05/2018

DIE GEMEINDE

Zeitschrift für die kommunale Selbstverwaltung in Schleswig-Holstein

Schwerpunktthemen: IT, Datenschutz und Informationssicherheit

- *Lukas Gundermann,* Die neue EU-Datenschutz-Grundverordnung – was ändert sich bei der Datenverarbeitung durch Kommunen? Teil 1: Einordnung der DSGVO, Rechtsgrundlagen der Datenverarbeitung
- *Dr. Werner Degenhardt, Andreas Amann, Jan Koppelmann, Frank Weidemann,* SiKoSH besiegt den großen Weißen Hai
- *Nikolaus Stapels,* Angriff auf eine Kommune – Vorgehensweise von Cyber-Kriminellen
- *Oliver Maas,* Integriertes Antrags- und Fallmanagement – kostenlose Online-Lösungen für die Kommunen in Schleswig-Holstein

70. JAHRGANG ISSN 0340-3653 C 3168 E

SHGT Schleswig-Holsteinischer GEMEINDETAG

Deutscher Gemeindeverlag GmbH Kiel

DIE GEMEINDE

Zeitschrift für die kommunale Selbstverwaltung in Schleswig-Holstein

Herausgeber Schleswig-Holsteinischer Gemeindetag

70. Jahrgang · Mai 2018

Impressum

Schriftleitung:
Jörg Bülow
Geschäftsführendes Vorstandsmitglied

Redaktion:
Daniel Kiewitz

Anschrift Schriftleitung und Redaktion:
Reventlouallee 6, 24105 Kiel
Telefon (0431) 57 00 50 50
Telefax (0431) 57 00 50 54
E-Mail: info@shgt.de
Internet: www.shgt.de

Verlag:
Deutscher Gemeindeverlag GmbH
Jägersberg 17, 24103 Kiel
Postfach 1865, 24017 Kiel
Telefon (0431) 55 48 57
Telefax (0431) 55 49 44

Anzeigen:
W. Kohlhammer GmbH
Anzeigenmarketing
70549 Stuttgart
Telefon (0711) 78 63 - 72 23
Telefax (0711) 78 63 - 83 93
Preisliste Nr. 37, gültig ab 1. Januar 2017.

Bezugsbedingungen:
Die Zeitschrift „Die Gemeinde" erscheint monatlich; einmal jährlich können zwei Hefte zu einem Doppelheft zusammengefasst werden. Bezugspreis ab Verlag jährlich 90,00 € zzgl. Versandkosten. Einzelheft 11,20 € (Doppelheft 22,40 €) zzgl. Versandkosten. Abbestellungen: 6 Wochen vor Jahresende beim Verlag.
Die angegebenen Preise enthalten die gesetzl. Mehrwertsteuer.

Druck: dfn! Druckerei Fotosatz Nord, Kiel
Satz & Gestaltung:
Agentur für Druck und Werbung, Laboe

Für unverlangt eingesandte Manuskripte und Bildmaterial übernehmen Verlag und Redaktion keine Verantwortung.
Die Redaktion behält sich Kürzungen und Überarbeitungen vor. Rücksendung erfolgt nur, wenn Rückporto beiliegt.

ISSN 0340-3653

Titelbild: Sommer im Naturpark Hüttener Berge
Foto: Hans-Claus Schnack, Klein Wittensee

Inhaltsverzeichnis

Schwerpunktthemen: IT, Datenschutz und Informationssicherheit

Dieser Ausgabe liegt eine Beilage des Deutschen Gemeindeverlages bei.

Wir bitten um Beachtung.

Die neue EU-Datenschutz-Grundverordnung – was ändert sich bei der Datenverarbeitung durch Kommunen?

Teil 1: Einordnung der DSGVO, Rechtsgrundlagen der Datenverarbeitung

Lukas Gundermann, LL.M. (Edinburgh), Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) ist derzeit in aller Munde. Sie hat, neben einschlägigen Skandalen um soziale Netzwerke, dazu geführt, dass das Thema Datenschutz in den Fokus gerückt ist. In der Tat entdecken manche Stellen bei dieser Gelegenheit Rechtspflichten, die bereits nach altem Recht und damit schon seit vielen Jahren galten. Ein großer Teil der Aufmerksamkeit wird von mehr oder weniger seriösen, häufig selbst ernannten Experten erzeugt, die durch die Lande ziehen und jenen öffentlichen und privaten Stellen den baldigen Untergang voraussagen, die sich nicht für deftige Honorare beraten lassen. Befeuert wird das Ganze durch die hohen Bußgelder, die nach der DSGVO von den Datenschutz-Aufsichtsbehörden künftig verhängt werden können: bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes. Das Bundesdatenschutzgesetz hatte bisher als maximales Bußgeld 300.000 Euro vorgesehen. Aus dem Umstand, dass der neue Höchstbetrag das sechsundsechzigfache des alten beträgt, wurde schon abgeleitet, dass die Aufsichtsbehörden jetzt alle Bußgelder mal 66 nehmen müssten; wo früher 1.000 Euro verhängt wurden, sollten nun 66.000 Euro verhängt werden.

Abseits von solchen abwegigen Vorstellungen soll in diesem Beitrag herausgearbeitet werden, welche Änderungen durch die DSGVO tatsächlich auf öffentliche Stellen und namentlich auf Kommunen zukommen. Dabei wird die DSGVO zunächst in ihren rechtlichen Kontext eingeordnet. Nach einem kurzen Blick auf den Anwendungsbereich und ein paar Begriffe wenden wir uns schließlich den Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten zu, die für öffentliche Stellen künftig gelten und werfen am Ende dieses ersten Teils noch einen Blick auf die Vorschriften zur Zweckänderung bei der Datenverarbeitung. Im zweiten Teil wird es um die Rechte der Betroffenen, die organisatorischen Pflichten der Verantwortlichen sowie um die aufsichtsbehördlichen Maßnahmen und den Rechtsschutz dagegen gehen.

1. Geschichte

Bereits seit 1995 gibt es eine europäische Regelung zum Datenschutz: die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Diese Richtlinie stammt aus einer Zeit vor dem Internet, Smartphones, Facebook und Tinder. Es wurde schnell offenbar, dass eine neue Regelung des Datenschutzes im Internetzeitalter geboten war. Zudem hatte es in der Zwischenzeit auch rechtliche Entwicklungen auf Ebene des EU-Rechts gegeben. Bekanntlich hatte das Bundesverfassungsgericht im Jahr 1983 ein neues Grundrecht entdeckt: das informationelle Selbstbestimmungsrecht. Allerdings ist dieses für den Laien im Grundgesetz kaum auffindbar, der Begriff Datenschutz findet sich dort nicht ausdrücklich. Anders im sog. Primärrecht der EU (den die EU konstituierenden Rechtsnormen): Mit dem Vertrag von Lissabon wurde die Europäische Grundrechtecharta Teil des EU-Rechts. In Art. 8 findet sich nicht nur das Recht auf Datenschutz für alle Bürger der EU, sondern auch einige der wichtigsten Grundsätze des Datenschutzes: Zweckbindung, Verarbeitung nur auf Rechtsgrundlage, Auskunft und andere Rechte der Betroffenen, unabhängige Aufsichtsbehörde. Daneben findet sich in Art. 16 des Vertrags über die Arbeitsweise der EU nicht nur eine Wiederholung des Grundrechts auf Datenschutz, sondern auch die Kompetenz zur Gesetzgebung der EU in diesem Bereich. Diese Kompetenz hat die EU mit der DSGVO wahrgenommen.

Die Arbeiten an der DSGVO begannen schon vor 2010 und zogen sich über einen selbst für die EU-Gesetzgebung erstaunlich langen Zeitraum hin. Dies hatte nicht zuletzt damit zu tun, dass interessierte Lobbygruppen intensiv daran arbeiteten, effektivere datenschutzrechtliche Vorschriften zu verwässern. Es ist nicht zuletzt dem langen Atem des Grüne-Abgeordneten im EU-Parlament Jan-Philip Albrecht (dem künftigen Umweltminister in Schleswig-Holstein) zu verdanken, dass das Gesetzeswerk schließlich erfolgreich verabschiedet wurde.

Die DSGVO wurde am 4.5.2016 im Amtsblatt der EU verkündet. Art. 99 der DSGVO besagt, dass sie am 20. Tag nach der Verkündung in Kraft tritt und ab dem 25.5.2018 gilt. Es soll hier nicht untersucht werden, wie eine Rechtsvorschrift gleichzeitig in Kraft sein und (noch) nicht gelten kann (diese Konstellation erinnert den Autor an Schrödingers Katze, die gleichzeitig lebendig und tot ist). Hinzuweisen ist aber darauf, dass die neuen rechtlichen Vorgaben seit gut zwei Jahren bekannt sind. Daher wird es bei der Umsetzung auch keine weitere Karenzzeit geben (wiewohl dies schon von manchen Stellen gefordert wurde).

2. Einordnung der DSGVO in den Kontext alter und neuer Datenschutzvorschriften

In der deutschen Diskussion wird die DSGVO meist mit den geltenden Vorschriften zum Datenschutz im Bundesdatenschutzgesetz (BDSG) und in den Landesdatenschutzgesetzen (LDSG) verglichen. Dieser Vergleich hinkt allerdings. Richtiger wäre es, die DSGVO mit ihrer europäischen Vorgängervorschrift zu vergleichen, der Richtlinie 95/46/EG. Ein solcher Vergleich zeigt, dass viele Regelungen der DSGVO bereits Entsprechungen in der 95er-Richtlinie haben und lediglich weiterentwickelt wurden. Dies gilt z.B. für die meisten Grundsätze in Art. 5 Abs. 1 DSGVO (wie z.B. die Verarbeitung nach Treu und Glauben und auf rechtmäßige Weise), die sich schon in Art. 6 der 95er-Richtlinie finden. Der entscheidende Unterschied ist die Wahl des Regelungsinstruments durch die EU. Die Richtlinie 95/46/EG war wie jede EU-Richtlinie an die Mitgliedstaaten adressiert und machte diesen Vorgaben dazu, welche Vorschriften zum Datenschutz zu erlassen sind. Die Mitgliedstaaten setzten die

Richtlinie oft verzögert um und nahmen sich dabei einige Freiheiten. Die DSGVO ist eine EU-Verordnung und gilt somit unmittelbar. Der deutsche Gesetzgeber verzichtete bei der Umsetzung der 95er-Richtlinie aus guten Gründen darauf, den Grundsatz der Verarbeitung nach Treu und Glauben in deutsches Recht zu übernehmen. Gerade für öffentliche Stellen in Deutschland ergibt sich die Bindung an Recht und Gesetz schon aus Art. 20 Abs. 3 GG. Für den zivilrechtlichen Begriff „Treu und Glauben" ist daneben im öffentlichen Recht kein Raum. Unter der DSGVO gilt dieses Prinzip jetzt jedoch unmittelbar nach Art. 5 Abs. 1 DSGVO. Auf der Ebene des EU-Rechts hat sich damit im Vergleich zur 95er-Richtlinie nicht viel geändert. Auf Ebene des deutschen öffentlichen Rechts ist allerdings nicht klar, wie die jetzt unmittelbar geltende Verpflichtung auf Treu und Glauben in die Rechtsanwendung zu integrieren ist. Das Beispiel soll zeigen, dass manche Fragen und Probleme bei der Rechtsanwendung aus der spezifischen Konstellation herrühren, dass ein Rechtsbereich, der bisher durch EU-Recht überformt, aber durch nationales Recht geregelt war, nun durch unmittelbar anzuwendendes EU-Recht geregelt wird.

Namentlich für den öffentlichen Bereich wird die Lage allerdings dadurch entschärft, dass die DSGVO eine Reihe von Öffnungsklauseln enthält. Diese erlauben es dem nationalen Gesetzgeber, eigene Regelungen zu treffen, z.T. schreiben sie solche Regelungen auf Ebene der Mitgliedstaaten vor. An diesen Stellen wirkt die DSGVO eher wie eine Richtlinie, die einen gewissen Spielraum für die Mitgliedstaaten lässt. Allerdings führen diese Öffnungsklauseln dazu, dass es nicht ausreicht, in die DSGVO zu schauen, um die Rechtslage zu beurteilen. Zusätzlich ist der Blick in das nationale Recht geboten, welches die Öffnungsklauseln ausfüllt. Dieses findet sich wie schon bisher in allgemeinen Datenschutzgesetzen (auf Bundesebene das BDSG, auf Landesebene die LDSG) sowie in bereichsspezifischen Vorschriften, d.h. Fachgesetzen, die (auch) Vorgaben zur Verarbeitung von personenbezogenen Daten enthalten.

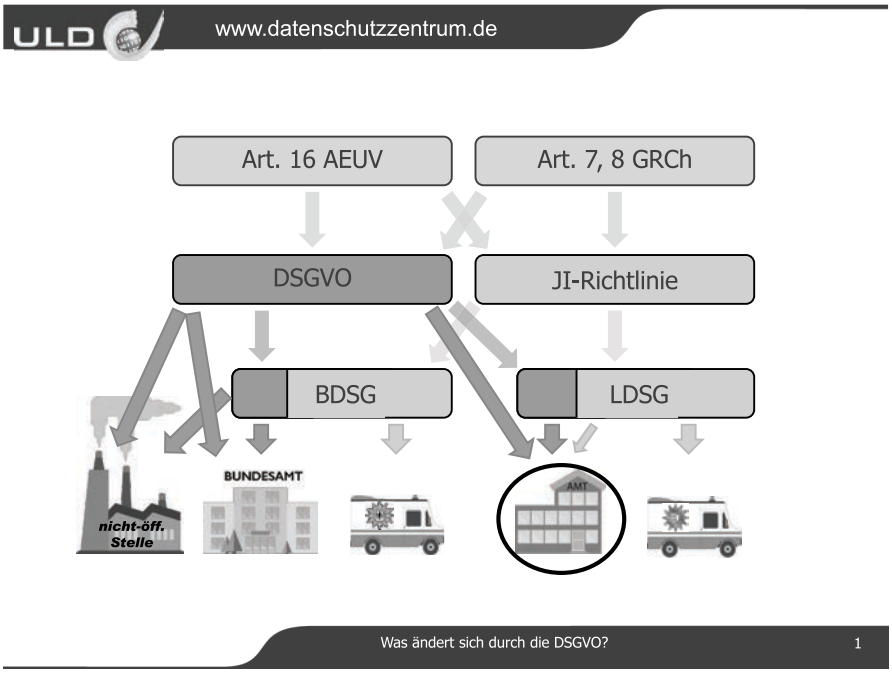
Der Blick des Rechtsanwenders muss also zwischen der DSGVO und dem nationalen Recht hin und her schweifen. Leider aber ist die Lage noch komplexer. Zeitgleich mit der DSGVO wurde im EU-Amtsblatt eine weitere Rechtsvorschrift veröffentlicht: die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie). Aus bestimmten Gründen hatte die EU sich entschlossen, die Datenschutzvorschriften für diesen Bereich in einem separaten Regelungsinstrument zusammenzufassen und dafür das Instrument einer Richtlinie zu wählen. Offensichtlich gelten diese Richtlinie bzw. die zu ihrer Umsetzung erlassenen nationalen Vorschriften für den Bereich der Strafverfolgung durch die Polizei und die Justiz sowie der Gefahrenabwehr durch die Polizei. Wegen der Nähe zur Strafverfolgung fällt allerdings auch die Verfolgung von Ordnungswidrigkeiten unter die Richtlinie. Dies ist von Bedeutung für alle Bußgeldverfahren, die von den Kommunen betrieben werden. Namentlich im Bereich der Verfolgung von Verkehrsordnungswidrigkeiten, wo es in den Fachgesetzen an konkreten Vorgaben zur Verarbeitung personenbezogener Daten fehlt, werden die Vorschriften zur Umsetzung der JI-Richtlinie zur Anwendung kommen. Bei der Gefahrenabwehr, die durch die kommunalen Ordnungsbehörden betrieben wird, bleibt es bei der Anwendung der DSGVO und der ergänzenden mitgliedstaatlichen Regelungen.

Zur Wahrnehmung der Öffnungsklauseln der DSGVO und zur Umsetzung der JI-Richtlinie hatte der Bundesgesetzgeber schon frühzeitig mit den Vorarbeiten begonnen, so dass ein neues BDSG bereits im Juni 2017 verabschiedet werden konnte – noch vor der Bundestagswahl 2017. Auf Landesebene begannen die Vorarbeiten später, so dass ein Gesetzentwurf für ein neues LDSG erst im Januar 2018 in den Landtag eingebracht wurde. Wie auf Bundesebene finden sich hier die Ausfüllung der Öffnungsklauseln der DSGVO und die Umsetzung der JI-Richtlinie zusammengefasst in einem Gesetz (in einigen anderen Bundesländern soll dies in zwei unterschiedliche Gesetze aufgespalten werden). Aufgrund mangelnder Abstimmung bei der Erstellung des Gesetzentwurfs waren noch einige Änderungen im parlamentarischen Prozess nötig, um einen halbwegs konsistenten Entwurf zu erzeugen. Dieser wurde am 27. April 2018 vom Schleswig-Holsteinischen Landtag verabschiedet, so dass das neue LDSG rechtzeitig zum 25. Mai 2018 in Kraft treten kann. Zum Zeitpunkt der Abfassung dieses Beitrags war das neue LDSG noch nicht verkündet worden, so dass hier für den vollständigen Text nur auf die letzte Landtagsdrucksache dazu (19/664) verwiesen werden kann.

Die Grafik versucht, die relevanten Rechtsgrundlagen darzustellen. Eine Kommune in Schleswig-Holstein (eingekreist) muss bei der Rechtsanwendung die DSGVO selbst sowie den 2. Teil des LDSG berücksichtigen, der die Öffnungsklauseln der DSSGVO umsetzt. Soweit Ordnungswidrigkeitsverfahren betrieben werden, ist auch der 3. Teil des LDSG zu berücksichtigen. Nicht berücksichtigt sind hier bereichsspezifische Vorschriften.

3. Anwendungsbereich, Begriffe

Die DSGVO unterscheidet nicht zwischen öffentlichen und nicht-öffentlichen Stellen, wie es das deutsche Datenschutzrecht traditionell tut. Allerdings ist der nationale Gesetzgeber auch nicht gehindert, eine solche Unterscheidung einzuführen, solange diese nicht mit den verbindlichen Vorgaben der DSGVO kollidiert. Das LDSG-neu regelt grundsätzlich im Bereich der Öffnungsklausen der DSGVO für die öffentlichen Stellen des Landes. Wie schon bisher sind dies die „Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger



der öffentlichen Verwaltung“ (§ 2 Abs. 1 LDSG-neu). Allerdings gibt es eine wichtige Ausnahme: Nach § 1 Abs. 4 LDSG-neu soll das Gesetz keine Anwendung finden, „soweit öffentliche Stellen nach Absatz 1 am Wettbewerb teilnehmen und personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten.“ Dann soll für den Bereich der Wettbewerbsteilnahme das BDSG gelten. Als Beispiel nennt die Gesetzesbegründung das UKSH (und andere von öffentlich-rechtlichen Trägern geführte Krankenhäuser), soweit die Patientenversorgung betroffen ist. Auch im kommunalen Bereich kann es solche Konstellationen geben, z.B. wenn eine Gemeinde einen Eigenbetrieb unterhält, der in einem der Bereiche aktiv ist, die dem Wettbewerb unterfallen (z.B. Strom- und Gasversorgung). Entsprechendes gilt für Verkauf von Holz aus kommunalen Wäldern. Hier unterfällt die Verarbeitung der Kundendaten dem BDSG, aber alle andere kommunalen Verarbeitungen und namentlich die der Beschäftigtendaten dem LDSG.

In Art. 4 finden sich ausführliche Definitionen der zentralen Begriffe. Manche davon sind neu, andere weichen von der bisherigen Definition ab.

„Personenbezogene Daten“ liegen nicht nur dann vor, wenn ein Klarname genannt wird. Es genügt, dass der Betroffene individualisiert werden, d.h. ein Eins-zu-Eins-Bezug zwischen den Daten und einer Person hergestellt werden kann. Damit sind auch z.B. Autonummern oder IP-Adressen personenbezogen.

„Verarbeitung“ ist nach wie vor jede Aktivität, die an oder mit personenbezogenen Daten ausgeführt wird. In der Definition werden eine Vielzahl von Beispielen genannt, unter anderem „Offenlegung durch Übermittlung“ wo bisher nur von Übermittlung die Rede war. Eine Rechtsänderung durch den etwas verunglückten Begriff ergibt sich nicht.

Die „datenverarbeitende Stelle“ des LDSG-alt wird nun zum „Verantwortlichen“. Verantwortlicher ist, „wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Dabei ist es nicht erforderlich, dass der Verantwortliche selbst die Daten verarbeitet. So kann auch eine Stelle, die lediglich die Infrastruktur vorgibt, zum Verantwortlichen werden. Meist wird es sich dann bei dieser Stelle und den Stellen, die die praktisch mit den Daten umgehen, um gemeinsam für die Verarbeitung Verantwortliche im Sinne von Art. 26 DSGVO handeln. Der Verantwortliche ist Adressat der meisten zentralen Pflichten in der DSGVO. Die bisher als Auftragsdatenverarbeiter bezeichnete Rolle heißt nunmehr vereinfacht „Auftragsverarbeiter“.

Neuerdings definiert werden „genetische Daten”, „biometrische Daten“ und „Gesundheitsdaten”, alle gehören zu den sensiblen Daten nach Art. 9 Abs. 1 DSGVO (siehe unten).

4. Rechtsgrundlagen für die Datenverarbeitung

4.1 Allgemeines

Wie schon bisher gilt für die Verarbeitung ein Verbot mit Erlaubnisvorbehalt: Die Verarbeitung ist nicht zulässig, es sei denn, eine Rechtsgrundlage erlaubt sie ausdrücklich. Dabei macht die DSGVO zunächst keine Unterscheidung zwischen der Datenverarbeitung durch öffentliche bzw. durch private („nicht-öffentliche“) Stellen. Diese im deutschen Datenschutzrecht hergebrachte Differenzierung ist dem europäischen Datenschutzrecht fremd. Allerdings finden sich dann in einzelnen Vorschriften der DSGVO doch Öffnungsklauseln und Vorgaben, die es dem deutschen Gesetzgeber erlauben, bei der hierzulande hergebrachten unterschiedlichen Regelung für den privaten und den öffentlichen Bereich zu bleiben.

Von dem grundsätzlichen Verbot der Verarbeitung personenbezogener Daten ausgenommen ist die Verarbeitung „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ (Art. 2 Abs. 2 Buchstabe c). Die Reichweite dieser sog. Haushaltsausnahme ist nicht immer ganz klar. Jedenfalls dann, wenn eine Privatperson Daten anderer Personen im Internet veröffentlicht, wird der Anwendungsbereich der Haushaltsausnahme verlassen (EuGH, 06.11.2003 - C-101/01).

In der DSGVO finden sich die Rechtsgrundlagen für die Datenverarbeitung in Kapitel II („Grundsätze“). Die erste Vorschrift hier ist der schon erwähnte Art. 5, der die Grundsätze für die Verarbeitung personenbezogener Daten enthält. Diese sind selbstverständlich einzuhalten und müssen vor allem bei der Gestaltung von neuen Verarbeitungsprozessen beachtet werden. Allerdings stellen die Grundsätze des Art. 5 selbst keine Rechtsgrundlagen dar, auf welche die Verarbeitung gestützt werden kann. Die eigentlichen Erlaubnisnormen, die festlegen, wann personenbezogene Daten verarbeitet werden dürfen, finden sich in Art. 6 Abs. 1 DSGVO.

Wie schon im bisherigen Recht findet sich hier zunächst die Einwilligung (Art. 6 Abs. 1 Buchstabe a). Die Anforderungen an eine wirksame Einwilligung sind in Art. 7 ausgeführt. Schriftform ist nicht erforderlich, allerdings muss der Verantwortliche die Einwilligung nachweisen können. Im öffentlichen Bereich dürfte die Einwilligung eher selten und nur bei Zusatzangeboten zum Einsatz kommen, die außerhalb dessen liegen, was zu den gesetzlichen Aufgaben der öffentlichen Stelle gehört. Zum einen bestehen wegen des im öffentlich-rechtlichen Bereichs im Grundsatz gegebenen Über-Unterordnungsverhältnisses erhebliche Zweifel an der Freiwilligkeit der Einwilligung (Art. 7 Abs. 4). Zum anderen ist es aus verfassungsrechtlichen Gründen für öffentliche Stellen nicht zulässig, auf der Grundlage einer vermeintlichen Einwilligung den ihnen gesetzlich erlaubten Satz von personenbezogenen Daten zu erweitern. So dürfte eine Gemeinde nicht auf Grundlage einer Einwilligung im Melderegister weitere, im BMG nicht genannte Daten speichern.

Art. 6 Abs. 1 enthält weitere Rechtsgrundlagen, die für öffentliche Stellen nicht relevant sind, wie die Verarbeitung zur Erfüllung eines Vertrags (Buchstabe b) oder zur Wahrung berechtigter Interessen des Verantwortlichen (Interessenabwägung, Buchstabe f).

Die für öffentliche Stellen relevante Rechtsgrundlage findet sich in Buchstabe e). Danach ist die Verarbeitung zulässig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Anders als bei den meisten anderen Varianten in Art. 6 Abs. 1 wirkt Buchstabe e) jedoch nicht selbst als Rechtsgrundlage. Vielmehr bildet die Norm den Rahmen für die Öffnungsklauseln in Art. 6 Abs. 2 und 3. Das Verhältnis von Abs. 2 zu Abs. 3 bleibt schleierhaft, scheinen beide doch das gleiche zu regeln und daher verzichtbar (vgl. Reimer, in: Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 6 Rn. 29-30, beck-online). Hier soll auf den leichter lesbaren Abs. 2 abgestellt werden. Dieser lautet:

„Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.“

Diese Öffnungsklausel erlaubt es dem deutschen Gesetzgeber, genauer zu bestimmen, wann die Voraussetzungen von Art. 6 Abs. 1 Buchstabe f) vorliegen, wann also die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem Verantwortlichen übertragen wurde.

Die DSGVO geht hier erkennbar davon aus, dass durch bereichsspezifisches Recht („spezifische Anforderungen“, „präziser bestimmen“) für bestimmte, konkrete Verarbeitungsvorgänge im öffentlichen Bereich Regelungen erlassen werden. Nun ist dies in Deutschland schon vor vielen

Jahren erfolgt, weil deutsches Verfassungsrecht bereichsspezifische Rechtsgrundlagen für die Datenverarbeitung erforderte. Hier erlaubt die DSGVO, dass bestehende Regelungen „beibehalten" werden können. Das ist eine sehr gute Nachricht für die Datenschutzregelungen im öffentlichen Bereich. Zwar trifft den Gesetzgeber auf Bundes- und Länderebene die Pflicht zu prüfen, ob die bereichsspezifischen Gesetze den Anforderungen genügen. Man kann aber getrost davon ausgehen, dass dies in den allermeisten Fällen zu bejahen ist und die zahlreichen bereichsspezifischen Regelungen nicht geändert werden müssen. (Änderungsbedarf ergibt sich z.T. allerdings mit Blick auf die Verarbeitung von „sensiblen Daten", dazu sogleich.)

Allerdings ist der deutsche Gesetzgeber hier noch einen Schritt weitergegangen (und zwar zunächst auf Bundesebene, d.h. beim BDSG, da dieses als erstes Gesetz zur Ausfüllung der Öffnungsklauseln erlassen wurde). Hier wurde, gestützt auf die Öffnungsklausel in Art. 6 Abs. 2 und 3, mit § 3 BDSG auch eine allgemeine Rechtsgrundlage zur Datenverarbeitung durch öffentliche Stellen aufgenommen, die vom Wortlaut praktisch mit Art. 6 Abs. 1 Buchstabe e) identisch ist. Der Gesetzgeber des LDSG Schleswig-Holstein ist diesem Vorbild mit § 3 Abs. 1 LDSG-neu gefolgt. Damit steht eine in der Praxis sehr wichtige Rechtsgrundlage für solche Fälle zur Verfügung, bei denen keine der bereichsspezifischen Regelungen angewendet werden kann. Dem Vernehmen nach sieht man diese Auslegung der Öffnungsklausel bei der EU-Kommission eher kritisch, allerdings hat es wohl noch keine offizielle Kommunikation dazu gegeben.

4.2 Erlaubnis zur Verarbeitung sensibler Daten

Neben der allgemeinen Zulässigkeitsvorschrift in Art. 6 Abs. 1 enthält die DSGVO noch spezielle Vorschriften dazu, wann die Verarbeitung von „besonderen Kategorien personenbezogener Daten" erlaubt ist. Dies umfasst die folgenden Datenkategorien:

Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Eine ähnliche Kategorisierung gab es schon in der 95er-Richtlinie und infolge dessen auch im deutschen Recht. Herkömmlich werden diese Daten oft als „sensible Daten" bezeichnet. Für diese Daten gilt ein besonderes Verbot mit Erlaubnisvorbehalt, wobei die Schwelle für die Zulässigkeit der Verarbeitung hier generell höher sein soll. In welchem Verhältnis stehen nun die Zulässigkeitsnormen nach Art. 9 und Art. 6? Die deutschen Aufsichtsbehörden sind der Auffassung, dass die Vorschriften wie ein doppelter Filter wirken: für sensible Daten müssen zunächst die speziellen Voraussetzungen nach Art. 9 Abs. 2 vorliegen. Ist dies der Fall, so muss auch eine Erlaubnisnorm nach Art. 6 Abs. 1 die Verarbeitung allgemein erlauben. In der Praxis ist dies meist kein Problem, da die strengeren Vorgaben des Art. 9 Abs. 2 meist die weniger strikten des Art. 6 Abs. 1 mitumfassen.

