollte nicht isoliert den Kassenbereich betrachten, sondern ganzheitlich die komplette Verwaltung einschließlich aller Außenstellen umfassen.

Ein Bestandteil der IT-Sicherheit ist auch der sichere Umgang der Mitarbeiter mit der eingesetzten Software. So werden fahrlässige Fehler im sicherheitsrelevanten Bereich vermieden.

Fazit und Ausblick

Die Digitalisierung der Verwaltung ist ein gemeinsames Ziel des Bundes, der Länder und Kommunen. Die Zukunft wird dafür Lösungen mit einem immer höheren Automatisierungsgrad bringen. Gleichzeitig wird auch die Sicherheit der technischen Lösungen den steigenden Anforderungen gerecht.

Gefährdungen der Kassensicherheit werden wahrscheinlich im Wesentlichen aus zwei Richtungen entstehen. Zum einen werden gezielte und hoch spezialisierte Angriffe über die IT erfolgen. Aufgrund der komplexen Anforderungen werden die Angriffe sehr professionell durch eine kleine Personengruppe erfolgen. Diese Gefährdung lässt sich durch die beschriebenen Maßnahmen nur reduzieren, jedoch nicht verhindern. Die Folge ist eine Verlagerung der Suche nach Schwachstellen im Sicherheitskonzept. So werden zum anderen die in den Prozess involvierten Personen zum Ziel des Angriffs. Damit besteht auch immer ein erhöhtes Sicherheitsbedürfnis in den Prozessschritten, in denen Menschen beteiligt sind. Social Engineering beschäftigt sich genau mit diesem Phänomen und konzentriert sich dabei auf die Eigenschaften von Menschen (z. B. Hilfsbereitschaft, Vertrauen, Angst, Respekt vor Autoritäten).

Die Dienstanweisung zur Errichtung und zum Geschäftsgang der kommunalen Kasse ist der erste und zugleich wichtigste Baustein für die Kassensicherheit. Dienstanweisungen sind ein wichtiges Element der Verwaltungsorganisation, der Gewährleistung der Rechtmäßigkeit und fester Bestandteil des internen Kontrollsystems (IKS). Das IKS dient dem Abwenden von vermeidbaren Risiken, z. B. durch Betrug oder Handlungsunsicherheiten. Damit Dienstanweisungen ihre Funktion im IKS vollumfänglich erfüllen können, müssen diese, neben der regelmäßigen Kommunikation gegenüber Beschäftigten, stets miteinander verzahnt und aufeinander, insbesondere mit der Hauptsatzung, abgestimmt werden. Ebenfalls empfehlen wir, Dienstanweisungen jährlich auf Anwendbarkeit, Praktikabilität und Aktualität zu prüfen. Das Muster des *Sächsischen Städte- und Gemeindetages* ist dafür eine sehr gute Grundlage, die auf die aktuellen und örtlichen Bedürfnisse hin anzupassen ist.

Sicherheit macht Arbeit und kostet Geld, dessen sollten sich alle Beteiligten bewusst sein. Vorsätzlicher Betrug wird sich nicht verhindern lassen, auch zukünftig nicht. Aber die Möglichkeiten der fahrlässigen und vorsätzlichen Gefährdung können durch geeignete Maßnahmen erheblich verringert werden. Der Fokus muss neben den Anforderungen der IT-Sicherheit auch weiterhin auf der personellen und organisatorischen sowie räumlichen und sachlichen Kassensicherheit liegen. Wenn Prozesse im Zuge der Digitalisierung angepasst werden, sind sämtliche sicherheitsrelevanten Fragestellungen auf den Prüfstand zu stellen. Alle genannten Anforderungen an die Kassensicherheit sind auch bei der Digitalisierung von Verwaltungsaufgaben weiterhin zu berücksichtigen und mit einem entsprechenden Rechtekonzept durchzusetzen. Das Zauberwort Digitalisierung suggeriert nicht selten eine Sicherheit, die womöglich nicht durchgängig besteht. Die Einhaltung sämtlicher Kassenvorschriften ist daher noch immer im Zuge der Dienstaufsicht und durch Kassenprüfungen regelmäßig zu überprüfen. Auch wenn es keine absolute Sicherheit geben wird, so sind doch immer – in einem vertretbaren Rahmen – Anstrengungen zu unternehmen.

Die Notwendigkeit einer Cyberversicherung

Jens Bockmann
Ostdeutsche Kommunalversicherung a. G.

Wir stehen derzeit am Anfang einer neuen digitalen Ära. Ihr Hauptmerkmal ist die allgegenwärtige Konnektivität. Diese reicht vom privaten Bereich, allgemein bekannt unter dem Begriff »Smart Home«, d. h. intelligente Licht- und Heizungssteuerung, vernetzte Kühlschränke und Entertainmentsysteme, bis hin zur Industrie 4.0, also der intelligenten Vernetzung von Maschinen und Abläufen in der Industrie mit Hilfe von Informations- und Kommunikationstechnologien.

Geschätzt mehr als 8,4 Milliarden miteinander verbundene Geräte waren im Jahr 2017 verfügbar. Zudem sind 63 Prozent aller Geräte im Endkundenbereich im Einsatz. In absoluten Zahlen sind das 5,3 Milliarden Geräte. Und man geht davon aus, dass die Anzahl verbundener Geräte bis 2020 auf 20,4 Milliarden anwachsen wird.[1]

Dies bietet für den Verbraucher mehr Lebensqualität, für den Kleinunternehmer z. B. Zugang zu mehr Kunden, für Behörden die Vereinfachung von Verwaltungsvorgängen z. B. durch Cloud-Lösungen und im Bereich der Industrie läuten das Internet der Dinge, Maschine-zu-Maschine-Kommunikation und Produktionsstätten, die immer intelligenter werden, eine neue Epoche ein.

Aber nicht nur Verbraucher, Unternehmen und Behörden profitieren von Vernetzung und Digitalisierung. Auch Kriminellen ermöglichen es diese vereinfachten Prozesse, Angriffe auf digitale Systeme und Geräte effektiver und erfolgreicher zu gestalten. Es sind viele Geräte und Systeme mit dem Internet verbunden, aber längst sind nicht alle auch vor Angriffen aus dem Netz ausreichend geschützt.

Der finanzielle Anreiz für Cyberkriminelle wächst stetig, so dass diese auch zunehmend in die Entwicklung von neuen, raffinierten Angriffs- und Hacking-Methoden investieren. Diese reichen vom einfachen Datendiebstahl über die Datenvernichtung oder Datenkorruption, der Sperrung von Systemen mit anschließender Erpressung bis hin zur umfangreichen Industriespionage.

Dass die Gefahr eines Schadens durch Cyberangriffe in einer zunehmend vernetzten Welt steigt, ist wohl unstrittig. Eine Befragung von 720 in Deutschland ansässigen Unternehmen hat ergeben, dass jedes dritte Unternehmen bereits Opfer von Cybercrime geworden ist. Als häufigste Delikte gaben die Unternehmen Computerbetrug, Manipulation von Konto- und Finanzdaten sowie Ausspähen und Abfangen von Daten von Kunden, Passwörtern oder Firmeninterna an. Weitere Untersuchungen ergaben, dass die meisten Cyber-Attacken auf eine unzureichend geschützte IT-Infrastruktur zurückzuführen sind.[2] Dies betrifft ebenso Behörden, Ämter und kommunale Betriebe. So hat z. B. das Landesrechenzentrum in Thüringen allein im Jahr 2017 etwa 98.000 Angriffe aus sogenannten Botnetzen auf Computern in Ministerien, Landtag, Polizei und anderen Landesbehörden festgestellt. Außerdem sei bei etwa 29.000 E-Mails an elektronische Post-Konten des Landes eine Infektion mit Schadsoftware festgestellt worden.[3]

Im Jahr 2017 registrierte die Polizei deutschlandweit knapp 86.000 Cybercrime-Attacken. Der durch Computerbetrug angerichtete Schaden wird offiziell mit 71 Millionen Euro angegeben. Das geht aus dem Lagebild »Cybercrime« des BKA hervor. Dies sind jedoch nur die bekannten Fälle. Die Dunkelziffer liegt hier noch um ein Vielfaches höher. Wie groß die Differenz zwischen Statistik und dem Dunkelfeld sein könne, habe vor zwei Jahren eine Untersuchung in Mecklenburg-Vorpommern gezeigt. Danach waren 99,2 Prozent der Fälle nicht bekannt geworden. Für lediglich 0,8 Prozent lagen Anzeigen vor. Hinzu komme, dass auch ein einzelner Angriff, der Millionen Computer oder Datensätze zum Ziel habe, statistisch als ein Delikt gezählt werde, so der Experte Sven Heuchert vom Landeskriminalamt Erfurt.[4]

Doch unter Cyber-Risiken versteht man nicht nur Hackerangriffe von außen. Vielfach sind es auch sogenannte »Innentäter«, die durch gezielte Eingriffe in geschützte IT-Systeme erheblichen Schaden verursachen. Das sind aktuelle oder ehemalige Mitarbeiter des Unternehmens. 62 Prozent der Unternehmen, die in den vergangenen zwei Jahren

1 https://www.cnet.de/88169463/mehr-sicherheit-im-smarten-zuhause/

2 https://www.compliance-manager.net/fachartikel/cyber-sicherheit-rueckt-den-fokus-der-bafin-356634674

3 https://www.focus.de/regional/erfurt/internet-zehntausende-cyberangriffe-auf-rechner-der-landesbehoerden_id_6558682.html

4 https://www.thueringer-allgemeine.de/leben/blaulicht/zahl-der-cyber-angriffe-steigt-in-thueringen-kontinuierlich-id226291511.html

Opfer von Spionage, Sabotage oder Datendiebstahl wurden, haben die Täter in diesem Personenkreis identifiziert.

Hierzu ein Schadenbeispiel:

Ein Mitarbeiter aus der Informationstechnik überwirft sich mit seinem Unternehmen und verliert seine Stelle. Dabei wird allerlei schmutzige Wäsche gewaschen, so dass er wilde Rachegelüste entwickelt. Er legt sich einen Schlachtplan zurecht, den er akribisch in einem Aktenordner dokumentiert, und dringt mit seinem Insiderwissen in das Firmennetzwerk ein. Über das Darknet führt er seinen Rachekrieg. Auf einmal kommen Internetuser nicht mehr auf die Seite von Kommunen, für die das Unternehmen als Dienstleister tätig ist, sondern auf Pornoseiten. Jeden Tag entsteht mehr Chaos, die Unternehmensführung ist verzweifelt.

Der Fall hat im vergangenen Jahr den größten Cyberschaden eines Versicherers in Deutschland ausgelöst. 3 Millionen Euro betrugen die Kosten für IT-Forensik, Krisenkommunikation und für Betriebsunterbrechungen. »Ohne uns hätte das Unternehmen große Probleme gehabt, die Krise zu managen, und hätte wahrscheinlich einen äußerst dramatischen wirtschaftlichen Schaden davongetragen«, sagt Robert Dietrich, Deutschlandchef des britischen Spezialversicherers Hiscox. Das beschriebene Risiko, dass sich ein frustrierter Mitarbeiter an seinem Arbeitgeber rächen will, sei real. Doch die meisten Unternehmen seien darauf nicht eingestellt. »Es gibt ein Urvertrauen in die eigene Belegschaft – nach dem Motto: Ich lege meine Hand ins Feuer«, sagt er.[5]

Die Sicherheit von IT-Infrastrukturen und Daten entwickelt sich in der öffentlichen Verwaltung zur zentralen Herausforderung der kommenden Jahre. Das sagen 95 Prozent der Entscheider in Verwaltungen des Bundes, der Länder und Kommunen. 53 Prozent sehen die eigenen Abläufe und Systeme bereits gut aufgestellt, um auch künftige Cyber-Risiken in den Griff zu bekommen sowie die Anforderungen des Datenschutzes zu erfüllen. 46 Prozent arbeiten an der Modernisierung. Das sind Ergebnisse der Studie »Branchenkompass Public Services 2018« von Sopra Steria Consulting und dem FAZ-Institut. Im Rahmen der Untersuchung wurden Entscheider in 100 Verwaltungen deutschlandweit befragt.[6]

Wie die Internetseite »Treffpunkt-Kommune.de« berichtet, rückt das Thema IT- und Datensicherheit im Vergleich zu 2016 in der öffentlichen Verwaltung noch mehr in den Mittelpunkt. Grund ist nicht nur die zunehmende Zahl illegaler Handlungen im Computer- und Telekommunikationsbereich. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht auch die Einflussnahme auf politische Prozesse durch Cyberangriffe als ein relativ neues Phänomen, vor dem sich Verwaltungen schützen müssen.

Die Dominanz von Sicherheitsthemen ist zudem eine direkte Folge des fortschreitenden Ausbaus der Digitalisierung. Der Aufbau einer digitalen Verwaltung zählt für mehr als acht von zehn befragten Verwaltungsentscheidern zu den derzeit wichtigsten Aufgaben. Unmittelbar damit verbunden ist die sicherere Verarbeitung wachsender Datenmengen.

Alle diese Cyber-Risiken können natürlich erhebliche Kosten verursachen und gehen oft einher mit rechtlichen Folgen, Informationspflichten und Reputationsschäden, oder einer Unterbrechung des Verwaltungs- und Geschäftsbetriebes.

Klassische Versicherungslösungen, wie Sach- oder Haftpflichtversicherungen leisten hier nur einen sehr begrenzten Schutz.

Ein sehr umfangreiches Deckungskonzept bietet hier die Cyberversicherung. Die durch die OKV – Ostdeutsche Kommunalversicherung a. G. angebotene Cyberversicherung bietet einen optimalen Schutz für kommunale Gebietskörperschaften, wie Städte, Landkreise und Gemeinden, aber auch für kommunale Betriebe, z. B. der Energie- und Wasserversorgung, bei Hackerangriffen, Datenverlust – auch von physischen Daten – oder Verstößen gegen Datenschutzgesetze.

Versicherungsschutz besteht hier u. a. für Schäden aufgrund von gezielten und ungezielten Angriffen von innen (eigene Mitarbeiter) und außen (externe Quellen, z. B. Spam, Malware, Hacker-Angriffe, DDoS-Attacken, sonstige Cyber-Vorfälle), von Eingriffen in das IT-System z. B. durch Pishing, durch Schadprogramme, wie Viren, Würmer oder Trojaner oder von Denial-of-Service-Angriffen.

