Rödl & Partner

FOKUS PUBLIC SECTOR

Ausgabe: JANUAR 2019

Informationen für Entscheider in Verwaltung, Unternehmen und Politik

Liebe Leserin, lieber Leser,

Wir wünschen Ihnen ein gesundes und erfolgreiches Jahr 2019 und freuen uns, Sie auch im neuen Jahr wieder mit aktuellen Themen aus Verwaltung, Unternehmen und Politik regelmäßig begleiten zu dürfen.

Zum Auftakt unserer ersten Newsletter Ausgabe im neuen Layout informieren wir Sie über die neue Berechnungsgrundlage für die Bewertung von Pensionsrückstellungen. Mit dem Schreiben vom 19. Oktober 2018, hat das Bundesfinanzministerium Stellung zu der Anwendung der neuen Richttafeln und den damit einhergehenden Übergangsregelungen genommen. Mehr dazu erfahren Sie im ersten Beitrag.

Rödl & Partner hat zusammen mit dem Finanzenverlag Fondgesellschaften, Banken und Vermögensverwalter geprüft und den Transparenten Bullen für eine anlegergerechte Informationspolitik in Publikums- und Spezialfonds verliehen. Lesen Sie in unserem Beitrag, welche Anbieter der Investmentfonds den Preis mit nach Hause nehmen konnten.

Der Ausbau der Breitbandinfrastruktur in Deutschland ist ein komplexes Geflecht, das vor allem auch vergaberechtliches Know how erfordert. Wir zeigen auf, welche Grundlagen erfüllt sein müssen und welche Praxisprobleme auftreten können, wenn vergabe- und fördermittelrechtliche Bestimmungen in Einklang gebracht werden müssen.

Wenn ein steuerlicher Querverbund durch eine verbindliche Zusage bestätigt wurde, wird dieser von der Finanzverwaltung im Rahmen einer Betriebsprüfung nicht geprüft. So zumindest der Grundsatz bisher. Gilt das weiterhin oder gibt es Änderungen dazu? Lesen Sie mehr in unserem Beitrag.

Durch die DSGVO mussten viele Landesdatenschutzgesetze angepasst werden. Daher ist es auch für Gebietskörperschaften und Unternehmen des Öffentlichen Sektors eine Herausforderung, die Bestimmungen einzuhalten. Wir bieten Ihnen in dieser Ausgabe einen kurzen Überblick zur DSGVO und zum Datenschutzmanagement.

Lesen Sie außerdem, warum viele Behörden immer noch kein Informations-Sicherheitsmanagementsysteme haben, wie Cybersecurity-Ratings bei der Beurteilung der Cybersecurity-Resilienz helfen können und was kommunale Rechnungsprüfungsämter unternehmen müssen, um den Anschluss bei der digitalen Rechnungsprüfung nicht zu verlieren.

MARTIN WAMBACH
Geschäftsführender Partner

HEIKO PECH
Partner

Neue Berechnungsgrundlagen für die Bewertung von Pensionsrückstellungen

von Peter Alfes

Für die Ermittlung von Pensionsrückstellungen werden die allgemein anerkannten "Heubeck-Richttafeln“ als Berechnungsgrundlage herangezogen. Im Sommer 2018 wurden neue Heubeck-Richttafeln veröffentlicht ("Heubeck-Richttafeln 2018 G"), die in den meisten Fällen zu einem Anstieg der Pensionsrückstellungen führen werden. Die Aktualisierung bringt die biometrischen Rechnungsgrundlagen für Pensionsverpflichtungen in Deutschland auf den neuesten Stand und berücksichtigt dabei erstmals auch sozioökonomische Auswirkungen auf die Lebenserwartung.

Das Bundesfinanzministerium hat mit Schreiben vom 19.10.2018 zur Anwendung der neuen Richttafeln und den damit einhergehenden Übergangsregelungen Stellung genommen (BMF-Schreiben vom 19.10.2018, IV C 6 - S 2176/07/10004:001).

STEUERLICHE ANERKENNUNG

Für die Bewertung von Pensionsrückstellungen gelten die anerkannten Regeln der Versicherungsmathematik (§ 6a Abs. 3 Satz 3 EStG). Die Richttafeln von Professor Klaus Heubeck setzen diese in der Praxis zutreffend um und werden auch steuerlich anerkannt.