Für die Verarbeitung von sensiblen Daten durch öffentliche Stellen ist vor allem die Erlaubnis nach Art. 9 Abs. 2 Buchstabe g) von Belang. Danach ist die Verarbeitung dann zulässig, wenn sie „auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich" ist. Hier sind drei Elemente von Interesse: Zuerst stellt die Norm durch den Verweis auf das Recht des Mitgliedstaates eine Öffnungsklausel zur Verfügung, der Bereich kann also durch nationales Recht geregelt werden. Weiterhin reicht hier im Gegensatz zu Art. 6 Abs. 2 Buchstabe e nicht ein einfaches öffentliches Interesse, sondern es ist ein „erhebliches" öffentliches Interesse notwendig. Und schließlich muss das nationale Recht „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" vorsehen.

Weitere Öffnungsklauseln mit Relevanz für den öffentlichen Bereich finden sich in Art. 6 Abs. 2 Buchstabe i) für Zwecke des öffentlichen Gesundheitswesens und in Art. 6 Abs. 2 Buchstabe j) für Archivzwecke, wissenschaftliche oder historische Forschungszwecke und statistische Zwecke. Neben der Verhältnismäßigkeit der Rechtsgrundlage wird auch hier jeweils das Vorhandensein von „Maßnahmen" gefordert.

Der Gesetzgeber des BDSG hat versucht, die geforderten angemessenen und spezifischen Maßnahmen zu konkretisieren, siehe § 22 Abs. 2 BDSG-neu. Genannt werden dort neben technisch-organisatorische Maßnahmen allgemein und konkreten Techniken wie Pseudonymisierung und Verschlüsselung auch z.B. die „Sensibilisierung" der Mitarbeiter, gemeint sind wohl Schulungen. Der Landesgesetzgeber ist diesem Vorbild mit § 12 Abs. 2 und 3 LDSG-neu gefolgt. Viel wird mit diesem Ansatz jedoch nicht bewirkt, denn die Pflicht, angemessene technisch-organisatorische Maßnahmen zu treffen, ergibt sich schon aus Art. 32 DSGVO, und zwar für alle Kategorien von Daten, nicht nur für sensible.

Wie zu Art. 6 Abs. 1 Buchstabe e) erläutert, kann jedenfalls auch im Hinblick auf die Verarbeitung von sensiblen Daten bereichsspezifisches Recht geschaffen oder beibehalten werden, wenn es die Voraussetzungen erfüllt. Ein Beispiel könnte § 3 Abs. 1 Nr. 11 BMG sein, der die Speicherung der Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft und damit die Verarbeitung von Daten über religiöse Überzeugungen vorschreibt. Hier wäre nun zu prüfen, ob die Verarbeitung einem „erheblichen öffentlichen Interesse" dient und ob die angemessenen und spezifischen Maßnahmen vorgesehen sind. Soweit ersichtlich, hat der Gesetzgeber des BMG dies allerdings noch nicht getan. Änderungen des BMG im Zusammenhang mit dem Inkrafttreten der DSGVO gab es nicht. Allerdings ist der Prozess von Folgeänderungen auf Bundesebene noch lange nicht abgeschlossen. Zwar gab es schon ein sog. Omnibusgesetz, mit dem eine Reihe von Anpassungen im Fachrecht erfolgte, namentlich in der AO und im SGB (Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17.07.2017, BGBl. 2541). Dem Vernehmen nach sind jedoch noch weitere Omnibusgesetze auf Bundesebene in Vorbereitung, mit denen entsprechende Änderungen im Fachrecht bewirkt werden sollen.

Auf Landesebene finden sich Änderungen im Fachrecht, mit denen eine DSGVO-konforme Rechtsgrundlage zur Verarbeitung von sensiblen Daten geschaffen werden soll, vor allem für Zwecke des öffentlichen Gesundheitswesens. So wurde durch das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 27.04.2018 ein neuer Absatz 6 an § 16 GDG angefügt, der den Trägern des öffentlichen Gesundheitsdienstes die Verarbeitung von sensiblen Daten erlaubt, „soweit dies im Einzelfall zur Erfüllung von Aufgaben nach diesem Gesetz erforderlich ist". Offenbar geht der Gesetzgeber hier davon aus, dass für alle Aufgaben nach dem GDG ein erhebliches öffentliches Interesse besteht. Weiterhin wird über einen Verweis auf § 12 LDSG-neu auch die Geltung der dort beschriebenen angemessenen und spezifischen Maßnahmen angeordnet.

Wie bei der allgemeinen Zulässigkeitsklausel nach Art. 6 Abs. 1 Buchstabe e) haben sowohl der Bundes- als auch der Landesgesetzgeber eine Generalklausel zur Zulässigkeit der Verarbeitung von sensiblen Daten ins BDSG (§ 22 Abs. 1)

bzw. ins LDSG (§ 12 Abs. 1) eingefügt. Auf diese kann wiederum zurückgegriffen werden, sollte sich in den bereichsspezifischen Regelungen der Fachgesetze keine Rechtsgrundlage finden.

5. Zweckbindung, Zweckänderungen

In Art. 5 Abs. 1 Buchstabe b) findet sich der Grundsatz der Zweckbindung: „personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt (…) nicht als unvereinbar mit den ursprünglichen Zwecken".

Interessanterweise kommt es hier zu einer Lockerung des schon aus dem alten Recht bekannten Zweckbindungsgrundsatzes. War bisher von einer Zweckidentität auszugehen („dürfen nur für den Zweck weiterverarbeitet werden, für den sie rechtmäßig erhoben worden sind", § 13 Abs. 2 LDSG-alt), so wird jetzt nur noch Vereinbarkeit der Zwecke verlangt. In Art. 6 Abs. 4 stellte die DSGVO ein paar Kriterien bereit, um festzustellen, ob die Verarbeitung zu dem neuen Zweck mit dem alten vereinbar ist. Dazu gehören u.a.: Verbindung zwischen den Zwecken, Art der personenbezogenen Daten (bei sensiblen Daten eher keine Vereinbarkeit) und das Vorhandensein geeigneter Garantien zum Schutz der Rechte der Betroffenen wie Verschlüsselung oder Pseudonymisierung.

Diese neuen Regelungen machen die Verwendung von einmal erlangten Informationen für ähnliche Zwecke deutlich einfacher. So wird z.B. im Kontext von Vollstreckungen durch kommunale Vollstreckungsbeamte oft gefragt, ob die in einem Verfahren erlangte Kontoinformation des Schuldners auch für die Vollstreckung in einem anderen Verfahren verwendet werden kann. Nach hiesiger Auffassung wäre dies zu bejahen, wenn es bei beiden Verfahren um gemeindliche Abgaben geht. Eine Verbindung zwischen den Zwecken liegt in der Durchsetzung der kommunalen Abgabenforderungen, zugleich ist die Kontoinformation kein sensibles Datum nach Art. 9 Abs. 1 DSGVO.

Auch der Aspekt der geeigneten Garantien und hier namentlich der Pseudonymisierung kann hilfreich sein. So ist es unter der DSGVO eindeutig, dass auch Pseudonyme personenbezogene Daten sind und dass daher für ihre Verarbeitung eine Rechtsgrundlage erforderlich ist. Bisher half hier § 11 Abs. 6 LDSG-alt, der es erlaubte, pseudonymisierte Daten zu verarbeiten und auch zu übermitteln, wenn der Verantwortliche keinen Zugriff auf die Zuordnungsfunktion, also die Zuordnung der Pseudonyme zu den Klarnamen, hat. Zwar findet sich eine solche Vorschrift jetzt nicht mehr. Allerdings kommt man zu praktisch gleichen Ergebnissen, wenn man die Zweckänderung der Daten unter der Bedingung zulässt, dass diese sicher pseudonymisiert sind.

Darüber hinaus enthält Art. 6 Abs. 4 eine Öffnungsklausel, die es den Mitgliedstaaten erlaubt, für die in Art. 23 Abs. 1 genannten Zwecke weitere ausdrückliche Zweckdurchbrechungen zuzulassen. Diese ist im LDSG-neu in § 4 wahrgenommen worden. In Anlehnung an die entsprechende Norm des BDSG-neu ist die zweckändernde Verarbeitung der Daten z.B. dann erlaubt, wenn dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. Nach § 4 Abs. 2 LDSG-neu ist die Zweckänderung bei sensiblen Daten allerdings darauf beschränkt, dass die Verarbeitung für den neuen Zweck auf eine Vorschrift gestützt werden kann, die die Verarbeitung sensibler Daten erlaubt.

Neben der Erlaubnis der ausdrücklichen Zweckänderung findet sich in § 3 Abs. 2 noch die Fiktion einer Zweckerstreckung: „Zu dem Zweck der Verarbeitung personenbezogener Daten gehört auch die Verarbeitung zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung, zur Durchführung von Organisationsuntersuchungen und zur Prüfung und Wartung von automatisierten Verfahren. Dies gilt auch für die Verarbeitung personenbezogener Daten zu Aus- und Fortbildungszwecken, soweit nicht schutzwürdige Interessen der betroffenen Person entgegenstehen." Damit wird eine ähnliche Regelung des § 13 Abs. 5 LDSG-alt fortgeführt. Als Öffnungsklausel beruft sich der Gesetzgeber auf die allgemeine Öffnungsklausel für den öffentlichen Bereich in Art. 6 Abs. 2 und 3.

Der Beitrag wird in der nächsten Ausgabe fortgesetzt.

SiKoSH besiegt den großen Weißen Hai

Dr. Werner Degenhardt, Andreas Amann, Jan Koppelmann, Frank Weidemann

Über die Informationstechnologie der deutschen Behörden wird seit dem Bundestags-Hack im Herbst 2015 viel in den Medien berichtet. Leider nicht ausnahmslos Positives.

Schlagzeilen wie „Trojaner legt Computer der [Gemeinde, Stadt, Landkreis] Verwaltung lahm" sind in unschöner Regelmäßigkeit zu sehen und machen darauf aufmerksam, dass die digitale Verwaltung nicht so sicher ist, wie wir uns das wünschen.

Beim Cyberangriff auf den Bundestag (Bundestag-Hack) haben sich die Hacker Medienberichten zufolge mit einer E-Mail-Adresse der Vereinten Nationen getarnt. Eine E-Mail mit dem Absender „un.org" hat offensichtlich einen Link zu einem angeblichen "UN News Bulletin" enthalten, der in Wirklichkeit zu einer mit Schadsoftware präparierten Seite führte. Ein sogenannter „drive-by-exploit", bei dem der Besuch einer Website durch dort enthaltenen Code (JavaScript, Java, Adobe Flash) Schadsoftware auf dem aufrufenden Rechner installiert.

Das Argument, dass dieser bedauerliche Vorfall an der fragmentierten, von vielen unterschiedlichen Personengruppen selbst verwalteten und schlecht kontrollierbaren Netzinfrastruktur gelegen hätte und geeignete technische Maßnahmen den Erfolg des Angriffs verhindert hätten, wurde kürzlich durch den Bundes-Hack widerlegt.

Hier gelang es den Angreifern offenbar über den Anhang einer Phishing-E-Mail, einen Trojaner auf dem Webserver der Bundesakademie für öffentliche Verwaltung (BAKöV) in Brühl zu hinterlegen. Die Bundesakademie für öffentliche Verwaltung ist an das Regierungsnetz Informationsverbund Berlin-Bonn (IVBB) angeschlossen. Der Trojaner wurde Anfang 2017 aktiv, erforschte das Netzwerk und schaffte es, so viele Informationen zu bekommen, dass die Angreifer Administrator-Rechte auf wenigstens 17 Arbeitsplatzrechnern im Auswärtigen Amt bekamen.

Bundestags-Hack und Bundes-Hack sind zwar schlimm, aber der Abfluss von Staatsgeheimnissen beeinträchtigt den Lebensalltag der Bürger nicht so unmittel-

bar wie ein „Rathaus-Hack“, der Standesamt, öffentliche Baumaßnahmen und die Feuerwehr lahmlegt oder Bewerbungen auf Ausschreibungen öffentlich macht.
Der „Rathaus-Hack“ – wie die ZEIT Online im November 2017 titelte – ist beim gegenwärtigen Stand der Abwehr-Technologie und beim gegenwärtigen Stand sicheren Verhaltens der Mitarbeiterinnen und Mitarbeiter auch für einen nur wenig begabten Hacker eine leichte Übung. „Egal ob Dorf oder Großstadt: Eine Mischung aus fehlender Risikowahrnehmung, schlecht programmierter Software und Fahrlässigkeit ist offensichtlich Alltag in vielen Rathäusern“ schreibt die ZEIT.
Wie passen der Aufbau des vom Bürger erwarteten eGovernment und der allgemeine Stand der Digitalisierung der kommunalen Verwaltung zusammen? Nicht sehr gut, wie die Ergebnisse der von der Unternehmensberatung Sopra Steria durchgeführten Studie „European Digital Government Barometer 2017“ zeigen: Für jeden zweiten Bundesbürger ist das Risiko von Datenphishing-Angriffen eine wesentliche Hürde, die ihn an der Nutzung von E-Government-Angeboten hindern würden.

Informationssicherheit ist eines der wichtigsten Handlungsfelder der nächsten Jahre.

„Das Informationssicherheitsmanagement ist zu einer zentralen Aufgabe geworden“, schreibt der Landesrechnungshof Schleswig-Holstein in seinen Bemerkungen 2017.
Informationssicherheitsmanagement ist erfolgreich, wenn

- Technologien (sichere Technik, kontrollierter Zugang zu Gebäuden, Geräten und Diensten)
- Prozesse (Richtlinien, Risikomanagement, Krisenmanagement) und
- Menschen (Sensibilisierung, Schulung, Sicherheitskultur)

aufeinander abgestimmt sind und sich schnell, flexibel, nachhaltig und dauerhaft an die immer neuen Bedrohungslagen anpassen können, wobei Menschen die bis heute am wenigsten beherrschte Komponente sind.

Schleswig-Holstein vorn

Der Landesrechnungshof schreibt in den Bemerkungen 2017 auch in dankenswerter Klarheit, dass es Informationssicherheit ohne Beteiligung der Mitarbeiterinnen und Mitarbeiter nicht geben kann und dass Sensibilisierungs- und Schulungsmaßnahmen eine Daueraufgabe sind.
Das Projekt SiKoSH (siehe Hinweise [SiKoSH] am Ende) hat ein innovatives Sensibilisierungs- und Schulungskonzept entwickelt und in Zusammenarbeit mit der Landeshauptstadt Kiel getestet.
Grundlage für die Schulungsplanung von SiKoSH ist der Baustein ORP.3 (Sensibilisierung und Schulung) des IT-Grundschutzkompendiums. Das Schulungskonzept folgt den Standards des National Institute of Standards and Technology (NIST)[1], die auch von ENISA[2] und BAköV[3] für die Strukturierung von Sensibilisierungsmaßnahmen übernommen worden sind.
Für Schulungen im Bereich Informationssicherheit NIST nennt drei unterschiedliche Lernsituationen und Lernkontexte

- Awareness
- Training
- Bildung

Awarenessmaßnahmen sind Maßnahmen zur Steigerung der Aufmerksamkeit für das Thema Informationssicherheit. Informationssicherheit soll den Benutzerinnen und Benutzern als wichtiges Thema bekannt sein und als bedeutsames Thema für den eigenen Arbeits- und Wirkungsbereich anerkannt werden. Beispiele sind Präsentationen zum Datenschutzrecht, Veranstaltungen wie „Die Hacker kommen“, Verteilen von Anleitungen, Rundschreiben des Bürgermeisters, Hinweise auf Berichterstattung in der Presse.
Training will relevante Fähigkeiten und Fertigkeiten vermitteln, richtiges Verhalten stärken, falsche Verhaltensweisen löschen. Training ist für die Trainer und die Trainierten aufwendiger als Awarenessmaßnahmen und hat starke Übungsanteile.
„Bildung“ bezieht sich auf die Ausbildung von Personen, die sich der Informationssicherheit als Profession verschrieben haben. Bildung bezeichnet Spezialisten mit großer Erfahrung und tiefem Verständnis, mit Weitblick und der Fähigkeit, schon Anzeichen von Schadsituationen zu erkennen und proaktiv zu reagieren.
SiKoSH geht davon aus, dass für erfolgreiches Lernen von sicheren Verhaltensweisen eine dauerhafte Grundaufmerksamkeit für Angelegenheiten der Informationssicherheit geschaffen und aufrechterhalten werden muss. Mit anderen Worten: Vor der Durchführung von Schulungsmaßnahmen sollten bereits Maßnahmen zur Sensibilisierung gegenüber der Informationssicherheit getroffen werden[4].
SiKoSH empfiehlt die Durchführung von Phishing-Simulationen, da diese in besonderer Weise geeignet sind, die Themen „Datenschutz“ und „Informationssicherheit“ im persönlichen Arbeitskontext der Mitarbeiterinnen und Mitarbeiter und die Organisationskultur einer Einrichtung zu verankern und sichere Verhaltenskomponenten zu trainieren.
Der SiKoSH-Ansatz geht davon aus, dass die Unterstützung der Amtsleitung, eine fehlertolerante Organisationskultur und emotional bereichernde partizipative didaktische Methoden Grundlage für die Nachhaltigkeit von kompetentem Sicherheitshandeln sind.
Da Themen aus dem Bereich Datenschutz und Informationssicherheit in die Berichterstattung der Publikumspresse Eingang gefunden haben, kann eine grundlegende „Awareness“ für den Themenbereich vorausgesetzt werden und für die Sensibilisierungsbemühungen bei den Mitarbeiterinnen und Mitarbeitern kommunaler Einrichtungen genutzt werden.
Es ist sinnvoll, die öffentliche Berichterstattung auch in den internen Medien (z.B. Mitarbeiterzeitschrift) aufzugreifen und darzustellen, dass das, was anderen widerfahren ist, auch in der eigenen kommunalen Einrichtung leidvolle Realität werden kann.
Phishing ist der wichtigste Pfad, über den Angreifer in kommunale Netzwerke und alle anderen Netzwerke kommen können. In seinen modernen Erscheinungsformen wie „Spear Phishing“ und „Business Email Compromise“ ist ein Phishing-Angriff schwer zu erkennen und Benutzer müssen dauerhaft trainiert werden, um unsichere Verhaltensweisen zu verlernen und sichere Verhaltensweisen zu lernen (siehe [Hinweise „Was ist Phishing und warum fallen wir darauf herein] am Ende).
Phishing-Simulation ist eine Trainingsmethode mit einem hohen Wirkungsgrad und einem guten Preis-Leistungsverhältnis. Die Methode hat sich in den letzten Jahren als Königsweg für das Training der Mitarbeiterinnen und Mitarbeiter im Umgang mit gefährlichen E-Mails und Websites etabliert. SiKoSH empfiehlt deshalb die regelmäßige Durchführung von Phishing-Trainings in der Form von Phishing-Simulationen, etwa in der Form eines Basistrainings, Trainings zur Festigung sicherer Verhaltensweisen und ad-hoc Trainings beim Auftauchen neuer Phishing-Formen.
Schulungen zur Verankerung und Vertiefung von sicheren Verhaltensweisen sind effizienter und motivierender, wenn für die Seminargestaltung moderne didaktische Aufbereitungen wie Social-Engineering Spiele oder Sicherheitsparcours verwendet werden.
Eine Änderung der didaktischen Formate ist vor allem deswegen nötig, weil die etablierten Formate nicht den gewünschten Erfolg hatten. Informationssicherheit bei Mitarbeiterinnen und Mitarbeitern entsteht dann, wenn in einer problema-

---

1 https://www.nist.gov/
2 https://www.enisa.europa.eu/
3 http://www.bakoev.bund.de
4 S. SiKoSH-Beispiel Sensibilisierung

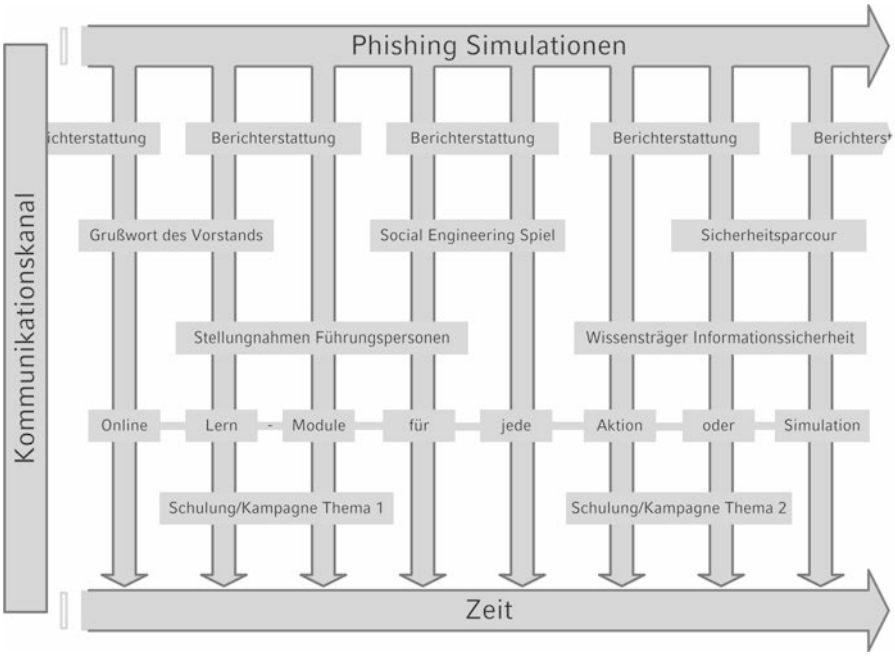


Abbildung 1: SiKoSH-Konzept Sensibilisierung und Schulung

tischen Situation das richtige Verhalten aktiviert wird.
In der noch immer weit verbreiteten „Nürnberger Trichter Didaktik" hat der Lerner die Aufgabe, den Lernstoff mehr oder weniger passiv durch Präsentationen und andere Formen des Frontalunterrichts mehr oder weniger passiv aufzunehmen und in seinem Gedächtnis abzuspeichern. Auf diese Weise eignet er sich nach und nach das Wissen des (überlegenen) Lehrers an. Das funktioniert, aber das Resultat ist in der Regel „träges Wissen", das in der konkreten Handlungssituation nicht oder zumindest nicht nutzbringend abgerufen werden kann.
Lerntheorien, die nach der kognitiven und systemtheoretischen Wende in der Psychologie entstanden, gehen davon aus, dass sich Lernen aus Handeln entwickelt. Handeln findet in Kontexten statt (sozial, technisch, organisatorisch, etc.) und ist situativ und kontextuell gebunden. Die zentralen Merkmale dieser (konstruktivistischen) Lerntheorien sind die Annahme von individuellen und aktiven Lernprozessen, die Betonung der Situationsgebundenheit und der Wichtigkeit der Lerngemeinschaft.
Daher ist es wichtig, Kolleginnen und Kollegen zur Übernahme der (informellen) Rolle des Meinungsführers und Wissensträgers für Fragen der Informationssicherheit zu ermutigen und zu fördern. Probleme der Informationssicherheit treten im Arbeitsfluss unvorhersehbar auf und müssen ad-hoc gelöst werden. Die schnellste und beste Möglichkeit, um „jetzt gleich" kontextbezogene Hilfe zu bekommen, ist immer die Kollegin und der Kollege, die sich am besten mit der Lösung eines Problems auskennen und als „Wissensträger Informationssicherheit" die entstandene Verhaltensunsicherheit kompetent und produktiv auflösen können.
Es ist in hohem Maße sinnvoll, den erreichten Trainingsstand in einem Online-Schulungssystem abzubilden. Mitarbeiterinnen und Mitarbeiter brauchen die Möglichkeit, sich unabhängig von Zeit und Ort zu informieren und das Gelernte zu vertiefen. Es ist kein Zufall, dass gerade im Online-Lernen Kontextbezogenheit und Spielelemente (siehe Stichworte wie Gamifizierung, situiertes Lernen) als Garanten für Lernerfolg betrachtet werden.

Wichtige und aktuelle Themen der Informationssicherheit können und sollen in speziellen Kampagnen und Schulungen thematisiert werden, am besten maßgeschneidert für spezielle Zielgruppen, die ja immer in speziellen Kontexten und Situationen mit den Herausforderungen von Informationssicherheit und Datenschutz umgehen müssen.
Mit der Zeit entsteht so auch die vom Landesrechnungshof Schleswig-Holstein geforderte Sicherheitskultur. Die einfachste Definition von Kultur bezeichnet ja die Art und Weise „Wie wir es hier machen." Sicherheitskultur definiert sich damit durch das Handeln der Mitarbeiterinnen und Mitarbeiter, die eine Organisation ausmachen.

Live-Phishing-Training bei der Landeshauptstadt Kiel

Die Landeshauptstadt Kiel ist Mitglied im Arbeitskreis SiKoSH (siehe Hinweise [SiKoSH: Sicherheit für Kommunen in Schleswig-Holstein] am Ende) und wollte das SiKoSH-Konzept „Sensibilisierung und Schulung" dem Test der Realität unterziehen.
Damit ein Live-Phishing-Training durchgeführt werden kann, müssen mindestens vier Funktionen der kommunalen Einrichtung die Maßnahme befürworten:

- Leitung
- Personalrat
- Datenschutzbeauftragter
- IT-Abteilung

Im Falle der Landeshauptstadt Kiel war das der Fall. Die Zustimmung konnte unter anderem wegen einer technischen Entscheidung von SiKoSH erfolgen: Der

	Phishing E-Mail	Lernziel
1	eingebetteter Link auf vergiftete Website	Mitarbeiterinnen und Mitarbeiter sollen Merkmale von Phishing-E-Mails erkennen und darauf achten, nicht auf eingebettete Links mit unbekannten Ziel-Websites zu klicken.
2	pdf-Anhang mit eingebettetem Schadcode	Mitarbeiterinnen und Mitarbeiter sollen lernen, .pdf und andere Anhänge von unbekannten Absendern nicht oder erst nach Rückfrage bei den Sachverständigen des IT-Service zu öffnen.
3	Klartext-Link auf eine Website außerhalb der Domänen der Landeshauptstadt Kiel mit einem HTML-Formular zur Eingabe von Benutzername und Passwort der dienstlichen Geräte	Mitarbeiterinnen und Mitarbeiter sollen lernen, die Authentisierungsinformationen (Benutzername, Passwort) für ihre dienstlichen Geräte niemals in HTML-Formulare im Internet einzugeben. Sie sollen außerdem lernen, dass die Social-Engineering Signale Autorität (Absendeadresse IT-Leiter) und Knappheit (Sperrung Zugang zum Internet) Anlass zur gründlichen Prüfung der E-Mail sein sollten.

Abbildung 2: Lernziele der Live-Phishing-Trainings

in der Phishing-Simulation verwendete Phishing-Simulator ist eine Open-Source-Anwendung, die als Teil des SiKoSH-Werkzeugkastens nach entsprechender Anpassung allen Kommunen zur Verfügung stehen soll.
Die Entscheidung für eine an die Bedingungen und Bedürfnisse von kommunalen Einrichtungen anpassbare Open-Source-Anwendung macht es möglich, dass

- keine Daten von Mitarbeiterinnen und Mitarbeitern an einen externen Anbieter übermittelt werden (viele Anbieter operieren im nicht-europäischen Ausland)
- Gesamtablauf und alle Daten vollständig unter der technischen und organisatorischen Kontrolle der kommunalen Einrichtung bleiben
- die Phishing-Angriffe genau auf die Bedingungen und Bedürfnisse jeder individuellen kommunalen Einrichtung angepasst werden können (so wie die für die nächsten Jahre vorhergesagten echten Phishing-Angriffe auch arbeiten)
- die Kosten für ein Training sich größtenteils nur auf die Selbstkosten (Personalstunden) belaufen, hinzu kommen ggf. Kosten für eine externe Unterstützung hinsichtlich der inhaltlichen und technischen Ausgestaltung der Kampagnen.

Das Live-Phishing-Training für die Mitarbeiterinnen und Mitarbeiter der Landeshauptstadt Kiel wurde in drei Aussendungen durchgeführt, die die gebräuchlichsten Phishing-Angriffe simulierten (siehe Abbildung 2).

Live-Phishing-Training Landeshauptstadt Kiel – Aussendung 1

In der ersten Aussendung des Live-Phishing-Trainings wurde den Mitarbeiterinnen und Mitarbeitern der Landeshauptstadt Kiel eine typische Phishing-E-Mail geschickt, die im Ernstfall versucht hätte, durch einen Drive-by-Exploit Schadsoftware auf dem Rechner der Mitarbeiterin oder des Mitarbeiters zu installieren (siehe Hinweise „Drive-by-Exploit“ am Ende).
Der Text der simulierten Phishing-E-Mail der Kampagne ist eine mögliche, aber recht unwahrscheinliche Aktion der Finanzabteilung der Landeshauptstadt Kiel: Die Gehaltsmitteilung soll nicht mehr an die Büro-Adresse gehen, sondern an die Privatanschrift.
Die E-Mail enthält viele typische Merkmale von Phishing-E-Mails. Sie kann an Hand einiger Merkmale sehr leicht als „zweifelhafte Zusendung“ bewertet werden:

1. Die Absendeadresse „info@gehaltskasse.com“ ist den Empfängern nicht bekannt. Sie wurde für die Phishing Simulation erst eingerichtet. Es ist nicht glaubhaft, dass die Landeshauptstadt die Verwaltung der Bezüge an ein externes Unternehmen gegeben hätte.
2. Die Landeshauptstadt spricht die Mitarbeiterinnen und Mitarbeiter in ihren E-Mails normalerweise persönlich an.
3. Dass „datenschutzrechtliche Gründe“ dazu führen sollen, die Gehaltsmitteilung an die Privatadresse der Mitarbeiter zu senden, wirkt eigenartig. Aus Gründen des Datenschutzes den Versand der Gehaltsmitteilung an die Privatanschrift einzustellen, wäre glaubwürdiger.
4. „über die Arbeitgeberanschrift“ ist falsch, es muss heißen „an die Arbeitgeberanschrift“
5. Die Landeshauptstadt Kiel schickt an ihre Mitarbeiterinnen und Mitarbeiter keine E-Mails, in denen über einen Link etwas bestätigt werden soll. Sicher nichts datenschutzrechtlich Relevantes und ganz sicher nichts, was das Gehalt betrifft.
6. Die Signatur „Gehaltskasse der Landeshauptstadt Kiel“ sieht nicht aus wie eine in der Landeshauptstadt übliche Signatur. Insgesamt auch nicht wie eine seriöse Signatur einer seriösen Behörde. Außerdem kommen die Gehaltsbescheinigungen von der Versorgungsausgleichskasse der Kommunalverbände in Schleswig-Holstein.
7. „maschinel“ … da ist ein Schreibfehler übersehen worden – schlechte Grammatik und Schreibfehler sind typisch für Phishing-E-Mails.