Versichert ist hierbei auch das Abhandenkommen von Daten, nicht nur in digitaler Form, sondern auch von physischen Daten, wie z. B. durch das Verlieren von Laptops oder USB-Sticks mit personenbezogenen Daten.

Weiterhin besteht Versicherungsschutz für Schäden aufgrund von Bedienfehlern, also von unsachgemäßer Bedienung des IT-Systems durch fahrlässiges, auch grob fahrlässiges Handeln oder Unterlassen, welches die Veränderung, Beschädigung, Zerstörung, Löschung, Verschlüsselung oder das Abhandenkommen von Daten zur Folge hat.

Ebenfalls versichert sind Folgen von Datenrechtsverletzungen, also Verstöße insbesondere gegen gesetzliche Datenschutzbestimmungen wie das Bundesdatenschutzgesetz, die Datenschutzgrundverordnung oder vergleichbare ausländische Rechtsnormen zum Datenschutz oder gegen Geheimhaltungspflichten.

Im Rahmen der gesetzlichen oder vertraglichen Informationspflichten anfallende Kosten zur Benachrichtigung der Betroffenen und Kosten, die bei der Anzeige und Meldung der Datenrechtsverletzung entsprechend den gesetzlichen Vorgaben entstehen, werden übernommen.

Zwei weitere wichtige Bausteine sind zum einen der Versicherungsschutz für Schäden durch Cyber-Diebstahl, bei denen durch eine Netzwerkssicherheitsverletzung abhandengekommene Gelder oder Wertpapiere oder durch unzulässige Nutzung von Voice-over-IP-Verbindungen Vermögensschäden entstanden sind. Der zweite Baustein ist die Betriebsunterbrechungsversicherung, welche für Kommunen bis 50.000 Einwohner einfach und unkompliziert als pauschale Tagesentschädigung im Schadenfall zur Verfügung steht.

Diese vorgenannten Punkte allein bieten schon einen umfangreichen Versicherungsschutz. Entscheidendes Element der OKV-Cyberdeckung ist jedoch der unbegrenzte, direkte Zugriff auf die erfahrenen Spezialisten der Hi-Solutions AG, eines der führenden Beratungsunternehmen für Cyber-Risiken, auf die Sie im Bedarfsfall 24 Stunden, 7 Tage die Woche Zugriff haben und die Ihnen im Falle eines Cyber-Vorfalls sofort Hilfestellung durch eine erste Notfall- und Krisenunterstützung, auch wenn die Situation noch unklar ist und der Eintritt nur vermutet wird, zur Verfügung stehen.

5 https://www.cyberdirekt.de/post/der-angriff-kann-auch-von-innen-kommen/2222/
6 https://www.soprasteria.de/newsroom/publikationen/studie/branchenkompass-public-services-2018

Hier erfolgt die Bereitstellung hochkarätiger interner und externer Spezialisten, wie Forensiker, IT-Spezialisten, Rechtanwälte, PR-Berater usw.

Über HiSolutions steht von der ersten Minute an ein exklusiver Dienstleister mit seinem gesamten Expertennetzwerk zur Seite, welcher bis zum Abschluss des Schadenfalles, ggf. auch vor Ort, unterstützt.

Das Konzept bietet neben der exklusiven Kooperation mit der HiSolutions AG umfangreiche präventive Maßnahmen und Service-Dienstleistungen, die auch zu einer Verbesserung der internen Organisation und zu mehr Risikobewusstsein führen. Dazu gehören u. a.:

- Cyber-Krisenprävention (individuelle Erstellung eines Cyber-Krisenplans)
- Webbasiertes Cyber-Training zur Sensibilisierung der eigenen Mitarbeiter inkl. individuellem Zertifikat
- Telefonische Soforthilfe durch IT-Krisenexperten
- Option einer vorvertraglichen Cyber-Risikobewertung durch HiSolutions bei komplexen Risiken.

Die OKV hat in ihrer Cyberversicherung auf den Haftpflichtdeckungsbaustein verzichtet, da Sie, als Kommune oder kommunale Einrichtung, generell über den Kommunalen Schadenausgleich der Länder Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt und Thüringen (KSA) den Haftpflichtdeckungsschutz abgeschlossen haben. Dadurch wollten wir ein auf Ihre Bedürfnisse abgestimmtes Konzept erschaffen. Denn der Deckungsschutz des KSA erstreckt sich auch auf Cyber-Risiken und besteht für den Fall, dass das Mitglied aufgrund gesetzlicher Haftpflichtbestimmungen von einem Dritten auf Schadenersatz in Anspruch genommen wird. Ein mögliches Szenario könnte zum Beispiel sein, dass ein Hacker Daten von Bürgern ausspäht und missbraucht. Diese Bürger verlangen sodann Schadenersatz von der Kommune. Wer den Haftpflichtdeckungsschutz des KSA in Anspruch nimmt, ist also gegen Haftpflichtansprüche, die aus Cyber-Risiken resultieren, versichert und kann etwaige Schadenersatzansprüche wie gewohnt dem KSA anzeigen.

Abschließend sei an dieser Stelle nochmals gesagt, dass es trotz größter Anstrengungen und Präventionen keine 100 %ige Sicherheit gibt. Es kommen täglich hunderttausende neue Viren, Würmer und andere Schadsoftware in den Umlauf. Diese können nicht sofort durch Virenscanner erkannt werden. Bis hier entsprechende Updates entwickelt und eingespielt werden sind die Systeme teilweise ungeschützt.

Um sich hier vor hohen Kostenrisiken zu schützen und die dringend erforderliche Unterstützung im Schadenfall erhalten zu können, ist die Cyberversicherung eine Möglichkeit.

Den passenden Versicherungsschutz bieten wir als Ostdeutsche Kommunalversicherung an. Angebote zur Cyberversicherung können Sie unter betrieb@okv.de unverbindlich anfordern oder auch direkt bei Ihrem zuständigen Direktionsbevollmächtigten der OKV.

Auf den Blackout vorbereitet – Krisenmanagement bei der MITNETZ STROM

Udo Stöckel
enviaM

Es ist ein fast unvorstellbares Szenario: Der Strom fällt aus. Internet und Mobilfunk brechen völlig zusammen. Die Versorgung mit Gütern aller Art, wie Treibstoff, Lebensmitteln, Medikamenten und Bargeld, wird knapp. Bei Mensch und Tier steigt die Seuchengefahr. Die öffentliche Sicherheit ist kaum noch gegeben.

Würde diese Konstellation – ein Blackout – uns unvorbereitet treffen, sind Untersuchungen zufolge bereits nach 3 Tagen erste Todesopfer zu beklagen. Bei einem Blackout bricht das Stromnetz in einem weiträumigen Gebiet vollständig zusammen. Die Wiederherstellung der Energieversorgung kann dann Tage dauern.

Grundsätzlich ist das Stromnetz in Deutschland sicher und europaweit am besten ausgebaut. Das Übertragungs- und Verteilnetz ist auf technisches, systemisches Versagen oder auf gravierende Witterungsereignisse vorbereitet. Potenzieren sich jedoch die Einflüsse und kommt es zu einem Dominoeffekt, ist ein Blackout nicht auszuschließen.

In der jüngeren Vergangenheit sind zunehmend Cyberangriffe auf die Steuerzentralen der Energieversorger zu verzeichnen. Zugleich ist die Systemstabilität aufgrund der schwankenden Einspeisung regenerativer Anlagen in Gefahr. Diese Gefährdungen haben die Netzbetreiber erkannt und entsprechende Maßnahmen ergriffen.

Die enviaM-Gruppe ist gut vorbereitet

enviaM hat gemeinsam mit ihrer Netzgesellschaft, der Mitteldeutschen Netzgesellschaft Strom GmbH, (MITNETZ STROM) ein umfassendes, präventives Krisenmanagement aufgebaut. Dazu gehören unter anderem Maßnahmen in den Bereichen Krisenorganisation, Kommunikation, Personalschulung, Krisenszenarien sowie Ressourcenplanung mit Notfallkonzepten.

Bei einem Blackout sind in der Notfallplanung im gesamten Netzgebiet Sammelpunkte mit einer unabhängigen Stromversorgung sowie einer technischen Grundausstattung definiert. Die für solche Szenarien eingesetzten Kollegen besitzen eine Checkliste, wie sie sich in einem solchen Ausnahmefall verhalten müssen. Ihr Einsatz an den jeweiligen Sammelpunkten ist zeitlich gestaffelt, um die personellen Ressourcen über einen längeren Zeitraum sicher stellen zu können.

Trafostation

Umspannwerk Flöha

Eine wesentliche Herausforderung ist der Aufbau von Kommunikationswegen. Dazu hat MITNETZ STROM 52 Satellitentelefone über ihr Netzgebiet verteilt und entsprechende Verantwortungen vergeben. Die Telefone müssen permanent geladen und einsatzbereit sein. Erforderliche Außenantennen, zum Beispiel an den Räumlichkeiten der Einsatzleitungen oder an den Sammelpunkten, sind von den Kollegen zu montieren. Der Umgang mit den Satellitentelefonen ist regelmäßig zu üben.

Des Weiteren gilt ein wichtiges Augenmerk der Treibstoffversorgung der 26 mobilen Netzersatzanlagen, der rund 350 Einsatzfahrzeuge und der stationären Netzersatzanlagen. Dafür wurden mobile Tankanhänger beschafft und stationäre Tanks eingebaut. Zudem bestehen Kooperationsverträge mit dem Technischen Hilfswerk und dem Großtanklager in Hartmannsdorf, um im Ereignisfall gemeinsam agieren zu können.

Netzersatzanlage

Für das Personal in der zentralen Netzleitstelle in Taucha bei Leipzig sind Netzwiederaufbauszenarien hinterlegt und Anwendungsschulungen entwickelt. Ebenso finden für die Mitarbeiter im Netzgebiet regelmäßig Antihavarietrainings statt, um schnell einen notwendigen Netzwiederaufbauprozess zu etablieren. MITNETZ STROM schult aber nicht nur eigenes Personal, sondern auch Feuerwehren in den Kommunen zur Brandbekämpfung und Hilfeleistung im Bereich elektrischer Anlagen.

Bürgermeister haben eine besondere Bedeutung

Gerade in Krisensituationen kommt den Vertretern der Kommunen, allen voran den Bürgermeistern und Bürgermeisterinnen, eine besondere Rolle zu. Sie sind Ansprechpartner Nummer eins für die Bürgerinnen und Bürger sowie Hilfeteams, wenn es um die Koordination der Maßnahmen vor Ort geht. Auch die notwendigen Kommunikationsstränge zu übergeordneten Behörden liegen in der Hand des Behördenleiters.

Wir als enviaM-Gruppe sind uns dieser Bedeutung bewusst und haben Oberbürgermeister, Bürgermeister oder Amtsdirektoren in die Meldeketten der Störungskommunikation aufgenommen. Kommt es zu Stromausfällen im Netzgebiet der MITNETZ STROM, erhalten die Stadt- bzw. Gemeindeoberhäupter der betroffenen Kommunen automatisiert eine SMS. Natürlich erfolgt auch eine Benachrichtigung, wenn die Stromversorgung wiederhergestellt werden konnte.

Mit diesem Service wollen wir den Bürgermeisterinnen und Bürgermeistern die Möglichkeit geben, auf Anfragen aus der Bevölkerung bzw. der Hilfeteams reagieren zu können und weitere Institutionen zu informieren.

Sensibilisierung der jungen Generation

Die Stromversorgungsqualität in Deutschland ist seit Jahren auf einem konstant hohen Niveau. Der sogenannte SAIDI-Index (System Average Interruption Duration Index) gibt die durchschnittliche Versorgungsunterbrechung je angeschlossenem Letztverbraucher in Minuten pro Jahr an und wird von der Bundesnetzagentur erhoben. Hier rangiert Deutschland mit einem Wert von rund 15 Minuten in 2017 weit vor vielen anderen europäischen Ländern. Dies führt dazu, dass vor allem jüngere Generationen eine hohe Versorgungssicherheit als selbstverständlich wahrnehmen. Zur Sensibilisierung, wie hoch die Abhängigkeit vom Strom ist und welche Alternativen zur Steckdose existieren, bietet die enviaM-Gruppe im Netzgebiet der MITNETZ STROM einen Blackout-Erlebnistag an. Die Schüler der siebenten bis zwölften Klassen erleben hier einen außergewöhnlichen Unterrichtstag und müssen sich mit viel Ideenreichtum und Kreativität den stromlosen Herausforderungen stellen.

Im Netzgebiet der MITNETZ STROM ist die Energiewende bereits weit fortgeschritten. Der Anteil von EEG-Strom am Letztverbraucherabsatz betrug in 2018 bereits 108 % (bundesweit 40 %). Was es heißt, ein

Stromnetz mit verschiedenen erneuerbaren Energien zu managen, lässt sich mit unserem Experimentierkoffer »Smart Grid« erfahren. Schaffen es die Schüler ab der achten Klasse ein Netz aus verschiedenen volatilen Einspeisern aufrecht zu erhalten? Weitere Energiekoffer zu Windenergie, Photovoltaik und New Energy schaffen für unterschiedlichste Altersgruppen ähnliche Herausforderungen.

Bei Bedarf informieren wir Sie gern detailliert zu unserem Krisenmanagement und unseren Services für Kommunen. Wenden Sie sich in diesem Falle gern an Udo.Stoeckel@mitnetz-strom.de.

Energieeffizienznetzwerke für Kommunen – ein Erfolgsmodell

Maritha Dittmer
Geschäftsführerin der KBE Kommunale Beteiligungsgesellschaft mbH an der envia

Foto: Christian Kortüm

Zentrales Ziel der Energiewende ist der Klimaschutz. Um diesen zu verbessern, müssen wir die Energieeffizienz deutlich steigern. Nach dem Willen der Bundesregierung soll der Primärenergieverbrauch in Deutschland deshalb bis 2020 um 20 Prozent gegenüber dem Jahr 2008 sinken. Schon jetzt steht fest, dass wir die Vorgaben deutlich verfehlen werden. Nach Angaben des Bundesumweltministeriums ist der Primärenergieverbrauch im Berichtszeitraum bislang um lediglich 10,3 Prozent zurückgegangen.