ZEITLICHE ANWENDUNG

Die "Heubeck-Richttafeln 2018 G" sind erstmals am Ende des Wirtschaftsjahres zugrunde zu legen, das nach dem 20.7.2018 (Tag der Veröffentlichung der neuen Richttafeln) endet. Der Gesetzgeber erlaubt es jedoch übergangsweise die "Richttafeln 2005 G" noch für Wirtschaftsjahre anzuwenden, die vor dem 30.6.2019 enden. Dem Bilanzierenden ist damit die Anwendung der neuen Richttafeln zum 31.12.2018 freigestellt.

Der Übergang auf die neuen Richttafeln ist einheitlich für alle Pensionsverpflichtungen und alle sonstigen versicherungsmathematisch zu bewertenden Bilanzposten vorzunehmen.

AUSWIRKUNGEN DER NEUEN RICHTTAFELN

Die Auswirkungen der Anwendung der Richttafeln 2018 G dürften nach Auffassung von Heubeck – bei großen, durchschnittlich gemischten Beständen – bilanzsteuerrechtlich zu Zuführungen zu den Pensionsrückstellungen im Umfang von ca. 0,5 Prozent bis 1,2 Prozent und handelsbilanzrechtlich von 1,0 Prozent bis 2,0 Prozent führen. Im Einzelfall kann es abhängig vom Rechnungszins, der Bestandszusammensetzung und der Gehaltsdynamik sowie Fluktuation zu unterschiedlichen Effekten kommen.

VERTEILUNG DES UNTERSCHIEDSBETRAGES

Die neuen Richttafeln führen zu einem Unterschiedsbetrag in der Bewertung der Pensionsrückstellung. Dieser Mehraufwand kann gem. § 6a Abs. 4 Satz 2 EStG auf mindestens 3 Wirtschaftsjahre gleichmäßig verteilt der Pensionsrückstellung zugeführt werden. Sofern ein Minderbetrag entstehen sollte, gelten diese Regelungen analog.

AUSWIRKUNG AUF KOMMUNALE PENSIONSRÜCKSTELLUNGEN

Es ist anzunehmen, dass auch im kommunalen Bereich die Pensionsrückstellungen – analog zu den Rückstellungen in der Steuerbilanz – um 0,5 Prozent bis 1,2 Prozent steigen werden. Anwendungs- oder Übergangsregelungen wurden bislang noch nicht verlautbart.

KONTAKT FÜR WEITERE INFORMATIONEN

Peter Alfes
Steuerberater, Wirtschaftsprüfer
T +49 221 949 909 450
E peter.alfes@roedl.com

UMFASSEND INFORMIERT

REVISIONSSICHERE ARCHIVIERUNG DURCH DIGITALE DOKUMENTEN-STEUERUNG RICHTIG UMSETZEN.

Weitere Informationen zur Veranstaltung finden Sie unter
www.roedl.de/seminare

www.roedl.de/assurance-it

→ Finanzen

Rödl & Partner und der Finanzenverlag verleihen den Transparenten Bullen für eine anlegergerechte Informationspolitik in Publikums- und Spezialfonds

Die Wirtschaftsprüfungsgesellschaft Rödl & Partner und der Finanzenverlag haben erstmals Fondsgesellschaften, Banken und Vermögensverwaltern sowie semi-institutionellen Geldanlegern den Transparenten Bullen für eine anlegergerechte Informationspolitik in ausgewählten Publikums- und Spezialfonds verliehen.

Transparenz hat sich in der Geldanlage zu einem herausragenden Kriterium entwickelt. Interessierte Privatleute, aber vor allem semi-institutionelle Anleger, wie Kommunen, Verbände, Stiftungen, kirchliche Organisationen und Kranken- und Pensionskassen äußern regelmäßig den Wunsch, hinter das Handwerk eines Vermögensverwalters oder eines Fondsmanagers zu blicken. Bei den mit dem Transparenten Bullen ausgezeichneten Publikums- und Spezialfonds ist dies gewährleistet. Dort, wo Factsheet, Verkaufsprospekt, Jahres- und Halbjahresbericht sowie die wesentlichen Anlegerinformationen (KIID) an ihre Grenzen stoßen, liefert der Transparenzbericht die benötigten Informationen. Er gibt schlichtweg ein umfassendes Bild des jeweiligen Fonds ab. Keine Information bleibt im Verborgenen, kein Risiko unerkannt. Und in vielen Fonds schlummern eine Menge Informationslücken, die eine geforderte sachgerechte Kontrolle und Überwachung gerade für semi-institutionelle Anlegergruppen, die treuhänderisch „fremde“ Gelder bewirtschaften müssen und vor allem bei schwankungsintensiven Marktphasen und Entwicklungen sofort mit Anfragen aus Gremien oder Aufsichtsbehörden konfrontiert sind, nicht möglich machen.