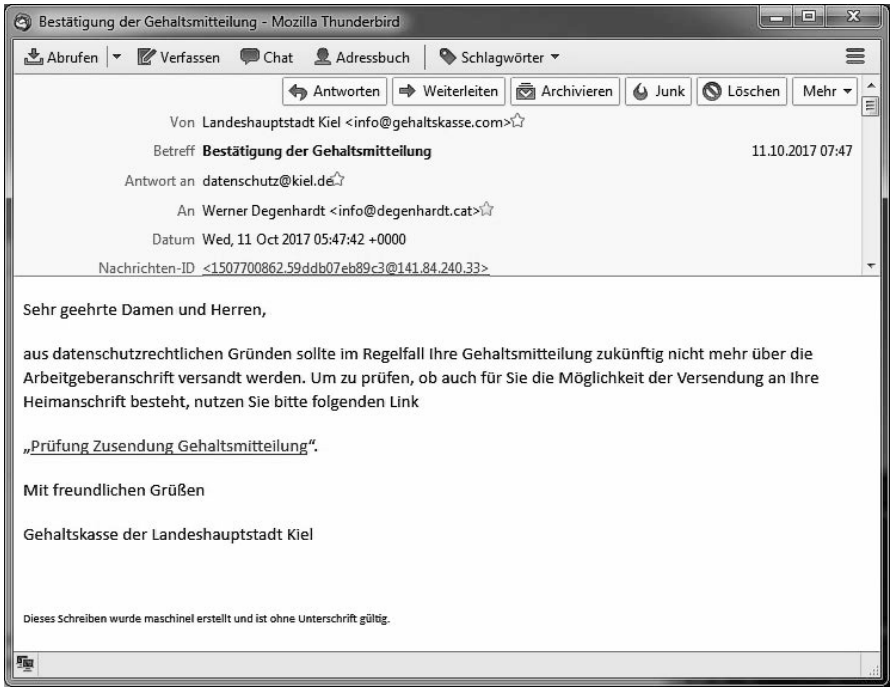


Abbildung 3: Phishing E-Mail der Aussendung 1

Der Klick auf den eingebetteten Link „Prüfung Zusendung Gehaltsmitteilung“ führte dazu, dass eine Webseite „Sie wurden gefischt“ mit Erläuterungen und weitergehenden Hinweisen geöffnet wurde (sieheAbbildung 7).
Die Phishing-Simulation startete am Mittwoch, den 11.10.2017 um 08:53 und endete am 13.10.2017 um 10:32. Insgesamt haben 28% der Mitarbeiterinnen und Mitarbeiter auf den eingebetteten Link geklickt und die „Sie wurden gefischt“–Seite gesehen. Nachzügler unter den Mitarbeiterinnen und Mitarbeiter bekommen seitdem eine Hinweisseite (Hinweis: „Diese Seite gibt es nicht mehr“) im Browser angezeigt.
Der erste Klick auf den eingebetteten Link wurde 1 Minute nach dem Beginn der Aussendungen registriert. Drei Stunden nach dem Beginn der Aussendung der simulierten Phishing E-Mail hatten schon zwei Drittel aller Aufrufe der – in einem echten Angriffsszenario schädlichen – Webseite stattgefunden.
Dieses für Phishing-Angriffe typische Phänomen spricht dafür, dass

1. Präventive Maßnahmen zur Vermeidung ungünstigen Nutzerverhaltens und die
2. Reaktion der IT-Abteilung sofort nach Bemerken eines Phishing-Angriffs

die beiden wichtigsten organisatorischen Maßnahmen sind.
Um die organisatorische Abwehrfähigkeit gegen Angriffe zu testen, hatten die Organisatoren des Live-Phishing-Trainings den IT-Servicedesk und die Personalabteilung nicht vorab informiert. Der IT-Servicedesk reagierte zügig und fragte 15 Minuten nach Beginn der Aussendung beim IT-Leiter an, ob die definierten Informations- und Abwehrmaßnahmen eingeleitet werden sollten.

Datenschutz, IT-Abteilung und Personalamt bekamen viele Nachfragen per Telefon und E-Mail. Datenschutz und Informationssicherheit war für einige Tage und Wochen ein viel diskutiertes Thema in der Landeshauptstadt.

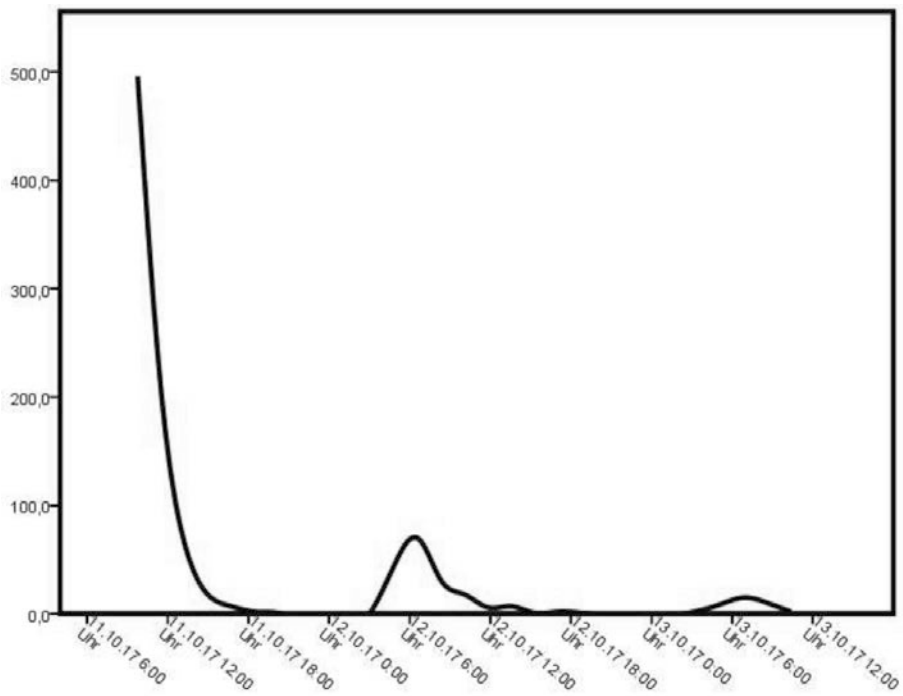


Abbildung 4: Klickverlauf Live-Phishing-Training Aussendung 1

Eine Klickrate von 28% aller von der Phishing-E-Mail erreichten Mitarbeiter gibt Anlass zu vier Fragen:

1. Warum haben so viele Mitarbeiterinnen und Mitarbeiter auf den Link in der E-Mail geklickt?
2. Warum haben nicht mehr Mitarbeiterinnen und Mitarbeiter auf den Link in der E-Mail geklickt?
3. Wie beurteilen Mitarbeiterinnen und Mitarbeiter die Auflösung der Kampagne (siehe Abbildung 7: Auflösungsseite - Live-Phishing-Training Aussendung 1)?
4. Was halten die Mitarbeiterinnen und Mitarbeiter von dieser für sie doch ungewöhnlichen und neuen Schulungsmaßnahme in Sachen Datenschutz und Informationssicherheit?

Auch wenn die Organisatoren der Kampagne sich selbst auf eine „ergebnisoffene" Haltung verpflichtet hatten, etwas weniger wäre ihrer Meinung nach doch mehr gewesen. Die Auswertung von E-Mails, Telefongesprächen und Fokus-Gruppen im Nachgang zeigt recht deutlich, was die primären Anreize für den Klick waren:

1. Bei der Absendeadresse wird tendenziell schon nach dem Lesen des Texts „Landeshauptstadt Kiel" geschlossen, dass es sich um eine offizielle E-Mail der Landeshauptstadt handelt. Der Rest der Adresszeile wird ignoriert.
2. Das Wort „Gehaltsmitteilung" legt nahe, dass es um Geld geht und das gibt dem Vorgang Wichtigkeit und Dringlichkeit.
3. Die Zusendung der Gehaltsmitteilung an die Privatadresse war anscheinend ein von vielen Mitarbeiterinnen und Mitarbeitern heimlich gehegter Wunsch.
4. Ein Teil der Mitarbeiterinnen und Mitarbeiter der Landeshauptstadt Kiel geht davon aus, dass das Behördennetz und die elektronische Kommunikation im Behördennetz per se sicher sind und eigene Achtsamkeit unnötig wäre.

Im internationalen Vergleich von Erst-Trainings ist die Klickrate in der Landeshauptstadt für eine gut gemachte Spear-Phishing E-Mail allerdings eher positiv zu bewerten. Klickraten von 50% sind durchaus im Rahmen des Normalen. Der Grund, warum die Klickrate in der Landeshauptstadt doch deutlich darunter blieb, liegt zweifelsohne an der offenen Gesprächskultur.

In der Regel werden Abweichungen von den normalen Wahrnehmungsmustern trotz der eingebauten Ablenkungen der Phisher unterschwellig wahrgenommen. Irgendwie wirkt die E-Mail doch „komisch". Kann die Mitarbeiterin oder der Mitarbeiter ihre / seine Zweifel „jetzt" durch eine Nachfrage bei einer Kollegin oder einem Kollegen oder durch Anruf beim IT-Servicedesk verifizieren, bleibt der Klick aus. Bleibt er mit seinem nicht ganz so guten Bauchgefühl allein, gewinnen im intrapersonalen Entscheidungsprozess oft die in der Phishing E-Mail eingebauten positiven Anreize. In der Landeshauptstadt haben ein gut funktionierender IT-Servicedesk und hilfsbereite Kollegen eine höhere Klickrate verhindert.

Die Anmutung der Auflösungsseite der Kampagne wurde von den Mitarbeiterinnen und Mitarbeitern positiv beurteilt. Ein lustiger Hai kommt viel besser an als ein erhobener Zeigefinger. Die erklärenden Texte allerdings fanden bei den Leserinnen und Lesern keinen großen Anklang. „Zu viel Text, zu lang", war der Tenor der Aussagen dazu, auch empfohlene Weiterbildungsmaßnahmen wie das Behörden-IT-Sicherheitstraining (BITS) wurden bisher zu selten konsultiert.

Bis auf wenige Ausnahmen wurde das Live-Phishing-Training durch die Mitarbeiterinnen und Mitarbeiter sehr positiv beurteilt. Sie stellen fest, dass sie durch das Training etwas gelernt haben und dass das Gelernte auch für zuhause sehr nützlich ist. Deutlich spürbar ist aber auch die Erwartung, dass die IT-Abteilung die Durchleitung von „bösen" E-Mails verhindert. Beiträge des behördlichen Datenschützers in der Mitarbeiterzeitschrift der Landeshauptstadt versuchten im Nachgang diese unrealistische Erwartungshaltung zu korrigieren.

Live-Phishing-Training
Landeshauptstadt Kiel – Aussendung 2

Im zweiten Training setzte der Text der simulierten Phishing-E-Mail den Phishing-Versuch in den Kontext vorweihnachtlich froher Stimmung der Mitarbeiterinnen und Mitarbeiter der Landeshauptstadt. Er nutzt die Erwartung aus, am Ende eines Arbeitsjahres auch ein „Danke" zu hören für die geleistete Arbeit. Dass das „Danke" gleich mit einem Glühwein-Gutschein daher kommt, macht die Zuschrift nur noch sympathischer.

Wenn die Mailempfängerin bzw. der Mailempfänger die E-Mail nicht als Phishing-Versuch einstufte und den Anhang öffnete, musste sie / er die Adobe Acrobat Sicherheitswarnung bewusst durch Anklicken ignorieren:

„Das Dokument versucht eine Verbindung zur folgenden Website aufzubauen: https://weihnachtsmarkt.cemt-kiel.de. Ist cemt-kiel.de vertrauenswürdig? Wenn Sie die Website für vertrauenswürdig einstufen, wählen Sie „Zulassen". Wenn Sie die Website nicht als vertrauenswürdig einstufen, wählen Sie „Blockieren".

Insgesamt haben 14% der Mitarbeiterinnen und Mitarbeiter die Website als vertrauenswürdig eingestuft und den CEMT-Weihnachtsmarkt-Gutschein geöffnet. Der im Dokument enthaltene Code leitete auf eine Website weiter. Dort gab es keinen Gutschein, sondern den Hinweis auf die Faustregel:

„Wenn man eine Sicherheitswarnung beim Öffnen eines Anhangs bekommt

Abbildung 5: Phishing-E-Mail der Aussendung 2

und nicht weiß, welche Folgen es hat, wenn man die Datei trotzdem öffnet: Den IT-Service fragen, bevor Sie die Datei öffnen!"

Live-Phishing-Training
Landeshauptstadt Kiel – Aussendung 3

Der Text der simulierten Phishing-E-Mail der dritten Aussendung vermittelt dringenden Handlungsbedarf für die Aufrechterhaltung des Zugangs zum Internet. Die Phishing-E-Mail verwendet die grundlegenden Techniken eines BEC-Angriffs (Business Enterprise Compromise) bzw, CEO-Fraud:

1. die Identität eines hochrangigen oder zumindest bekannten Mitglieds der Einrichtung wird übernommen: hier – der IT-Leiter der LH Kiel Jan Koppelmann
2. die Wichtigkeit sofortiger Aktion wird nahegelegt: hier – Kein Internet mehr
3. eine gefahrgeneigte und schädliche Handlung wird gefordert: hier – Eingabe der Credentials (Benutzername und Passwort)

Allerdings gab es für die Mitarbeiterinnen und Mitarbeiter auch Hinweise, die als Anzeichen für eine Schad-E-Mail hätten gewertet werden können:

1. Klartext-Link in der E-Mail https://www.klel.de/internetisicherheit ist keine bekannte Domäne aus dem Arbeitsumfeld der LH Kiel, sondern eine Tippfehler-Domain (klel statt kiel; der Buchstabe „i" ist durch den Buchstaben „l" ersetzt, eine Fälschung, die selten erkannt wird)
2. die Mitarbeiterinnen und Mitarbeiter der LH Kiel sind angehalten, keinesfalls Credentials (Benutzername, Passwort) in Web-Formulare einzugeben, wie z.B. in das Formular der Phishing-E-Mail „Internetsicherheit – Zugang bestätigen"
3. der URL in der Adresszeile des Browsers zeigt ebenfalls die Tippfehler-Domain und ist – wenn man die Adresszeile überhaupt wahrnimmt – ein deutlicher Hinweis auf eine zweifelhafte Seite.

Der Klick auf die Tippfehlerdomain führte auf ein HTML-Formular, in die Benutzername und Passwort eingegeben werden konnte. Um zu verhindern, dass Mitarbeiterinnen und Mitarbeiter tatsächlich ihre Zugangsberechtigungen kompromittieren, führte schon die Eingabe von zwei Zeichen des Benutzernamens oder ein Zeichen des Passworts oder das Klicken auf den Anmelde-Button zur Anzeige der "Education Page" mit dem Hinweis:
„Selbstverständlich erfassen wir nicht, wie Sie auf diese Simulation reagiert haben – und wir haben technisch dafür gesorgt, dass niemand seine kompletten Anmeldedaten in der von uns gestalteten Seite eingeben kann. Denn die Landeshauptstadt wird Sie niemals auffordern, Ihre persönlichen Anmeldedaten preiszugeben! Verraten Sie Ihr Kennwort niemandem, auch keinem Kollegen, Vorgesetzten oder Systemverantwortlichen – schon gar nicht im Internet".
Insgesamt haben 24% der Mitarbeiterinnen und Mitarbeiter auf den Klartext-Link in der Phishing-E-Mail geklickt. Insgesamt 18% der Mitarbeiterinnen und Mitarbeiter haben versucht, Benutzernamen und Passwort in das HTML-Formular einzutragen.
Die Klickquote erscheint zunächst erschreckend hoch, ist aber „normal" und auch der Grund, warum – nach allen Prognosen – die Phisher in den nächsten zwei Jahren mit Organisationen und Unternehmen mit CEO Fraud und BEC (Business Email Compromise) überziehen werden. Die Mitarbeiterinnen und Mitarbeiter der Landeshaupt zeigen sich nach dem Live-Phishing-Training allerdings sensibilisiert, manche sogar alarmiert. Man ist vorbereitet.

Zusammenfassung

Die Organisatoren bei der Landeshautstadt Kiel bewerten das Ergebnis des Live-Phishing-Trainings ausgesprochen positiv.

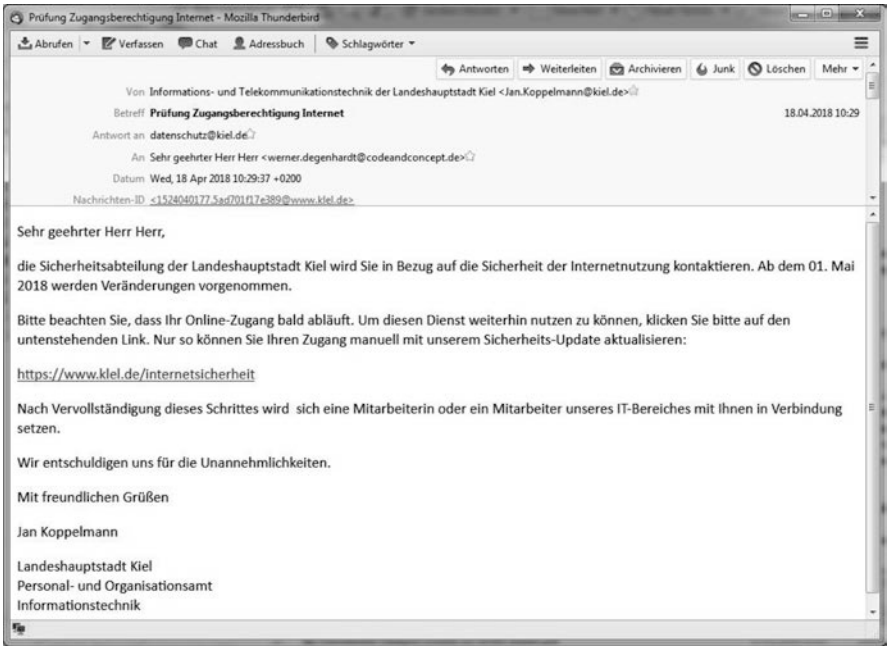


Abbildung 6: Simulierte Phishing-E-Mail

„Vorrangiges Ziel unseres Sicherheitstrainings war es, dazu anzuregen, mit den Kolleginnen und Kollegen über das Thema IT-Sicherheit ins Gespräch zu kommen“, so Andreas Amann, Datenschutzbeauftragter der Stadt, „und das ist uns eindrucksvoll gelungen. Wir hatten keine Erwartungshaltung, wie hoch die Quoten hätten sein sollen, nur gehofft, sie würden geringer ausfallen. Aber die lebhaften Diskussionen und natürlich auch die Erprobungen des Ernstfalles haben uns viele wichtige Erkenntnisse gebracht, die dazu führten, dass E-Mail in der Stadtverwaltung sicherer geworden ist und zukünftig noch sicherer werden wird“.

Das zeige sich an einem einfachen Beispiel: „Vor unserer Kampagne wurde ich in meiner langjährigen Tätigkeit als Datenschutzbeauftragter nie gefragt, ob ein beigefügter Link oder ein E-Mail-Anhang wirklich ‚echt' ist, jetzt scheinen solche Nachfragen zur Normalität zu gehören. Die Reaktionen der Kolleginnen und Kollegen hätten gezeigt, „egal, ob die Benutzer sich über das eigene Verhalten geärgert haben oder sich vielleicht sogar ertappt fühlten oder sich darüber freuten, die Phishing-Mail erkannt zu haben, sie sind weiterhin im ‚Aufmerksamkeitsmodus' bei der Bearbeitung von E-Mails. Und genau dieses ‚gesunde Misstrauen' zu erzeugen, war unser Ziel“.

Mit dem Training habe man zugleich „auf einfache Weise zeitgleich bis zu 3000 Mitarbeiterinnen und Mitarbeiter dort erreicht, wo Sie im dienstlichen und auch im privaten Bereich am häufigsten mit Angriffen rechnen müssen - beim täglichen Umgang mit E-Mails“. Das sei im normalen Arbeitsalltag, bei dem nicht immer ausreichend Zeit für Schulungsmaßnahmen bleibt, ein wichtiger Faktor.

Die Reaktion eines Kollegen steht für viele andere und hat den Datenschutzbeauftragten besonders gefreut: „Ich bin auch auf Eure Aktion hereingefallen. Aber da habe ich wirklich mal etwas gelernt, was ich ja auch zu Hause gebrauchen kann“. Solche Reaktionen habe man zuvor weder mit den „typischen Verboten“, noch mit Artikeln in der Mitarbeiterzeitschrift oder mit den angebotenen „klassischen Fortbildungen“ erreichen können.

Und „ganz nebenbei“ erfüllt die Landeshauptstadt Kiel mit dem Live-Phishing-Training auch die gesetzlichen Vorgaben der Datenschutz-Grundverordnung (DSGVO):

- Art. 32 (Sicherheit der Verarbeitung) 1.d „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“
- Art. 39 (Aufgaben des Datenschutzbeauftragten) 1.b „Überwachung … der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen“
- Art. 47 (Verbindliche interne Datenschutzvorschriften) 2.n „geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten“

Letzten Endes hat die Landeshauptstadt Kiel diese Anforderungen erfüllt und die Arbeit hinter sich. Alle anderen haben sie möglicherweise noch vor sich.

Abbildung 7: Auflösungsseite - Live-Phishing-Training Aussendung 1

Erläuterungen zum Drive-by-Exploit

Erzählt man einem „normalen“ Internetnutzer, dass er sich durch den bloßen Besuch einer Website einen Trojaner einfangen kann, dann ist die normale Reaktion ungläubiges Staunen. Leider ist der Drive-by-Exploit aber Realität, wie die aus dem BSI Bericht „Die Lage der IT-Sicherheit in Deutschland 2014“ entnommene Grafik zeigt.

Der Erfolg von Drive-by-Exploits beruht auf dem Zusammenspiel von Nachlässigkeiten oder Fehlern der Anbieter von Webseiten und technischen, organisatorischen und menschlichen Nachlässigkeiten oder Fehlern bei Nutzern dieser Webseiten.

Auch Suchergebnisseiten von Google können vergiftet sein und z.B. über bei Google eingeschleuste Werbebanner Schadsoftware auf den Zielrechnern installieren.

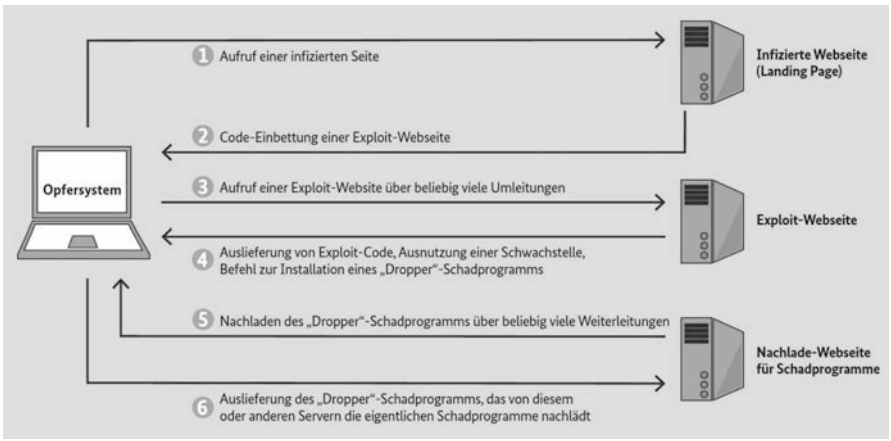


Abbildung 8: Wie ein Drive-by-Exploit funktioniert

Was ist Phishing und warum fallen wir darauf herein?

Phishing hat sich in den letzten Jahren zum wichtigsten Angriffsvektor auf die Sicherheit von vernetzten Rechnern entwickelt. So stellt zum Beispiel der IBM Cyber Security Index 2014 fest, dass in über 95 % aller Sicherheitsvorfälle „menschliche Fehler“ eine Rolle spielen – am häufigsten das Öffnen eines mit Schadsoftware infizierten E-Mail-Anhangs oder der Aufruf einer unsicheren Internetadresse im Browser.

Die Bezeichnung „Phishing" charakterisiert das Vorgehen des Angreifers. Es wird ein Köder ausgelegt und wenn das Opfer auf den Köder reagiert, hängt es am Haken und macht dann - sehr oft - was der Fischer will.

Der Fischer verwendet dazu Werkzeuge des Social Engineering und des Cognitive Engineering. Er nutzt Automatismen und Gewohnheiten der menschlichen Wahrehmung und des menschlichen Sozialverhaltens aus, um eine vermeintlich vertrauenswürdige Kommunikationssituation zu schaffen. In diesem vermeintlich vertrauenswürdigen Handlungskontext macht dann der Benutzer die gewünschten „Fehler".

Der Köder kann in der Form von E-Mails ausgelegt werden, etwa als Botschaft in einer Social Network Plattform, als SMS oder auch als Telefonanruf. Oft werden mangelnde Aufmerksamkeit und Flüchtigkeitsfehler ausgenutzt, wie zum Beispiel im Falle von Tippfehlerdomains (www.gogle.com, www.googl.com, etc., die im Falle von Google aber alle auf die richtige Website weitergeleitet werden).

Oft sind die Köder Links auf Websites, die dem Original täuschend ähnlich nachgebaut sind und den Benutzer dazu verführen, die gesuchte Information einzugeben, einen Anhang zu öffnen oder eine bestimmte Website zu besuchen. Der in der E-Mail eingebettete Link geht z.B. augenscheinlich auf www.stadtsparkasse.de, im HTML-Code zeigt er in Wirklichkeit aber auf vvww.stadtsparkasse.de.

Es ist unwahrscheinlich, dass der Benutzer bemerkt, dass der Angreifer im URL das erste ‚w' durch zwei ‚v' ersetzt hat, selbst wenn er die Mühe auf sich nimmt, die URL zu inspizieren oder den HTML-Code der E-Mail zu untersuchen.

Phishing benutzt Werkzeuge des Social Engineering und des Cognitive Engineering, um Benutzer zu Handlungen zu veranlassen, die sich ohne diese Manipulation nicht ereignet hätten.

Phishing ist Betrug im Internet und aus vier Gründen so erfolgreich:

1. Im Internet ist es viel leichter, seine wirkliche Identität zu verbergen oder die Identität eines anderen - vertrauenswürdigen - Gegenübers anzunehmen als in der analogen Welt.
2. Es ist im Internet viel billiger, den Betrug zu realisieren als in der analogen Welt. Der Aufbau einer Website kostet nur Bruchteile des Aufbaus eines falschen Bürogebäudes.
3. Die Reichweite des Internet ist unendlich viel größer als die Reichweite einer Drückerkolonne.
4. Der Angreifer kann im Internet anonym bleiben und aus Ländern angreifen, die der juristischen Verfolgung der Straftat entzogen sind.

Phishing ist Social Engineering, das am kürzesten und zutreffendsten vielleicht so definiert wird: Social Engineering ist die Kunst und die Wissenschaft, andere Menschen dazu zu bringen, sich so zu verhalten, wie man es selbst will.

Man kann Social Engineering als eine Sammlung von Methoden beschreiben, die angeborene oder habitualisierte Reaktionsweisen von Menschen ausnutzen, um sie zu Handlungen zu veranlassen, die nicht notwendigerweise in ihrem eigenen wohlverstandenen Interesse sind.

Phishing nutzt vor allem soziale Heuristiken aus, um den Benutzer zu unbedachten Handlungen zu verführen. Der Begriff „Heuristik“ bezeichnet einfache, effiziente Regeln, die sich durch evolutionäre Prozesse gefestigt haben oder erlernt wurden.

Heuristiken erleichtern Menschen Entscheidungsfindungen und Problemlösungen in komplexen Situationen ungemein und machen sie in vielen Fällen erst möglich. Heuristiken wirken oft wie Instinkte, wie Handlungsketten, die durch einen einfachen Auslösereiz in Gang gesetzt werden und weitgehend automatisch ablaufen.

Die wichtigsten sozialen Heuristiken sind

- Reziprozität
- Kommitment & Konsistenz
- Soziale Bewährtheit
- Autorität
- Sympathie
- Knappheit

Reziprozität bezeichnet das Gefühl der Verpflichtung, auf ein Geschenk mit einer Gegenleistung zu reagieren, ein Freundschaftsangebot zu erwidern, eine Warnung „Ihr Internetzugang wird gesperrt“ mit dem Befolgen des Vorschlags „Benutzername und Passwort eingeben“ zu quittieren.