Viele Energieeffizienz-Potentiale nach wie vor ungenutzt

Viele Energieeffizienz-Potentiale sind nach wie vor ungenutzt. Diese Erkenntnis ist nicht neu. Dabei mangelt es nicht an guten Ideen. Im Gegenteil: Bereits Ende 2014 hatte die Bundesregierung im Nationalen Aktionsplan für Energieeffizienz (NAPE) ein ganzes Bündel von Maßnahmen beschlossen. Ein Beispiel ist die Gründung von Energieeffizienznetzwerken. Bis 2020 sollen bundesweit 500 Energieeffizienznetzwerke entstehen. Mit ihnen sollen 75 Petajoule Primärenergie und 55 Millionen Tonnen Kohlendioxid eingespart werden. Die Initiative wird neben der Bundesregierung von 22 Wirtschaftsverbänden getragen.

Startschuss: Im Juli 2016 wurde das erste Energieeffizienznetzwerk für Kommunen der enviaM-Gruppe gegründet. Die Teilnehmer kamen dazu in Markkleeberg mit dem enviaM-Vertriebsvorstand Dr. Andreas Auerbach (Mitte) zusammen. *Foto: Thorsten Schack.*

Die dahinterstehende Idee ist denkbar einfach: Mehrere Teilnehmer einer Region und/oder einer Branche schließen sich freiwillig zu einem Netzwerk zusammen, um gemeinsam über einen Zeitraum von mehreren Jahren ihre Energieeffizienz zu steigern. Sie verständigen sich dazu auf ein gemeinsames Energieeinsparziel und die dafür notwendigen Maßnahmen. Die Mitglieder unterstützten sich bei der Umsetzung gegenseitig durch einen systematischen und zielgerichteten, aber unbürokratischen Erfahrungs- und Ideenaustausch. Sie senken so nicht nur ihren Energieverbrauch und die damit verbundenen Kohlendioxid-Emissionen, sondern auch ihre Energiekosten.

enviaM-Gruppe Vorreiter bei Gründung von Energieeffizienznetzwerken

Bis heute sind bundesweit mehr als 230 Energieeffizienznetzwerke entstanden. Damit ist man von der Zielmarke noch ein gutes Stück entfernt, aber auf einem vielversprechenden Weg. Auch in Ostdeutschland sind zahlreiche Energieeffizienznetzwerke ins Leben gerufen worden. Fünf von ihnen betreibt die enviaM-Gruppe. Der führende regionale Energiedienstleister in Ostdeutschland geht damit mit gutem Beispiel voran. Zu den Teilnehmern gehören Kommunen, Stadtwerke und Unternehmen. Besonders groß ist das Interesse bei Städten und Gemeinden.

Die enviaM-Gruppe versteht sich als Initiator, Moderator, Berater und Teilnehmer der Energieeffizienznetzwerke. Das erste seiner Art für Kommunen wurde vom Unternehmen im Juli 2016 gegründet. Ihm gehören die Städte Frohburg, Groitzsch und Wurzen, die Gemeinden Doberschütz, Großpösna und Löbnitz sowie die Verbandsgemeinden An der Finne und Droyßiger-Zeitzer Forst an.

Beeindruckende Erfolgsbilanz

Das Energieeffizienznetzwerk hat nach drei Jahren Laufzeit ein Energieeinsparziel von rund 1.700 Megawattstunden und eine damit verbundene Senkung der Kohlendioxid-Emissionen von rund 630 Tonnen pro Jahr erreicht. Damit wurden die ursprünglich angestrebten Vorgaben deutlich übertroffen.

Unter dem Strich wurden mehr als 240 Einzelmaßnahmen ermittelt, von denen bereits eine Reihe umgesetzt worden sind. Grundlage dafür waren Gebäude- und Wärmeanalysen. Schwerpunkte sind die Umrüstung der Straßenbeleuchtung, der Auf- und Ausbau der Eigenerzeugung

von Energie sowie die Nutzung von Elektrofahrzeugen und die damit verbundene Einrichtung von Ladesäulen. Werden alle Handlungsempfehlungen befolgt, sinken die Energiekosten insgesamt um 252.000 Euro pro Jahr. Damit werden die kommunalen Kassen deutlich entlastet.

Die enviaM-Gruppe unterstützte die Städte und Gemeinden auch bei der Einführung von Energiemanagement-Systemen, beriet diese zu energietechnischen Fragen und informierte sie zu Fördermöglichkeiten. Insgesamt fanden zwölf Netzwerktreffen statt. Hinzu kamen vier Schulungsveranstaltungen. Als sehr hilfreich für die tägliche Arbeit erwies sich ein vom Unternehmen zur Verfügung gestelltes online gestütztes Energiemanagement-System. Damit konnten die Kommunen ihren Energieverbrauch, ihre Energiekosten und ihre Kohlendioxid-Emissionen genau erfassen.

Die Kommunen lobten vor allem den Praxisbezug des Energieeffizienznetzwerks. Das Motto »Von der Praxis für die Praxis!« wurde von Beginn an durchgängig gelebt. Die enviaM-Gruppe und die beteiligten Städte und Gemeinden denken deshalb auch über den Förderzeitraum 2019 hinaus über eine Fortsetzung des Energieeffizienznetzwerks nach. Auch weiterhin soll es eine gemeinsame Plattform für den Informations- und Erfahrungsaustausch geben.

Rege Nachfrage der Kommunen

Das erste Energieeffizienznetzwerk für Kommunen der enviaM-Gruppe kann in jeder Hinsicht als Erfolgsmodell bezeichnet werden. Der Energiedienstleister hat deshalb im August 2018 ein zweites Energieeffizienznetzwerk für Kommunen eingerichtet. Ihm gehören die Städte Arnstein, Harzgerode, Leuna und Lützen sowie die Gemeinden Elsteraue und Salzatal an. Es will an die Erfolge des ersten Energieeffizienznetzwerkes anknüpfen. Ein drittes Energieeffizienznetzwerk für Kommunen befindet sich in Planung. Hierfür zeigen vor allem Städte und Gemeinden im Raum Südsachsen Interesse.

Mit ihrem Engagement in den Energieeffizienznetzwerken unterstreichen die teilnehmenden Kommunen ihre Schlüsselrolle für den Wandel der Energieversorgung. Sie setzen die Energiewende vor Ort aktiv um und sind so ein Vorbild für Bürger und Unternehmen. Es bleibt zu wünschen, dass sie viele Nachahmer finden.

Die Energieeffizienznetzwerke für Kommunen der enviaM-Gruppe leben vom regelmäßige Austausch der Teilnehmer, der von allen Vertretern sehr geschätzt wird. *Foto: Thorsten Schack.*

Die Verkehrswende ist ein wesentlicher Bestandteil der Energiewende. Die Mitglieder der Energieeffizienznetzwerke für Kommunen zeigen großes Interesse am Thema Elektromobilität und lassen sich dazu gern vom Energiedienstleister beraten. *Foto: Thorsten Schack.*

Aus der Presse

Pressemitteilung Nr. 12/19

SSG zur Vereinfachung und Verbesserung von Förderverfahren: Kommission legt einen richtungsweisenden Bericht vor, den die Staatsregierung zügig aufgreifen sollte

Der Sächsische Städte- und Gemeindetag (SSG) hält den heute vorgestellten Kommissionsbericht für richtungsweisend zur Modernisierung und Vereinfachung der sächsischen Förderverfahren. Hervorzuheben sind aus kommunaler Sicht beispielsweise die Vorschläge zur Zusammenlegung von Förderrichtlinien, zur Neuansiedlung aller kommunalen Förderprogramme bei der Landesdirektion sowie zur Umstellung auf ein mehrjähriges Maßnahmeplanverfahren, das den Kommunen mehr Planungssicherheit bringen wird.

Stefan Skora, Oberbürgermeister der Stadt Hoyerswerda und Präsident des SSG sagte dazu: *»Die Kommission zur Vereinfachung und Verbesserung von Förderverfahren hat in der Gesamtschau gute Arbeit geleistet. Der Bericht enthält zahlreiche positive Impulse, die die sächsische Förderlandschaft fortentwickeln können. Nun liegt der Ball wieder bei der Staatsregierung, die die wichtigsten Anregungen schnellstmöglich aufgreifen und umsetzen sollte.«*

Der SSG hat etliche Vorschläge in die Kommission eingebracht. Leider konnten sich einige wichtige Vorschläge der kommunalen Ebene, wie die Überführung zahlreicher Förderprogramme in Pauschalförderungen oder die generelle Abschaffung von baufachlichen Stellungnahmen, nicht durchsetzen. *»Wir halten den Kommissionsbericht auch insoweit für den Auftakt und nicht für den Abschluss eines dringend notwendigen Modernisierungsprozesses«*, so **Skora**.

Hintergrund:
Die Kommission zur Vereinfachung und Verbesserung von Förderverfahren wurde von der Staatsregierung am 15. Mai 2018 eingesetzt. In der Kommission wirkten mit Herr Dr. Tilmann Schweisfurth, Präsident a. D. des Landesrechnungshofes Mecklenburg-Vorpommern (Vorsitz), Herr Stefan Rix, Vizepräsident des Sächsischen Rechnungshofes, Herr Markus Ulbig, Staatsminister des Innern a. D., Herr André Jacob, Geschäftsführendes Präsidialmitglied des Sächsischen Landkreistages, Herr Mischa Woitscheck, Geschäftsführer des SSG, Herr Ulrich Hörning, Bürgermeister und Beigeordneter für Allgemeine Verwaltung der Stadt Leipzig sowie Herr Prof. Dr. Joachim Ragnitz, stellvertretender Leiter des ifo Instituts, Niederlassung Dresden.

Dresden, 20. Mai 2019

Pressemitteilung Nr. 13/19

Sächsischer Städte- und Gemeindetag ruft zu hoher Wahlbeteiligung zu den Europa- und Kommunalwahlen auf

Der Sächsische Städte- und Gemeindetag (SSG) ruft zu einer hohen Wahlbeteiligung an den Europa- und Kommunalwahlen am 26. Mai 2019 auf.

Mischa Woitscheck, Geschäftsführer des Verbandes, sagte dazu: *»Das sächsische Superwahljahr 2019 geht am Sonntag in seine erste Runde. Die Bürgerinnen und Bürger entscheiden, wer ihre Interessen in Straßburg, Brüssel und vor Ort in den nächsten Jahren vertreten wird. Ich rufe alle Bürgerinnen und Bürger auf, sich an den Wahlen zu beteiligen. In den Stadt-, Gemeinde- und Ortschaftsräten wird mit viel Engagement und Sachverstand wertvolle ehrenamtliche Tätigkeit geleistet. Eine hohe Wahlbeteiligung ist nicht nur Anerkennung für das Geleistete, sondern wird den Gewählten für ihre zukünftigen Aufgaben den Rücken stärken.«*

Der Geschäftsführer des kommunalen Spitzenverbandes wies anlässlich der Kommunalwahlen auf das Positionspapier zur Stärkung kommunaler Selbstverwaltung hin, dass der Landesvorstand des SSG im April 2019 beschlossen hat. *»Das Positionspapier will ausdrücklich die Handlungsspielräume der Stadt- und Gemeinderäte erweitern. Das Verfassungsrecht auf kommunale Selbstverwaltung darf nicht nur auf dem Papier stehen, sondern muss durch weite und motivierende Handlungsspielräume vor Ort auch gelebt werden können*, so **Woitscheck**.

Neben der Wahl des Europäischen Parlaments finden am kommenden Sonntag in allen sächsischen Städten und Gemeinden Stadtrats- bzw. Gemeinderatswahlen statt. Daneben werden zahlreichen Ortschaftsräte gewählt und in 13 Städten und Gemeinden auch Bürgermeisterwahlen durchgeführt. Die Wahllokale sind von 8 bis 18 Uhr geöffnet. Briefwähler müssen ihre Wahlbriefe so rechtzeitig abschicken, dass sie am Wahltag bei der auf dem Wahlbriefumschlag aufgedruckten Adresse bis spätestens 18 Uhr eintreffen.

Der SSG unterstützt die Stadt- und Gemeinderäte in ihrer Arbeit und gibt eine aktualisierte Ausgabe seines »Taschenbuches für die Ratsarbeit« heraus. In dem Buch werden in komprimierter und verständlicher Form u. a. die Rechte und Pflichten von Gemeinderäten, der Ablauf von Gemeinderatsitzungen aber auch die Grundzüge des kommunalen Finanzausgleichs und der kommunalen Haushalts- und Rechnungsführung erläutert. Das Taschenbuch kann u. a. auf der Internetseite des Verbandes, www.ssg-sachsen.de, bestellt werden.

Dresden, 24. Mai 2019

Pressemitteilung Nr. 14/19

Sächsischer Städte- und Gemeindetag gratuliert Oberbürgermeister Jung zur Wahl zum Städtetags-Präsidenten

Der Sächsische Städte- und Gemeindetag (SSG) gratuliert Herrn Oberbürgermeister Jung aus Leipzig zur heutigen Wahl zum Präsidenten des Deutschen Städtetages.

Der Präsident des SSG, Oberbürgermeister **Stefan Skora** aus Hoyerswerda, sagte dazu: *»Wir freuen uns, dass seit heute mit Burkhard Jung ein sächsischer Oberbürgermeister an der Spitze des Deutschen Städtetages steht. Wir schätzen Burkhard Jung als ebenso leidenschaftlichen wie durchsetzungsfähigen Interessenvertreter, was er schon oft auch als 1. Vizepräsident des SSG unter Beweis gestellt hat. Wir wünschen Burkhard Jung viel Erfolg auf der Bundesebene.«*

Zur Person: Burkhard Jung wurde am 07.03.1958 in Siegen/Westfalen geboren. Nach seiner Schulzeit und dem Studium war er Lehrer für Deutsch und Evangelische Religion. 1991 erhielt er die Abordnung als Schulleiter an das Evangelische Schulzentrum Leipzig. Ab 1999 arbeitete Jung in der Stadtverwaltung Leipzig als Beigeordneter und übernahm im Jahr 2006 als Nachfolger von Wolfgang Tiefensee die Amtsgeschäfte als Oberbürgermeister der Stadt Leipzig. Oberbürgermeister Jung ist seit 2008 1. Vizepräsident des SSG und seit 2013 Stellvertreter des Präsidenten des Deutschen Städtetages.

Dresden, 6. Juni 2019

Pressemitteilung Nr. 15/19

SSG weist Befürchtungen des Bundes der Steuerzahler zu flächendeckenden Grundsteuererhöhungen zurück

Der Sächsische Städte- und Gemeindetag hat heute Berichterstattungen in den überregionalen Zeitungen zurückgewiesen, in denen vor dem Hintergrund der aktuell diskutierten Grundsteuerreform vor durchschnittlichen Grundsteuererhöhungen i. H. v. 70 % gewarnt wurde. Laut den Medienberichten betreffe dies insbesondere »den Osten«. Dabei wurde auf entsprechende Veröffentlichungen des Bundes der Steuerzahler verwiesen.