Insgesamt wurden 36 Transparente Bullen für eine anlegergerechte Transparenz- und Informationspolitik verliehen. Ein Bulle ging jeweils an die semi-institutionellen Anleger Alte Hansestadt Lemgo, Landesverband Lippe und an die Missionszentale der Franziskaner, die jeweils Spezialfonds bewirtschaften. 31 Bullen gingen an namhafte Banken, unabhängige Vermögensverwaltungsgesellschaften und internationale Fondsgesellschaften. Dabei hat die DZ Privatbank allein 7 Bullen für ihre Fonds abgeräumt, mit denen vermögende Privatanleger und semi-institutionelle Anleger angesprochen werden. Die DJE Kapital AG hat 3 Bullen mit nach Pullach genommen. Zwei davon für ihre beiden Flagship-Fonds DJE Dividende & Substanz und Zins & Dividende. Das neue ESG-Reporting der Universal-Investment-Gesellschaft wurde mit einem Ehrenbullen ausgezeichnet. Ebenso erhielt das Bankhaus Donner & Reuschel für sein Premium-Reporting für Versorgungswerke einen Ehrenbullen.

Apropos Alte Hansestadt Lemgo: Stadtkämmerer und Erster Beigeordneter Dirk Tolkemitt erzählte in einem Impulsvortrag von seinen Erfahrungen mit der kommunalen Geldanlage. Gerade für die Argumentation gegenüber Rat, Verwaltung und Öffentlichkeit sei es wichtig, dass das Handwerk und die Ergebnisse der Vermögensverwaltung transparent analysiert, bewertet und dargestellt werden. Der Transparenzbericht helfe dabei, die Arbeit professionell darzustellen, das Konzept verständlich zu machen und die Aussagen zur Vermögensverwaltung in dem speziellen Fall der Absicherung von

Pensionsverpflichtungen zu belegen. „Ein wesentlicher Vorteil des Transparenzberichts ist ja, dass eine neutrale Instanz das Berichtswesen übernimmt und für die gesetzlich geforderte Überwachung und Kontrolle in der

Kapitalanlage eintritt“, sagt Dirk Tolkemitt. Er ruft daher Kommunen und Verbände auf, sich mit dem Thema gezielt auseinanderzusetzen.

In einem von zwei Praxis-Workshops im Vorfeld der Preisverleihung hat der renommierte Kapitalmarktrechtler Dr. Christian Waigel, zusammen mit Sabine Härtl von der DJE Kapital AG und Sissy Koch von Rödl & Partner die Preisträger darüber informiert, inwieweit der Transparenzbericht die neuen MiFid II-relevanten Informationen verarbeiten kann. „Damit wollen wir einen weiteren Mehrwert schaffen und der Transparenz-Community auch in Zeiten fortschreitender Regulierung das richtige Instrumentarium an die Hand geben“, betont Sissy Koch, Leiterin Vermögenscontrolling von Rödl & Partner.

„Die Entwicklung zeigt, dass sich vor allem Privatbanken und die absolut führenden Kapitalverwaltungsgesellschaften um größere Transparenz in ihren Flaggschifffonds bemühen. Der Nutzen für den Anleger wird dabei schnell deutlich: Die Informationspolitik gewährt ein hohes Maß an Einsicht in das Fondsmanagement, ferner werden mögliche Informationsdefizite durch eine verständliche Aufbereitung von vorhandenen Informationen ausgeglichen. Transparenz bedeutet hier also vor allem mehr Sicherheit in der Anlageentscheidung, was wiederum Qualität bedeutet. Letztlich ist das nichts anderes als die Basis für Vertrauen und trifft mit dem Gedanken den modernen Zeitgeist, der von Information und Transparenz geprägt ist“, sagt Alexander Etterer, Partner bei Rödl & Partner und Leiter des Fachbereichs Vermögensreporting/Vermögenscontrolling.