Kommitment und Konsistenz beziehen sich auf den Wunsch der meisten Menschen, gegebene Zusagen einzuhalten und zu einmal gefassten Meinungen zu stehen. Diese Heuristik wird im analogen Alltag von Verkäufern durch die „foot in the door“ und „low ball“ Technik ausgenutzt, im Internet zum Beispiel bei den sogenannten Nigeria-Scams: Der Angreifer fängt klein an mit der Bitte um seelischen Beistand und hat am Ende die Vorauszahlung in der Hand.

Soziale Bewährtheit steht für die Tendenz, sich in unklaren Situationen daran zu orientieren, was andere tun.

Das Erzeugen von Sympathie ist eine der wirksamsten Beeinflussungsmöglichkeiten überhaupt. Menschen lassen sich leichter von Personen beeinflussen, die sie mögen, mit denen sie Interessen teilen, die sie attraktiv finden.

Autorität ist nach Sympathie das zweitwirksamste Angriffsmittel und funktioniert vor allem dort hervorragend, wo Strukturen der Über- und Unterordnung die Kommunikation regeln. Das ist vor allem auch in Behörden der Fall, in denen der Mitarbeiter traditionell großes Vertrauen in die Kompetenz und die Fürsorge der Vorgesetzten hat.

Knappheit spielt bei fast allen Beeinflussungsversuchen eine Rolle. Wenn man den Eindruck hat, dass die Chance vertan ist, wenn man nicht gleich reagiert, dann führt der gefühlte Zeitmangel dazu, dass man Entscheidungen unter emotionalen Bedingungen fällt, die man - im Rückblick - als „vernünftiger" Mensch nie so gefällt hätte.

Untersuchungen zum Nutzerverhalten machen wenig Hoffnung, dass technische Vorkehrungen überhaupt die Wirksamkeit von Phishing vermindern könnten:

1. Menschen beurteilen die Rechtmäßigkeit und Vertrauenswürdigkeit von Websites nach deren "look and feel", das von einem Angreifer leicht nachgemacht werden kann.
2. Viele Benutzer verstehen die Sicherheitswarnungen ihrer Webbrowser nicht oder haben kein Vertrauen in diese Warnungen.
3. Obwohl Benutzer wissen, was Phishing ist und sich über die Gefahren im Klaren sind, verringert das nicht ihre Anfälligkeit für Phishing.
4. Auch wenn Benutzer schwerwiegende Konsequenzen einer "falschen" Entscheidung fürchten müssen, ändert das ihr Verhalten nicht.
5. Die meisten technischen Sicherheitsvorkehrungen sind für die Benutzer nicht benutzbar und haben mitunter sogar gegenteilige Effekte.

Der grundlegende Schluss aus allen vorliegenden Untersuchungen zum Thema Phishing kann nur lauten, dass Benutzer von elektronischen Geräten und Anwendungen über keine geeigneten Mechanismen verfügen, angemessen auf Phishing zu reagieren. Das liegt im Wesentlichen daran, dass kognitive und soziale Heuristiken menschlicher Wahrnehmung und menschlichen Verhaltens dem Angreifer in die Hand spielen.

Die gute Nachricht ist allerdings, dass das Erkennen von betrügerischer Kommunikation im Internet und angemessene Reaktionen darauf trainiert werden können.

Am effizientesten ist eingebettetes Training: Benutzern werden Phishing-Mails geschickt, die in ihrem Arbeitskontext vorkommen können. Wenn sie auf eine Phishing-Mail hereinfallen, bekommen sie ein spezielles Online-Training, mit dem sie üben, wie sie auf diesen speziellen Typ von Angriff richtig reagieren. Wenn die Trainingseinheiten in ein geeignetes Warnsystem integriert sind, dann ist ihre Wirksamkeit noch besser.
Das Vorgehen ist in der Tradition konstruktivistischer Lerntheorien gut begründet. Nutzertraining erscheint zunächst aufwendiger als herkömmliche Sensibilisierungsbemühungen. Es ist aber aus den gezeigten Gründen sicher, dass Spear-Phishing nur mit "Spear Learning" begegnet werden kann.

Die 10 Gebote wirksamen Sicherheitstrainings

Viele Spezialisten für Informationssicherheit denken, dass es ausreicht, Menschen mit Informationen über Probleme der Informationssicherheit zu versorgen und schon würde sich auch ihr Sicherheitsverhalten ändern. Sie mussten allerdings in den vergangenen zwei Dekaden lernen, dass Awareness wenig mit Verhaltensänderung zu tun hat.
Ein fundamentales Problem liegt darin, dass die meisten Sensibilisierungskampagnen von Sicherheitsspezialisten oder Marketingprofis gemacht werden, von Leuten, die nicht als Lern- und Didaktiksachverständige ausgebildet worden sind.
Was dabei herauskommt sind überfrachtete und ermüdende Präsentationen oder verfehlte Werbebotschaften. Der erhoffte Fortschritt bei der Verbesserung des Sicherheitsverhaltens von Nutzern bleibt aus, trotz aller Bemühungen.
Um dieses Rätsel zu lösen, ist es wichtig, sich die Grundsätze der Lerntheorie bewusst zu machen und sich zu vergegenwärtigen, wie Menschen überhaupt etwas lernen.

1. **Kleine Dosierungen**
   Menschen lernen besser, wenn sie sich auf kleine Informationseinheiten konzentrieren können, die sich in vorhandene Wissensstrukturen einbauen lassen. Die Annahme, man könnte 55 Themen in 15 Minuten abdecken und jemand würde sich das alles merken können und auch noch sein Verhalten entsprechend ändern, ist realitätsfern.

2. **Wiederholung**
   Menschen lernen durch Wiederholung. Ohne häufiges Feeback und die Gelegenheit, Gelerntes praktisch anzuwenden, verblassen selbst gut eingeübte Fähigkeiten. Sicherheitstraining sollte eine fortlaufende Dauerveranstaltung sein, nicht ein einziges Seminar.

3. **Trainieren im Kontext**
   Menschen erinnern sich besser an den Kontext als an den Inhalt. Für Sicherheitstrainings ist es wichtig, den Lerninhalt im selben Kontext zu vermitteln, in dem der Lernende auch angegriffen wird.

4. **Botschaften variieren**
   Konzepte werden am besten gelernt, wenn man ihnen in vielen verschiedenen Kontexten begegnet und sie in unterschiedlichen Arten und Weisen dargestellt werden.

5. **Lernende einbeziehen**
   Wenn wir aktiv in den Lernprozess einbezogen sind, lernen wir besser. Wenn ein Lerner üben kann, wie man Phishing-E-Mails erkennt oder gute Passworte erzeugt, führt das zu einer deutlichen Verbesserung des Lernerfolgs.

6. **Unmittelbares Feedback**
   Feedback ist am wirksamsten, wenn es sofort erfolgt. Wenn ein Benutzer auf eine Phishing-Simulation hereinfällt und sofort erfährt, warum das passiert ist, dann merkt er sich das.

7. **Geschichten erzählen**
   Wenn Menschen Lerninhalte eingebettet in Geschichten nahebracht werden, bilden sie emotionale Bindung zum Material aus und bleiben besser und länger engagiert.

8. **Denken lassen**
   Menschen brauchen die Möglichkeit, über ihren Fortschritt nachzudenken und ihn zu bewerten, bevor sie zu weiterem Fortschritt fähig sind. Sicherheitstraining sollte den Teilnehmern Gelegenheit geben, über die vermittelten Informationen nachzudenken, ihre Stichhaltigkeit zu prüfen und zu eigenen Schlussfolgerungen zu kommen.

9. **Der Lernende bestimmt das Tempo**
   Jeder lernt auf seine eigene Art und Weise. Ein „one-size-fits-all“ Sicherheitstraining ist zum Scheitern verurteilt, weil es nicht berücksichtigt, was für das individuelle Lernbedürfnis am besten ist.

10. **Konzeptuelles und prozedurales Wissen anbieten**
    Konzeptuelles Wissen zeigt das Große und Ganze und zeigt Lernenden, wie sie ein Problem lösen können. Prozedurales Wissen konzentriert sich auf die unterschiedlichen Handlungen, die das Problem lösen.
    Die Kombination von beiden Wissensarten verbessert den Lernerfolg. Ein Benutzer braucht zum Beispiel eine prozedurale Unterweisung, um zu verstehen, dass eine bestimmte IP-Adresse in einer URL ein Hinweis auf eine Phishing-E-Mail ist. Andererseits braucht er auch ein konzeptionelles Verständnis aller Bestandteile einer URL, damit er den Unterschied zwischen einer IP-Adresse und einem Domain-Namen erkennen kann, sonst hält er womöglich etwas wie www4.google.com für eine Phishing-URL

    Von den Verfassern übersetzt nach Joe Ferrara, Ten commandments for effective security training, https://www.csoonline.com/article/2131688/security-awareness/ten-commandments-for-effective-security-training.html, zuletzt aufgerufen am 06.05.2018.

Wer ist SiKoSH?

Im Auftrag der Kommunalen Landesverbände in Schleswig-Holstein führt das KomFIT das Projekt SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) durch. In Zusammenarbeit mit kommunalen Praktikern aus Schleswig-Holstein sowie Partnern aus anderen Bundesländern erarbeitet das Projekt zahlreiche Hilfestellungen zum Aufbau eines nachhaltigen Informationssicherheitsmanagementsystems (ISMS) innerhalb von Kommunalverwaltungen. Fachlich wird das Projekt dabei tatkräftig durch das Unabhängige Landeszentrum für Datenschutz, den Landesrechnungshof, Dataport und durch externe Berater unterstützt.

Warum ist Informationssicherheit so wichtig?

- Informationssicherheit rechtfertigt das Vertrauen der Bürgerinnen und Bürger in eine sichere Verarbeitung ihrer Daten und ist somit auch zwingende Voraussetzung für eine weitere Öffnung der Behördennetze (Stichwort: E-Government).
- Informationssicherheit ist gesetzlich vorgeschrieben, z. B. beim Betrieb kommunaler Webseiten oder zur Wahrung von Amtsgeheimnissen.
- Die technisch-organisatorischen Maßnahmen zur Verbesserung der Informationssicherheit sind auch ein integraler Bestandteil zur Gewährleistung datenschutzrechtlicher Ziele.
- Informationssicherheit schützt Investitionen, indem zum Beispiel das Risiko eines Datenverlustes und aufwändiger Wiederherstellungsmaßnahmen reduziert wird.

Was versteht man unter der SiKoSH-Vorgehensweise?

Die SiKoSH-Vorgehensweise ist im SiKoSH-Standard ‚Vorgehensweise beim Aufbau eines kommunalen ISMS' beschrieben. Logisch zusammenhängende Teilsicherheitsprozesse werden im SiKoSH-Prozessmodell in einzelnen Phasen zusammengefasst (siehe Abbildung 9).

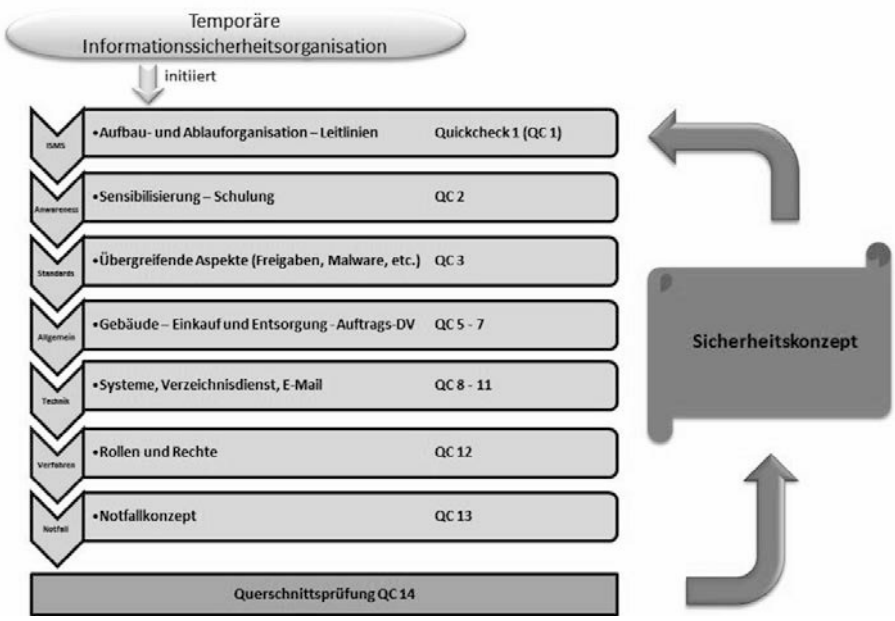


Abbildung 9: Das SiKoSH-Prozessmodell

Jede SiKoSH-Phase wird mit einem sogenannten Quickcheck gestartet. Dieser ermöglicht anhand zahlreicher kontextbezogener Kontrollfragen einen schnellen Überblick über die Sicherheitslage.
Zu jeder Phase werden unterschiedliche Dokumente z. B. in Form von Leitlinien, Konzepten oder Beispielen bereitgestellt, die kommunal angepasst werden können. Für die ‚Phase 1' (Aufbau- und Ablauforganisation ISMS) sind dieses vor allem eine Informationssicherheitsleitlinie und Material zur Bestellung und Regelung des Aufgabenfeldes eines Informationssicherheitsbeauftragten.
Nach Ablauf der ‚Phase 1' und somit Umsetzung der obligatorischen organisatorischen Aufgaben kann der Fokus dann auf eine frei gewählte Phase gelegt werden. SiKoSH empfiehlt, mit der Mitarbeitersensibilisierung zu beginnen.
Neben IT-spezifischen Phasen, die sich z. B. mit Hardware oder mit Verfahren beschäftigen, werden auch allgemeine Aspekte wie z. B. die Gebäudesicherheit betrachtet.
Nach Durchlauf der einzelnen Prozesse stehen mit dem ‚Quickcheck 14' Prüffragen bereit, die den Erfolg der zwischenzeitig umgesetzten SiKoSH-Maßnahmen transparent machen.
Nach Dokumentation der Maßnahmen im Sicherheitskonzept, auch hierfür gibt es eine Unterstützung, beginnt der Iterationsprozess im Sicherheitszyklus wieder von vorne und ermöglicht somit Nachbesserungen und die gezielte Reaktion auf neue Bedrohungen.

Wo finde ich die SiKoSH-Dokumente?
Alle Arbeitsergebnisse sind unter www.sikosh.de abrufbar. Für Rückfragen stehen wir sehr gerne unter sikosh@komfit.de zur Verfügung.

Wie geht es weiter?
Zur Sicherung der Nachhaltigkeit und zur Gewährleistung, dass die Projektergebnisse situationsbezogen überarbeitet und fortgeschrieben werden, ist die Gründung eines schleswig-holsteinischen Forums für kommunale Informationssicherheitsbeauftragte geplant. Die Einladung zu einer konstituierenden Sitzung soll im ersten Halbjahr 2018 erfolgen.

Über die Autoren:

Werner Degenhardt ist Akad. Dir. und CIO i.R. an der LMU München und Spezialist für Human Factors in der Informationssicherheit bei Code and Concept (werner.degenhardt@codeandconcept.de).

Andreas Amann ist Behördlicher Datenschutzbeauftragter der Landeshauptstadt Kiel (andreas.amann@kiel.de).

Jan Koppelmann ist IT-Leiter der Landeshauptstadt Kiel (jan.koppelmann@kiel.de).

Frank Weidemann ist Projektleiter im Kommunalen Forum für Informationstechnik e.V. – KomFIT (frank.weidemann@komfit.de).

Technische Umsetzung der Phishing-Simulation durch Code and Concept (www.codeandconcept.de).

Angriff auf eine Kommune – Vorgehensweise von Cyber-Kriminellen

Aus den dunklen Ecken des Internets greifen sie an: Cyber-Kriminelle

Nikolaus Stapels

Sie wollen spionieren und gehen hochprofessionell und umsichtig dabei vor. Ihr Motiv ist das schnelle Geldverdienen. Der Tatort ist das Internet und die IT der betroffenen Firmen.

1. Das Verschmelzen der alten und der neuen Welt
In der alten Welt sind Kriminelle physisch in Unternehmen und öffentliche Einrichtungen eingedrungen; sie haben Alarmanlagen und Bewegungsmelder ausgeschaltet, um so eindringen zu können.
In der neuen digitalen Welt wandelt sich das Ganze: was früher der Einbruch war, ist heute der Datendiebstahl.
Und auch die Einbrecher werden immer moderner. Wo früher noch sogenannte Gaunerzinken verwendet wurden, gibt es heute Apps und Datenbanken, in denen „interessante" Häuser mit Informationen hinterlegt sind. Ein Blick vom Einbrecher vor Ort in die App und er erhält die gewünschten Informationen, bspw. ob die Eigentümer arbeiten oder ob es Hunde oder Bewegungsmelder gibt. Der klassische Einbrecher digitalisiert sich!
Und auch die Motive des Hackers wandelten sich in den letzten Jahren. Früher waren es vorwiegend allein agierende Hacker, die mit ihren Attacken Berühmtheit und Ansehen erlangen wollten und ihre Spuren nicht gut verwischten. Heutzutage schließen sich immer mehr Hacker kriminellen Organisationen an. Dort herrschen Hierarchien mit strengen Verhaltenskodexen, und nicht jeder kann dort Mitglied werden - häufig sind persönliche Kontakte wichtig. Wird man in diese Kreisen jedoch aufgenommen, verändert sich die Arbeitsweise eines Hackers drastisch.
Hat ein Hacker (oder Cracker) vorher noch zufällig seine Opfer ausgesucht und

nur kurzzeitig versucht, in fremde Systeme einzudringen, um Daten zu entwenden - gemäß dem Motto „so wenig Aufwand wie möglich" – so arbeitet er fortan bei Advanced Persistent Threat (APT)-Angriffen mit. APT bedeutet zu Deutsch „fortschrittliche andauernde Bedrohung", da die Kriminellen häufig eigene Software speziell für den Angriff nutzen. APT´s starten zielgerichtet auf ein Unternehmen. Dabei sind die Täter beharrlich und lassen sich Zeit (andauernd). Bei einem APT spielt es keine Rolle, ob das Ziel in einer Woche oder einem Jahr erreicht wird, wichtig ist nur, dass es erreicht wird. Keine Behörde, Branche oder Unternehmen ist gegen solch eine Attacke zu 100% geschützt. In der Regel sehen es die Cyber-Kriminellen dabei auf Ziele ab, die ihnen einen hohen Profit bringen.

2. Wie gehen Cyber-Kriminelle vor?

2.1 Auswahl eines geeigneten Opfers (Phase I)

Anhand eines Angriffs auf eine öffentliche Einrichtung wird aufgezeigt, wie Cyber-Kriminelle vorgehen:

Eine Kommune in Süddeutschland soll angegriffen werden, es geht darum, Informationen von Bürgern zu erhalten.

Ein Grund, warum öffentliche Einrichtungen gerne angegriffen werden, sind Kundendatensätze. Diese können im Darknet ca. 30€ je Datensatz bringen, wenn folgende Daten gestohlen werden: Name, Adresse, Geburtsdatum, Kommunikations- und Bankdaten.

Der Ablauf des Angriffs lässt sich auch auf ein kleines Unternehmen und eine kleine Kommune anwenden.

Zu unserer Beispielkommune.

Es ist gerade 10:17 Uhr – die meisten Mitarbeiter sind bereits am Arbeitsplatz, checken Emails, führen Telefonate, nehmen Anfragen entgegen… ein ganz normaler Arbeitsalltag. Sie wissen nicht, dass sie soeben nach ausgiebiger Recherche als DAS lukrative Ziel für einen Angriff ausgewählt wurden… der Hacker „L3g!0n" (ausgesprochen Legion) lächelt zufrieden und nickt… er hat sein nächstes Opfer gefunden…

2.2 Auswahl seines Spezialistenteams „Alpha-H4ck3r" (Phase II)

Nachdem das Ziel identifiziert und analysiert wurde, beginnt umgehend Phase II.

„L3g!0n" stellt sich seine Crew aus Spezialisten zusammen, diese lassen sich auf speziellen Webseiten im Darknet finden. Für dieses Ziel werden mehrere Spezialisten benötigt, unter anderem mehrere auf Social Engineering spezialisierte Hacker. Diese sollen durch eine zwischenmenschliche Beeinflussung die Opfer u.a. dazu bewegen, vertrauliche Informationen preiszugeben. Daneben werden spezialisierte Hacker für die IT-Landschaft der anzugreifenden Kommune benötigt.

Da „L3g!0n" sich bereits in einschlägigen Foren im Darknet bewegt, findet er zügig seine ausgewählten Hacker, um dieses Projekt anzugehen. Normalerweise braucht man persönliche Bürgen, um in solche Foren zu gelangen – die braucht er schon lange nicht mehr… er ist bereits bekannt, und die ausgewählten Spezialisten, die bereits mehrere Jobs für ihn erledigt haben, folgen sofort seinem Aufruf. Da er allerdings noch ein paar neue Spezialisten benötigt, checkt er bei den registrierten Hackern die Skill-Levels, welche ihm aussagekräftig zeigen, welche Fähigkeiten der jeweilige Hacker vorweisen kann. Die Skill-Levels steigen nach erfolgreichen Aufträgen und werden in der Agenda aufgelistet. Je mehr und kompliziertere Fälle auf der Agenda auftauchen, desto besser und herausfordernder werden die nächsten Aufträge für einen Hacker… und besser bezahlt, in der Regel mit Bitcoins. Bitcoins, ein dezentrales Zahlungssystem für eine digitale Währung. Der Vorteil für die Hacker ist die Anonymität bei der Zahlung. Es ist mit den richtigen Voraussetzungen nicht mehr möglich, den Sender und Empfänger der Transaktion zu ermitteln. Dies bietet einen besseren Schutz der Anonymität als eine konventionelle Überweisung.

2.3. Das Sammeln von Informationen (Phase III)

Nur kurze Zeit später steht seine Spezialisten-Crew „Alpha-H4ck4r" für dieses Projekt fest. Es beginnt die Phase 3, die Social Engineere machen sich ans Werk. Sie recherchieren über die Kommune alles, was sie über das Opfer im Internet finden können. Hierbei erhalten sie, u. a. über die Webseite, Informationen über die Mitarbeiter. Es werden gezielt die Social Media Plattformen nach Mitarbeitern durchsucht, dabei werden z. B. bei „Xing" mehrere falsche Profile generiert und genutzt, damit der Besuch des Hackers nicht zu sehr auffällt. Durch diese Art der Informationsgewinnung erhalten die Angreifer wertvolle Informationen über die Firma und deren Mitarbeiter.

Es konnten u. a. folgende interessante Informationen über die Firma gesammelt werden:

- mehrere Mitarbeiter sind unzufrieden, haben sich negativ über den Arbeitgeber geäußert und Lebensläufe für Recruiter veröffentlicht;
- eine Mitarbeiterin hat Selfies von sich am Arbeitsplatz gemacht und auf einer Social Media Plattform veröffentlicht - im Hintergrund sind Login Daten auf Zetteln zu lesen;
- es gibt mehrere Firmen, die die Kommune als Referenzkunden hinterlegt haben;
- für mehrere Standorte werden Mitarbeiter gesucht - hier besteht die Möglichkeit eines Praktikums;
- Hobbys und Freizeitgestaltung mehrerer Führungskräfte konnten ermittelt werden;
- Auf Bildern ist erkennbar, dass Mitarbeiter Funkmäuse für Ihre Dienstlaptops nutzen;
- Es gibt mehrere Bilder aus den Firmengebäuden, auf denen sind Kopierer zu sehen mit dem Namen des für die Wartung zuständigen Unternehmens.

Akribisch sammelt „Alpha-H4ck3r" alle Informationen und setzt so in einer Übersicht das Informations-Puzzle zusammen – Informationen über verschiedene Führungskräfte, über den Aufbau von Abteilungen und welche Mitarbeiter diese umfassen. Nachdem die ersten Vorbereitungen abgeschlossen sind, macht sich das Hacker-Team nun Gedanken, welche Angriffsmethode und Vorgehensweise am effektivsten sind.

2.4 Die Auswahl der Angriffsstrategie (Phase IV)

Üblicherweise wird bei solch einem Angriff eine nicht öffentlich bekannte Sicherheitslücke im Betriebssystem oder der genutzten Software ausgenutzt; dies nennt sich Zero-Day-Angriff. Solche Zero-Day-Exploits können im Darknet gekauft werden. Ein Exploit ist ein Programm bzw. ein Programmcode, mit dessen Hilfe sich die Hacker einen Zugang zu Systemen verschaffen; solch ein Exploit kann mit der Brechstange eines Einbrechers verglichen werden. Mit beiden kann der Einbrecher sich Zugang zu fremdem Eigentum verschaffen. Der große Vorteil bei der Nutzung eines Zero-Day-Exploits ist es, dass ein Unternehmen sich nicht gegen etwas schützen kann, das allgemein nicht bekannt ist.

Während „Alpha H4ck3r" noch Informationen über das Unternehmen sammelt, wird der Angriffscode bereits von unserem Hacker „L3g!0n"geschrieben und für verschiedene Formate, wie PDF, Word, Excel etc. vorbereitet.

Phase IV: Es werden nun verschiedene Angriffswege bzw. verschiedene Szenarien durchgespielt, dazu werden u.a. auch die Erkenntnisse der Social Engineere herangezogen.

Folgende Angriff-Szenarien sind u. a. möglich:

- Es wurde herausgefunden, dass einige Führungskräfte E-Zigaretten rauchen; dies war u. a. auf Bildern und den beigetretenen Gruppen auf Social-Media-Plattformen ersichtlich; der Angriff könnte hier über infizierte E-Zigaretten erfolgen, welche über den USB-Port des Dienst-Laptops geladen werden können. Die Zigaretten werden als Geschenk an die Führungskräfte verschickt.

- Die Führungskräfte haben feste Parkplätze, verschiedene „normale“ Mitarbeiter haben sich darüber in sozialen Medien aufgeregt, dass diese nicht von den Mitarbeitern genutzt werden dürfen, auch nicht, wenn die Führungskraft auf Dienstreise/im Urlaub ist. Da bekannt ist, auf welchen Parkplätzen die Führungskräfte parken, kann leicht ein Angriff über ausgelegte USB-Sticks initiiert werden.
  Neben der Fahrertür könnte ein USB-Stick mit der Aufschrift „Mitarbeiter Abbaupläne“, „Gehaltsliste“, „Bonifikationen“ platziert werden.
  Durchschnittlich sieben von zehn neugierigen Mitarbeitern schauen nach, was sich darauf befindet, bevor der Stick in der IT-Abteilung landet.
- Es könnten Werbegeschenke an Abteilungsleiter verschickt werden, diese könnten u. a. Computer-Mäuse oder USB-Sticks mit Wanzen sein, welche sich aktivieren, sobald jemand spricht; das gesprochene Wort wird dann automatisch in Text umgewandelt und gezielt nach bestimmten Wörtern durchsucht.
- Es werden neue Mitarbeiter gesucht, es bestünde die Möglichkeit, vorab ein Praktikum zu absolvieren. Getarnt als Praktikant könnte jemand dann Schadsoftware einschleusen.
- Neben der Möglichkeit, jemanden persönlich einzuschleusen, gibt es auch die Option, eine Bewerbungsmail mit schadhafter Software zu verschicken; das Unternehmen wird dies i.d.R. kennen, dennoch wird diese gleiche Angriffsmethode angewandt, weil immer wieder Mitarbeiter durch fehlende Konzentration, Stress oder Zeitdruck darauf hereinfallen.
- Über das sogenannte „Spear Phishing“ könnten ausgewählte Mitarbeiter durch den Erhalt von auf sie zugeschnittenen Nachrichten angegriffen werden. Das Spezialistenteam hat bspw. herausgefunden, dass einige Mitarbeiter begeisterte Thailand-Urlauber sind, diese würden dann in der nächsten Zeit gezielt Informationen zu Thailand mit Geheimtipps erhalten. Nachdem die Opfer nach einiger Zeit und einigen Mails später Vertrauen gefasst hätten, würde der zweite Schritt folgen – diese könnten, nachdem sie sich mit einem Passwort registriert haben, durch die Eingabe von Informationen eine Thailandreise gewinnen. Das Hacker-Team weiß, dass viele Anwender für mehrere Anmeldungen dasselbe Passwort nutzen und missbraucht diesen Umstand nur zu gerne. Im dritten Schritt sollten die Opfer dann auf einen Link klicken, um Angebote für eine Thailandreise zu erhalten - mit 50% Nachlass. Durch den Besuch der Webseite wird dann der Schadcode im Hintergrund runtergeladen.
- Durch die Nutzung von Funkmäusen, sogenannten „MouseJacks“, könnten PC, Linux oder Mac angegriffen werden; und dieses auch, wenn der Rechner nicht mit dem Internet verbunden ist. Bei dem Angriff würden die Funksignale der Maus manipuliert. Wenn ein Nutzer einen linken Mausklick tätigte, dann übertrüge die Maus ein Funksignal zum Computer „linker Mausklick“. Und genau hier würde der Angriff ansetzen, das Signal würde überlagert und ein Schadcode statt dessen übertragen. Der Computer führt anschließend den Befehl aus. Die dafür notwendigen Werkzeuge kosten ca. 30 €.
- Auf Bildern vom Arbeitsplatz konnte der Dienstleister für die Wartung der Kopierer identifiziert werden, „Bürosysteme S+N“ (Name geändert). Durch die Fälschung von Ausweisen könnten „Techniker“ in die Firma gelangen, um die Festplatten aus den Geräten auszutauschen, welche i.d.R. alles speichern, was jemals kopiert, gedruckt oder gefaxt wurde. Dadurch könnten neue Einblicke in die Firma gewonnen werden.