»Das ist unverantwortliche Panikmache und berücksichtigt überhaupt nicht, dass die Städte und Gemeinden es durch die Neufestsetzung der Hebesätze in der Hand haben, die Reform aufkommensneutral zu gestalten. Die sächsischen Städte und Gemeinden haben wiederholt klargemacht, dass es Ihnen nicht darum geht, die notwendige Grundsteuerreform für Steuererhöhungen zu nutzen«, sagte der Geschäftsführer des SSG, **Mischa Woitscheck**, heute in Dresden. Auch der Deutsche Städtetag hat erst vor wenigen Tagen beschlossen, dass sich die Kommunen ausdrücklich zum Ziel einer aufkommensneutralen Reform auf Gemeindeebene bekennen und die örtlichen Hebesätze rechtzeitig anpassen werden.

2018 hatte das Bundesverfassungsgericht die geltenden Regelungen für die Einheitsbewertung von Grundvermögen für verfassungswidrig erklärt und dem Gesetzgeber eine Frist gesetzt, bis Ende 2019 eine neue Rechtsgrundlage für die Grundsteuer zu verabschieden. Kommt die Grundsteuerreform nicht bis zum Jahresende, gehen den sächsischen Städten und Gemeinden mehr als 500 Mio. Euro Einnahmen verloren. Auf der Basis des noch zu verabschiedenden neuen Grundsteuer- und Bewertungsrechts werden erst 2025 neue Grundsteuerbescheide ergehen.

Dresden, 6. Juni 2019

Pressemitteilung Nr. 16/19

SSG begrüßt den Beginn der parlamentarischen Beratungen zur Grundsteuerreform

Die heutige erste Lesung des Gesetzentwurfes zur Grundsteuerreform stimmt den Sächsischen Städte- und Gemeindetag (SSG) zuversichtlich, dass das Gesetzespaket gerade noch rechtzeitig beschlossen werden könnte. Nach einem Urteil des Bundesverfassungsgerichts hat der Bundesgesetzgeber bis zum Ende dieses Jahres eine Neuregelung zu treffen.

Mischa Woitscheck, Geschäftsführer des SSG, sagte dazu: *»Nachdem bereits viel wertvolle Zeit verstrichen ist, müssen Bundestag und Bundesrat nun Handlungsfähigkeit beweisen. Wegen der im Gesetzespaket enthaltenen Änderung des Grundgesetzes, müssen es beide Häuser mit einer Mehrheit von zwei Dritteln beschließen. Scheitert die Reform, droht allein für die sächsischen Kommunen ein Steueraufkommen von derzeit über 510 Millionen Euro jährlich wegzufallen. Das hätte dramatische Folgen, insbesondere für freiwillige kommunale Leistungen wie die Vereins- und Sportförderung«.*

Aus Sicht der sächsischen Städte und Gemeinden stellt das Gesetzespaket einen tragfähigen Kompromiss dar. Die Grundsteuer wird sich auch künftig am Grundstücks- und Gebäudewert orientieren. Das begrüßt der SSG. Die Öffnungsklausel für abweichende Regelungen der Bundesländer wird kritisch gesehen. Die Reform darf gegenüber den Vorgaben des Bundes jedenfalls keinen zusätzlichen kommunalen Aufwand erzeugen.

Eine klare Absage erteilt der kommunale Landesverband jüngsten Berichten überregionaler Medien, wonach die Grundsteuerreform gerade in den östlichen Bundesländern zu gravierenden Steuererhöhungen führen wird. *»Das ist Panikmache auf dem Rücken der Kommunen. Wir haben uns stets für eine gerechte und im Ergebnis aufkommensneutrale Reform eingesetzt«,* so **Woitscheck**.

Dresden, 27. Juni 2019

Pressemitteilung Nr. 17/19

Finanzlage der sächsischen Kommunen nicht so positiv, wie vom kommunalen Finanzreport der Bertelsmann Stiftung dargestellt

Der Sächsische Städte- und Gemeindetag (SSG) teilt die teils positive Darstellung der Finanzlage von Sachsens Kommunen durch die Bertelsmann Stiftung nicht. *»Wer gerade einmal zwei Drittel der bundesweiten Steuerkraft erreicht, hat keine Chance auf Spitzenplätze«,* sagte **Mischa Woitscheck**, Geschäftsführer des Kommunalen Spitzenverbandes.

Zwar bestätigt der heute vorgestellte 5. Kommunale Finanzreport der Bertelsmann Stiftung einmal mehr, dass die sächsischen Kommunen sich gut entwickelt haben, ihre Steuereinnahmen (2017: 833,55 Euro je Einwohner) aber nach wie vor deutlich unterhalb des deutschen Durchschnittsniveaus liegen. Der SSG bekräftigt daher den Befund der Bertelsmann-Studie, dass Sachsens Kommunen auf höhere Zuweisungen und Erstattungen des Bundes und des Freistaates Sachsen angewiesen sind.

Nicht bestätigen kann der SSG die Einschätzung der Bertelsmann-Stiftung, die sächsischen Kommunen verfügten über gestiegene Rücklagen und einen soliden Puffer für Einnahmerückgänge. Diese Einschätzung übersieht, dass die sächsischen Kommunen im Wesentlichen keine Rücklagen für zukünftige Investitionen oder Einnahmerückgänge bilden, sondern Liquidität für die laufende Aufgabenerfüllung vorhalten, wie dies auch bei Bund, Land und den Unternehmen der Fall ist.

»Die sächsischen Städte und Gemeinden versuchen sich schon seit Jahren an der Quadratur des Kreises. Trotz niedriger Steuereinnahmen bauen sie Schulden ab, vermeiden weitgehend Kassenkredite und setzen auf Investitionen. Die Städte und Gemeinden haben sich dabei auf die Mittel beschränkt, die sie einnehmen. Die Folge ist, dass heute in vielen Gemeinden Mängel und Investitionsstaus auftreten und die Einwohner den Eindruck gewinnen, dass es an vielen Ecken und Enden fehlt«, so **Woitscheck**.

Allein im kommunalen Straßenbau fehlen den sächsischen Kommunen nach der aktuellen Antragsrunde der Förderrichtlinie für den kommunalen Straßenbau rund 170 Mio. Euro Fördermittel. Auch in anderen Förderbereichen wie den Kindertagesstätten und den Schulen gibt es über die vom Freistaat Sachsen bereitgestellten Mittel hinaus erheblichen zusätzlichen Fördermittelbedarf. Die Rückstände werden nur durch eine maßgebliche Erhöhung der staatlichen Zuweisungen und Fördermittel abgebaut werden können.

Dresden, 9. Juli 2019

Aus Büchern und Zeitschriften

Neuerscheinungen

JULIA WERNER, CHRISTIAN EBEL, CHRISTIAN SPANNAGEL, STEPHAN BAYER (HRSG.)

Flipped Classroom – Zeit für deinen Unterricht

Praxisbeispiele, Erfahrungen und Handlungsempfehlungen

1. Auflage 2018, 244 Seiten, Broschiert, ISBN 978-3-86793-790-0, 25,00 €, Verlag Bertelsmann Stiftung, Carl-Bertelsmann-Str. 256, 33311 Gütersloh, Tel.: 05241-810, Fax: 05241-81681396, E-Mail: info@bertelsmann-stiftung.de, www.bertelsmann-stiftung.de

Flipped Classroom bedeutet: Die üblichen Aktivitäten inner- und außerhalb des Klassenzimmers werden umgedreht. Die Schülerinnen und Schüler eignen sich die von der Lehrkraft digital zur Verfügung gestellten Inhalte – etwa in Form von Lernvideos – eigenständig zu Hause an. Da im Unterricht nicht in ein neues Themengebiet eingeführt werden muss, steht die »gewonnene« Zeit zur Verfügung, um die Kinder und Jugendlichen gezielt zu unterstützen und individuell zu fördern. Der Unterricht kann stärker für die Übung, Anwendung und Reflexion des Gelernten genutzt werden. So zumindest die Erwartungen an den Ansatz und die Theorie.

Im Pilotprojekt »Flip your class!« haben Berliner Schulen unter wissenschaftlicher Begleitung der Pädagogischen Hochschule Heidelberg erste Unterrichtskonzepte zur Methode Flipped Classroom erstellt und in einem Design-Research-Ansatz erprobt. Dieser Band präsentiert Erkenntnisse aus dem Projekt und gibt Handlungsempfehlungen für die Praxis. Zudem dokumentiert er die Erfahrungen von Lehrkräften aus ganz Deutschland, die schon länger mit diesem Ansatz arbeiten: Beispiele aus unterschiedlichen Unterrichtsfächern, Schulformen und -stufen vermitteln die vielfältigen Einsatzmöglichkeiten der Methode. Ergänzend fließt die Perspektive von Praktikerinnen und Praktikern aus Deutschland, Österreich und der Schweiz von der Flipped Classroom Convention 2017 ein.

BERTELSMANN STIFTUNG (HRSG.)

Gute Ganztagsschulen entwickeln

Zwischenbilanz und Perspektiven

1. Auflage 2019, 260 Seiten, Broschiert, ISBN 978-3-86793-788-7, 28,00 €, Verlag Bertelsmann Stiftung, Carl-Bertelsmann-Str. 256, 33311 Gütersloh, Tel.: 05241-810, Fax: 05241-81681396, E-Mail: info@bertelsmann-stiftung.de, www.bertelsmann-stiftung.de

Wenn Kinder und Jugendliche regelmäßig an guten Ganztagsangeboten teilnehmen, erzielen sie bessere Lernerfolge – das belegt die Forschung. Doch wie entwickelt sich der Ausbau der Ganztagsschulen? Welche Erfahrungen sammeln Eltern, Lehrkräfte und Schulleiter? Wo kommt ganztägiges Lernen derzeit noch an seine Grenzen? Was benötigen Ganztagsschulen in Deutschland, um ihr Potenzial für gutes Lernen entfalten zu können, und woran lässt sich Qualität im Ganztag festmachen? Der Band »Gute Ganztagsschulen entwickeln« beantwortet diese Fragen anhand aktueller Forschungsergebnisse und liefert aussagekräftiges Zahlenmaterial. Kurze Porträts ausgesuchter Schulen illustrieren Entwicklungspfade und Meilensteine hin zur guten Ganztagsschule.

KLAUS DOPPLER/BERT VOIGT

Feel the Change! Wie erfolgreiche Change Manager Emotionen steuern

2018, 288 Seiten, Hardcover, ISBN 978-3-593-50920-4, 39,95 €, Campus Verlag GmbH; Kurfürstenstraße 49, 60486 Frankfurt am Main, Tel.: 069 976516-0, Fax: 069 976516-78, E-Mail: info@campus.de, www.campus.de

Nichts ruft bei Mitarbeitenden so starke Emotionen hervor, wie die Ankündigung großer Veränderungen. Von Angst um den Arbeitsplatz bis zynischem Fatalismus ist alles dabei. Auf die Wucht der geäußerten oder unterschwellig brodelnden Gefühle ist kein Change-Manager vorbereitet. Klaus Doppler und Bert Voigt haben das Emotionsmanagement zum Kernthema ihrer Beratungs- und Coachingarbeit gemacht. Sie geben Führungskräften Tools an die Hand, mit denen sie die Verbindlichkeit herstellen, die ihre Mitarbeitenden brauchen. Dann klappt's auch mit dem gegenseitigen Vertrauen!

MING ZENG

Smart Business – Alibabas Strategie-Geheimnis

2019, 288 Seiten, Hardcover, ISBN 978-3-593-50994-5, 34,95 €, Campus Verlag GmbH; Kurfürstenstraße 49, 60486 Frankfurt am Main, Tel.: 069 976516-0, Fax: 069 976516-78, E-Mail: info@campus.de, www.campus.de

Worin besteht das Geheimnis hinter dem sagenhaften Aufstieg des chinesischen Vorzeigeunternehmens Alibaba? Ist es Jack Ma, sein schillernder Gründer, oder etwa ein besonderer Algorithmus? Ming Zeng, seit 2006 Alibabas Chief Strategy Officer, verrät in diesem Buch erstmals, worin Alibabas Besonderheit besteht. Das Geheimnis liegt in seiner Strategie – der Strategie eines »Smart Business«, das auf maschinellem Lernen, Algorithmen und künstlicher Intelligenz beruht. Ming Zeng verrät, wie Alibaba neue Technologien dazu verwendet, sein Entscheidungsverhalten zu verbessern und konkrete Handlungsschritte abzuleiten. Für Alibaba ist Strategie bereits viel mehr als das übliche analysieren, planen und umsetzen. In »Smart Business« präsentiert Ming Zeng erstmals die revolutionäre Vorgehensweise, die er mit seinem Team entwickelt hat. Das Ergebnis ist ein grundlegend neues Set von Tools, das Unternehmen zur Entwicklung und Umsetzung einer smarten Strategie verhilft. Das Geheimnis von Alibaba könnte auch ihr Erfolgsgarant werden!

ÖMER ATIKER

Das Survival-Handbuch digitale Transformation

2018, 296 Seiten, Hardcover, ISBN 978-3-593-50921-1, 34,95 €, Campus Verlag GmbH; Kurfürstenstraße 49, 60486 Frankfurt am Main, Tel.: 069 976516-0, Fax: 069 976516-78, E-Mail: info@campus.de, www.campus.de

Digitalisierung ist wichtig und alle machen mit. Doch in der Praxis bleiben die Ergebnisse weit hinter den Erwartungen zurück. Widerstände, Unwissenheit, Angst, Politik: Die digitale Transformation scheitert nicht an der Technik, sondern an der Organisation. All das Neue nützt nichts, wenn Hunderte von Mitarbeitenden damit nichts anfangen können.

Ömer Atiker zeigt, welches die wirklichen Probleme bei der Digitalisierung sind und wie sie gelöst werden. Er liefert zu Situationen des geschäftlichen Alltags ganz konkrete Maßnahmen, mit denen

Führungskräfte ihre Belegschaft in Bewegung bringen. Damit sich der Wahnsinn in Grenzen hält und die digitale Transformation auch wirklich klappt!