KONTAKT FÜR WEITERE INFORMATIONEN

Alexander Etterer
Diplom-Betriebswirt (FH)
T +49 221 949 909 600
E alexander.etterer@roedl.com

→ Vergaberecht

Vergabe Breitbandnetzinfrastruktur – Ein langer Weg zum schnellen Internet?

von Freya Schwering

Bei der Vergabe von Breitbandnetzinfrastruktur gilt es, vergaberechtliche und fördermittelrechtliche Bestimmungen in Einklang zu bringen. Hierzu ist nicht selten die Quadratur des Kreises notwendig, wie der Beitrag zeigen wird. „Vergabe Breitbandnetzinfrastruktur – Ein langer Weg zum schnellen Internet?" beschreibt den geförderten Ausbau von Breitbandnetzinfrastruktur aus vergaberechtlicher Perspektive.

EINFÜHRUNG

Seit 2015 fördert der deutsche Staat den flächendeckenden Breitbandausbau. Vor allem im ländlichen Raum erwies sich der Breitbandausbau aufgrund hoher Investitionskosten im Verhältnis zu einer geringen Anzahl an potenziellen Kunden als unwirtschaftlich.[1] Durch Fördergelder sollen Anreize für Unternehmen geschaffen werden, den ländlichen Raum zu erschließen. Flankiert wird der geförderte Breitbandausbau durch das DigiNetzG.[2] Aufgrund dieses Gesetzes können Synergieeffekte durch die Mitverlegung von Breitbandnetzinfrastruktur beim Ausbau von bspw. Strom- bzw. Gasnetzen erzeugt werden.

AUSSCHREIBUNGSPFLICHT? „SICHER IST SICHER!"

Kommunen und Landkreise sind Gebietskörperschaften und damit öffentliche Auftraggeber im Sinne des GWB.[3] Soweit sie als Nachfrager von Breitbandnetzinfrastruktur am Markt auftreten, sind sie grundsätzlich zur Ausschreibung verpflichtet. Das Gleiche gilt für juristische Personen des öffentlichen oder privaten Rechts, wie etwa das kommunale Stadtwerk. Neben dem Vergaberecht regelt auch das Fördermittelrecht, dass „der Zuwendungsempfänger aufgrund des Förderrechts verpflichtet ist, den Fördergegenstand in einem offenen und transparenten Verfahren auszuschreiben".

Von dieser grundsätzlichen Pflicht zur Ausschreibung nach dem Vergaberecht sieht § 116 Abs. 2 GWB eine Ausnahme vor. Danach kann von einer Ausschreibung abgesehen werden, die hauptsächlich den Zweck hat, dem öffentlichen Auftraggeber die Bereitstellung oder den Betrieb öffentlicher Kommunikationsnetze (...) für die Öffentlichkeit zu ermöglichen". Noch nicht abschließend gelöst ist, unter welchen Voraussetzungen die Bereitstellung bzw. der Betrieb von Breitbandnetzinfrastruktur von der Ausnahme erfasst wird. Letztlich sprechen die besseren Gründe dafür, dass die eng auszulegende Ausnahme nicht in jedem Fall von der Pflicht zur Durchführung eines Vergabeverfahrens befreit. Jedenfalls sollte ein offenes und transparentes Verfahren im Sinne eines strukturierten Bieterverfahrens durchgeführt werden, um neben dem Fördermittelrecht auch dem Beihilferecht zu genügen.

VERFAHRENSGESTALTUNG

Die Gestaltung einer solchen Ausschreibung orientiert sich stark an der Art des Fördergegenstandes. Gegenstand der Förderung sind das Wirtschaftlichkeitslückenmodell und das Betreibermodell. Im Rahmen des Wirtschaftlichkeitslückenmodells erhält der Betreiber der Breitbandnetzinfrastruktur die Differenz zwischen den Einnahmen und allen Kosten des Netzaufbaus und -betriebs. Ausgeschrieben wird demnach ein Netzbetreiber, der auch das Netz aufbaut. Beim Betreibermodell werden der Netzaufbau und/oder der -betrieb getrennt gefördert. In einem solchen Fall wird etwa ein Betreiber als Pächter von bestehender Netzinfrastruktur gesucht.