Dies ist nur eine kleine Auswahl von Angriffsstrategien, welche das Hacker-Team „Alpha-H4ck3r“ in Erwägung zieht und zeigt nur oberflächlich auf, welche Möglichkeiten es gibt, um in eine Firma einzudringen.
Um die Sicherheitsabwehr von Firmen zu überwinden, werden in der Regel mehre Angriffswege parallel durchgeführt. Bei solch einem Angriff ist es nicht wichtig, wie lange der Angriff dauert, einzig die Erreichung des Ziels steht im Vordergrund. Deshalb sind diese zielgerichteten Angriffe so schwer abzuwehren.

2.5 Das Einschleusen des Schadcodes (Phase V)

Um den Erfolg versprechendsten Weg zu finden, zieht unser Hacker „L3g!0n“ nun zwei externe Berater hinzu und diskutiert mit diesen und seinem bereits vorhandenen Team „Alpha-H4ck3r“ die Vielzahl von Möglichkeiten, die sich ihnen eröffnet haben. Nach einigen Stunden wurden alle Vor- und Nachteile der einzelnen Strategien gegeneinander abgewogen und bezüglich der Effektivitätswahrscheinlichkeit analysiert. Ihre Strategie steht nun fest und der Angriff kann beginnen.

Phase V: Es wird versucht, den Schadcode in die Zielumgebung zu liefern.

Die einfachste und effektivste Möglichkeit, um in die Systeme einzudringen, ist das Einbeziehen der Mitarbeiter des Unternehmens. Dabei werden die menschlichen Schwächen - u. a. Neugierde und Stress - ausgenutzt.

Da neues Personal gesucht wird, verschickt „Alpha-H4ack3r“ zunächst die „Bewerbungsmail“ mit einem Link zur Dropbox. Da diese Angriffsmethode vielen Unternehmen heutzutage jedoch bekannt ist, hat dieser Angriff auf den ersten Blick keinen großen Erfolg. Dennoch werden mehrere hochwertige Bewerbungen verschickt, zum einen in der Hoffnung, dass doch ein unachtsamer Mitarbeiter den Anhang öffnet und somit den Schadcode runterlädt, zum anderen sollen diese die Mitarbeiter und die IT-Abteilung konditionieren. So wird kontinuierlich jeden Tag ein schadhaftes Word Dokument verschickt; im Unternehmen wissen nun alle, dass dies sofort gelöscht werden muss.
Die Anzahl der Mails erhöht sich im Laufe der Zeit auf 50 schadhafte Word-Bewerbungen pro Woche. Während sich alle auf die Word-Bewerbungen konzentrieren, kommt eine Bewerbung per PDF. Diese ist erst einmal nicht schädlich, aber wenn der Nutzer auf den Link in der PDF klickt, dann lädt sich auch hier die Schadsoftware herunter und der Rechner ist infiziert.
Die Schadsoftware „versteckt“ sich dann erst einmal im System und wird zu einer bestimmten Uhrzeit, z.B. erst am Samstag um 20 Uhr gestartet, wenn kaum noch ein Mitarbeiter im Unternehmen ist.
Durch einen falschen Klick in solch einer PDF-Bewerbung konnte von „Alpha-H4ck3r“ mehrere verschiedene Remote-Access-Trojaner (RAT) eingeschleust werden, welche Hintertüren öffneten, um Rechner fernsteuern zu können. Damit die vorhandene Antiviren-Software ausgetrickst werden kann, wird der Trojaner mit einer Tarnkappe versehen, dem „Rootkit“, mit deren Hilfe der Trojaner tief im Betriebssystem versteckt wird.
In den ersten sechs Wochen konnten darüber hinaus mehrere Mitarbeiter auf eine Webseite gelockt werden, die Bali-Reisen mit 50% Nachlass verspricht. Diese haben sich dort registrieren müssen, so dass „Alpha-H4ck3r“ mit den gewonnenen Daten unter anderem in die privaten Mailpostfächer eindringen konnte. Und das mit den berechtigten Login-Daten, da einige Mitarbeiter tatsächlich für verschiedene Webseiten dasselbe Passwort genutzt haben.
Da einzelne Mitarbeiter sich berufliche Mails an ihr privates Mailpostfach weitergeleitet hatten, konnten auch so noch weitere interne Informationen über das Unternehmen gesammelt werden. Besonders bemerkenswert – und von unserem Hacker-Team mit belustigtem Kopfschütteln festgestellt – war ein Mitarbeiter, der im „Media Center“ ein Word Dokument mit dem Namen „Passwortliste – Geheim.docx“ hochgeladen hatte.
Somit offenbarten sich Alpha-H4ck3r“ alle seine privaten und beruflichen Passwörter, die jeweiligen Zahlencodes für die

Tiefgarage und verschiedene Bereiche im Unternehmen.
Zu „L3g!0n“s voller Zufriedenheit werden nun bereits seit Tagen über den eingeschleusten Trojaner wertvolle Informationen gesammelt. Diese Daten werden jedoch nicht sofort ausgeschleust, sondern erst einmal zentral im gehackten Unternehmen gesammelt.
Des Weiteren wurde von „L3g!0n“ ein deutscher Hacker beauftragt, sich bei dem Unternehmen zu bewerben und dort ein Praktikum zu beginnen. Das Einschleusen des Hackers mit gefälschten Unterlagen und Social-Media-Profilen war kein Problem. Diesem Mitarbeiter wurden schon während des Praktikums als Entwicklungsinformatiker weitere Zugriffsrechte gewährt, so dass er mit seiner eigenen Anmeldung bereits tiefergehende Informationen zu verschiedenen Projekten sammeln konnte.
Ausgestattet mit mehreren Hardware-Keyloggern - einer Art USB-Stick, der zwischen Tastatur und Computer gesteckt wird und alles speichert, was geschrieben wird - konnten von Mitarbeitern und Hauptabteilungsleitern sämtliche Login-Daten mitgelesen werden. Das Abrufen der Passwörter funktioniert per Funk über ein Tablet, das der deutsche Hacker mit in die Firma gebracht hat.
In der Mittagspause konnte sich dieser Hacker mit den gewonnenen Daten ohne Probleme als Hauptabteilungsleiter einloggen und Daten kopieren. Bei den Hauptabteilungsleitern waren die USB-Ports gegenüber den normalen Arbeitnehmern nicht gesperrt, so konnten Daten auf eine externe Festplatte kopiert werden.
Nach ein paar Tagen brach der Hacker das Praktikum dann plötzlich ab, mit der Begründung, dass er etwas Besseres in seiner Nähe gefunden habe.
Über die Hintertür im System konnte währenddessen das Hacker-Team Daten im System sammeln und für das Ausschleusen vorbereiten. Dazu wurden die Daten in eine Rar-Datei gepackt und verschlüsselt. Am darauffolgenden Wochenende wurden dann die Dateien in kleineren Paketen auf einen Server im Ausland hochgeladen.
Nachdem die Daten erfolgreich über mehrere Server anonymisiert werden konnten, sind diese nun im Hauptquartier angekommen und können von unserem Hacker gesichtet werden. Zufrieden stellt er fest, dass es sich bei den Projekten u. a. um die Integrierung neuer Hardware für verschiedene Bundeswehrstützpunkte im In- und Ausland handelt.

2.6 Das Verwischen von Spuren (Phase VI)

Phase VI: In der vorletzten Phase werden von dem Spezialisten bei „Alpha-H4ck3r Z“ vorhandene Beweise auf dem infizierten System vernichtet. Das Hauptziel ist es, dass alle eventuellen Spuren des Angriffs auf dem System entfernt werden. Dazu wird u. a. Software genutzt, die automatisch Protokolle und Software vom System löscht. Auch manuell wird noch vieles gelöscht und verwischt. Im Anschluss werden dann noch mehrere Hintertüren eingebaut, für den Fall, dass das Team in der Zukunft nochmals in das System eindringen möchte.

2.7 Der Verkauf der Daten (Phase VII)

Phase VII: Unser Hacker „L3g!0n“ verkauft nun die Daten, was sich leichter anhört als es in Wirklichkeit ist. Um in diese speziellen Foren zu gelangen, musste er sich seinerzeit mehreren Interviews mit verschiedenen Mitgliedern stellen. Der Zugang zum gewünschten Forum war kostenpflichtig und kostet für 12 Monate 12.000 $. Dadurch hat aber jedes Mitglied die Möglichkeit, die passenden Ansprechpartner für seine Produkte zu finden. Es werden dort neben Firmengeheimnissen auch Zugänge zu Bankkonten, PayPal, etc, angeboten.
Der Aufbau der Seite ähnelt einer Kleinanzeigen-Seite, es wird ein kostenloses Inserat eingestellt sowie ein sehr geringer Teil der Daten bzw. eine Übersicht der vorhandenen Daten. Aufgrund des Namens vom gehackten Unternehmen haben sich sehr schnell interessierte Käufer gemeldet; vorwiegend aus Russland und China. Zur besseren Qualitätssicherung wurde den interessierten Käufern ein Einblick in die Daten gewährt; dies geschieht durch eine Remote-Verbindung, so dass keine Daten übertragen werden, sondern der Käufer sich die Daten lediglich ansehen konnte wie bei einer TeamViewer-Sitzung. Nachdem die Daten gesichtet wurden, können nun Gebote abgegeben werden….
Die Verhandlungen dauerten insgesamt eine Woche und die Daten konnten letztendlich für 3,4 Mio. $ verkauft werden.
Das Team hat ungefähr 150 Tage in das Projekt investiert. Insgesamt 10 engagierte Hacker waren im Kern-Team von „Alpha-H4ck3r“ tätig und haben in der Zeit zusammen 750.000 $ zuzüglich einer Bonifikation von 10% des Erlöses verdient; jeder Hacker hat somit insgesamt 109.000 $ verdient.
Für externe Berater und den eingeschleusten Hacker wurden 20.000 $ bezahlt
Der Verdienst von „L3g!0n“ beläuft sich somit auf 2.290.000 $ in „nur“ 150 Tagen.
„L3g!0n“ arbeitet mit seinem Team bereits am nächsten Projekt – voraussichtlicher Erlös zwischen 6,5 und 8,25 Mio. $.

3. Fazit

Daten sind der Rohstoff des 21. Jahrhunderts. Im Untergrund blüht der Handel mit hochsensiblen Daten und Schadsoftware; dabei wird der Einstieg für Kriminelle immer einfacher. Durch verschiedene Foren im Darknet können Cyber-Kriminelle mit relativ wenig Aufwand viel Geld verdienen.
Wenn man von „Hackerangriffen“ und „Cybercrime“ hört, dann denken viele sofort an den typischen „Nerd“, der im Keller sitzt und das Tageslicht scheut.
Um als Täter aktiv mitmachen zu können, bedarf es weder tiefergehenden Wissens noch Programmierkenntnisse. Jeder kann theoretisch innerhalb von 72 Stunden eine kriminelle Laufbahn starten. Die nötigen Tools und Anleitungen finden sich schnell in Foren und auf „Youtube“.
Darüber hinaus ist die Größe einer Kommune kein Indiz dafür, ob diese für einen Hacker interessant ist. Vor allem kleine sind bei Hackern sehr beliebt, da es dort – so wird vermutet – weniger IT-Sicherheit gibt und viele ungeschützte „vermeintlich nicht wertvolle“ Daten.
Um sich dagegen zu schützen, müssen u.a. die Mitarbeiter sensibilisiert werden, denn sie müssen wissen, wie Cyberkriminelle vorgehen und was dies für den Arbeitgeber bedeuten kann.
Des Weiteren sollten Kommunen die Absicherung der Restrisiken durch Versicherungen berücksichtigen, diese können keinen Cyberangriff verhindern, jedoch die finanziellen Folgen abfedern. Hier lohnt es sich, mit einem Versicherer über mögliche Konzepte zu sprechen.

Über den Autor:

Nikolaus Stapels, geboren 1979, ist selbständiger VdS-Fachberater für Cyber-Security, zertifizierter IT-Risk-Manager sowie Information-Security-Officer gemäß ISO 21001 und BSI Grundschutz. Seit vielen Jahren konzentriert er sich auf das Thema IT-Sicherheit in Klein- und mittelständischen Unternehmen und Kommunen.
Er unterstützt und berät Unternehmen und Kommunen deutschlandweit bei der Entwicklung und Umsetzung einer Cyber-Security-Strategie; dazu zählt u. a. die Absicherung der Cyber-Risiken und die Sensibilisierung von Mitarbeitern. In zahlreichen Vorträgen zeigt er diesen auf, u. a. mithilfe von Live-Hacking, welche Gefahren im Internet lauern.

Integriertes Antrags- und Fallmanagement – kostenlose Online-Lösungen für die Kommunen in Schleswig-Holstein

Oliver Maas, Koordinator des KomFIT

Das Onlinezugangsgesetz (OZG) vom 14.08.2017 verpflichtet Bund und Länder, ihre Verwaltungsleistungen bis zum 31.12.2022 auch elektronisch über sog. Verwaltungsportale anzubieten. Über die Länder trifft diese Verpflichtung auch die Kommunen, die in vielen Fällen für die Durchführung der bundes- und landesrechtlichen Regelungen zuständig sind. Bundesweit wurden über alle Verwaltungsebenen hinweg vorerst 575 Verwaltungsleistungen identifiziert, die künftig auch elektronisch anzubieten sind.

Die Umsetzung des OZG stellt für Bund, Länder und Gemeinden eine große Herausforderung dar, die von einer einzelnen Kommunalverwaltung alleine nicht gemeistert werden kann. Daher wird der Bund z. B. die notwendige Softwarelösung für die Verknüpfung der Verwaltungsportale von Bund und Ländern zu dem vorgeschriebenen Portalverbund zur Verfügung stellen. Der Portalverbund stellt sicher, dass Nutzer über alle Verwaltungsportale von Bund und Ländern einen barriere- und medienbruchfreien Zugang zu elektronischen Verwaltungsleistungen dieser Verwaltungsträger erhalten. In Schleswig-Holstein wird die Verknüpfung voraussichtlich über den Zuständigkeitsfinder (www.zufish.schleswig-holstein.de) erfolgen, in welchem die Kommunalverwaltungen dann nicht mehr nur die Informationen und Links für Online-Verfahren zu den EG-Dienstleistungsrelevanten Leistungen, sondern für alle ihre Verwaltungsleistungen pflegen müssen. Damit wird gewährleistet, dass der Online-Service für die Anmeldung eines Hundes zur Hundesteuer bei der Gemeinde X auch über ein Internetportal des Bundes, jedes Landes und jeder Kommune direkt gefunden und aufgerufen werden kann.

Neben dem Zuständigkeitsfinder und der Anbindung an den Portalverbund stellt das Land für die Kommunen in Schleswig-Holstein zahlreiche weitere Komponenten seiner E-Government-Infrastruktur kostenlos für die Nutzung zur Verfügung. Dazu gehören insbesondere interoperable Servicekonten, die künftig auch die Anmeldung bei Diensten des Bundes oder anderer Länder ermöglichen werden sowie Online-Bezahlfunktionen, die Nutzung der Online-Ausweisfunktion des Personalausweises und das von den Kommunalen Landesverbänden und dem Einheitlichen Ansprechpartner Schleswig-Holstein AöR (EA-SH) initiierte intergierte Antrags- und Fallmanagement (iAFM) als wichtigstes Werkzeug zur Bereitstellung von Online-Antragsverfahren. Darüber hinaus übernimmt das Zentrale IT-Management des Landes die landesweite Koordinierung der Umsetzung des OZG beim Land und den Kommunen.

Auch wenn das Land die technische Infrastruktur für die Umsetzung bereitstellt, die Kosten für deren Betrieb und auch die Gesamtumsetzungskoordinierung für das OZG übernimmt, wird die fachliche Arbeit für die Bereitstellung der künftig benötigten Online-Dienste im Wesentlichen eine Aufgabe der Kommunalverwaltungen sein.

Dieses ist aber für die Kommunen in Schleswig-Holstein allerdings nichts Neues. Denn seit 2015 bereits, also zwei Jahre vor dem Inkrafttreten des OZG, arbeiten das Kommunale Forum für Informationstechnik (KomFIT) und der EA-SH mit dem Projekt iAFM / iWOBIS an dem Ziel, alle geeigneten Verwaltungsleistungen der schleswig-holsteinischen Kommunalverwaltungen und des EA-SH online zur Verfügung zu stellen. Nach dem Prinzip einige für alle sind in den vergangenen Jahren zahlreiche Lösungen entstanden, die von allen Kommunalverwaltungen im Land kostenfrei mitgenutzt werden können. Hierfür haben einige Verwaltungen die fachliche Vorarbeit geleistet und die erforderlichen Prozesse und Informationen zusammengetragen. Aus dieser Vorarbeit werden dann die Online-Antragsverfahren durch die Kommune selbst, den EA-SH, eine andere Verwaltung oder Dataport modelliert. Anschließend wird die Lösung durch fachliche Mitstreiter getestet und freigegeben. Danach steht sie allen Kommunalverwaltungen zur Mitnutzung zur Verfügung. Für die Mitnutzung kann die Lösung mit dem Wappen / Logo der eigenen Verwaltung versehen und die Farbgestaltung an den eigenen Internetauftritt angepasst werden.

Die Übermittlung der Antragsdaten an die Verwaltungen, die alle oder einzelne iAFM-Verfahren nutzen, erfolgt sicher über das Landesnetz, wahlweise als E-Mail an ein Funktionspostfach oder über den aus dem Meldewesen bekannten Nachrichtenbroker. Dieser Weg erlaubt auch die direkte Übergabe der Daten an Fachver-

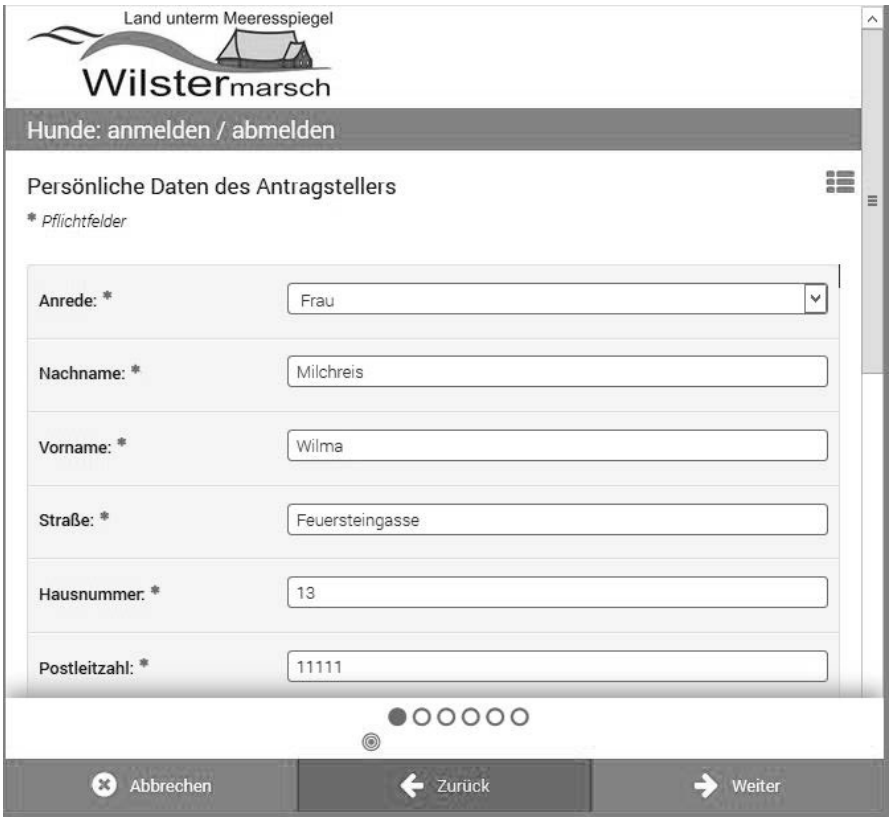


Abbildung: iAFM-Verfahren auf einem Tablet

fahren innerhalb der Verwaltung und damit die medienbruchfreie Weiterverarbeitung. Selbstverständlich sind die Lösungen mit allen Endgeräten vom PC bis zum Smartphone uneingeschränkt nutzbar. Bei Bedarf kann die Online-Ausweisfunktion des Personalausweises und des elektronischen Aufenthaltstitels zur Identifizierung der Antragsteller genutzt werden und eine Online-Bezahlfunktion zur Verfügung gestellt werden.

Durch die Nutzung der iAFM-Verfahren kann eine Kommunalverwaltung bereits heute ein vielfältiges Online-Angebot für Bürgerinnen, Bürger und Unternehmen zur Verfügung stellen. Damit wird die Verwaltung in der Öffentlichkeit als moderner Dienstleister wahrgenommen. Gleichzeitig können die internen Prozesse durch die verbesserte Datenqualität der online gestellten und validierten Anträge und ggf. durch die automatisierte Weiterverarbeitung im Fachverfahren optimiert werden. Außerdem können alle iAFM-Verfahren auch auf Bürgerterminals in der Verwaltung oder an anderen geeigneten Orten angeboten werden. So wird z. B. auch Bürgerinnen und Bürger ohne eigenes Lesegerät ermöglicht, die Online-Ausweisfunktion des Personalausweises zu nutzen, wenn dieses für einzelne Verfahren erforderlich ist.

Für Bürgerinnen, Bürger und Unternehmen ist die Verwaltung über die iAFM-Verfahren jederzeit erreichbar. Bei der Online-Antragstellung können Sie sich auf eine sichere und nachvollziehbare Übermittlung verlassen, das Endgerät ihrer Wahl benutzen und sogar erforderliche Anlagen, die bisher nur in Papierform vorliegen, mit dem Smartphone oder Tablet scannen und dabei direkt zum Antrag hochladen. Auch kann ein Bürgerterminal als „Fast Lane“ dienen und z. B. bei starkem Publikumsandrang eine Antragstellung ohne lange Wartezeit ermöglichen.

Die bereits für Kommunen und den EA-SH verfügbaren iAFM-Verfahren sowie die Lösungen, die momentan entwickelt werden, finden Sie im Anschluss an diesen Beitrag.

Ein Projekt wie das iAFM / iWOBS lässt sich nur mit kompetenten und verlässlichen Partnern realisieren. Die Projektleitung liegt dabei beim KomFIT. Das Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung stellt die E-Government-Basisdienste für die Kommunen zur Verfügung und finanziert die Weiterentwicklung der Basisdienste sowie die Neu- und Weiterentwicklung von iAFM-Verfahren durch Dataport. Die Kommunalen Landesverbände finanzieren Schnittstellen und die Verfahrensentwicklung durch weitere externe Partner. Der EA-SH hat die Entwicklung und Pflege der iAFM-Verfahren übernommen, die in seinen fachlichen Zuständigkeitsbereich fallen. Der Kreis Nordfriesland entwickelt und pflegt ausgewählte iAFM-Verfahren, insbesondere aus dem Aufgabenbereich der Kreise. Dataport leistet den technischen Betrieb der Basisdienste des Landes und entwickelt sie weiter. Außerdem entwickelt und pflegt Dataport iAFM-Verfahren im Auftrag des Projektes. Die Erweiterung der iAFM-Verfahren um interne Workflows, die Anbindung von Contentmanagementsystemen und Fach-verfahren außerhalb des Landesnetzes hat sich die Netz-Werkstatt auf ihre Fahnen geschrieben.

Um möglichst schnell und am Bedarf der Bürgerinnen und Bürger, Unternehmen und Verwaltungen orientiert alle benötigten und geeigneten Verwaltungsleistungen online zur Verfügung stellen zu können, baut das KomFIT künftig eine über die bisherigen Projektpartner hinausgehende Community auf. Ihre Mitglieder verpflichten sich, z. B. Entwickler und fachliche Ansprechpartner zur Verfügung zu stellen, Fachverfahrensanbindungen herzustellen oder alle innerhalb der Community entwickelten Verfahren selbst zu nutzen. Alle Communityergebnisse werden entsprechend den Nutzungsbestimmungen des Landes allen Trägern öffentlicher Verwaltung zur Mitnutzung zur Verfügung gestellt. Damit leisten die Kommunen einen wichtigen Beitrag zur Umsetzung des OZG in Schleswig-Holstein.

Wenn Sie Fragen zum Projekt haben, ein iAFM-Verfahren mitnutzen, Vorschläge für weitere Lösungen einbringen oder die Entwicklung weiterer Lösungen fachlich unterstützen möchten, setzen Sie sich einfach per E-Mail iafm_iwobis@komfit.de oder telefonisch mit Angela Köhnke-Treptow (Tel. 0431/570050-84) oder Oliver Maas (Tel. 0431/570050-81) in Verbindung. Aktuell wird Unterstützung für ein iAFM-Verfahren für die jährliche Meldung zur Zweitwohnungssteuer gesucht, dessen Umsetzung in Kürze starten wird.

unter https://www.komfit-blog,de/iafm-iwobis/ finden Sie einen Gesamtüberblick zum Projekt, eine laufend fortgeschriebene Übersicht der verfügbaren und in der Entwicklung befindlichen Verfahren sowie die notwendigen Schritte, um iAFM-Verfahren mitnutzen zu können.

Bereits verfügbare iAFM-Verfahren

- Antrag auf Auskunft aus dem Baulastenverzeichnis
- Aufstellung von Verkehrszeichen
- Gutachterausschuss – Online-Befragung zu einem Kaufvertrag durchführen
- Gutachterausschuss – Online-Befragung zu einem Kaufvertrag initiieren
- Hunde: anmelden / abmelden
- KFZ: Wiederzulassung
- Kleiner Waffenschein
- Monitoringbericht Ausgleichsflächen
- Nachreichen von Dokumenten
- Onlinebewerbung
- Pflegegradrechner – Ermittlung der Pflegegrade für Kinder nach § 15 SGB
- Pflegegradrechner – Ermittlung der Pflegegrade nach § 15 SGB
- Stellenausschreibung
- Antrag auf Erteilung einer Erlaubnis gemäß § 7 Sprengstoffgesetz (SprengG)
- Antrag auf Erteilung einer Erlaubnis nach § 33c Gewerbeordnung (GewO)
- Antrag auf Erteilung einer Erlaubnis nach § 33i Gewerbeordnung (GewO) zum Betrieb einer Spielhalle
- Antrag auf Erteilung einer Erlaubnis zur Ausübung eines Pfandleih-Gewerbes gem. § 34 Gewerbeordnung (GewO)
- Antrag auf Erteilung einer gaststättenrechtlichen Erlaubnis
- Antrag auf Erteilung einer Waffenherstellungs-, Waffenhandels- und Stellvertretererlaubnis nach § 21 Abs. 1 WaffG
- Antrag auf Festsetzung eines Wochenmarktes gem. § 69 GewO i. V. m. § 67 Gewerbeordnung (GewO)
- Anzeige des Überlassens einer Schusswaffe gemäß § 34 Abs. 2 S. 2 Waffengesetz (WaffG)
- Anzeige eines Wanderlagers gemäß § 56a Gewerbeordnung (GewO)
- Befähigungsschein nach § 20 Sprengstoffgesetz (SprengG)
- Einheitlicher Ansprechpartner – Anerkennung von Berufsqualifikationen
- Erlaubnis nach §§ 34c-i Gewerbeordnung (GewO)
- Erteilung, Erweiterung, Verlängerung einer Reisegewerbekarte (auch Gewerbelegitimationskarte)
- Erwerb und Umgang mit explosionsgefährlichen Stoffen
- Gaststätten-Gestattung
- Gewerbeabmeldung
- Gewerbeanmeldung
- Gewerbeummeldung
- Handwerksrolle: Eintragung
- Handwerksrolle/Gewerbeverzeichnisse: Löschung von Eintragungen
- LKW-Fahrverbot an Sonn- und Feiertagen sowie an Samstagen in der Hauptferienzeit: Ausnahmegenehmigung
- Online Anfrage
- Private Feuerwerke: Ausnahmegenehmigung
- Schaustellung von Personen – Erlaubnis
- Single Point of Contact – Recognition professional qualifications
- Sondernutzung des öffentlichen Straßenraums

iAFM-Verfahren in Entwicklung

- An- / Abmeldung Hundesteuer mit Fachverfahrensanbindung + ePayment
- Antrag auf Auskunft aus dem Baulastenverzeichnis mit GIS-Einbindung
- Anzeige von Erdaufschlüssen
- Assistent zur Beantragung von Arbeitslosengeld, SGB II
- Hilfe zur Pflege

- Infektionsmeldung
- Kartenführerschein (Umtausch)
- Kfz-Außerbetriebsetzung
- Kfz: Adressänderung, Neuzulassung, Umschreibung
- Tierbestandsanzeige
- universeller Bezahlassistent
- Touristenvisum: Verpflichtungserklärung für die Einladung eines Ausländers

Rechtsprechungsberichte

VK Rheinland-Pfalz:
Kommunale
Wohnungsbaugesellschaften
sind öffentliche Auftraggeber

Die Vergabekammer Rheinland-Pfalz hat mit Beschluss vom 21. Dezember 2017 - VK 1-24/17 - die öffentliche Auftraggeberschaft kommunaler Wohnungsbaugesellschaften bestätigt und Folgendes festgestellt:

1. Bei der Auslegung des Tatbestandsmerkmals „im Allgemeininteresse liegende Aufgaben" ist der im Gesellschaftsvertrag verankerte Zweck der Gesellschaft maßgebend.
2. Soziale Wohnraumförderung und Wohnraumbewirtschaftung dienen ebenso wie die Verwaltung kommunalen Immobilienvermögens dem Allgemeininteresse.