URSULA BREDEL/CHRISTIANE MAASS

Leichte Sprache

2016, 560 Seiten, Hardcover, ISBN 978-3-411-75616-2, 39,99 €, Bibliographisches Institut GmbH, Dudenverlag, Mecklenburgische Straße 53, 14197 Berlin, Tel.: 030 897 85 82-81, Fax: 030 897 8597-8233, E-Mail: kundenservice@duden.de, https://shop.duden.de

Die Dudenredaktion und die Autorinnen, Ursula Bredel und Christiane Maaß, legen das erste umfassende Handbuch zum Thema Leichte Sprache vor. Es richtet sich an Wissenschaftler(innen), fortgeschrittene Studierende, Mitarbeiter(innen) in öffentlichen Verwaltungen, Übersetzer(innen) und andere Personen, die sich mit dem Thema Leichte Sprache beschäftigen.

Im ersten Teil des Bandes wird Leichte Sprache definiert und ihre Genese dargestellt. Es werden die gesetzlichen Grundlagen aufgezeigt sowie die Adressat(inn)en von Texten in Leichter Sprache beschrieben. Weiterhin werden die existierenden Regelwerke zum Übersetzen in Leichte Sprache kritisch gewürdigt; die Herstellung von Texten in Leichter Sprache wird in den Kontext verschiedener Übersetzungstheorien gestellt.

Im zweiten Teil werden die existierenden Regeln für Leichte Sprache auf wissenschaftlicher Grundlage präzisiert, die Strukturen Leichter Sprache rekonstruiert und Forschungsdesiderate formuliert. Im Ergebnis werden Prinzipien Leichter Sprache formuliert und Vorschläge für die Umsetzung abgestufter Reduktionsvarianten des Deutschen (»einfache« Sprache) vorgelegt.

ANTONÍN KAŇA

Großes Tschechisch-Deutsches Wörterbuch für die öffentliche Verwaltung

2. bearbeitete und erweiterte Ausgabe 2019, 308 Seiten, ISBN 978-80-7502-321-6, 20,00 €, Nakladatelství Leges, s.r.o., Lublaňská 4/61, Praha 2, www.knihyleges.cz

Mit mehr als 20.000 tschechischen Termini und ihren deutschen Entsprechungen füllt die vorgelegte Ausgabe eine spürbare Lücke im Angebot der zweisprachigen Fachwörterbücher für die öffentliche Verwaltung. Zugleich reflektiert es den raschen Wandel der öffentlichen Verwaltung in den letzten Jahren in der Tschechischen Republik.

Die erste Ausgabe aus dem Jahre 2011 reagierte auf die damaligen bedeutenden Systemänderungen, insbesondere im Bereich der Gebietsverwaltung und die durch den Beitritt zur EU geschaffenen interregionalen und grenzüberschreitenden Kooperationsstrukturen.

Die zweite Ausgabe erfasst jetzt darüber hinaus die mit der fortschreitenden Umsetzung des »Strategischen Rahmens der Entwicklung der öffentlichen Verwaltung der Tschechischen Republik für den Zeitraum 2014-2020« zusammenhängenden umfangreichen Projekte. Es handelt sich insbesondere um neue, aus dem Gesetz über den Staatsdienst folgende Begriffe (z. B. Einführung des Beamtenrechts).

Mit der Digitalisierung und ihren neuen Kommunikationsformen zwischen öffentlichen Stellen und Bürgern hat sich auch die Anzahl der Termini auf dem Gebiet des E-Governments wesentlich erhöht. Es werden auch die mit der Administrativgliederung der Tschechischen Republik und die mit den Änderungen der Organisationsstruktur der tschechischen öffentlichen Verwaltung zusammenhängende Begriffe aktualisiert und ergänzt. Die wesentliche Zunahme der internationalen Aktivitäten im Bereich der öffentlichen Verwaltung zeigt sich auch in den mit dem Erfahrungsaustausch zwischen den neuen und alten EU-Staaten sowie im Rahmen der Tätigkeit der internationalen Organisationen verbundenen Begriffen.

Die Liste der Abkürzungen wurde aktualisiert und ergänzt, vor allem aufgrund der neuen Gesetze aus dem Bereich des E-Governments und des Gesetzes über den Staatsdienst. Die Literaturliste wurde wesentlich reduziert, es werden vor allem die aktuellen tschechisch-deutschen Wörterbücher und die verschiedene elektronische Hilfsmittel angeführt.

Das Wörterbuch wird somit all denen von großem Nutzen sein, die als Verwaltungsakteure mit ihren tschechischen Partner kommunizieren. Es kann aber auch Juristen, Studenten, Dolmetschern und Fachübersetzern nützen, die in oben angeführten Bereichen der öffentlichen Verwaltung Fachausdrücke benötigen und benützen.

CHRISTIAN KEITEL

Zwölf Wege ins Archiv

2018, 285 Seiten, kartoniert, ISBN 978-3-515-12156-9, 29,00 €, Franz Steiner Verlag GmbH, Birkenwaldstr. 44, 70191 Stuttgart, Tel.: 0711/25 82 – 0, Fax: 0711/25 82 – 390, E-Mail: service@steiner-verlag.de, www.steiner-verlag.de

In der heutigen Informationsgesellschaft sind wir mehr denn je auf die langfristige Verfügbarkeit von Wissen angewiesen. Dennoch sind praktisch alle digital gespeicherten Informationen und fast alle seit 1840 erstellten Papierdokumente gefährdet. Zugleich gibt es keinen offenen und interdisziplinären Diskurs zu den relevanten Erhaltungsfragen.

Ausgehend von diesem Befund beschreibt Christian Keitel zentrale Fragestellungen und Methoden einer künftigen Archivwissenschaft: Versteht man alle auf Erhaltung spezialisierten Einrichtungen als Archive, können Ansätze der klassischen Archivwissenschaft (Archival Science), der täglichen Praxis in den klassischen Gedächtnisinstitutionen (Bibliotheken, Archive, Museen) und in der freien Wirtschaft, des Records Managements, der Digital Curation und der Informatik zusammengeführt und weiterentwickelt werden. Dafür liefert Keitel mit diesem Band wichtige Impulse: In zwölf Kapiteln diskutiert er die aktuellen Fragen der Archive zu Bewertung, Erschließung, Archivierungsstrategien sowie Nutzung und verortet sie in ihrem historischen Kontext.

Nachauflagen

DENKHAUS/RICHTER/BOSTELMANN

E-Government-Gesetz/Onlinezugangsgesetz: EGovG/OZG

mit E-Government-Gesetzen der Länder und den Bezügen zum Verwaltungsverfahrensrecht

Kommentar

1. Auflage 2019, 1.024 Seiten, Hardcover, 139,00 €, ISBN: 978-3-406-72413-8, Verlag C. H. Beck, Wilhelmstraße 9, 80801 München, Tel.: 089 38189-0, Fax: 089 38189-480, E-Mail: bestellung@beck.de, www.beck.de

Das E-Government-Gesetz des Bundes ist im ersten Teil der Kommentierung umfassend erläutert. Insbesondere Fragen zu elektronischer Kommunikation und Schriftformersatz, elektronischen Bezahlmöglichkeiten und Rechnungen, zu elektronischer Aktenführung, Open Data sowie zu IT-Organisation, Georeferenzierung und Barrierefreiheit sind ausführlich behandelt.

Das Onlinezugangsgesetz des Bundes befasst sich u.a. mit der Verpflichtung zur Bereitstellung von Online-Verwaltungsleistungen und ihrer Verknüpfung im Rahmen eines Portalverbunds. Es wird im zweiten Teil des Werkes kommentiert.

Von den Ländern erlassene E-Government-Gesetze und ihre wesentlichen Besonderheiten werden schließlich in Form einer Differenzkommentierung erklärt.

Vorteile auf einen Blick

- erläutert das EGovG und seine Abweichungen in den Landesgesetzen
- beinhaltet auch die angrenzenden Gesetze VwVfG, VwZG, VwGO, ZPO, PAuswG und DE-Mail-G
- verfasst von versierten, an der Entstehung von E-Government-Gesetzen beteiligten Regierungsbeamten

Perfekt für die Verwaltung und verwaltungsnahe Einrichtungen auf der Ebene von Bund, Ländern und Kommunen sowie für Gerichte, Rechtsanwälte und Unternehmen, Universitäten und Hochschulen.

LÜHR/JABKOWSKI/SMENTEK (HRSG.)

Handbuch Digitale Verwaltung

2019, 536 Seiten, 79,00 €; ISBN 978-3-8293-1377-3, Kommunal- und Schul-Verlag GmbH & Co. KG, Konrad-Adenauer-Ring 13, 65187 Wiesbaden, www.kommunalpraxis.de, E-Mail: info@kommunalpraxis.de

Digitale Techniken sind längst in die Verwaltungspraxis eingezogen. Das neue Online-Zugangsgesetz (OZG) beinhaltet eine Chance für die Verbesserung der Qualität der öffentlichen Verwaltung.

Die Diskussion über Digitalisierung der öffentlichen Verwaltung ist von einem Hype erfasst. Eigentlich ist alles schon gesagt. Es muss nur noch realisiert werden.

Die Herausforderung an alle Digitalisierer ist allerdings, wie die Umsetzung konkret geleistet werden kann.

Wie gestalten wir diesen Prozess der Veränderung? Können wir auf Beispiele zurückgreifen? Was können wir von unseren europäischen Nachbarn lernen? Wie nehmen wir die Bürger*innen und die Wirtschaft als User unserer Dienstleistungen mit? Wie werden die Beschäftigten einbezogen? Welche Qualifizierungsmaßnahmen müssen ergriffen werden? Was muss beim Datenschutz beachtet werden?

Das Handbuch Digitale Verwaltung zeigt auf, wer die digitale Verwaltung steuert, organisiert und kontrolliert.

Umfassend dargestellt werden der rechtliche Rahmen, Ansätze zur Umsetzung der Digitalen Verwaltung, Vertriebswege der öffentlichen Verwaltung, die Aufgabenverteilung und Organisation der digitalen Verwaltung, Barrierefreiheit bei der elektronischen Kommunikation, Datenschutz und Datensicherheit, Anwendungsbereiche der Digitalisierung, Bürgerbeteiligung, Digitalisierung und demografischer Wandel.

Das neue Handbuch stellt für die Betroffenen, die Fachleute und die Entscheider vertiefte Informationen bereit und soll eine Hilfestellung im Prozess der Digitalisierung öffentlicher Dienste sein.

Ergänzungslieferungen

SÄCHSISCHER STÄDTE- UND GEMEINDETAG UND SÄCHSISCHER LANDKREISTAG (HRSG.)

Sozialhilferecht in Sachsen

Sammlung der in Sachsen geltenden bundes- und landesrechtlichen Bestimmungen zur Grundsicherung und Sozialhilfe mit Richtlinien

Loseblattwerk, ca. 2.360 Seiten, 2 Ordner, 69,00 €, 58. Ergänzungslieferung mit Stand Januar 2019, ISBN 978-3-415-01593-7, Richard Boorberg Verlag GmbH & Co KG, Scharrstr. 2, 70563 Stuttgart, Tel.: 0711 7385-0, Fax: 0711 7385-100, E-Mail: bestellung@boorberg.de, www.boorberg.de

Diese Ergänzungslieferung berücksichtigt alle Vorschriften, die bis 31.12.2018 erlassen wurden und bis 01.04.2019 in Kraft getreten sind. Hingewiesen sei auf folgende Änderungen:

Band 1 (»Richtlinien-Band«)

Die Sozialhilferichtlinien (SHR) erfuhren Änderungen in den Randnummern 34.01, 38.01, 38.04-38.08, 94.01, 94.02, 97.01-97.08.

Im Anhang wurden berücksichtigt:

- Delegationssatzung vom 11.06.2018: Anhang A 420.21/I
- Neue Barbeträge ab 01.01.2020: Anhang A 423.111
- Orientierungshilfe zu den Schnittstellen der Eingliederungshilfe: Anhang A 425.0/I
- Orientierungshilfe zur Gesamtplanung (§§ 117 ff. SGB IX/§§ 141 ff. SGB XII): Anhang A 425.5
- Neue Düsseldorfer Tabelle und neue Unterhaltsrichtlinien des OLG Dresden (Stand jeweils 01.01.2019): Anhang A 429.31/I, Anhang A 429.31/II
- Änderung des Sächsischen Flüchtlingsaufnahmegesetzes aufgrund der Gesetze vom 11.12.2018 (SächsGVBl. S. 712) und vom 14.12.2018 (SächsGVBl. S 782): Anhang A 484.3

Band 2 (»SGB-Band«)

Änderungen waren u.a. veranlasst durch

- das Betriebsrentenstärkungsgesetz vom 17.08.2017 (BGBl. I S. 3214): Änderung von § 118 SGB XII[1]

1 Änderungen traten zum 01.01.2019 in Kraft.

- die (neue) Sozialhilfedatenabgleichsverordnung vom 20.02.2018 (BGBl. I S 207)
- das Gesetz zur Verlängerung befristeter Regelungen im Arbeitsförderungsrecht … vom 10.07.2018 (BGBl. I S. 1117): Änderung u. a. von §§ 46a und 136 SGB XII
- das Familiennachzugsneuregelungsgesetz vom 12.07.2018 (BGBl. I S. 1147)
- die Regelbedarfsstufen-Fortschreibungsverordnung 2019 vom 19.10.2018 (BGBl. I S. 2016)
- das GKV-Versichertenentlastungsgesetz vom 11.12.2018 (BGBl. I S. 2387)
- das Pflegepersonal-Stärkungsgesetz vom 11.12.2018 (BGBl. I S. 2394)
- das Teilhabechancengesetz vom 17.12.2018 (BGBl. I S. 2583)
- das Qualifizierungschancengesetz vom 18.12.2018 (BGBl. I S. 2651)

SCHAFFLAND/WILTFANG

Datenschutz-Grundverordnung (DS-GVO)/ Bundesdatenschutzgesetz (BDSG)

Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften

Loseblattwerk, 2 Ordner, 3.256 Seiten, ISBN: 978-3-503-17404-1, im Abo 122,00 € zzgl. Ergänzungslieferungen, Grundwerk im Einzelbezug 212,00 €, Ergänzungslieferung 5/19 mit Stand Mai 2019, 64,60 €, Erich Schmidt Verlag GmbH & Co, Genthiner Str. 30 G, 10785 Berlin; Tel.: 030 250085-0, Fax: 030 250085-870, E-Mail: ESV@ESVmedien.de, Bestellmöglichkeit online unter www.esv.info/978-3-503-17404-1

Die Lieferung 5/19 enthält ein weiteres Update zur DS-GVO und zum BDSG.