VERHANDLUNGSVERFAHREN BEI AUFTRAGSVERGABE

Aufgrund der Komplexität des Vergabegegenstandes ist die Ausschreibung als Verhandlungsverfahren mit vorgeschaltetem Teilnahmewettbewerb möglich. Die Bieter reichen in diesem Verfahren einen Teilnahmeantrag ein.

[1] Brüning, „Wettbewerb beim Ausbau des Breitbandnetzes zwischen kommunalen Unternehmen", in: der gemeindehaushalt 11/2018, S. 241; Handelsblatt, „Der Breitbandausbau wird noch viel teurer als geplant", Beitrag vom 14. November 2018.
[2] Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze.
[3] Gesetz gegen Wettbewerbsbeschränkungen.

Im Rahmen des Teilnahmewettbewerbs wird die Eignung der Bieter geprüft. Sofern die Unternehmen als geeignet einzustufen sind, werden sie zur Abgabe eines Erstangebotes aufgefordert. Hierzu haben die Unternehmen mindestens 30 Tage Zeit. Die eingereichten Erstangebote werden mit den Bietern verhandelt. Verhandeln heißt, dass Auftraggeber und Bieter den Vertragsinhalt solange erörtern, bis klar ist, wie Leistung und Gegenleistung konkret beschaffen sein sollen. Im Anschluss werden die Bieter zur Abgabe von endgültigen Angeboten aufgefordert. Das wirtschaftlichste Angebot wird schließlich bezuschlagt.

VERHANDLUNGSVERFAHREN BEI KONZESSIONSVERGABE

Eine Konzession liegt vor, wenn das wirtschaftliche Betriebsrisiko für die Nutzung der Breitbandnetzinfrastruktur bei dem Konzessionsnehmer – dem Unternehmen, das den Zuschlag erhält – liegt. Da im Falle des Breitbandausbaus das Unternehmen Fördermittel erhält, stellt sich die Frage, ob das Unternehmen tatsächlich ein Betriebsrisiko trägt. Die VK Münster[4] entschied jüngst, dass keine Konzession vorläge, wenn der Bieter aufgrund der Fördermittel Bau bzw. Betrieb der Breitbandnetzinfrastruktur überwiegend finanzieren könne. Der Bieter sei dann nicht mehr den Unwägbarkeiten des Marktes ausgesetzt. Im Einzelfall ist daher zu prüfen, wie stark sich das Betriebsrisiko durch die Zuwendung von Fördermitteln verringert. Bei der Verfahrensgestaltung steht dem Konzessionsgeber ein großer Gestaltungsspielraum zur Verfügung. Denkbar ist z. B. ein Verhandlungsverfahren ohne Teilnahmewettbewerb.

PRAXISPROBLEME

ZEITDRUCK

Immanent ist den Ausschreibungen von Breitbandnetzinfrastruktur stets zeitlicher Druck aufgrund des Bewilligungszeitraumes der Fördermittel. Dieser Zeitraum wird durch den Fördermittelgeber festgelegt und erstmals mit vorläufigem Zuwendungsbescheid festgesetzt. Binnen dieses Zeitraums müssen die Breitbandinfrastruktur errichtet und die Fördermittel abgerufen worden sein. Je nach Größe bzw. Struktur des auszubauenden Gebiets muss mit bis zu 48 Monaten gerechnet werden. Daher gilt es, unnötige Verzögerungen bei der Vergabe zu vermeiden. Flankierend kann eine Verlängerung des Bewilligungszeitraumes beim Fördermittelgeber beantragt werden, deren positive Verbescheidung aber keinen Automatismus darstellt.

VERÄNDERUNG DER KALKULATIONSGRUNDLAGEN

Neben dem Zeitplan müssen die Kalkulationsgrundlagen im Blick behalten werden. Zu den Kalkulationsgrundlagen, die den Bietern zur Verfügung gestellt werden, zählen etwa eine Liste mit den auszubauenden Adressen, deren Lage im GIS-Datenformat und die Höhe der gewährten Zuwendung sowie der Bewilligungszeitraum. Diese Kalkulationsgrundlagen können sich im Laufe des Verfahrens ändern. Beispielsweise kann ein Änderungsbescheid über den Bewilligungszeitraum (antragsgemäß) ergehen. Bei einer bloßen Änderung des Bewilligungszeitraums ist die so geänderte Kalkulationsgrundlage in das Verfahren einzuführen.