In dem zugrundeliegenden Sachverhalt schrieb eine kommunale Wohnungsbaugesellschaft, deren einzige Gesellschafterin eine Gebietskörperschaft ist, die Erbringung von Hausmeisterdienstleistungen in einem nationalen und weitgehend formfreien Vergabeverfahren aus. Das Angebot des Bieters (B) lag über dem EU-Schwellenwert i. H. v. 209.000 Euro. Die Wohnungsbaugesellschaft informierte B über die Absicht, ein anderes Unternehmen zu bezuschlagen, ohne eine ordnungsgemäße Vorabinformation nach § 134 GWB zu erteilen. Auf die Rüge machte sie geltend, sie sei kein öffentlicher Auftraggeber und aus diesem Grund nicht an das Vergaberegime für oberschwellige Vergabeverfahren gebunden. Der im Handelsregister eingetragene Gesellschaftszweck sei für die öffentliche Auftraggebereigenschaft unerheblich. Entscheidend sei allein, dass keine Aufgaben im Allgemeininteresse nichtgewerblicher Art erfüllt werden. Dies ergebe sich unter anderem daraus, dass die Finanzierung ihrer Bauvorhaben aus eigenen Kapital- und Kreditmitteln erfolge, die sie über den freien Kapitalmarkt rekrutiere. B berief sich auf eine unzulässige Direktvergabe.

Die Vergabekammer bejahte mit ihrer Entscheidung die Qualität der kommunalen Wohnungsbaugesellschaft als öffentlicher Auftraggeber gem. § 99 Nr. 2 GWB. Die strittige Tatbestandsvoraussetzung „im Allgemeininteresse liegende Aufgaben" ergebe sich aus dem Gesellschaftszweck, der in erster Linie die soziale Wohnraumförderung und -bewirtschaftung sowie auch die Verwaltung kommunalen Immobilienvermögens vorsehe. Die Wohnungsbaugesellschaft habe nicht vortragen können, woraus sich ergeben soll, dass der Gesellschaftszweck nicht mehr verfolgt werde. Vielmehr ergebe sich die zwingend an öffentlichen Zielen ausgerichtete Aufgabenwahrnehmung auch aus den Vorgaben der rheinland-pfälzischen Gemeindeordnung zur wirtschaftlichen Betätigung der Gemeinden (§§ 85 ff. GO-RP). Unter Hinweis auf den Beschluss des OLG Brandenburg vom 06.12.2016 (6 Verg 4/16, IBRRS 2017, 2194 = VPR 2017, 124), sei eine – wenn auch überwiegende – Aufgabenwahrnehmung, die nicht nur öffentlichen Zwecken dient, unerheblich. Es komme nicht darauf an, wo der Schwerpunkt der Tätigkeit liege. Ein relativ geringer Teil der Aufgabenwahrnehmung im Allgemeininteresse reiche zur Bejahung des Tatbestandsmerkmals aus. Das zweite streiterhebliche Tatbestandsmerkmal der Nichtgewerblichkeit sei erfüllt, weil die öffentliche Hand finanzielle Rückendeckung gewährleistet und damit die Wohnungsbaugesellschaft nicht dem gleichen wirtschaftlichen Marktrisiko wie andere Marktteilnehmer ausgesetzt sei. Hieran ändere auch die Tatsache nichts, dass sowohl private als auch öffentliche Investoren am Finanzierungskonzept in gleicher Weise partizipieren könnten.

Die Entscheidung bestätigt, dass sich die kommunalen Wohnungsbaugesellschaften nicht durch Teilnahme am Wettbewerbsmarkt aus der öffentlichen Auftraggeberrolle verabschieden können. Die Verbindung von sozialem Wohnungsbau mit wirtschaftlichen Gesichtspunkten entspricht dem typischen Bild heutiger kommunaler Wohnungsbaugesellschaften.

VG Neustadt:
Kein Rechtsschutz bei Forderung
in Höhe von 0,03 Euro

Das Verwaltungsgericht Neustadt an der Weinstraße hat mit Beschluss vom 26.04.2018 - N 200/18.NW - einen Vollstreckungsantrag über eine Forderung von 0,03 Euro mit der Begründung abgelehnt, dass ein Rechtsschutzsuchender das Gericht nicht für unnütze oder unlautere Zwecke in Anspruch nehmen darf.

In dem zugrundeliegenden Verfahren führte ein ehemaliger Bewohner der Stadt Neustadt an der Weinstraße (im Folgenden Vollstreckungsgläubiger) im Frühjahr 2012 ein vorläufiges Rechtsschutzverfahren gegen die Stadt Neustadt an der Weinstraße (im Folgenden Vollstreckungsschuldnerin), das mit Beschluss vom 08.05.2012 eingestellt wurde. Anfang Dezember 2017 stellte der Vollstreckungsgläubiger in dieser Sache einen Kostenfestsetzungsantrag. Daraufhin setzte die Urkundsbeamtin des VG Neustadt an der Weinstraße mit Kostenfestsetzungsbeschluss vom 12.01.2018 die von der Vollstreckungsschuldnerin an den Vollstreckungsgläubiger zu zahlenden Kosten auf 2,90 Euro fest. Der Beschluss wurde der Vollstreckungsschuldnerin am 17.01.2018 zugestellt. Der mittlerweile in München wohnhafte Vollstreckungsgläubiger forderte die Vollstreckungsschuldnerin daraufhin am 29.01.2018 mit Fristsetzung zum 12.02.2018 zur Zahlung auf. Am 18.02.2018 stellte der Vollstreckungsgläubiger bei Gericht einen Antrag auf Vollstreckung der ihm zustehenden Forderung gegen die Vollstreckungsschuldnerin und machte geltend, bisher sei keine Zahlung eingegangen. Die Vollstreckungsschuldnerin antwortete daraufhin, sie habe einen Betrag von 2,91 Euro sofort am 19.01.2018 auf das Konto bei der Bank überwiesen, welches aufgrund der vorherigen Angaben des Vollstreckungsgläubigers hinterlegt gewesen sei. Es handele sich hierbei wohl um das Konto der Mutter des Vollstreckungsgläubigers. Der Vollstreckungsgläubiger antwortete darauf, ihm sei das von der Vollstreckungsschuldnerin bezeichnete Bankkonto nicht bekannt. Im Übrigen sei eine schuldbefreiende Zahlung auf das Bankkonto seiner Mutter nicht möglich. Die Vollstreckungsschuldnerin teilte daraufhin mit Schreiben vom 04.04.2018 mit, am 27.03.2018 sei eine Rücküberweisung des von ihr auf das Konto der Mutter des Vollstreckungsgläubigers angewiesenen Betrags in Höhe von 2,91 Euro getätigt worden. Sie werde den genannten Betrag daher nun auf das in der Zwischenzeit vom Vollstreckungsgläubiger als das Seinige mitgeteilte Konto weiterleiten. Der Vollstreckungsgläubiger bestätigte am 06.04.018, inzwischen sei auf seinem Konto eine Zahlung der Vollstreckungs-

schuldnerin in Höhe von 2,91 Euro eingegangen. Nach der Verrechnung ergebe sich allerdings noch eine offene Restforderung in Höhe von 0,03 Euro wegen angefallener Zinsen. Diese mache er weiterhin geltend.
Das VG hat den Vollstreckungsantrag des Vollstreckungsgläubigers abgelehnt. Zur Begründung führte es an, dem Vollstreckungsantrag fehle bereits das erforderliche Rechtsschutzinteresse. Nachdem die Vollstreckungsschuldnerin dem Vollstreckungsgläubiger mittlerweile den ursprünglich geforderten Betrag von 2,91 Euro auf das nachträglich mitgeteilte Bankkonto überwiesen habe und diesbezüglich Erledigung eingetreten sei, stehe nur noch der vom Vollstreckungsgläubiger zuletzt geltend gemachte Betrag in Höhe von 0,03 Euro im Streit. Zwar gewährleiste das Grundgesetz effektiven und möglichst lückenlosen richterlichen Rechtsschutz gegen Akte der öffentlichen Gewalt. Dennoch könne der Zugang zu den Gerichten von bestimmten Zulässigkeitsvoraussetzungen, namentlich von einem bestehenden Rechtsschutzbedürfnis, abhängig gemacht werden. Dies werde abgeleitet aus dem auch im Prozessrecht geltenden Gebot von Treu und Glauben, dem Verbot des Missbrauchs prozessualer Rechte sowie dem auch für die Gerichte geltenden Grundsatz der Effizienz staatlichen Handelns. Der Rechtsschutzsuchende dürfe daher das Gericht nicht für unnütze oder unlautere Zwecke in Anspruch nehmen. Nicht schutzwürdig sei insbesondere ein Interesse, das nach allgemeiner Anschauung als so gering anzusehen sei, dass es nicht die Inanspruchnahme der staatlichen Rechtsschutzeinrichtungen, nämlich der Gerichte, rechtfertige. Das VG sei vorliegend der Meinung, dass es sich bei einem Betrag von 0,03 Euro, um den es nach Zahlung der 2,91 Euro nur noch gehe, um einen wirtschaftlich so geringen Wert handele, dass er die Inanspruchnahme von gerichtlichem Rechtsschutz objektiv nicht mehr gerechtfertigt erscheinen lasse. Das Rechtswesen sei für die Gemeinschaft ein kostbares und zugleich sehr kostspieliges Gut. Bei 0,03 Euro gehe es dem Vollstreckungsgläubiger ersichtlich nicht mehr um wirtschaftliche Interessen, sondern um das Prinzip des "Rechthabens". Dies allein sei jedoch nicht schutzwürdig. Dem Begehren des Vollstreckungsgläubigers fehle im Übrigen auch deswegen das Rechtsschutzinteresse, weil er den Vollstreckungsantrag verfrüht gestellt habe.

OVG Berlin-Brandenburg: Flüchtlingsunterbringung in Sporthalle durfte sportlicher Nutzung vorgehen

Das Oberverwaltungsgericht Berlin-Brandenburg hat mit Beschluss vom 26.04.2018 - OVG 6 N 46.17 - entschieden, dass es rechtmäßig war, einem Sportverein von Dezember 2015 bis September 2016 die Nutzung einer Sporthalle, die als Notunterkunft für Flüchtlinge sichergestellt war, für den Vereinssport zu verweigern und den Antrag des klagenden Vereins auf Zulassung der Berufung gegen das seine Klage abweisende Urteil des Verwaltungsgerichts Berlin abgelehnt.
Zur Begründung führte das Gericht aus, dass Sportvereine einen Anspruch auf ermessensfehlerfreie Entscheidung über einen Antrag auf Nutzung einer öffentlichen Sportanlage für den Vereinssport hätten. Dieser Anspruch setze jedoch voraus, dass die Sportanlage in dem maßgeblichen Zeitraum für eine Nutzung zu sportlichen Zwecken zur Verfügung steht. Aufgrund der Sicherstellung der Halle als Notunterkunft sei dies im maßgeblichen Zeitraum nicht der Fall gewesen.
Das Land Berlin war laut OVG auch berechtigt, die sofortige Nutzung der Halle als Notunterkunft anzuordnen. Wegen der seit Monaten anhaltend hohen Flüchtlingszahlen sei es darauf angewiesen gewesen, neben Gemeinschafts- und Notunterkünften auch Sporthallen für die Unterbringung von Flüchtlingen zu nutzen. Die Entscheidung für die Nutzung von Sporthallen sei nach Angaben des Landes nur als letztes zur Verfügung stehendes Mittel getroffen worden. Flüchtlingsunterkünfte hätten häufig innerhalb von Stunden geschaffen werden müssen. Andere leerstehende Gebäude seien hierfür etwa wegen fehlender sanitärer Einrichtungen oft nicht in Betracht gekommen. Für eine Abwägung der Belange einzelner Sportvereine sei in dieser Lage ersichtlich kein Raum gewesen.

Aus der Rechtsprechung

Urteil des OVG Schleswig vom 06.12.2017 - 3 LB 11/17 -

GG Art. 3 Abs. 1, 28 Abs. 2 S. 1, 31, 74 Abs. 1 Nr. 11
Verf SH Art. 6 Abs. 2, 9 S. 1, 54 Abs. 1
BeamtStG §§ 5 Abs. 1, 3 Abs. 2, 4 Abs. 2
LBG § 7 Abs. 5 S. 1
GstG §§ 1, 2 Abs. 1 und Abs. 2, 15 Abs. 1 und Abs. 2
GO §§ 28 S. 1 Nr. 20, 40 Abs. 3 und 4, 43, 45, 46, 102 Abs. 2 S. 1 Nr. 3, 104, 106
GmbHG §§ 13 Abs. 1 und 52 Abs. 1
AktG § 111 Abs. 1 und 2
BGleiG §§ 2, 3 Abs. 1 Nr. 5 und Nr. 9
BGremBG § 1
LHO § 65 Abs. 1 Nr. 3
EigVO §§ 1 Abs. 1, 2 Abs. 4, 5 Abs. 2

Geltungsbereich des landesrechtlichen Gleichstellungsgebotes in kommunalen Gremien privatrechtlich organisierter Gesellschaften

Leitsatz der Redaktion:
Das landesrechtliche Gleichstellungsgebot ist von einer Gemeinde- bzw. Stadtvertretung auch zu beachten, wenn sie Vertreter/innen in Gremien privatrechtlich organisierter Gesellschaften entsendet.

Zum Sachverhalt:
Die Beteiligten streiten um die Anwendbarkeit des Gleichstellungsgesetzes bei der Entscheidung über die Entsendung von Mitgliedern in den Aufsichtsrat der … GmbH (... GmbH). Die Stadt Husum ist Mehrheitsgesellschafterin dieser GmbH, die laut ihres Gesellschaftsvertrages einen Aufsichtsrat aus neun Mitgliedern hat. Er setzt sich zusammen aus fünf von der Stadt Husum und vier von der … GmbH zu entsendenden Mitgliedern. Die Amtszeit der Aufsichtsratsmitglieder ist auf vier Jahre begrenzt. In der Sitzung vom 25. Juni 2015 beschloss der Kläger, der als Gemeindevertretung der Stadt Husum für die Bestellung der fünf Aufsichtsratsmitglieder zuständig ist, vier Männer und eine Frau als Mitglied bzw. als Ersatzmitglied in den Aufsichtsrat zu entsenden.

Diesem Beschluss lagen folgende Entsendungsvorschläge der vertretenen Fraktionen zugrunde:
1. CDU-Fraktion - zwei Männer
2. SPD-Fraktion - eine Frau und ein Mann
3. WGH-Fraktion - ein Mann
4. Fraktion Bündnis 90/Die Grünen - zwei Frauen.

Über diese Vorschläge wurde in der Reihenfolge ihres Einganges abgestimmt. Nachdem den Vorschlägen 1) bis 3) ent-

weder mit mehr Ja- als Nein-Stimmen bzw. einstimmig zugestimmt worden war, kam der unter Nummer 4) angeführte Vorschlag der Fraktion Bündnis 90/Die Grünen nicht mehr zur Abstimmung. Im Protokoll über die Sitzung des Klägers vom 25. Juni 2015 zu TOP 9 hieß es zur Begründung, es seien fünf Personen in den Aufsichtsrat der ... GmbH entsendet worden.

Am 30. Juni 2015 legte der Beklagte gegen den Beschluss des Klägers vom 25. Juni 2015 Widerspruch ein. Er führte zur Begründung aus, durch diese Beschlussfassung werde die Vorschrift des § 15 Abs. 1 Gleichstellungsgesetz (GstG) verletzt, weil sowohl in Bezug auf die Mitglieder als auch auf die Stellvertretungen eine geschlechterparitätische Besetzung hätte erfolgen müssen. Mithin seien jeweils drei Frauen und zwei Männer als Mitglieder bzw. als Ersatzmitglieder zu benennen, da in der vorigen Amtszeit weibliche Mitglieder im Aufsichtsrat unterrepräsentiert gewesen seien. Entsprechende Personalvorschläge der Fraktionen seien bei der Beschlussfassung nicht berücksichtigt worden.

Der Beklagte forderte den Kläger auf, seinen Beschluss aufzuheben, um in seiner nächsten Sitzung eine rechtskonforme Beschlussfassung herbeizuführen. Zu diesem Zweck legte der Beklagte für die Sitzung des Klägers am 24. September 2015 einen Beschlussvorschlag zur Aufhebung des Beschlusses vom 25. Juni 2015 vor.

Der Kläger beschloss in der Sitzung vom 24. September 2015, den Vorschlag des Beklagten abzulehnen. Dies beanstandete der Beklagte am 28. September 2015 mit der Begründung, der Beschluss vom 25. Juni 2015 sei aufzuheben, da er gegen § 15 Abs. 1 GstG verstoße.

Der Kläger hat am 11. Juli 2016 Klage vor dem Schleswig-Holsteinischen Verwaltungsgericht erhoben, mit der er sich gegen die Beanstandung des Beklagten gewendet hat. Der Kläger hat im Wesentlichen geltend gemacht, die Beanstandung sei rechtswidrig, da § 15 Abs.1 GstG für den Fall der Entsendung von Mitgliedern in den Aufsichtsrat nicht anwendbar sei. Das Gleichstellungsgesetz gelte nicht für juristische Personen des Privatrechts, wie hier die ... GmbH, um deren Aufsichtsratsbesetzung es gehe.

Darüber hinaus erfasse das Gleichstellungsgesetz auch ehrenamtlich tätige Personen im Aufsichtsrat nicht. Selbst wenn § 15 Abs. 1 GstG einschlägig sein sollte, so gelte vorliegend eine Ausnahme, weil die Vorgabe der geschlechterparitätischen Besetzung des Aufsichtsrates einen unzulässigen Eingriff in die kommunale Selbstverwaltung darstelle. Diese Vorgabe verletze die in sein Ermessen gestellte Entscheidung über die Auswahl der entsprechenden Mitglieder. Die Besetzung des Aufsichtsrates sei vielmehr entsprechend dem Verfahren nach d'Hondt unter Berücksichtigung der Fraktionsstärke vorzunehmen, so dass die Personalvorschläge der kleineren Fraktionen unberücksichtigt bleiben müssten, wenn die verfügbaren Aufsichtsratsplätze bereits durch die Personalvorschläge der großen Fraktionen besetzt seien. Dabei sei es den Fraktionen überlassen, ggf. qualifizierte Frauen in ihren Personalvorschlag aufzunehmen. Darüber hinaus stehe dem § 15 Abs. 1 GstG höherrangiges Bundesrecht entgegen. Zunächst schreibe das Gesellschaftsrecht Mindestfrauenanteile für die Aufsichtsräte nur bei solchen Gesellschaften vor, die der Mitbestimmung unterlägen oder börsennotiert seien. Nach dem Bundesgleichstellungsgesetz seien Unternehmen, an denen die öffentliche Hand mit mehr als 50 % beteiligt sei, wie hier, vom Anwendungsbereich des Gleichstellungsrechts ausgenommen. Schließlich fehle dem Landesgesetzgeber für das Gleichstellungsgesetz Schleswig-Holstein die Gesetzgebungskompetenz, da der Bund von seiner konkurrierenden Gesetzgebungszuständigkeit für das Recht der Wirtschaft Gebrauch gemacht habe.

Der Kläger hat beantragt,
festzustellen, dass die Beanstandung des Beklagten vom 28. September 2015 des von ihm in der Sitzung am 24. September 2015 unter TOP 7 gefassten Beschlusses rechtswidrig ist.

Der Beklagte hat beantragt,
die Klage abzuweisen.

Er hat geltend gemacht, das Gleichstellungsgesetz sei auf die streitbefangene Entsendung von Aufsichtsratsmitgliedern anwendbar, weil das Gesetz gemäß § 2 Abs. 1 Satz 1 GstG für Gemeinden gelte und auf deren Gremienbesetzung anwendbar sei. Danach sei die geschlechterparitätische Besetzung des Aufsichtsrates zwingend, weil spezifische Anforderungen des Gesellschaftsrechts dem nicht entgegenstünden.

Schließlich sei auch das Demokratieprinzip nicht verletzt, weil der sogenannte Spiegelbildlichkeitsgrundsatz für die Besetzung des Aufsichtsrats nicht gelte. Vielmehr seien die Aufsichtsratsmitglieder an die Weisungen der Gemeinde gebunden, handelten damit exekutiv und müssten in ihrer Zusammensetzung nicht die politischen Kräfteverhältnisse der Gemeindevertretung wiedergeben. Da hinreichend qualifizierte Frauen für die Aufsichtsratsbesetzung vorgeschlagen worden seien, sei ein Ausnahmetatbestand von der Sollvorschrift des § 15 Abs. 1 GstG nicht gegeben. Mit Urteil vom 21. Dezember 2016, auf dessen Inhalt wegen der weiteren Einzelheiten des Sachverhalts sowie der Entscheidungsgründe verwiesen wird, hat das Verwaltungsgericht die Klage abgewiesen.

Mit der vom Senat durch Beschluss vom 11. Juli 2017 wegen grundsätzlicher Bedeutung zugelassenen Berufung verfolgt der Kläger sein Begehren weiter und trägt zur Begründung ergänzend im Wesentlichen vor: Sein Benennungs- und Entsendungsbeschluss vom 25. Juni 2015 verstoße nicht gegen geltendes Recht; er habe das Gleichstellungsgesetz zu Recht

nicht angewendet. Denn bei der Auslegung von § 15 GstG seien der in § 1 GstG definierte Gesetzeszweck sowie der in § 2 GstG definierte Geltungsbereich zu berücksichtigen. Zweck des Gleichstellungsgesetzes sei, die Gleichstellung der Frauen im öffentlichen Dienst zu fördern. Damit ziele das Gesetz auf die formal dem öffentlichen Dienst zugehörigen Beschäftigten ab, zu denen weder die Mitglieder der Gemeindevertretungen noch Mitglieder von Aufsichtsräten externer Gesellschaften gehörten. Dem entspreche auch der Wortlaut des § 2 GstG, welcher in Absatz 1 den Geltungsbereich unter anderem auf Gemeinden erstreckt und in Absatz 2 Bezug nimmt auf Beschäftigte im Sinne des Gleichstellungsgesetzes und diese definiert. Dazu zählten weder die Mitglieder der Gemeindevertretungen noch die Mitglieder von Aufsichtsräten externer Gesellschaften. Insoweit sei der Wortlaut eindeutig. Schließlich laute die Überschrift des Gleichstellungsgesetzes „Gesetz zur Gleichstellung der Frauen im öffentlichen Dienst". Der Begriff „Aufsichtsräte" in § 15 Abs. 1 GstG erstrecke sich demnach ausschließlich auf solche des öffentlichen Dienstes. Dies entspreche auch der Vorstellung des Gesetzgebers, was ein Umkehrschluss aus § 15 Abs. 2 GstG zeige. Danach gelte für Organisationen, die nicht Träger der öffentlichen Verwaltung sind, oder sonstige gesellschaftliche Gruppierungen hinsichtlich der Benennung und Entsendung von Vertreterinnen und Vertretern für öffentlich-rechtliche Beschluss- und Beratungsgremien § 15 Abs. 1 GstG entsprechend. Damit habe der Gesetzgeber in § 15 Abs. 2 GstG ausdrücklich und klarstellend definiert, dass selbst für Organisationen, die nicht Träger der öffentlichen Verwaltung sind, die vom Gleichstellungsgesetz erfasste Zweckbestimmung nur für Benennungen und Entsendungen in öffentlich-rechtliche Beschluss- oder Beratungsgremien gilt. Hätte der Gesetzgeber insoweit auch nicht öffentlich-rechtliche Beschluss- oder Beratungsgremien erfassen wollen, hätte er dies klar zum Ausdruck bringen müssen.
Gegen die vom Verwaltungsgericht vorgenommene Auslegung des § 15 Abs. 1 GstG bestünden verfassungsrechtliche Bedenken. Das Gebot der Bestimmtheit von Normen sei verletzt. Denn es sei für die Mitglieder der Gemeindevertretung nicht mit der hinreichenden Klarheit aus den Regelungen des Gleichstellungsgesetzes zu entnehmen, ob unter den Begriff „Aufsichtsräte" auch Aufsichtsräte externer Gesellschaften fielen. Zudem werde gegen das Gleichheitsgebot aus Art. 3 Abs. 2 GG verstoßen, weil zum Beispiel bei der Besetzung von Ausschüssen der Eigenbetriebe eine paritätische Besetzung nicht vorgesehen sei, sondern eine Verhältniswahl stattfinde. Es seien keine Gründe dafür ersichtlich, die Besetzung von Aufsichtsräten externer Gesellschaften anders vorzunehmen als diejenige von Ausschüssen der Eigenbetriebe. Ferner werde der Grundsatz der Verhältnismäßigkeit nicht beachtet. Schließlich liege ein Eingriff in den Wesensgehalt der kommunalen Selbstverwaltungsgarantie vor, denn die (vermeintliche) Vorgabe, dass in Aufsichtsräten Frauen und Männer jeweils hälftig berücksichtigt werden sollen, könne im Extremfall dazu führen, dass derartige Aufsichtsratssitze auf Dauer nicht besetzt und Gemeinden ihre Mitwirkungsrechte nicht ausüben könnten.

Der Kläger beantragt,
das Urteil des Schleswig-Holsteinischen Verwaltungsgerichts - 6. Kammer - vom 21. Dezember 2016 zu ändern und festzustellen, dass die Beanstandung des Beklagten vom 28. September 2015 des von ihm - dem Kläger - in seiner Sitzung am 24. September 2015 unter Tagesordnungspunkt 7 gefassten Beschlusses rechtswidrig ist.

Der Beklagte beantragt,
die Berufung zurückzuweisen.
Er trägt im Wesentlichen Folgendes vor:
§ 2 Abs. 1 Satz 1 GstG ordne an, dass das Gesetz und mithin § 15 Abs. 1 GstG für die Stadt Husum gelte. § 15 Abs. 1 GstG beanspruche bereits vom Wortlaut ausgehend eine Anwendung auf den Fall der Besetzung des Aufsichtsrats einer zivilrechtlich verfassten Eigengesellschaft. Denn die nicht abschließende Aufzählung von Gremien, bei deren Besetzung Männer und Frauen jeweils hälftig zu berücksichtigen seien, spreche für einen weiten Anwendungsbereich. Es handele sich auch nicht um einen Redaktionsirrtum, sondern um eine bewusste Regelung, was aus der ursprünglichen Gesetzesbegründung der Landesregierung deutlich werde. Die Norm sei auch hinreichend bestimmt.
Zudem gingen sowohl § 15 Abs. 1 als auch § 15 Abs. 2 GstG über den Bereich des öffentlichen Dienstes im engeren Sinne hinaus. Absatz 1 Satz 1 beziehe sich auf Tätigkeiten bei privaten Einrichtungen und Absatz 2 gelte für die Tätigkeit Privater in öffentlichen Einrichtungen. § 2 Abs. 2 GstG stehe der Anwendung des § 15 Abs. 1 GstG auf die Benennung und Entsendung der Vertreterinnen und Vertreter der Stadt Husum für den Aufsichtsrat der ... GmbH nicht entgegen. Gemeindevertreter seien weder Ehrenbeamtinnen oder Ehrenbeamte noch kommunale Wahlbeamtinnen oder Wahlbeamten.
Die Beschlüsse des Klägers verstießen gegen § 15 Abs. 1 GstG. Denn es liege kein atypischer Fall vor, der ein Abweichen von der gesetzlichen Vorgabe rechtfertige. Anders als Werkausschüsse von Eigenbetrieben, die Ausschüsse der Gemeindevertretung seien und deren Mitglieder von der Gemeindevertretung gewählt würden, hätten Kapitalgesellschaften eine eigene Rechtspersönlichkeit. Da es nicht einmal ein Gebot gebe, dass der Aufsichtsrat überhaupt mit Mitgliedern der Gemeindevertretung besetzt werde, gelte für Aufsichtsräte von Kapitalgesellschaften, an denen eine Gemeinde beteiligt ist, erst recht der Grundsatz der Spiegelbildlichkeit nicht. Deshalb komme auch eine Anknüpfung an den Geschlechterproporz in der Gemeindevertretung nicht in Betracht. § 15 Abs. 1 GstG verstoße nicht gegen die Garantie der kommunalen Selbstverwaltung. Diese bestehe ausdrücklich nur im Rahmen der Gesetze bzw. nur, soweit die Gesetze nicht ausdrücklich etwas anderes bestimmten. Entscheidend sei, dass die Verhältnismäßigkeit der Mittel gewahrt sei. Dies sei hier der Fall.

Aus den Gründen:
Die zulässige Berufung ist unbegründet. Das Verwaltungsgericht hat die Klage zu Recht abgewiesen. Die Beanstandung des Beklagten ist rechtmäßig, weil der Beschluss des Klägers vom 24. September 2015 die rechtswidrige Beschlussfassung vom 25. Juni 2015 aufrechterhalten hat.

I. Die Klage ist als Feststellungsklage gemäß § 43 Abs. 3 Satz 3 GO zulässig. Danach steht der Gemeindevertretung gegen die Beanstandung des Bürgermeisters oder der Bürgermeisterin die Klage vor dem Verwaltungsgericht zu. Das der Klageerhebung vorgeschaltete Verfahren nach § 43 Abs. 1 bis Abs. 3 Satz 1 und 2 GO ist vollständig und ordnungsgemäß durchgeführt worden. Der Beklagte hat dem Beschluss des Klägers vom 25. Juni 2015, eine Frau und vier Männer in den Aufsichtsrat der ... GmbH zu entsenden, innerhalb der Zwei-Wochenfrist des § 43 Abs. 2 Satz 1 GO am 30. Juni 2015 widersprochen (vgl. § 43 Abs. 1 GO) und seinen Widerspruch mit der Aufforderung versehen, den Beschluss wegen Verstoßes gegen § 15 Abs. 1 des Gesetzes zur Gleichstellung der Frauen im öffentlichen Dienst (Gleichstellungsgesetz – GstG) vom 13. Dezember 1994 (GVOBl. S. 562) in der Fassung der Änderung vom 16. März 2015 (GVOBl. S. 96) aufzuheben (vgl. § 43 Abs. 2 Satz 2 GO). Den vom Beklagten zu diesem Zwecke vorgelegten Beschlussvorschlag zur Aufhebung des Beschlusses vom 25. Juni 2015 hat der Kläger mit Beschluss vom 24. September 2015 abgelehnt (vgl. zur Pflicht der erneuten Beschlussfassung: § 43 Abs. 3 Satz 3 GO). Binnen der Zwei-Wochenfrist des § 43 Abs. 3 Satz 1 GO hat der Beklagte am 28. September 2015 den Beschluss wegen Verletzung von § 15 Abs. 1 GstG beanstandet.