Hervorzuheben ist der in Anhang 1 zu Art. 58 abgedruckte Prüfkatalog der Aufsichtsbehörde Bayerns. Er stellt eine wertvolle Hilfe dar, wenn ein Unternehmen sich vergewissern will, ob es sachgerecht den Datenschutz organisiert hat. Auch können die ergänzenden ausführlichen kommentierenden Erläuterungen in Art. 58 Rdn. 7a bis 7d nützlich sein.

Die Kommentierungen zu § 4 BDSG (Videoüberwachung) sind wegen zahlreicher Veröffentlichungen von Rechtsprechung und Literatur neu gefasst worden.

Ab Kennziffer 7025 haben wir damit begonnen, Verlautbarungen der Datenschutzkonferenz (der Aufsichtsbehörden des Bundes und der Länder), die für den Praktiker von Bedeutung sein können, zu veröffentlichen. Siehe auch die unter Kz. 7015 ff. zum BDSG 2003 wiedergegebenen Verlautbarungen, die für die Praxis weiterhin nützlich sind, da sich materiell-rechtlich gegenüber dem BDSG 2003 nur wenig geändert hat.

QUECKE/SCHMID/MENKE/REHAK/WAHL/VINKE/BLAZEK/ SCHAFFARZIK/TROMMER

Gemeindeordnung für den Freistaat Sachsen (GOFS)

Ergänzbarer Kommentar mit weiterführenden Vorschriften

Loseblattwerk, 3 Ordner, 5.918 Seiten, ISBN: 978-3-503-03407-9, 162,00 € im Abonnement; Lieferung 2/19 mit Stand April 2019, 54,80 €, Erich Schmidt Verlag GmbH & Co, Genthiner Str. 30 G, 10785 Berlin; Tel.: 030 250085-0, Fax: 030 250085-870, E-Mail: ESV@ESVmedien.de, Bestellmöglichkeit online unter 18386-9

In den Vorschriftenteil wie in die Kommentierungen aufgenommen wurde die Verordnung des Sächsischen Staatsministeriums des Innern vom 12.11.2018 zur Durchführung der SächsGemO und der SächsLKrO in Bezug auf das Kommunalverfassungsrecht (SächsKomVerfRDVO). Mit dieser VO wurden verschiedene Verordnungen, u. a. die DVO SächsGemO, die VO zur Durchführung von Bürgerentscheiden und die VwV Gemeindenamen außer Kraft gesetzt. In der VO vom 12.11.2018 werden u. a. neu geregelt:

- Aufgaben der Großen Kreisstädte,
- Name und Bezeichnung der Gemeinden,
- Benennung von Gemeindeteilen,
- Genehmigung kommunaler Wappen und Flaggen,
- Zuständigkeit d. Rechtsaufsichtsbehörde bei Gebietsänderungen,
- Durchführung von Bürgerbegehren und Bürgerentscheid,
- Einwohnerversammlungen und Einwohnerantrag.

In die Kommentierungen eingearbeitet wurde neuere Rechtsprechung u. a. zur:

- Beitragserhebungspflicht der Gemeinden (BVerwG, Beschl. vom 16.11.2017 – 10 B 2/17),
- Ausfertigung von Satzungen (BVerwG, Beschl. vom 21.06.2018 – 4 BN 34/17),
- Verpflichtung von sog, Hinterliegern zur Bereitstellung einer eigenen Grundstücksentwässerungsanlage (u. a. SächsOVG, Beschl. vom 28.08.2018 – 4 A 33/17),
- Anberaumung einer Einwohnerversammlung (VG Chemnitz, Urt. vom 17.01.2018- I K 157/16),
- (verneinten) Verpflichtung eines Rechtsnachfolgers zur Beachtung einer (abwasserrechtlichen) Anordnung (VG Dresden, Beschl. vom 17.01.2018 – 13 L 1411/17.

HAUCK/NOFTZ

Sozialgesetzbuch SGB II: Grundsicherung für Arbeitsuchende

Kommentar

Loseblattwerk, Lieferung 2/19 – Stand April 2019, 59,60 €, Lieferung 3/19 – Stand Mai 2019, 60,60 €, Gesamtkommentar: 302,00 € ohne Fortsetzungsbezug, 136,00 € zuzüglich Fortsetzungslieferungen, 5.456 Seiten in 3 Ordnern, ISBN 978-3-503-06374-1, Erich Schmidt Verlag GmbH & Co, Genthiner Str. 30 G, 10785 Berlin, Tel.: 030 250085-0, Fax: 030 2500858-70, E-Mail: ESV@ESVmedien.de, www.esv.info/978-3-503-06374-1

Mit der Ergänzungslieferung 2/19 werden Überarbeitungen zu Kommentierungen von zentralen Vorschriften des SGB II vorgelegt:

- K § 42a (Darlehen) durch Dietrich Hengelhaupt
- K § 8 (Erwerbstätigkeit) und K § 44a (Feststellung von Erwerbstätigkeit und Hilfebedürftigkeit) durch Leandro Valgolio

Die Ergänzungslieferung 3/19 enthält im Schwerpunkt folgende Überarbeitungen zu Kommentierungen des SGB II:

- K § 10 (Zumutbarkeit) durch Leandro Valgolio
- K § 16c (Leistungen zur Eingliederung von Selbständigen), K § 16d (Arbeitsgelegenheiten) und K § 16g (Förderung bei Wegfall der Hilfebedürftigkeit)

HAUCK/NOFTZ

Sozialgesetzbuch SGB III: Arbeitsförderung

Kommentar, 2. Auflage

Loseblatt-Kommentar, Lieferung 3/19, Stand: Mai 2019, 60,00 €, ISBN: 978-3-503-13861-6, Gesamtausgabe: 4.8556 Seiten in 3 Ordnern, DIN A5, Einzelbezug: 356,00 €, im Abonnement: 254,00 € zuzüglich Ergänzungslieferungen, ISBN: 978-3-503-13860-9, Erich Schmidt Verlag GmbH & Co, Genthiner Straße 30 G, 10785 Berlin; Tel.: 030 250085-0; Fax: 030 2500858-70; E-Mail: ESV@ESVmedien.de, Bestellmöglichkeit online unter http://www.esv.info/978-3-503-13861-6.

Die Lieferung 3/19 wird das Inhaltsverzeichnis aktualisiert und es werden zahlreiche Kommentierungen des SGB III an die Entwicklung von Gesetzgebung, Rechtsprechung und Literatur angepasst.

HAUCK/NOFTZ

Sozialgesetzbuch SGB VI: Gesetzliche Rentenversicherung

Kommentar

Loseblatt-Kommentar einschl. Lieferung 1/19 mit Stand April 2019, 58,00 €, Lieferung 2/19 mit Stand Mai 2019, 60,60 €; Gesamtkommentar: 182,00 €, ISBN 978-3-503-02877-1, 8.198 Seiten in 5 Ordnern, Erich Schmidt Verlag GmbH & Co, Genthiner Str. 30 G, 10785 Berlin, Tel.: 030 250085-0, Fax: 030 250085-870, E-Mail: ESV@ESVmedien.de, Bestellmöglichkeit online unter www.ESV.info/978-3-503-02877-1

Mit der Lieferung 1/19 wird der Kommentar weiter aktualisiert. Sie enthält eine Aktualisierung der Register sowie eine Überarbeitung zu K §§ 190a, 153, 154, 181, 275a, 275b, 287e, 287f, 291 und 319b, die aufgrund von Gesetzesänderungen und zwischenzeitlich ergangener Rechtsprechung erforderlich geworden sind.

Mit der Lieferung 2/19 wird der Kommentar weiter aktualisiert. Sie enthält eine Überarbeitung zu K §§ 9, 10, 42, 56, 58, 59, 89, 106, 109, 120c, 165, 249, 315a, und 319a, die aufgrund von Gesetzesänderungen und zwischenzeitlich ergangener Rechtsprechung erforderlich geworden sind.

HAUCK/NOFTZ

Sozialgesetzbuch SGB X: Verwaltungsverfahren, Schutz der Sozialdaten, Zusammenarbeit der Leistungsträger und ihre Beziehungen zu Dritten

Kommentar

Loseblattwerk, Lieferung 2/19 mit Stand April 2019, 59,60 €, Lieferung 3/19 mit Stand Juni 2019, 64,00 €, Gesamtkommentar: 154,00 €, 3.996 Seiten in 3 Ordnern, ISBN 978-3-503-08378-7, Erich Schmidt Verlag GmbH & Co, Genthiner Str. 30 G, 10785 Berlin, Tel.: 030 25008-50, Fax: 030 250085-870, E-Mail: ESV@ESVmedien.de, Bestellmöglichkeit online unter www.ESV.info/978-3-503-08378-7

Mit der 2. Lieferung 2019 wird insbesondere die Aktualisierung des Sozialdatenschutzes fortgesetzt: Zunächst wird die grundlegende EU-DSGVO entsprechend den Vorgaben der EU berichtigt, außerdem werden Neubearbeitungen von § 75 »Übermittlung von Sozialdaten für die Forschung und Planung«, § 82 »Informationspflichten bei der Erhebung von Sozialdaten bei der betroffenen Person« und § 82a »Informationspflichten, wenn Sozialdaten nicht bei der betroffenen Person erhoben wurden« vorgelegt. Abschließend wird mit der Neubearbeitung von § 103 »Anspruch des Leistungsträgers, dessen Leistungsverpflichtung nachträglich entfallen ist« diese Lieferung vervollständigt. § 104 folgt mit der nächsten Lieferung.

Mit der 3. Lieferung 2019 werden einerseits zur weiteren Aktualisierung des Sozialdatenschutzes Neubearbeitungen von § 76 »Einschränkung der Übermittlungsbefugnis bei besonders schutzwürdigen Sozialdaten«, § 83 »Auskunftsrecht der betroffenen Personen«, § 83a »Benachrichtigung bei einer Verletzung des Schutzes von Sozialdaten« sowie § 84 »Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch« vorgelegt. Andererseits wird die Überarbeitung der §§ 102 ff. fortgesetzt mit einer Erneuerung der Vorbemerkungen und der Neukommentierung des § 104 »Anspruch des nachrangig verpflichteten Leistungsträgers«.

HAUCK/NOFTZ

Sozialgesetzbuch SGB XI: Soziale Pflegeversicherung

Loseblatt-Kommentar einschließlich der Lieferung 1/19 mit Stand: April 2019, 64,00 €, Lieferung 2/19 mit Stand Juni 2019, 56,80 €, 4.520 Seiten in 2 Ordnern, ISBN 978-3-503-03642-4, 108,00 €, Erich Schmidt Verlag GmbH & Co, Genthiner Str. 30 G, 10785 Berlin, Tel.: 030 250085-0, Fax: 030 250085-305, E-Mail: ESV@ESVmedien.de, www.ESV.info, Bestellmöglichkeit online unter www.ESV.info/978-3-503-03642-4

Mit der Lieferung 1/19 werden die Gesetzesänderungen durch das GKV-Versichertenentlastungsgesetz und das Pflegepersonalstärkungsgesetz eingearbeitet und die Kommentierungen zu §§ 14 und 15, insbesondere zur Pflegebedürftigkeit bei Kindern, zu §§ 20 bis 23 zum versicherungspflichtigen Personenkreis sowie zur Vertretung des Pflegevorsorgefonds in gerichtlichen Verfahren gem. § 133 aktualisiert.

Die Lieferung 2/19 enthält die aufgrund der Änderung durch das PSG II schon zum 01.01.2017 erforderliche Aktualisierung des § 36 über die Pflegesachleistung der häuslichen Pflegehilfe sowie insbesondere Überarbeitungen von §§ 25 und 27 zum versicherten Personenkreis, von §§ 74 bis 76 zum Leistungserbringerrecht und der Regelungen zur Qualitätssicherung in § 113b, § 114 und § 114a.

PRAXIS DER KOMMUNALVERWALTUNG

Ratgeber für die tägliche Arbeit aller Kommunalpolitiker und der Bediensteten in Gemeinden, Städten und Landkreisen

Landesausgabe Sachsen: DVD-ROM Version 2.50 vom Mai 2019, Version, für 1 – 3 Plätze 99,00 € je DVD-ROM (inkl. Versand und MwSt.), Kommunal- und Schul-Verlag GmbH & Co. KG, Konrad-Adenauer-Ring 13, 65187 Wiesbaden, Telefon: 0611 88086-10, Telefax: 0611 88086-77, E-Mail: info@kommunalpraxis.de, www.kommunalpraxis.de

Folgende Beiträge haben sich in der Version 2.50 geändert:

1. Landesbeiträge

Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen (SächsVwVfZG)

Rolf-Dieter Kubitza, Regierungsdirektor a. D., ehem. Dozent an der Hochschule für öffentliche Verwaltung und Rechtspflege (FH), Fortbildungszentrum des Freistaates Sachsen, Meißen

Im Rahmen der §§ 2 Abs. 3 und 3 Abs. 1 SächsVwVfZG hat es einige klarstellende Entscheidungen Sächsischer Verwaltungsgerichte gegeben, die in die Kommentierung eingearbeitet wurden.

2. Bundesbeiträge

Gesetz über Ordnungswidrigkeiten

Von Georg Köberl, Verwaltungsdirektor, Landeshauptstadt München, Sabine Effner, Verwaltungsdirektorin, Landeshauptstadt München,

Dr. Elmar Nordhues, Verwaltungsdirektor, Landeshauptstadt München und Karl Schuff, Landeshauptstadt München
Der Text im Zusammenhang sowie die Kommentierung der §§ 71–134 OWiG wurden überarbeitet und auf den neuesten Stand der letzten Änderung vom 17.12.2018 gebracht.

Vergaberecht (VOB, VOL, VgV, SektVO, KonzVgV, VSVgV, VergStatVO, GWB und RPW)
Von Johannes-Ulrich Pöhlker, Ltd. Verwaltungsdirektor, Referent beim Hessischen Städte- und Gemeindebund a. D., Dr. Irene Lausen, Ministerialrätin, Referatsleiterin beim Hessischen Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung und Hans-Peter Müller, Dipl. Verwaltungswirt im Bundesministerium für Wirtschaft und Energie
Erstmals kommentiert wurden §§ 64–82 der VgV sowie der § 100 bis 114 GWB aus Teil 4 (Vergabe von öffentlichen Aufträgen und Konzessionen, Kapitel 1 Vergabeverfahren, Abschnitt 1 Grundsätze, Definitionen und Anwendungsbereich) sowie 115 bis 135 GWB aus Abschnitt 2 (Vergabe von öffentlichen Aufträgen durch öffentliche Auftraggeber, Unterabschnitt 1 Anwendungsbereich, Unterabschnitt 2 Vergabeverfahren und Auftragsausführung). Neu kommentiert wurden die §§ 1–3 VgV. Die abgedruckten Texte wurden aktualisiert.