II. Die Klage ist jedoch nicht begründet. Die Beanstandung des Beschlusses vom 24. September 2015, durch den der Beschluss vom 25. Juni 2015 zur Entsendung von Mitgliedern und Ersatzmitgliedern in den Aufsichtsrat der ... GmbH aufrechterhalten wird, ist rechtmäßig und verletzt den Beklagten nicht in seinen Rechten. Denn beide Beschlüsse des Beklagten, vier Männer und nur eine Frau als Mitglied bzw. als Ersatzmitglied in den Aufsichtsrat der ... GmbH zu entsenden, sind rechtswidrig, weil sie den Anforderungen an die geschlechterparitätische Gremienbesetzung gemäß § 15 Abs. 1 Satz 1 GstG nicht genügen. Nach § 15 Abs. 1 Satz 1 GstG sollen Frauen und Männer bei Benennungen und Entsendungen von Vertreterinnen und Vertretern für Kommissionen, Beiräte, Ausschüsse, Vorstände, Verwaltungs- und Aufsichtsräte sowie für vergleichbare Gremien, deren Zusammensetzung nicht durch besondere gesetzliche Vorschriften geregelt ist, jeweils hälftig berücksichtigt werden.

1. Die Norm ist anwendbar auf die Benennung und Entsendung von Vertreterinnen und Vertretern der Gemeinde in den Aufsichtsrat der ... GmbH. Dies ergibt sich bereits aus dem Wortlaut der Norm (a), aber auch aus der Gesetzeshistorie (b) sowie aus der Systematik des Gesetzes (c) und dessen Sinn und Zweck (d).

a) § 15 Abs. 1 Satz 1 GstG hat schon vom Wortlaut her einen weiten Anwendungsbereich, wie bereits die lange und ausdrücklich nicht abschließende Aufzählung zeigt („… sowie für vergleichbare Gremien"). Zudem folgt die Anwendbarkeit der Norm auf den Fall der Besetzung des Aufsichtsrats einer zivilrechtlich verfassten Eigengesellschaft (hier GmbH) aus der ausdrücklichen Nennung von „Vorständen… und Aufsichtsräten". Denn Vorstände und Aufsichtsräte sind typischerweise keine Organe, die im öffentlichen Dienst vorkommen, sondern solche des Gesellschaftsrechts (vgl. z.B. § 52 GmbHG, § 76 AktG, § 95 AktG).

b) Dieses Verständnis der Norm steht im Einklang mit dem Willen des Gesetzgebers.
In der Begründung des Gesetzentwurfs der Landesregierung zum damaligen § 13 Abs. 1 GstG, der weitgehend mit dem heutigen § 15 Abs. 1 GstG übereinstimmt, heißt es (vgl. LT-Drs. 13/1898, S. 29, 30):
„Der Verwaltung stehen eine Vielzahl von Benennungs- und Entsendungsrechten für die Besetzung verschiedenster Gremien zu. Absatz 1 verpflichtet die Träger der öffentlichen Verwaltung durch eine Art. 6 Satz 2 der schleswig-holsteinischen Landesverfassung konkretisierende Sollvorschrift, bei der Benennung und Entsendung von Beschäftigen in Gremien Männer und Frauen zu gleichen Teilen zu berücksichtigen. Anders als in Art. 6 Satz 2 der Landesverfassung gilt diese Verpflichtung nicht ausschließlich für öffentlich-rechtliche Beschluss- und Beratungsgremien, sondern etwa auch für Aufsichtsräte von Kapitalgesellschaften, für die einem Träger der öffentlichen Verwaltung Besetzungsrechte zustehen."
Mit dieser Begründung bezieht sich der Gesetzgeber unter anderem auf die in § 28 Satz 1 Nr. 20, § 102 Abs. 2 Satz 1 Nr. 3, § 104 GO, § 65 Abs. 1 Nr. 3 LHO normierten Benennungs- und Entsendungsrechte von Gemeinden und Land für die Besetzung verschiedenster Gremien in Gesellschaften privater Rechtsform. Der Träger der öffentlichen Verwaltung (vgl. zum Begriff: § 2 Abs. 1 LVwG) hat sich danach die Besetzungsrechte vorzubehalten, wenn er - wie hier - an einer Gesellschaft des Privatrechts beteiligt ist. Es gibt keine Anhaltspunkte dafür, dass es sich um ein Redaktionsversehen handeln könnte. Vielmehr spricht nicht nur die Gesetzesbegründung, sondern auch der Umstand, dass z.B. in § 102 Abs. 2 Satz 1 Nr. 3 GO (§ 102 GO betrifft Gründung von und Beteiligung an Gesellschaften des privaten Rechts) und in § 65 Abs. 1 Nr. 3 LHO (§ 65 LHO betrifft die Beteiligung an privatrechtlichen Unternehmen) gleichermaßen wie in § 15 Abs. 1 Satz 1 GstG von „Aufsichtsräten" die Rede ist, dafür, dass jeweils Aufsichtsräte als Organ einer privatrechtlich organisierten Gesellschaft gemeint sind.

c) Auch aus der systematischen Stellung der Norm im Gefüge des Gleichstellungsgesetzes folgt nichts anderes.
aa) § 15 Abs. 1 GstG beansprucht Geltung für die entsendende Gemeinde und nicht für das Gremium, in das entsandt wird - hier die ... GmbH -. Dies ergibt sich aus § 2 Abs. 1 Satz 1 GstG. Diese Vorschrift ordnet an, dass das Gleichstellungsgesetz u.a. für Gemeinden gilt. Die Gemeinde - d.h. die Stadt Husum - ist es, die gemäß § 15 Abs. 1 Satz 1 GstG bei Benennungen und Entsendungen von Vertreterinnen und Vertretern für Gremien durch ihre Gemeindevertretung (vgl. § 28 Satz 1 Nr. 20 GO) tätig wird.

bb) Die vorstehende Auslegung des § 15 Abs. 1 Satz 1 GstG steht auch im Einklang mit § 1 Satz 2 Nr. 3 GstG. Danach fördert das Gesetz die Gleichstellung der Frauen im öffentlichen Dienst insbesondere durch die gerechte Beteiligung von Frauen an allen Lohn-, Vergütungs- und Besoldungsgruppen sowie in Gremien. Wie die Überschrift von § 1 GstG „Gesetzeszweck" zum Ausdruck bringt, enthält die Norm keine abschließende Festlegung des Anwendungsbereichs des Gleichstellungsgesetzes, sondern trifft nur eine Aussage dazu, was das Gesetz fördern soll. Die ausdrückliche Nennung der Beteiligung von Frauen „in Gremien" deutet darauf hin, dass nach dem Verständnis des Gleichstellungsgesetzes „öffentlicher Dienst" auch die Tätigkeit für einen öffentlichen Rechtsträger in einer privatrechtlichen Gesellschaft sein kann. Dass der Begriff „öffentlicher Dienst" im Gleichstellungsgesetz eine weitreichende Bedeutung hat, ergibt sich auch aus § 15 Abs. 2 GstG. Danach gilt § 15 Abs. 1 GstG entsprechend, wenn u.a. Organisationen, die nicht Träger der öffentlichen Verwaltung sind, zur Benennung und Entsendung von Mitgliedern für öffentlich-rechtliche Beschluss- oder Beratungsgremien berechtigt sind.

cc) § 2 Abs. 2 GstG ist auf die vorliegende Konstellation nicht anwendbar und steht deshalb der Anwendbarkeit von § 15 Abs. 1 GstG nicht entgegen. § 2 Abs. 2 Satz 1 GstG definiert, wer Beschäftigte im Sinne des Gesetzes sind, nämlich Beamtinnen und Beamte, Richterinnen und Richter, Angestellte, Arbeiterinnen und Arbeiter sowie Auszubildende der Träger der öffentlichen Verwaltung nach Absatz 1. § 2 Abs. 2 Satz 2 GstG besagt, dass das Gesetz nicht für Ehrenbeamtinnen und Ehrenbeamte und kommunale Wahlbeamtinnen und Wahlbeamte gilt. Weder kennt § 15 Abs. 1 GstG die Beschäftigteneigenschaft als Tatbestandsvoraussetzung, noch zählen Gemeindevertreterinnen und -vertreter, über deren Entsendung in den Aufsichtsrat der ... GmbH zu befinden war, zu den in § 2 Abs. 2 Satz 2 GstG aufgezählten Beamtengruppen. Sie sind keine Ehrenbeamtinnen und Ehrenbeamte im Sinne von § 5 Abs. 1 i.V.m. § 3 Abs. 2 BeamtStG; denn sie nehmen keine hoheitsrechtlichen oder solche Aufgaben wahr, die aus Gründen der Sicherung des Staates oder des öffentlichen Lebens nicht ausschließlich Personen übertragen werden dürfen, die in einem privatrechtlichen Arbeitsverhältnis stehen. Aus demselben Grund sind sie auch keine kommunalen Wahlbeamtinnen und Wahlbeamten. Wahlbeamtinnen und Wahlbeamten sind gemäß § 7 Abs. 5 Satz 1 LBG Beamtinnen und Beamte auf Zeit, für deren Berufung in das Beamtenverhältnis es einer Wahl bedarf. Das Beamtenverhältnis auf Zeit dient gemäß § 4 Abs. 2 BeamtStG der befristeten Wahrnehmung von Aufgaben nach § 3 Abs. 2 BeamtStG oder der zunächst befristeten Übertragung eines Amtes mit leitender Funktion.

d) Sinn und Zweck des § 15 Abs. 1 GstG ist es, der Verwirklichung des Grundrechtes der Gleichberechtigung von Frauen und Männern zu dienen und die Gleichstellung der Frauen im öffentlichen Dienst zu fördern. Dies soll dazu beitragen, strukturelle Benachteiligungen von Frauen bei der Vergabe von Arbeitsplätzen und bei

der beruflichen Entwicklung auszugleichen oder zu mindern.

2. Der Kläger hat mit seinen Beschlüssen gegen § 15 Abs. 1 Satz 1 GstG verstoßen, indem er die gesetzliche Vorgabe, wonach Frauen und Männer jeweils hälftig berücksichtigt werden sollen, nicht beachtet und vier Männer und eine Frau in den Aufsichtsrat der ... GmbH entsandt hat. Zwar handelt es sich bei § 15 Abs. 1 Satz 1 GstG um eine Soll-Vorschrift. Derartige Normen sind aber im Regelfall für die mit ihrer Durchführung betraute Behörde rechtlich zwingend und verpflichten sie, grundsätzlich so zu verfahren, wie es im Gesetz bestimmt ist. Im Regelfall bedeutet das „Soll“ ein „Muss“. Nur bei Vorliegen von Umständen, die den Fall als atypisch erscheinen lassen, darf die Behörde anders verfahren als im Gesetz vorgesehen (BVerwG, Beschl. v. 27.02.2003 - 1 WB 57.02 -, juris Rn. 28 m.w.N.). Anhaltspunkte dafür, dass ein atypischer Fall vorliegen könnte, sind nicht ersichtlich und werden vom Kläger auch nicht geltend gemacht. Das wäre etwa der Fall, wenn bei Beachtung der Geschlechterparität geeignete Bewerberinnen und Bewerber nicht oder in nicht ausreichender Zahl gefunden werden könnten. Mangelnde Eignung der von der Fraktion Bündnis90/Die Grünen vorgeschlagenen zwei Frauen war aber nicht der Grund für deren Nicht-Berücksichtigung. Vielmehr war der Kläger davon ausgegangen, dass der Vorschlag nicht mehr zu thematisieren war, nachdem die Entsendung allein nach dem Stärkeverhältnis der Fraktionen beschlossen worden war.

3. Gegen § 15 Abs. 1 GstG bestehen keine verfassungsrechtlichen Bedenken.
a) Die Norm genügt dem Bestimmtheitserfordernis. Dem entspricht eine Norm immer dann, wenn etwaige Auslegungsprobleme mit herkömmlichen juristischen Methoden bewältigt werden können (vgl. BVerfG, Urt. v. 22.11.2000 - 1 BvR 2307/94 u.a. -, BVerfGE 102, S. 254, 337, juris Rn. 326). Die Auslegung von § 15 Abs. 1 GstG kommt zu einem eindeutigen Ergebnis. Insoweit wird auf die vorstehenden Ausführungen unter II. 1. Bezug genommen.

b) § 15 Abs. 1 GstG steht auch im Einklang mit Art. 3 Abs. 1 GG (vgl. zur Geltung als allgemeiner Rechtsgrundsatz: BVerfG, Beschl. v. 02.05.1967 - 1 BvR 578/63 -, juris Rn. 30). Ein Verstoß gegen den aus Art. 3 Abs. 1 GG folgenden allgemeinen rechtsstaatlichen Grundsatz liegt entgegen der Ansicht des Klägers nicht darin begründet, dass § 15 Abs. 1 GstG zwar für die Entsendung in Aufsichtsräte von Kapitalgesellschaften, an denen eine Gemeinde beteiligt ist, aber nicht für die Mitgliedschaft in „Ausschüssen von Eigenbetrieben“ gilt.
Grundlegende Unterschiede zwischen einem Werkausschuss nach § 5 Abs. 2 Eigenbetriebsverordnung (EigVO) einerseits und dem Aufsichtsrat von Kapitalgesellschaften, an denen eine Gemeinde beteiligt ist, andererseits, rechtfertigen die Ungleichbehandlung im Hinblick auf die Anwendbarkeit des § 15 Abs. 1 GstG. Unberührt von dem Recht der Gemeindevertretung, nach § 45 GO einen Werkausschuss zu bilden und ihm bestimmte Entscheidungen zu übertragen, sind Eigenbetriebe der Gemeinden gemäß § 1 Abs. 1 EigVO wirtschaftliche Unternehmen ohne Rechtspersönlichkeit nach § 106 GO. Deren Werkleitung unterliegt der Aufsicht der Bürgermeisterin oder des Bürgermeisters (§ 2 Abs. 4 Satz 1 EigVO) oder, soweit sich die Gemeinde für einen Werkausschuss entschieden hat (§ 5 Abs. 2 EigVO i.V.m. § 45 GO), der Kontrolle durch diesen. Die Mitglieder des Werkausschusses werden - wie auch die Mitglieder anderer Ausschüsse - je nach Verlangen einer Fraktion im Wege der Verhältniswahl oder aber durch Mehrheitswahl gewählt (§ 46 Abs. 1, § 40 Abs. 3 und 4 GO). Ebenso wie Mitgliedern anderer Ausschüsse obliegt es ihnen, an der Kontrollaufgabe der Gemeindevertretungen mitzuwirken (§ 45 Abs. 1 1. Halbsatz GO). Sie haben einen Repräsentationsauftrag, so dass der Grundsatz der Spiegelbildlichkeit fortwirkt. Nach diesem Grundsatz müssen, wenn aus einem Organ heraus, in dem das Wahlvolk unmittelbar repräsentiert wird, andere Organe geschaffen werden, diese weiteren Organe in ihrer Zusammensetzung die Mehrheitsverhältnisse in dem übergeordneten Organ in ihrer politischen Gewichtung widerspiegeln (vgl. BVerfG, Urt. v. 08.12.2004 - 2 BvE 3/02 -, juris Rn. 46).
Für Aufsichtsräte von Kapitalgesellschaften - wie einer GmbH, an der die Gemeinde hier beteiligt ist - gelten hingegen andere Grundsätze. Anders als die Eigenbetriebe haben Kapitalgesellschaften eine eigene Rechtspersönlichkeit (vgl. z.B. § 13 Abs. 1 GmbHG). Die Aufgaben der Aufsichtsräte bestimmen sich nach dem Gesellschaftsrecht. Einem Aufsichtsrat einer GmbH kommt eine Überwachungs- und Prüfungsfunktion (§ 52 Satz 1 GmbHG i.V.m. § 111 Abs. 1 und Abs. 2 AktG) zu, ohne zugleich - anders als die Gemeindevertretung - oberstes Organ der Gesellschaft bzw. der Gemeinde zu sein. Die Benennung der Vertreterinnen und Vertreter der Gemeinde für einen Aufsichtsrat ist nicht als Wahl gemäß § 40 GO, sondern als Beschluss gemäß § 39 GO ausgestaltet, weshalb das politische Kräfteverhältnis der Gemeindevertretung nicht abzubilden ist. Die Mitglieder des Aufsichtsrats haben an der Repräsentationsfunktion der Gemeindevertretung nicht teil. Sie sind vielmehr bei Ausübung ihrer Aufsichtsratstätigkeit an die mehrheitlich beschlossenen Weisungen der Gemeindevertretung gebunden (§ 104 Abs. 2 i.V.m. § 25 Abs. 1 GO) und handeln - anders als die Gemeindevertreter oder Mitglieder von Ausschüssen (§ 32 Abs. 1 GO) - nicht in freier Ausübung eines Mandats.

c) § 15 Abs. 1 GstG verstößt auch nicht gegen die Garantie der kommunalen Selbstverwaltung gemäß Art. 28 Abs. 2 Satz 1 GG, Art. 54 Abs. 1 SHVerf.
Abgesehen davon, dass die Selbstverwaltungsgarantie des Art. 28 Abs. 2 Satz 1 GG ausdrücklich nur im Rahmen der Gesetze besteht und die landesverfassungsrechtliche Garantie des Art. 54 Abs. 1 SHVerf die Selbstverwaltung der Gemeinden ausdrücklich nur schützt, soweit die Gesetze nicht ausdrücklich etwas anderes bestimmen, sind Eingriffe in die kommunale Selbstverwaltung durch ein Gesetz oder aufgrund eines Gesetzes zulässig, soweit die gesetzliche Regelung durch hinreichende sachliche Gründe getragen ist, einem legitimen Zweck dient, den Anforderungen des Verhältnismäßigkeitsgrundsatzes genügt und den Kernbereich der Selbstverwaltungsgarantie unangetastet lässt (vgl. BVerfG, Urt. v. 21.11.2017 - 2 BvR 2177/16 -, juris, Rn. 69 ff. m.w.N.). Zu dem verfassungsrechtlich verbürgten Kernbereich zählen vor allem die gemeindlichen Hoheitsrechte (Gebiets-, Planungs-, Personal-, Organisations- und Finanzhoheit), die der Staat den Gemeinden im Interesse einer funktionsgerechten Aufgabenwahrnehmung in ihrem Grundbestand garantieren muss (BVerfG, Urt. v. 21.11.2017, a.a.O., juris Rn. 88). Dies zugrunde legend ist hier festzustellen, dass § 15 Abs. 1 GstG zwar in die Organisations- und Personalhoheit einer Gemeinde eingreift; der damit verfolgte Zweck dient aber der tatsächlichen Gleichstellung von Frauen und Männern und entspricht damit der Staatszielbestimmung des Art. 9 Satz 1 SHVerf, wonach es Aufgabe des Landes, der Gemeinden und Gemeindeverbände sowie der anderen Träger der öffentlichen Verwaltung ist, die rechtliche und tatsächliche Gleichstellung von Frauen und Männern zu fördern. § 15 Abs. 1 GstG verfolgt somit ein verfassungsrechtlich verbürgtes Ziel und damit zugleich einen legitimen Zweck.
Die damit einhergehende Einschränkung der Selbstverwaltungsgarantie ist nicht nur geeignet, den legitimen Zweck zu fördern, sondern die in § 15 Abs. 1 GstG getroffene Regelung ist für das Erreichen des damit verfolgten Zieles erforderlich und auch angemessen. Mit einer gesetzlichen Regelung, die eine Repräsentation von Frauen entsprechend dem Geschlechterproporz in der Gemeindevertretung vorsähe, wäre das Ziel der Gleichstellung von Frauen und Männern (hier in

Gestalt der geschlechterparitätischen Entsendung von Mitgliedern in den Aufsichtsrat) nicht ebenso wirksam gefördert. Der Eingriff in die Organisationshoheit der Gemeinde hat ein nur geringes Gewicht, weil § 15 Abs. 1 GstG keine absolute Einschränkung der Handlungsmöglichkeiten der Gemeinde begründet. Denn bei § 15 Abs. 1 GstG handelt es sich um eine Soll-Vorschrift, so dass in atypischen Fällen Ausnahmen zulässig sind.

4. § 15 Abs. 1 GstG verstößt auch nicht gegen höherrangiges Bundesrecht. Die bundesrechtlichen Normen haben einen anderen Anwendungsbereich als das Gleichstellungsgesetz, so dass Art. 31 GG (Bundesrecht bricht Landesrecht) nicht zum Tragen kommt.

a) § 15 Abs. 1 GstG gehört dem Kommunalrecht (Landesrecht) und nicht dem Gesellschaftsrecht (Bundesrecht) an. Das Verwaltungsgericht hat in seinem Urteil zu Recht hervorgehoben, dass der Kläger bei der ihm obliegenden Entsendungsentscheidung nicht Normadressat des GmbH-Gesetzes ist und § 52 Abs. 1 GmbHG interne Sonderregelungen für bestimmte Gesellschafter nicht ausschließt. Der Landesgesetzgeber war auch nicht durch Art. 74 Abs. 1 Nr. 11 GG gehindert, landesrechtliche Regelungen zur geschlechterparitätischen Gremienbesetzung zu erlassen. Das Verwaltungsgericht hat in seiner Entscheidung ebenfalls zutreffend ausgeführt, dass die konkurrierende Gesetzgebungszuständigkeit des Bundes für das Recht der Wirtschaft durch die in § 15 Abs. 1 GstG vorgesehene Gleichstellungsregelung nicht betroffen wird, weil diese Norm nur die internen Verhältnisse der Gesellschafterin Stadt Husum regelt.

b) Schließlich steht auch weder das Bundesgremienbesetzungsgesetz (BgremBG) noch das Bundesgleichstellungsgesetz (BGleiG) der landesrechtlichen Regelung zur geschlechterparitätischen Gremienbesetzung entgegen. Denn beide Gesetze gelten nur, soweit der Bund Mitglieder für Gremien bestimmen kann (§ 1 BGremBG), bzw. für Dienststellen des Bundes (§ 2 i.V.m. § 3 Abs. 1 Nr. 5 BGleiG) und Unternehmen mit Bezug zur Bundesverwaltung (§ 2 i.V.m. § 3 Abs. 1 Nr. 9 BGleiG).

Die Revision ist nicht zuzulassen, da Zulassungsgründe im Sinne des § 132 Abs. 2 VwGO nicht vorliegen.

Aus dem Landesverband

Finanzdiskussionen in der Wüste

Bericht über die Reise des Kämmererverbandes nach Israel

Auf Einladung des israelischen Kämmererverbands hatte ich im März die Gelegenheit, an der dortigen Tagung in Eilat im Süden Israels teilzunehmen. Die deutsche Delegation wurde verstärkt durch Kollegen aus Cuxhaven, Solingen und Neuss.
Angekommen in Tel Aviv, konnten wir mit den Kolleginnen und Kollegen aus Georgien Jerusalem besuchen. In der dortigen Grabeskirche zog es die Georgischen Kolleginnen und Kollegen unbedingt in die Grabkammer Jesu, wo immer nur 5 Personen zurzeit hineindürfen, und sie wirbelten damit den engen Zeitplan des Tages durcheinander. Aber wir sind rechtzeitig zum gemeinsamen Dinner mit Fortführung der am Tage begonnenen Fachgespräche in Jaffa eingetroffen. Die amerikanische Delegation war nun auch angekommen und israelische Kämmererkollegen brachten uns alle in guten Gesprächen zueinander.
Tags drauf um 8.30 Uhr startete die Bustour quer durch die Wüstenlandschaft Israels zur Festung Masada, errichtet von Heroes kurz vor Christi Geburt. Ein Bad im Toten Meer durfte nicht fehlen, und es ging sogleich weiter zum Kongressort Eilat. Dort folgte noch am Abend eine erste Zusammenkunft mit allen Delegierten. Fachgespräche und persönliches Kennenlernen in netter Atmosphäre auf der Dachterrasse des Hotels rundeten einen vielfältigen Tag ab.
Am Folgetag ging es morgens noch schnell in das Underwater Observatorium nahe Eilat, bevor anschließend die Eröffnungszeremonie des Kämmererkongresses begann. Anwesend waren rd. 200 israelische Kämmerer und die internationalen Teilnehmer aus China, Georgien, den USA und Deutschland. Der israelische Verbandsvorsitzende beschrieb den dortigen Finanzausgleich und betonte die enge Zusammenarbeit zwischen den dortigen Gemeinden. Weiter sprach der Direktor der DEXIA-Bank als Finanzinstitut für den öffentlichen Bereich und berichtete von öffentlichen Projekten, die von dort finanziert werden, z. B. im Bildungssektor und im Verkehrsbereich. Patrick Mc Coy aus New York berichtete von dortigen Verkehrsprojekten. Yuan Peiquan aus Shandong, China, erläuterte das dortige Finanzsystem, das modernisiert werden soll. Grußworte folgten auch seitens des

Eröffnung der Kämmerertagung in Eilat, Israel

Deutschen Delegationsleiters Frank Gensler zur Struktur des Deutschen Kämmererverbands und zu den Gemeinsamkeiten der Kommunen. David Khosruashvili aus Georgien beschrieb die schon freundlichen Beziehungen zum israelischen Verband und würdigte die Verdienste dieser jahrelangen Zusammenarbeit.
Der Kollege Patrick Mc Coy vom amerikanisch-kanadischen Verband sprach später noch zu den Konferenzteilnehmern und erläuterte die Struktur der Organisation mit 19.300 Mitgliedern, vorwiegend Kommunen, aber auch Regionen, Universitäten und auch dem Träger des öffentlichen Nahverkehrs in New York. Diese starke Gemeinschaft hat gutes Gehör bei der US-Regierung und somit auch in den Büros in Chicago und Washington D. C. gefunden. Der Verband kümmert sich um die Auswahl von ERP-Software für seine Mitglieder und vergibt sogar Stipendien. Die MTA als Träger des ÖPNV in New York befördert täglich 6,3 Mio. Menschen sowie 17 Mio. Tonnen Fracht im Jahr, womit die Straßen New Yorks erheblich entlastet werden. Aktuell wird die Grand Central Station in Manhattan unter laufendem Betrieb erweitert und das – für uns schon verwunderlich – im bestehenden Zeit- und Kostenrahmen.
Nach dem Abschluss des Kongresses ging es auf eine lange Busreise von Eilat nach Nazareth. Dort folgten das Abendessen und Fachgespräche mit hinzugekommenen israelischen Kollegen sowie den mitgereisten aus den USA und Georgien.
Am Folgetag standen die Besichtigung der Verkündigungskirche in Nazareth sowie ein Stadtrundgang auf dem Programm, bevor die Reise auf die Golan-Höhen fortgesetzt wurde, die von Israel im sog. Sechstageskrieg erobert wurden.
Zu guter Letzt folgte noch die Besichtigung von Tropfsteinhöhlen nahe Jerusalem, bevor ein Kollege uns mit seinem Wagen zurück zum Flughafen nach Tel Aviv brachte, so dass wir mit vielen neuen Eindrücken heimkehren konnten. Fachlicher Austausch also mal anders und überaus bereichernd.

Manfred Uhlig,
Kämmerer der Hansestadt Lübeck
– Mitglied im Fachverband der
Kämmerer SH

Veranstaltungsankündigung:

7. Forum Recht der kommunalen Wirtschaft am 26. Juni 2018 in Kiel

Schleswig-Holsteinischer GEMEINDETAG

Gemeinsam mit dem Institut für Öffentliches Wirtschaftsrecht an der Christian-Albrechts-Universität zu Kiel lädt der SHGT herzlich ein zum 7. Forum Recht der kommunalen Wirtschaft unter wissenschaftlicher Leitung von Prof. Dr. Christoph Brüning und Prof. Dr. Marcus Arndt am Dienstag, den 26. Juni 2018, 09:30 Uhr bis 16:30 Uhr in Kiel, Vortragssaal der Kunsthalle, Düsternbrooker Weg 1, 24105 Kiel.
Die kommunale Wirtschaft wird durch Gesetzgeber und Rechtsprechung auch in diesem Jahr vor neue Herausforderungen und Chancen gestellt. Die im Kieler Koalitionsvertrag angekündigte Weiterentwicklung des Vergaberechts beginnt in Kürze. Geplant ist ein neues Vergabegesetz Schleswig-Holstein. Dabei geht es u.a. um die Beseitigung von Mängeln des Tariftreue- und Vergabegesetzes und die Übernahme der Unterschwellenvergabeordnung in Schleswig-Holstein. Außerdem hat der Landtag die Pflicht zur Erhebung von Straßenausbaubeiträgen abgeschafft. Hieraus ergeben sich Rechtsfolgen und Handlungsoptionen.
Kommunale Abgaben und kommunale Gremien stehen im Fokus aktueller Rechtsprechung. Ob zur Tourismusabgabe, zur Zweitwohnungssteuer oder zu Strandbenutzungsgebühren: wichtige Urteile erfordern eine Reaktion der Praxis.
Ebenso praxisrelevant ist die neueste Rechtsprechung zur Erhebung von Gebühren für die Entwässerung von Straßen anderer Straßenbaulastträger. Außerdem hat das OVG im Dezember 2017 eine wichtige Entscheidung zur Beachtung der paritätischen Besetzung nach § 15 Gleichstellungsgesetz bei der Besetzung von Aufsichtsorganen kommunaler Unternehmen und anderen Gremien gefällt (S. Rubrik „Aus der Rechtsprechung“ in dieser Ausgabe).
Gemeinden finanzieren ihre Aufgaben nicht nur durch Abgaben, Schlüsselzuweisungen, Steueranteile und Gemeindesteuern. Ohne Eigenleistung von Bürgern, Sponsoring, Spenden und andere Sonderformen der Finanzierung wären viele kommunale Leistungen nicht möglich.
Mit diesen Themen auf dem 7. „Forum Recht der kommunalen Wirtschaft“ bietet der Gemeindetag den Gemeinden, Städten und Ämtern, Zweckverbänden, kommunalen Betrieben, Kommunalpolitikern, Angehörigen beratender Berufe sowie allen anderen am Recht der kommunalen Wirtschaft Interessierten Gelegenheit zur Teilnahme an einer von erstklassigen Rechtsexperten aus Wissenschaft, Anwaltschaft und Verwaltung gestalteten Fachtagung.
Prof. Dr. Christoph Brüning, Universitätsprofessor an der CAU Kiel, Prof. Dr. Marcus Arndt, Fachanwalt für Verwaltungsrecht und Honorarprofessor an der CAU Kiel, Prof. Dr. Marius Raabe, Fachanwalt für Vergaberecht und Fachanwalt für Verwaltungsrecht sowie Honorarprofessor an der CAU Kiel, Prof. Dr. Florian Becker, Universitätsprofessor an der CAU Kiel, Reimer Steenbock, Verbandsdirektor a. D. und Jörg Bülow, Gf. Vorstandsmitglied des SHGT, werden zu diesen und weiteren Themen referieren.