Kommunale Wirtschaftsförderung
Von Andre Reutzel, Erster Stadtrat der Stadt Walsrode
Ein Dauerthema für die Kommunalpolitik und die öffentlichen kommunalen Verwaltungen ist die Wirtschaftsförderung. Dazu wurden immer wieder Umfragen gestartet, die im Beitrag berücksichtigt sind. Auch 2018 wurden wieder Befragungen durchgeführt. Die Ergebnisse lagen bei Redaktionsschluss leider noch nicht vor und werden in die nächste Überarbeitung einfließen.

Soziale Wohnraumförderung
Herbert Feulner, Ltd. Ministerialrat beim Bayerischen Staatsministerium des Innern, für Sport und Integration, München
Der Beitrag wurde um Erläuterungen zum Baukindergeld erweitert.

JÄDE/DIRNBERGER/MICHEL/BAUER/BÖHME/RADEISEN/THOM/SPIEKERMANN

Bauordnungsrecht Sachsen

Kommentar mit Ergänzenden Vorschriften

Loseblattwerk in 2 Ordnern, 3.698 Seiten, ISBN 978-3-8073-0972-9, 159,99 EUR zzgl. Aktualisierungslieferungen, 79. Aktualisierung Stand April 2019, Verlagsgruppe Hüthig Jehle Rehm GmbH, Hultschiner Straße 8, 81677 München, Tel.: 089 218379-28, Fax: 089 218376-20, E-Mail: kundenbetreuung@hjr-verlag.de, www.rehmnetz.de

Mit dieser Aktualisierung wird die Kommentierung zu den §§ 6, 11, 40, 41, 44 und 45 überarbeitet.

Das Sächsische Architektengesetz wurde auf den aktuellen Stand gebracht.

WOYDERA/SUMMER/ZÄNGL

Beamtenrecht in Sachsen

Kommentar

Loseblattwerk, 6.504 Seiten in 5 Ordnern, 249,99 € zzgl. Aktualisierungslieferungen, ISBN 978-3-8073-0945-3, 113. Aktualisierung mit Stand Februar 2019, 114. Aktualisierung mit Stand April 2019, Verlagsgruppe Hüthig Jehle Rehm GmbH, Hultschiner Straße 8, 81677 München, Tel.: 089 218379-28, Fax: 089 218376-20, E-Mail: kundenservice@hjr-verlag.de, www.rehmnetz.de

Die Aktualisierung 113. enthält einen Teil der notwendigen Änderungen durch das Gesetz zur Weiterentwicklung des Beamtenrechts. Weitere Anpassungen sind in den nächsten Aktualisierungen enthalten. Darüber hinaus wurden, durch das Änderungsgesetz veranlasst, auch § 66 SächsBG (Unparteilichkeit bei Amtshandlungen) sowie § 71 SächsBG (Fernbleiben vom Dienst) überarbeitet. Auch wurden noch restliche Teile der Änderungen des SächsBG durch das Gesetz zur Weiterentwicklung des Sächsischen Dienstrechts vom 28. Juni 2018, SächsGVBl. S. 430, eingearbeitet und kommentiert.

Die Aktualisierung 114. enthält zu zahlreichen Paragrafen des SächsBG die Änderungen, die das Gesetz zur Weiterentwicklung des sächsischen Dienstrechts vom 28.06.2018 mit sich gebracht hat und deren Einarbeitung in die Kommentierung. Ebenso ist die Erstkommentierung des neuen § 81a (Erfüllungsübernahme bei Schmerzensgeldansprüchen) enthalten.

Weiterhin sind eingearbeitet die erfolgten Änderungen durch das Gesetz zur Änderung beamten-, besoldungs- und versorgungsrechtlicher Vorschriften zur Umsetzung der Verbeamtung von Lehrkräften im Freistaat Sachsen vom 11. Dezember 2018 (SächsGVBl. S. 714) sowie die Erstkommentierung des § 143a SächsBG.

STEGMÜLLER/SCHMALHOFER/BAUER

Beamtenversorgungsrecht des Bundes und der Länder

Kommentar mit Rechtsverordnungen und Verwaltungsvorschriften

Loseblattwerk in 7 Ordnern mit ca. 10.296 Seiten, ISBN: 978-3-7825-0193-4, 279,99 € zzgl. Aktualisierungslieferungen, 137. Aktualisierung mit Stand Januar 2019, 138. Aktualisierung mit Stand März 2019, Verlagsgruppe Hüthig Jehle Rehm GmbH, Hultschiner Straße 8, 81677 München, Tel.: 089 21837-928, Fax: 089 21837-620, E-Mail: kundenbetreuung@hjr-verlag.de, www.rehmnetz.de

Mit der 137. Aktualisierung werden die Erläuterungen zu § 50 BeamtvG vollständig überarbeitet und dabei sowohl die neuen DA-KG 2018 wie auch das BBVAnpG 2018/2019/2020 berücksichtigt.

Aufgrund der Aufnahme der Verwaltungsvorschriften wurden die Erläuterungen zu § 50d an die neuen Verwaltungsvorschriften zum BeamtVG angepasst.

Darüber hinaus erfolgte eine Anpassung der Erläuterungen zu § 50a und § 50f BeamtVG im Hinblick auf die seit 1. Januar 2019 geltenden sozialversicherungsrechtliche Rechengrößen.

Die Erläuterungen zu den §§ 51, 54, 55, 67 und 69b BeamtVG wurden unter Berücksichtigung der neuen Verwaltungsvorschriften und der aktuellen Rechtsprechung aktualisiert.

Wegen des BBVAnpG 2018/2019/2020 werden zudem die §§ 70, 71 BeamtVG umfassend überarbeitet.

Im Länderteil wurde im Bereich Baden-Württemberg das dortige Landesbesoldungsgesetz aktualisiert und außerdem die Kommentierung zu § 108 LBeamtVGBW überarbeitet. In Teil Nordrhein-Westfalen wurde der Kommentar zu § 68 LBeamtVGNW aktualisiert. Weitere Änderungen gab es in Bereich der Normen von Thüringen und bei der Kommentierung zur BeamtVÜV.

Der Schwerpunkt der 138. Aktualisierung liegt wieder bei der Aufnahme der neuen Verwaltungsvorschriften und der Einarbeitung aktueller Rechtsprechung:

Zu § 8 (Berufsmäßiger Wehrdienst und vergleichbare Zeiten) und § 9 (Nichtberufsmäßiger Wehrdienst) sind die Erläuterungen unter Berücksichtigung der neuen Verwaltungsvorschriften vollständig überarbeitet worden.

Aktualisierung der Erläuterungen zu den §§ 14 (Höhe des Ruhegehalts), 14a (Vorübergehende Erhöhung des Ruhegehaltes), 54 (Zusammentreffen mehrerer Versorgungsbezüge) und 66 (Beamte auf Zeit) BeamtVG anhand der neuesten Rechtsprechung.

Die Verwaltungsvorschriften zu § 50e (Vorübergehende Gewährung von Zuschlägen) wurden erstmalig in das Werk aufgenommen und die Erläuterungen zu § 50e an die BeamtVGVwV sowie an neuere Rechtsentwicklungen angepasst.

Weiter erfolgt eine Ergänzung der Erläuterungen zum Versorgungslastenteilungs-Staatsvertrag aufgrund zwischenzeitlicher Erfahrungen in der Anwendung.

Im Teil C gibt es folgende Änderungen:

Die Erläuterungen zu den Art. 1, 9 und 115 BayBeamtVG werden aktualisiert und dabei auch Änderungen im Normtext der Art. 9 und 115 BayBeamtVG berücksichtigt. Die Vorschrift des Art. 69 BayBeamtVG (Familienzuschlag) wird erstmalig und umfassend erläutert.

Zudem erfolgt die Aktualisierung des Beamtenversorgungsgesetzes von Sachsen-Anhalt und der entsprechenden Synopse sowie des Thüringer Beamtenversorgungsgesetzes nach Gesetzesänderungen.

SCHABEL/LEY

Öffentliche Auftragsvergabe im Binnenmarkt

Erläuterungen und Materialien zur Ausschreibung, Angebotsprüfung und Vergabe nach VOB, VOL und VOF mit EG-Vorschriften – Leitfaden

Loseblattwerk in 2 Ordnern mit 2.044 Seiten, 129,99 EUR zzgl. Aktualisierungen, 309,99 EUR ohne Aktualisierungen, ISBN 978-3-8073-0843-2, 47. Aktualisierung mit Stand April 2019, Verlagsgruppe Hüthig Jehle Rehm GmbH, Hultschiner Straße 8, 81677 München, Tel.: 089 21837-928, Fax: 089 21837-620, E-Mail: kundenbetreuung@hjr-verlag.de, www.rehmnetz.de

Das bringt Ihnen die 47. Aktualisierung

Am 31.01.2019 wurde die Neufassung der VOB/A beschlossen. Entgegen dem Beschluss vom 13.11.2018 betreffen die Änderungen nicht nur den 1. Abschnitt für nationale Bauvergaben, sondern auch den 2. Abschnitt für die EU-weite Vergaben und den 3. Abschnitt für Vergaben im Bereich Verteidigung und Sicherheit.

Der geänderte 1. Abschnitt soll im Zuständigkeitsbereich des Bundesbauministeriums ab dem 01.03.2019 angewendet werden. Hierzu soll zeitnah ein entsprechender Erlass erfolgen. Auf Landesebene ist der neue 1. Abschnitt bereits ab dem Tag der Veröffentlichung in den Bundesländern anzuwenden, welche in ihren Landesvergabegesetzen einen dynamischen Verweis auf die jeweils gültige Fassung der VOB/A beinhalten.

Die Änderungen des 2. Abschnitts für EU-weite Vergabeverfahren oberhalb eines Auftragswertes von 5.548.000,00 € netto treten noch nicht in Kraft. Hierzu ist zunächst eine Änderung der Vergabeverordnung (VgV) erforderlich, welche noch auf die Fassung des 2. Abschnitts aus dem Jahr 2016 verweist.

Die VOB/A in Kapitel C 1/3 wird daher mit dieser Lieferung nur bezogen auf Abschnitt 1 aktualisiert, die Abschnitte 2 und 3 folgen mit der nächsten Aktualisierung.

Die Ergänzungslieferung wird vervollständigt durch die Aktualisierung aller Landesvorschriften.

BREIER/DASSAU/FABER U. A.

TVöD – Entgeltordnung VKA – Eingruppierung in der Praxis

Kommentar

Online-Produkt, ISBN 978-3-8073-0124-2, 41,99 € Vierteljahrespreis für 3 Lizenzen zzgl. Aktualisierung, Loseblattwerk 129,99 € zzgl. Aktualisierungslieferungen, 2.166 Seiten, 21. Aktualisierung mit Stand Juni 2019, Verlagsgruppe Hüthig Jehle Rehm GmbH, Hultschiner Straße 8, 81677 München, Tel.: 089 21837-928, Fax: 089 21837-620, E-Mail: kundenbetreuung@hjr-verlag.de, www.rehmnetz.de

Das 21. Update bietet insbesondere die Erläuterung weiterer wichtiger Tätigkeitsmerkmale.

Zu den Schwerpunkten des Updates:

1. Im Teil C 1 werden die Erläuterungen zu § 12 TVöD (Eingruppierung) ergänzt und neue Rechtsprechung des BAG eingearbeitet.
2. Im Teil D 1.9 und D 1.10 werden die Vorbemerkung Nr. 9 (Unterstellungsverhältnisse) und die Vorbemerkung Nr. 10 (Ständige Vertreterinnen und Vertreter) umfassend erläutert. Diese Vorbemerkungen sind für all die Tätigkeitsmerkmale von Bedeutung, die die Eingruppierung entweder von unterstellten Beschäftigten abhängig machen (Leitungsfunktionen) oder von einer Vertretung, die auf Dauer angelegt ist und nicht nur in einer Abwesenheitsvertretung bei Urlaub oder Krankheit besteht.
3. Es werden mit dieser Aktualisierung folgende Tätigkeitsmerkmale ausführlich und mit Beispielen für die Praxis erläutert:
   - Tätigkeitsmerkmale für Meister, Teil D 1.2.2.4
   - HNO-Audiologie-Assistentinnen, Teil D 1.3.11.7
   - Logopäden, Teil D 1.3.11.8
   - Masseure und med. Bademeister, Teil D 1.3.11.9
   - Medizinisch-technische Assistentinnen, Teil D 1.3.11.10
   - Beschäftigte an Bühnen und Theatern, Teil D 1.3.27
4. Auf die Ärzte in kommunalen Krankenhäusern wird ganz überwiegend nicht der TVöD, sondern der mit dem Marburger Bund abgeschlossene TV Ärzte/VKA angewendet. Dort ist die Eingruppierung im Tariftext, §§ 15 ff., geregelt. Die Vorschriften werden ausführlich erläutert, Teil D 2.1.