Anmeldungen nimmt die Geschäftsstelle des SHGT unter Angabe der Kontaktdaten (Name, Gemeinde/ Amt/ Einrichtung, Telefonnummer) per Fax (0431-57005054) oder e-Mail: (info@shgt.de) entgegen. Es wird darum gebeten, den Unkostenbeitrag i.H.v. 30,- € incl. 19 % MwSt umgehend auf das Konto des SHGT, IBAN: DE71 2105 0170 0000 1733 85 bei der Förde Sparkasse mit Namensangabe unter dem Stichwort „Kommunalforum“ zu überwiesen. Er enthält bereits die Kosten für Kaffee und Mittagsimbiss.

Infothek

SHGT kritisiert hohe zweckgebundene Tranchen im Entwurf der Richtlinie zur Umsetzung des Schulbau- und Schulsanierungsprogramms des Landes (IMPULS 2030) - nur noch 27,4 Mio. € von 50 Mio. € für die Sanierung von Schulen

Der SHGT hat in einer gemeinsamen Stellungnahme mit den anderen Kommunalen Landesverbänden den Entwurf der Richtlinie zur Umsetzung des Schulbau- und Schulsanierungsprogramms des Landes (IMPULS 2030) kritisiert. Kernpunkt der Kritik ist insbesondere die vom Ministerium geplante zweckgebunde Aufteilung des Programms. Sie führt dazu, dass für allgemeine Investitionen in kommunalen Schulbau bzw. Schulsanierungen landesweit nur noch 27,4 Mio. € zur Verfügung stehen. Nach Auffassung des SHGT sind diese Zwecksetzungen zum Teil nicht von der Vereinbarung zwischen der Landesregierung und den kommunalen Landesverbänden vom 11. Januar 2018 gedeckt. Dies betrifft u.a. insbesondere die Mittelreservierung für Ersatzschulen in Höhe von 5,7 Mio. € und Lärmschutzmaßnahmen an Grundschulen in Höhe von 7 Mio. €. Es ist weiterhin das Ziel der Kommunalen Landesverbände, diese Mittel wie vereinbart den Kommunen zur Sanierung ihrer Schulen zur Verfügung zu stellen.

SHGT begrüßt Erlass zur Einführung eines landesweiten und einheitlichen Feuerwehrdienstausweises für die Mitglieder der Freiwilligen Feuerwehren

Der SHGT begrüßt den am 7. Mai 2018 im Amtsblatt für Schleswig-Holstein (374) veröffentlichten Erlass zur Einführung eines landesweiten und einheitlichen Feuerwehrdienstausweises für die Mitglieder der Freiwilligen Feuerwehren. Mit dem Erlass wurde nicht nur ein moderner Ausweis im Scheckkartenformat eingeführt, der den dem bisherigen Erlass aus dem Jahre 1969 (Amtsbl. SH 342), zugrundeliegenden roten Papierausweis („rote Pappe“) ablöst. Vielmehr ist der neue Ausweis zugleich Versichertenkarte der Hanseatischen Feuerwehr-Unfallkasse Nord und Ehrenamtskarte.

In dem ersten Erlassentwurf, der den Kommunalen Landesverbänden zur Anhörung übersandt wurde, war zunächst vorgesehen, dass sich jedes Feuerwehrmitglied zwingend ausweisen können muss. Der SHGT hatte daher in einer gemeinsamen Stellungnahme mit dem Städteverband die Einführung des modernen Dienstausweises zwar begrüßt, jedoch darauf hingewiesen, dass nicht in allen Wehren ein entsprechender (dienstlicher) Bedarf an einem Feuerwehrdienstausweis erkennbar ist. In der Regel werden Dienstausweise von Kameraden nachgefragt, um Angebote und Sonderrabatte von Firmen und Dienstleistern zu erhalten. Hierzu ist es in der Regel jedoch ausreichend, wenn die Mitgliedschaft schriftlich per Vordruck bestätigt wird. Vor diesem Hintergrund ist die nunmehr veröffentlichte Fassung des Erlasses zu begrüßen, da er lediglich die Möglichkeit vorsieht, dass Feuerwehren für sich einen Dienstausweis beschaffen können.

Die neuen Ausweise können ab sofort beim Versandhaus des Deutschen Feuerwehrverbandes bestellt werden. Die Daten (Name, Geburtstag, Foto, Ausweisnummer, Name der Feuerwehr…) können über das Verwaltungsprogramm Fox-112 online nach Erhalt eines Zugangscodes übermittelt werden. Die ersten 25.000 Bestellungen werden aus dem „Lottotopf“ des Landesfeuerwehrverbandes gefördert und sind zu einem Preis von je 1,82 € inkl. MwSt. (regulärer Preis: 2,32 €) erhältlich. Dieser Preis gilt unabhängig von der Bestellmenge. Gegen einen einmaligen Aufpreis von 15 € können die Ausweise mit dem Wappen der Gemeinde versehen werden. Weiterhin besteht die Möglichkeit, gegen Aufpreis den Ausweis mit einem Magnetstreifen oder RFID-Chip (Transponder) zu bestellen.

Weitere Informationen zum Feuerwehrdienstausweis sind auf der Internetseite des Landesfeuerwehrverbandes unter der Adresse www.lfv-sh.de unter der Rubrik „aktuelle Mitteilungen“ abrufbar.

Termine:

01.06.2018: Breitbandforum Schleswig-Holstein in Kiel

12.06.2018: Zweckverbandsausschuss des SHGT

14.06.2018: Kommunaltag Schleswig-Holstein auf der CeBIT

26.06.2018: 7. Forum Recht der kommunalen Wirtschaft in Kiel

04.07.2018: Landesvorstand des SHGT

04.07.2018: Parlamentarischer Abend der Kommunalen Landesverbände

Gemeinden und ihre Feuerwehr

Landesfeuerwehrversammlung 2018:

Freiwillige Feuerwehren mit mehr Mitgliedern und neuer Führungsspitze auf Zukunftskurs

Die 1349 Freiwilligen Feuerwehren in Schleswig-Holstein sind verlässlicher Garant für ein flächendeckendes Hilfeleistungssystem, für dessen Erhalt auf allen Verbands- und kommunalen Ebenen gearbeitet werden müsse. Das betonte die stellv. Landesverbandsvorsitzende Ilona Dudek in ihrem Bericht zur Landesfeuerwehrversammlung am 21. April 2018 in Reußenköge / Nordfriesland. Die Basis dafür – auskömmliche Mitgliederzahlen – sah die stellv. Vorsitzende als durchaus gegeben – auch wenn es vereinzelt Wehren gebe, die unter Personalmangel leiden und Probleme bei ihrer Tagesverfügbarkeit hätten. Dennoch weist die landesweite Mitgliederstatistik per 31.12.2017 nunmehr im vierten Jahr in Folge einen leichten Anstieg aus. 48.913 Männer und Frauen versahen zum Jahresende 2017 ehrenamtlichen Dienst – das sind 264 mehr als noch ein Jahr zuvor.

Mit Frank Homrich aus Wedel wählten die knapp 300 Delegierten einen neuen Landesverbandsvorsitzenden, der nun den Dienstgrad eines Landesbrandmeisters trägt. Homrich löst Detlef Radtke aus Lübeck ab, der seit 2006 im Amt war – nun aber aus gesundheitlichen Gründen nicht wieder kandidierte.

In der Koogshalle in Reußenköge wandte sich auch Ministerpräsident Daniel Günther (CDU) mit einem Grußwort an die Delegierten und Gäste. Günther würdigte die Feuerwehren im Land: „Was Sie für den Zusammenhalt in Schleswig-Holstein leisten, ist unbezahlbar und unverzichtbar. Jede einzelne Feuerwehr ist wichtig. Wir brauchen jede helfende Hand, in Zukunft noch mehr als bisher. Land und Kommunen vereint der Wunsch, dass sie gute Arbeits- und Einsatzbedingungen haben. Daher werden wir für 2019 und 2020 ein Sonderprogramm auflegen: Sechs Millionen Euro stellen wir zur Verfügung, um Gemeinden bei der Erweiterung, beim Ausbau oder Umbau von Feuerwehrhäusern unter die Arme zu greifen“, so der Ministerpräsident.

Jörg Bülow, geschäftsführendes Vorstandsmitglied des SHGT, wandte sich mit einem Grußwort an die Delegierten und Gäste der Landesfeuerwehrversammlung in Reußenköge

Auch Jörg Bülow, geschäftsführendes Vorstandsmitglied des SHGT, stellte in seinem Grußwort den Stellenwert der Freiwilligen Feuerwehren für die Sicherheit der Gemeinden im Land heraus und gab einen kurzen Überblick über aktuelle Feuerwehr-Themen, die in der Geschäftsstelle des SHGT derzeit aktiv begleitet werden. Dazu gehört etwa die Überarbeitung der Richtlinie zur Förderung des Feuerwehrwesens. Gezielte Förderanreize für Sammelbeschaffungen, eine Unterstützung und Beratung bei der Erstellung von Leistungsverzeichnissen, mehr Flexibilität bei der Förderung gebrauchter Fahrzeuge sowie eine höhere Rechtssicherheit in den Vergabeverfahren sind die zentralen Anliegen des SHGT. Besonders erfreulich sei es, so Bülow, dass es auf Initiative der Kommunalen Landesverbände gelungen sei, für die Jahre 2019 und 2020 ein Sonderprogramm „Feuerwehrerätehäuser“ in Höhe von insgesamt 6 Mio. € aufzulegen, das weit überwiegend dem kreisangehörigen Raum zugutekommen soll.

v.l.n.r.: Ministerpräsident Daniel Günther, bisheriger Landesbrandmeister Detlef Radtke und sein Nachfolger Frank Homrich

7.132 Brände (Rückgang um 2.629) wurden im Berichtsjahr bekämpft – darunter 622 Großbrände (Rückgang um 420). 21.712 Einsätze im Bereich der sogenannten Technischen Hilfe, z.B. bei Verkehrsunfällen oder Unwetterlagen, mussten geleistet werden. Das ist eine Steigerung um 2.327 Einsätze, die in erster Linie auf Unwetterlagen zurückzuführen ist. Die Zahl der Fehlalarme sank erneut von 6.046 auf 5.762. Unter „Sonstige Einsätze“ weist die Statistik 2.817 Einsätze (Rückgang um 1.916) aus.

Die vier Berufsfeuerwehren im Lande ergänzen die Statistik um 104.084 Rettungsdienst-Einsätze (+ 38.670), so dass die Gesamtzahl aller Feuerwehreinsätze im Berichtsjahr 141.507 beträgt.

„Die Einsatzzahlen spiegeln auch die Notwendigkeit eines flächendeckenden Hilfeleistungssystems mit funktionierenden Feuerwehren wider“, so der neue Landesbrandmeister Frank Homrich, der daher an die Kommunen als Träger des Brandschutzes appellierte, für auskömmliche Arbeits- und Ausstattungsbedingungen zu sorgen. Homrich kündigte Gespräche mit Politik und Verwaltung an, um gemeinsam alles zu unternehmen, um die Feuerwehren einsatzfähig zu halten. In der Zusammenarbeit mit den Kreis- und Stadtfeuerwehrverbänden versprach er einen offenen Dialog auf Augenhöhe. Laufende Projekte wie das verstärkte Werben und auch Halten von Mitgliedern, die Ausbildung von Konfliktlotsen und die Integration von Geflüchteten müssten unvermindert weitergeführt werden, kündigte der neue Landesbrandmeister an.

Als quasi letzte Amtshandlung stellte der scheidende Landesbrandmeister Detlef Radtke einen landeseinheitlichen Feuerwehr-Dienstausweis vor, den ab sofort alle Feuerwehrangehörigen im Land auf Antrag bekommen können. Die personifizierte Plastikkarte beinhaltet auch einen Versicherungsnachweis für die Hanseatische Feuerwehr-Unfallkasse Nord und die Ehrenamtskarte des Landes. Künftig sollen zudem weitere Bonusangebote für Feuerwehrangehörige geworben und in die Kar-

te implementiert werden. Die erste symbolische Karte nahm Ministerpräsident Daniel Günther entgegen.
Alle wichtigen Informationen sind auf der Homepage des Landesfeuerwehrverbandes Schleswig-Holstein unter www.lfv-sh.de/feuerwehrdienstausweis.html abrufbar. Darüber hinaus kann sich jede Firma / Einrichtung, die den Feuerwehrangehörigen im Lande besondere Aktionen oder Vergünstigungen gewähren möchte, an den Landesfeuerwehrverband Schleswig-Holstein (info@lfv-sh.de) wenden und wird auf Wunsch in die Übersicht aufgenommen, die regelmäßig aktualisiert und veröffentlicht wird.
Auf der Landesfeuerwehrversammlung wurden in den Landesvorstand gewählt:

- **Frank Homrich** (Wedel), zum Vorsitzenden des Landesfeuerwehrverbandes
- **Matthias Schütte** (Eckernförde), zum stellv. Landesverbandsvorsitzenden
- **Christian Albertsen** (Viöl), zum stellv. Landesverbandsvorsitzenden (ab.1.1.2019)

Im Rahmen der Versammlung wurden für ihre Verdienste um das Feuerwehrwesen geehrt:

- **Detlef Radtke** (Lübeck) Goldene Ehrennadel des Deutschen Feuerwehrverbandes und Ehrenmitgliedschaft im Landesfeuerwehrverband Schleswig-Holstein
- **Walter Gaul** (Lübeck), Deutsches Feuerwehr-Ehrenkreuz in Gold
- **Monika Radtke** (Lübeck), Deutsche Feuerwehr-Ehrenmedaille
- **Ilona Dudek** (Kiel), schleswig-holsteinisches Feuerwehr-Ehrenkreuz in Gold
- **Jörg Taube** (Heikendorf), schleswig-holsteinisches Feuerwehr-Ehrenkreuz in Gold
- **Andrea Witt** (Tökendorf), schleswig-holsteinisches Feuerwehr-Ehrenkreuz in Silber
- **Luey Hikmat** (Gröde), **Michel Schmidt** (Uelvesbüll), **Jan-Peter Petersen** (Ost-Langenhorn), Deutsches Feuerwehr-Ehrenkreuz in Bronze

Quelle: LFV-SH

Buchbesprechungen

PRAXIS DER KOMMUNALVERWALTUNG
Landesausgabe Schleswig-Holstein

Ratgeber für die tägliche Arbeit aller Kommunalpolitiker und der Bediensteten in Gemeinden, Städten und Landkreisen (Loseblattsammlung incl. 3 Online-Zugänge / auch auf DVD-ROM erhältlich)

Herausgegeben von:
Jörg Bülow, Dr. Jürgen Busse, Dr. Jürgen Dieter, Werner Haßenkamp, Prof. Dr. Hans-Günter Henneke, Dr. Klaus Klang, Prof. Dr. Hubert Meyer, Prof. Dr. Utz Schliesky, Prof. Dr. Gunnar Schwarting, Prof. Dr. Christian 0. Steger, Hubert Stubenrauch, Prof. Dr. Wolf-Uwe Sponer, Johannes Winkel und Uwe Zimmermann.

KOMMUNAL- UND SCHUL-VERLAG, 65026 Wiesbaden

Die vorliegende (nicht einzeln erhältliche) **534. Lieferung**, September 2017, Preis 79,90 Euro enthält:

C 11 - Juristische Probleme bei der Personalauswahl
Von Dr. Klaus Rischar
Mit dieser Überarbeitung wurde weitere aktuelle Rechtsprechung eingefügt.

K 4c- Gesetz über die Vermeidung und Sanierung von Umweltschäden (Umweltschadensgesetz- USchadG)
Von Dr. jur. Erich Gassner, Ministerialrat a. D., Rechtsanwalt und Dr.-Ing. Hans-Joachim Schemel, öffentlich bestellter und beeidigter Sachverständiger für Fachfragen der Eingriffsregelung und der Umweltverträglichkeitsprüfung.
Die Ausführungen zum USchadG wurden nahezu komplett überarbeitet, aktuelle Urteile wurden berücksichtigt.

K 31 a- Waffenrecht
Von Kurt Meixner, Ltd. Ministerialrat a. D.
Die Kommentierungen zu den §§ 5 (Zuverlässigkeit), 20 (Erwerb und Besitz von Schusswaffen durch Erwerber infolge eines Erbfalls), 34 (Überlassen von Waffen oder Munition, Prüfung der Erwerbsberechtigung, Anzeigepflicht), 50 (Gebühren und Auslagen) und 57 (Kriegswaffen) wurden überarbeitet.

L 3- Die Verantwortung der Gemeinden und Kreise bei der Wahl der Schöffinnen und Schöffen
Von Hasso Lieber. Rechtsanwalt, Staatssekretär für Justiz a. D., Vorsitzender des Bundesverbandes ehrenamtlicher Richterinnen und Richter, eherm. Präsident des Europäischen Netzwerkes der Organisationen Ehrenamtlicher Richter (European Network of Associations of Lay Judges-ENALJ)
Der Beitrag wurde komplett überarbeitet und enthält neben der Darstellung der aktuellen Rechtslage auch Vorschläge für den Gesetzgeber, wie durch eine Reform der Schöffenwahl der Aufwand für die kommunalen Verwaltungen verringert und gleichzeitig die Qualität der (künftigen) Amtsinhaber verbessert und infolgedesen die Strafverfahren effizienter werden könen.

L 12 SH - Straßen- und Wegegesetz des Landes Schleswig-Holstein (StrWG)
Von Richter am OVG Schleswig Reinhard Wilke, Bürgermeister Günther Gröller, fortgeführt von Richter Dr. Alexander Behnsen, tätig am Verwaltungsgericht Hamburg, Rechtsanwalt Dr. Bernd Hoefer und Richter am Verwaltungsgericht Dr. Christian Steinweg
Mit dieser Lieferung wurden die §§ 39-44a, 47 und 57 vollständig überarbeitet und neugefasst
Die Anhänge sind wieder auf dem aktuellen Stand.

Die vorliegende (nicht einzeln erhältliche) **535. Lieferung**, September 2017, Preis 79,90 Euro enthält:

H 5 - Die Sozialversicherung
Von Werner Gerlach, Vorstandsvorsitzender i.R.
Mit dieser Lieferung wurde die Kommentierung zu SGB V auf den aktuellen Stand gebracht.

J 9 SH - Landespflegegesetz (Ausführungsbestimmungen zur Pflegeversicherung in Schleswig-Holstein)
Von Ministerialrat a. D. Hans-Joachim Arndt
Der Beitrag wurde auf den aktuellen Stand gebracht; in den Anhang neu aufgenommen wurden die Alltagsförderungsverordnung und die Richtlinie über die Gewährung von Zuwendungen zur Förderung niedrigschwelliger Betreuungsangebote, Modellvorhaben zur Erprobung neuer Versorgungskonzepte und Versorgungsstrukturen, ehrenamtlicher Strukturen und der Selbsthilfe nach § 45 c und § 45 d SGB XI in Schleswig-Holstein.

Die vorliegende (nicht einzeln erhältliche) **536. Lieferung**, Oktober 2017, Preis 79,90 Euro enthält:

C 15 SH - Das Besoldungsrecht in Schleswig-Holstein unter besonderer Berücksichtigung der Kommunalbeamten
Begründet von Hans-Gerhard Fuhrmann, Ministerialrat a. D. und Dieter Siek, Oberamtsrat a. D., überarbeitet von Sylke Brandt, Dipl. Verwaltungswirtin, fortgeführt von Martina Neuendort, weiter fort-

geführt von Helmut Koch, Dipl.-Volkswirt, Dipl.-Verwaltungswirt (FH), Finanzministerium Schleswig-Holstein
Der Beitrag wurde auf den aktuellen Stand gebracht.

D 7 SH - Das Jagdrecht in Schleswig-Holstein
Kommentar von Dr. iur. Horst Schulz, Rechtsanwalt und Notar, Lübeck
Mit dieser Lieferung wurden die Kommentierungen zu den §§ 5 und 6 aus dem II. Abschnitt (Jagdbezirke und Hegegemeinschaften), §§ 11 und 14 aus dem 111. Abschnitt (Beteiligung Dritter an der Ausübung des Jagdrechts), § 15 aus dem IV. Abschnitt (Jagdschein), die §§ 19, 20, 22 aus dem V. Abschnitt (Jagdbeschränkungen, Pflichten bei der Jagdausübung und Beunruhigen von Wild), die §§ 29-35 aus dem VII. Abschnitt (Wild- und Jagdschaden) und § 42 aus dem X. Abschnitt (Straf- und Bußgeldvorschriften) BJagdG überarbeitet, ebenso die Kommentierungen zu den §§ 6 und 7 aus Abschnitt II (Jagdbezirke und Jagdausübungsrecht), die §§ 17, 17 a, 18, 21, 23 aus Abschnitt V (Jagdbeschränkungen und Jagdschutz), die §§ 26 und 29 aus Abschnitt VI (Jagdausübung), § 30 aus Abschnitt VII (Wild- und Jagdschaden) sowie § 37 aus Abschnitt IX (Ordnungswidrigkeiten) LJagdG überarbeitet.

Die vorliegende (nicht einzeln erhältliche) **537. Lieferung**, Oktober 2017,
Preis 79,90 Euro enthält:

A 27 SH -Gesetz über die Wahlen in den Gemeinden und Kreisen in Schleswig-Holstein
(Gemeinde- und Kreiswahlgesetz- GKWG)
Von Claus Asmussen, Ministerialdirigent, Landesrechnungshof Schleswig-Holstein und Hans-Jürgen Thiel, Oberamtsrat, Ministerium für Inneres und Bundesangelegenheiten Schleswig-Holstein
Die letzte Gesetzesänderung des § 30 GKWG (Wahlwerbung, unzulässige Veröffentlichung von Befragungen) wurde mit dieser Lieferung berücksichtigt.

B 1 SH -Gemeindeordnung für Schleswig-Holstein (Gemeindeordnung- GO)
Von Dr. Reimer Bracker, Ministerialdirigent a. D., Dr. Hartmut Borchert, Geschäftsführer beim Schl.-Holst. Gemeindetag a. D., Klaus-Dieter Dehn, Kommunalberater und zuvor Stellv. Geschäftsführer des Schl.-Holst. Landkreistages, Gerd Lütje, Bürgermeister a. D., Dr. Kurt-Friedrich von Schelіha, Ministerialdirigent a. D., Prof. Dr. Utz Schliesky, Direktor des Schleswig-Holsteinischen Landtages und Geschäftsführendes Vorstandsmitglied des Lorenz von Stein Instituts für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel, Dr. Joachim Schwind, Beigeordneter des Niedersächsischen Landkreistags, Dietrich Sprenger, Stellvertretender Geschäftsführer des Städteverbandes Schl.-Holst. a. D., Jochen von Allwörden, Geschäftsführendes Vorstandsmitglied des Städteverbandes Schl.-Holst., Prof. Dr. Marcus Arndt, Rechtsanwalt in Kiel, Jörg Bülow, Geschäftsführendes Vorstandsmitglied des Schl.-Holst. Gemeindetags, Jochen Nielsen, Dipl.-Verwaltungswirt, Referent beim Schl.-Holst. Gemeindetag, Frank Dieckmann, Dipl.-Volkswirt, Hauptkoordinator des Innovationsrings Neues Kommunales Rechnungswesen Schl.-Holst., Marc Ziertmann, Ass. jur., Dipl.-Verwaltungswirt, Stellv. Geschäftsführer beim Städteverband Schl.-Holst., Bernhard Schmaal, Stadtoberinspektor, Projektbeauftragter Doppik bei der Stadt Quickborn, Dr. Sönke E. Schulz, Geschäftsführendes Vorstandsmitglied des Schleswig-Holsteinischen Landkreistages, Gabriele Anhalt, Ministerialrätin, Landesrechnungshof Schleswig-Holstein, Frank Husvogt, Ltd. Verwaltungsdirektor, Leiter des Rechtsamts der Landeshauptstadt Kiel, Dr. Jakob Tischer, Ass. iur., Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel, Dr. Thilo Rohlfs, Kreisverwaltungsdirektor, Fachbereichsleiter Umwelt, Kommunal- und Ordnungswesen, Kreis Rendsburg-Eckernförde, Thorsten Ingo Wolf, Leiter des Rechtsamtes des Kreises Segeberg, Saskia Habelt, Regierungsdirektorin beim Landesrechnungshof Schleswig-Holstein, Kiel, Dr. Achmed El Bureiasi, Hochschullehrer an der FH für Verwaltung und Dienstleistung in Altenholz
Kommentierungen zu den §§ 1 (Selbstverwaltung) und 22 (Ausschließungsgründe) GO, die Kommentierungen zu den §§ 27, 28, 30-32, 32a, 33-37, 39, 40, 40a, 41, 42, 45c, 46, 47a, 47b, 47c GO wurden aktualisiert.

K 4a- Umweltverträglichkeitsprüfung (UVP)
Von Dr. Wolfgang Sinner, Vors. Richter am Bayerischen Verwaltungsgericht München, Prof. Dr. Ulrich M. Gassner, Mag. rer. publ., M. Jur. (Oxon.), Professor für Öffentliches Recht mit Schwerpunkt europäisches und nationales Umweltrecht an der Universität Augsburg und Dr. Joachim Hartlik, Inhaber des Büros für Umweltprüfungen und Qualitätsmanagement, Lehrte.
Mit dieser Lieferung wurden einmal mehr wichtige aktuelle Urteile des EuGH zur UVP, allen voran die Entscheidung vom 15.10.2015 im Vertragsverletzungsverfahren gegen Deutschland aufgenommen. Darüber hinaus wurde Anhang 3 mit Rechtsprechung des EuGH und nationaler Gerichte zur UVP neu bearbeitet.

K 8 - Bundesmeldegesetz (BMG)
Änderungen des Gesetzes wurden eingefügt.
Die vorliegende (nicht einzeln erhältliche) **538. Lieferung**, November 2017,
Preis 79,90 Euro enthält:

D 5 SH - Waldgesetz für das Land Schleswig-Holstein (Landeswaldgesetz - LWaldG)
Von Diplomforstwirt (Uni) Hans Jacobs
Die Kommentierung wurde umfassend aktualisiert und damit wieder auf den aktuellen Stand gebracht.

G 2 SH - Kindertagesstättengesetz Schleswig-Holstein
Prof. Dr. Mathias Nebendahl, Rechtsanwalt und Notar, Fachanwalt für Arbeitsrecht, Medizinrecht und Verwaltungsrecht, Kiel, Honorarprofessor an der Christian-Albrechts-Universität zu Kiel, Dr. Johannes Badenhop, Rechtsanwalt und Fachanwalt für Verwaltungsrecht Kiel, und Andrea Strämke, Dipl. Sozialarbeitein/Sozialpädagogin (FH) & Master Soziale Arbeit, Leiterin des Osterberg-Instituts der Karl Kübel Stiftung für Kind und Familie.
Bei der Neukommentierung liegt ein Schwerpunkt u.a. auf den Fragen der Finanzierung von Kindertageseinrichtungen. So werden Modelle von Finanzierungsvereinbarungen ebenso dargestellt wie die Förderprogramme des Bundes und des Landes zur Qualitätsentwicklung, Fachberatung oder zur Errichtung von Familienzentren.

Schaetzell/ Busse/ Dirnberger
Baugesetzbuch / Baunutzungsverordnung Kommentar

Kommunal- und Schul- Verlag
26. Nachlieferung, März 2018
2.258 Seiten,
Loseblattausgabe (in 2 Ordnern)
Format 16,5 x 23,5 cm
Bezugspreis: 149,00 Euro
ISBN: 978-3-86115-922-3

Verordnung über bauliche Nutzung der Grundstücke (Baunutzungsverordnung – BauNVO)
Von Gustav-Adolf Stange, Staatssekretär a.D.

Diese Lieferung berücksichtigt bis dahin bekannt gewordene Gerichtsentscheidungen sowie das einschlägige Schrifttum. Des Weiteren hat Berücksichtigung gefunden, dass die Baunutzungsverordnung neu gefasst wurde. Mit dieser Lieferung erhalten Sie die neuen Kommentierungen bis einschließlich § 10, die übrigen Seiten folgen im kommenden Monat.