BREIER/DASSAU/KIEFER †/LANG/LANGENBRINCK

TVöD-Kommentar

Kommentar

Online-Produkt, ISBN: 978-3-8073-2226-1, 254,99 € Vierteiljahrespreis für 3 Lizenzen zzgl. Aktualisierungslieferungen, 111. Aktualisierung mit Stand April 2019, 112. Aktualisierung mit Stand Juni 2019, Verlagsgruppe Hüthig Jehle Rehm GmbH, Hultschiner Straße 8, 81677 München, Tel.: 089 21837-928, Fax: 089 21837-620, E-Mail: kundenbetreuung@hjr-verlag.de, www.rehmnetz.de

Das 111. Update hat folgende Schwerpunkte:

1. Im Teil A 5 werden die Tabellen mit allen Stundenentgelten und sonstigen Berechnungen eingearbeitet, die ab 01.04.2019 gelten.
2. Im Teil B 1 des Werks wird als Anhang zu den Erläuterungen zu § 24 TVöD (Berechnung und Auszahlung des Entgelts) ein Muster angefügt, das für die Entgeltbescheinigung in der Praxis verwendet werden kann.
3. In die Kommentierung des § 26 TVöD (Erholungsurlaub) in Teil B 1 des Werks sind zum einen mehrere aktuelle Entscheidungen des BAG und des EuGH eingearbeitet. Unter anderem werden die EuGH-Entscheidungen vom 06.11.2018 in den Rechtssachen Max-Planck (C-684/16) und Kreuziger (C-619/16) eingehend beleuchtet. Nach einer kontroversen Auseinandersetzung in Rechtsprechung und juristischer Fachliteratur hat der EuGH damit die Frage geklärt, ob der Arbeitgeber seine Arbeitnehmer zwingen muss, ihren Erholungsurlaub einzubringen. Der EuGH hat dazu festgestellt, dass sich der Arbeitgeber auch dann auf einen Verfall des Urlaubs berufen kann, wenn er den Urlaub seiner Beschäftigten nicht vorher von sich aus selbst festgelegt hat (vgl. Erl. 5.1.1, Rn. 506). Allerdings müssen – so der EuGH in dieser Entscheidung – Arbeitgeber ihre Beschäftigten zukünftig über den Verfall von Urlaubsansprüchen informieren und sie auffordern, den Urlaub rechtzeitig einzubringen. Dies sollte rechtzeitig vor Ablauf der tariflichen Verfallsfristen geschehen. Hierzu enthält die Kommentierung nun einen Formulierungsvorschlag für Arbeitgeber für ein solches Aufklärungsschreiben (vgl. Erl. 5.1.1, Rn. 511). Auf die für den 19.02.2019 unter dem Aktenzeichen 9 AZR 541/15 verkündete Entscheidung des BAG unter Einbeziehung der vom EuGH beantworteten Vorlagefragen wird hingewiesen.
   Zum anderen wurde die Kommentierung um ausführliche Erläuterungen (vgl. Erl. 3.15, Rn. 153) zu den Möglichkeiten einer Rückforderung von zu viel gewährtem Urlaub ergänzt. Herausgearbeitet wird der Unterschied zwischen dem Rückforderungsverbot von Urlaub bei einem Ausscheiden in der ersten Jahreshälfte (Erl. 3.15.1, Rn. 153.3) und der demgegenüber möglichen Rückforderung in allen Fällen, in denen ein Teilurlaub aus anderen Gründen als dem Ausscheiden in der ersten Jahreshälfte entsteht, z. B. wegen der Inanspruchnahme von Elternzeit (Erl. 3.15.2, Rn. 153.8).
4. In die Erläuterungen zu § 30 TVöD (Befristete Arbeitsverhältnisse) im Teil B 1 ist umfangreiche Rechtsprechung, insbesondere des Bundesarbeitsgerichts, eingearbeitet. Besondere Aufmerksamkeit verdient das Urteil des BAG vom 23.01.2019 – 7 AZR 733/16 – juris. Unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts vom 06.06.2018 – 1 BvL 7/14 und 1 BvR 1375/14 – ZTR 2018, 404 – zur sachgrundlosen Befristung bei Vorbeschäftigung des Arbeitnehmers hat das BAG nunmehr entschieden, dass die sachgrundlose Befristung eines Arbeitsvertrags nach § 14 Abs. 2 Satz 2 TzBfG nicht zulässig ist, wenn zwischen dem Arbeitnehmer und dem Arbeitgeber bereits acht Jahre zuvor ein Arbeitsverhältnis von etwa eineinhalbjähriger Dauer bestanden hat, das eine vergleichbare Arbeitsaufgabe zum Gegenstand hatte (vgl. Rn. 131.10.1 zu § 30 TVöD).

Das 112. Update hat folgende Schwerpunkte:

1. In die Erläuterungen zu § 24 TVöD (Berechnung und Auszahlung des Entgelts) im Teil B 1 des Werks werden die aktuellen, ab dem 01.07.2019 geltenden Pfändungsfreigrenzen aufgenommen.
2. Im Teil B 1 sind die Erläuterungen zu § 33 TVöD (Beendigung des Arbeitsverhältnisses ohne Kündigung) ergänzt um Hinweise zur Versicherungspflicht in der gesetzlichen Sozialversicherung und der Zusatzversorgung nach Verlängerung des Arbeitsverhältnisses über die Regelaltersgrenze hinaus.
3. Im Teil B 4.5 werden die Vorschriften der durchgeschriebenen Fassung des TVöD für den Bereich Flughäfen, des TVöD-F, vervollständigt und die Änderungen der Änderungsvereinbarungen bis zur Nr. 12 vom 18.04.2018 eingearbeitet und erläutert. Inhaltlicher Schwerpunkt der Erläuterungen ist die nur im TVöD-F enthaltene Vorschrift des § 15.1 zum Feuerwehr- und Sanitätspersonal sowie die neueingefügte Anlage G zum TVöD-F. Hier ist als Ergebnis der bereits in der Tarifrunde 2016 vereinbarten Tarifverhandlungen über den Gesundheitsschutz der Flughafenfeuerwehr mit Wirkung vom 01.09.2018 ein Abs. 3 zu § 15.1 TVöD-F eingefügt worden, der auf die Regelungen der ebenfalls neu eingefügten Anlage G zum TVöD-F verweist. Die Anlage G, die in ihren insgesamt sieben Paragrafen die materielle Regelung zum Gesundheitsschutz der Flughafenfeuerwehr enthält, ist erläutert.
4. Der Teil E 1 des Kommentars betrifft die Vertragsmuster im Bereich der VKA. Durch eine Vielzahl neuer Entscheidungen in der Rechtsprechung einerseits und Gesetzesänderungen andererseits wurde eine grundlegende Überarbeitung einer erheblichen Zahl der dort enthaltenen Muster notwendig. Dies betraf z. B. die Anhebung des gesetzlichen Mindestlohns von 8,84 Euro auf 9,19 Euro zum 01.01.2019 und auf 9,35 Euro zum 01.01.2020. Die Änderungen im Teilzeit- und Befristungsgesetz vom 11.12.2018 wurden aufgenommen, insbesondere die des § 12 TzBfG zur Abrufarbeit (BGBl. I S. 2384). Hierzu wurde z. B. im Muster zur flexiblen Gestaltung der Arbeitszeit (E 1.1.5) in den Fußnoten kenntlich gemacht, dass nun auch gesetzlich in § 12 Abs. 3 TzBfG geregelt ist, dass der Anteil der einseitig vom Arbeitgeber abrufbaren zusätzlichen Arbeit nicht mehr als 25 Prozent der vereinbarten wöchentlichen Mindestarbeitszeit betragen darf. Damit hat der Gesetzgeber die Rechtsprechung des Bundesarbeitsgerichts vom 07.12.2005 – 5 AZR 535/04, siehe dazu auch Vorbem. 2.1.1 – kodifiziert (vgl. BT-Drucks. 19/3452, S. 20).
   Außerdem wurde die Änderung des § 309 Nr. 13 BGB in die allermeisten Muster eingearbeitet. Daraus ergibt sich, dass eine Bestimmung in Formulararbeitsverträgen unwirksam ist, durch die Erklärungen des Arbeitnehmers gegenüber dem Arbeitgeber an die Schriftform oder eine strengere Form gebunden sind. Etwas anderes gilt, wenn die Schriftform gesetzlich (wie bei der Kündigung des Arbeitsvertrages) oder tariflich (bei der Geltendmachung eines Anspruchs im Rahmen der Ausschlussfrist des § 37 TVöD) vorgesehen ist. Da der TVöD für die Kündigung einer Nebenabrede keine Form vorschreibt, darf hier deshalb keine strengere Form als die Textform verlangt werden (vgl. dazu z. B. § 6 im Muster E 1.1.1).
   In den Befristungsmustern wurde außerdem in den erläuternden Fußnoten die neue Rechtsprechung des Bundesverfassungsgerichts und des Bundesarbeitsgerichts zum Vorbeschäftigungsverbot bei der sachgrundlosen Befristung abgebildet. Danach ist eine sachgrundlose Befristung unzulässig, wenn mit demselben Arbeitgeber bereits zuvor ein befristetes oder unbefristetes Arbeitsverhältnis bestanden hat (vgl. dazu z. B. Fußnote 7 im Muster E 1.1.2.1). Die Dreijahresgrenze gilt nicht mehr (vgl. dazu Erl. 3.2 zu § 30 TVöD).

Außerdem wird nun in allen Befristungsmustern auf eine angekündigte Gesetzesänderung zur Befristungshöchstgrenze bei sachgrundlosen Befristungen hingewiesen (vgl. dazu z. B. Fußnote 12 im Muster E 1.1.16). Derzeit ist nach § 14 Abs. 2 Satz 1 TzBfG in der Gesetzesfassung vom 11.12.2018 die Befristung eines Arbeitsvertrages ohne sachlichen Grund bis zur Dauer von zwei Jahren zulässig. Allerdings will die Regierungskoalition die Befristung ohne Vorliegen eines sachlichen Grundes nur noch bis maximal 18 Monate gestatten und bei Unternehmern mit mehr als 75 Beschäftigten maximal 2,5 % der Belegschaft sachgrundlos befristen lassen. Da nicht auszuschließen ist, dass diese Gesetzesänderung beschlossen wird, obwohl sie bei den Änderungen im Teilzeit- und Befristungsgesetz vom 11.12.2018 (BGBl. I S. 2384 und BT-Drucks. 19/3452, S. 6) keine Berücksichtigung fand, müssen Arbeitgeber § 14 Abs. 2 TzBfG im Moment des Abschlusses eines sachgrundlos befristeten Arbeitsvertrages unbedingt auf seine aktuelle Fassung hin prüfen (aktuelle Fassung stets abrufbar unter: www.gesetze-im-internet.de/tzbfg/index.html).

5. Im Teil F 10 des Werks werden die Hinweise zu den Tarifverträgen zur Entgeltumwandlung im Bereich der VKA und des Bundes aktualisiert. Insbesondere wird auf die grundsätzliche Pflicht des Arbeitgebers, gem. § 1a Abs. 1a BetrAVG einen Zuschuss zum Entgeltumwandlungsbetrag des Arbeitnehmers zu zahlen, hingewiesen. Die Zuschusspflicht ist durch das Betriebsrentenstärkungsgesetz vom 17.08.2017 (BGBl. I S. 3214) eingeführt worden. Darüber hinaus werden die neuesten steuer- und sozialversicherungsrechtlichen Freibeträge eingearbeitet.
6. Im Teil F 10.4 wird der dort aufgenommene Auszug aus dem gemeinsamen Rundschreiben der Spitzenverbände der Sozialversicherungsträger aktualisiert.

Kommunalberatung/Kommunale Dienstleistungen

E-Government leicht gemacht. Mit der E-Akte von regisafe.

- zentrale Ablage
- direkter Zugriff
- optimierte Zusammenarbeit
- revisionssichere Archivierung
- Anbindung an Fachverfahren
- Einsparung von Zeit, Ressourcen und Kosten

regisafe ist eines der führenden Dokumentenmanagementsysteme im öffentlichen Umfeld, das neben der sicheren Verwaltung von Dokumenten eine Vielzahl an Funktionen bietet, die den Weg zur digitalen Verwaltung ebnen. regisafe wird bereits von vielen Kunden erfolgreich verwaltungsweit als zentrales System eingesetzt. Unser Ziel ist, dass alle unsere Kunden diesen Weg mit hoher Qualität und Zufriedenheit gehen können. Darum entwickeln wir unsere Lösungen und unser Serviceangebot ständig weiter.

Kontaktieren Sie uns - wir begleiten Sie gerne ins digitale Zeitalter.

comundus regisafe GmbH
Heerstraße 111 · 71332 Waiblingen · Fon 07151 96528-200
info@regisafe.de · **www.regisafe.de**

regisafe

Ein Unternehmen der comundus Gruppe

Die Kommunalversicherung
für Sachsen

Ihre Vorteile

- Hohe Spezialisierung und reichhaltige Erfahrung in vielfältigen kommunalen Versicherungsfragen
- Komplexe und individuell abgestimmte Versicherungskonzepte
- Einfluss auf die Unternehmenspolitik und -entwicklung in jährlichen Mitgliederversammlungen und Fachgremien

Unser Service

- Risikomanagement zum langfristigen Erhalt und zur Sicherung kommunalen Gemeindevermögens
- Maßgeschneiderte Umsetzung Ihrer Versicherungsbedürfnisse bei herausragendem Beitrags-Leistungs-Verhältnis
- Entlastung von Verwaltungsarbeit: Auf Wunsch schlüsseln wir Ihre Beiträge nach Kosten- oder Haushaltsstellen auf
- Optimale Beratung vor Ort in vielen Versicherungsfragen durch erfahrene Spezialisten
- Fachvorträge auf der Ebene der Gemeinden und Landkreise in diversen Versicherungssparten
- Kostenloser Versand von Fachinformationen und -zeitschriften gemeinsam mit dem KSA
- Online-Mitglieder-Service zur schnellen und unbürokratischen Anmeldung von Schäden

Unsere Produkte

- Sachversicherung (Gebäude, Inventar, Elektronik, Maschinen, Bauleistung, Elementar, Kunst, Musik, böswillige Beschädigung)
- Vermögenseigenschadenversicherung
- Haftpflichtversicherung
- Vermögensschadenhaftpflichtversicherung
- Gruppenunfallversicherung über Partner
- Rechtsschutz über Partner
- Cyberrisk-Versicherung über Partner

Immer für Sie da:
Ansprechpartner in Sachsen

Maik Franz
Tel. 030 914263-537
Mobil: 0170 2214508
maik.franz@okv.de

(Landkreise Görlitz, Leipzig, Meißen, Nordsachsen, Sächsische Schweiz-Osterzgebirge, Städte Dresden, Leipzig)

Wilfried Gärtner
Tel. 030 914263-532
Mobil: 0170 2214506
wilfried.gaertner@okv.de

(Landkreis Bautzen)

Alexander Zippel
Tel. 030 914263-536
Mobil: 0170 2214509
alexander.zippel@okv.de

(Landkreise Erzgebirgskreis, Mittelsachsen, Vogtlandkreis, Zwickau, Stadt Chemnitz)

OKV

Ostdeutsche
Kommunalversicherung a. G.
Plauener Straße 163-165
Haus C
13053 Berlin

www.okv.de

Unsere Partner: KSA – Kommunaler Schadenausgleich der Länder Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt und Thüringen, **WGV** – Versicherung AG, **BGV** – Versicherung AG, Hiscox – NI für Deutschland