Ändert sich bspw. die Anzahl der auszubauenden Adressen (durch einen eigenwirtschaftlichen Netzausbau eines Unternehmens), ergeben sich für den gleichen Sachverhalt eine förderrechtliche und eine vergaberechtliche Fragestellung. Der neue Sachverhalt ist an den Fördermittelgeber in Form eines Änderungsantrages heranzutragen, wenn die Änderung nicht nur geringfügig ist. Eine enge Abstimmung mit dem Fördermittelgeber ist ratsam. Aus vergaberechtlicher Sicht stellt sich die Frage, ob durch die veränderte Kalkulationsgrundlage die Identität des Ausschreibungsgegenstandes geändert wird. Dann stünde eine Benachteiligung derjenigen Unternehmen im Raum, die sich auf die ursprünglich ausgeschriebene Leistung nicht beworben haben, sich aber gerne auf die nun ausgeschriebene Leistung beworben hätten. Bei einem Wegfall von auszubauenden Adressen wird „nur“ die Anzahl der zu erschließenden Adressen und daraus folgend die gewährte Zuwendung reduziert. Ein vergaberechtlich schwieriger Identitätswechsel erscheint wenig naheliegend. Anders könnte es hingegen zu beurteilen sein, wenn einem Auftraggeber ein sog. „Technologie-Upgrade“ antragsgemäß bewilligt wird. In diesem Fall ändert der Auftraggeber den Ausbau mit einer Übertragungsrate von 50 MBit/s auf einen Ausbau von mindestens 100 Mbit/s symmetrisch (= Glasfaser). Hierin kann eine Benachteiligung der Unternehmen liegen, die einen Glasfaserausbau angeboten hätten, sich aber nicht am Verfahren beteiligt haben, da zunächst nur eine geringere Übertragungsrate ausgeschrieben war. Hier gilt es die jeweilige Änderung im Einzelfall genau zu prüfen.

KONTAKT FÜR WEITERE INFORMATIONEN

Freya Schwering
Rechtsanwältin, Europajuristin
T +49 911 9193 3511
E freya.schwering@roedl.com

[4] Vergabekammer Münster, Beschluss vom 25. Januar 2018, VK 1 – 43/17, unter Hinweis auf BGH, Beschluss vom 8. Februar 2011, X ZB 4/10 „Abellio“.

SMART MOBILITY

On-Demand-Lösungen für Städte & Landkreise

Fachsymposium

21. Februar 2019

IMPULSVORTRÄGE

von Rödl & Partner, ADAC und insertEFFECT

PRAXISBEISPIELE

Berlkönig in Berlin und Wittlich Shuttle in Wittlich

Diskutieren Sie mit **Vertretern des Verbandes Deutscher Verkehrsunternehmen und des Deutschen Städtetages**

Lernen Sie Mobilitätsdienstleister und ihre Angebote kennen:
CleverShuttle | ioki | PPS/EDV | Uber | ViaVan | Wunder

Weitere Informationen zur Veranstaltung finden Sie unter
www.roedl.de/seminare

→ Energiewirtschaft

Wird Ihr steuerlicher Querverbund weiterhin anerkannt?

von Benjamin Hufnagel, Marcel Reinke und Manuel Maul

Es gilt seit jeher der Grundsatz, dass ein steuerlicher Querverbund, der durch eine verbindliche Zusage bestätigt wurde, von der Finanzverwaltung im Rahmen einer Betriebsprüfung nicht beleuchtet wird und die Ergebnisse entsprechend saldiert werden können. Bloß gilt dies wirklich so uneingeschränkt?

Es ist so, dass auf eine verbindliche Zusage nur solange eine bindende Wirkung enthält, wie der Sachverhalt, der der verbindlichen Zusage zugrundeliegt, tatsächlich auch so umgesetzt wurde. Änderungen des tatsächlichen Sachverhalts können daher im schlimmsten Falle dazu führen, dass die verbindliche Zusage ihre Wirkung verliert.

Der Großteil der uns bekannten verbindlichen Zusagen ist 15 Jahre und älter, sodass sich bspw. die Laufzeiten des BHKW langsam aber sicher dem Ende neigen. Ein Austausch eines BHKW führt jedoch regelmäßig dazu, dass es sich nicht um eine Umsetzung des ursprünglichen Sachverhalts handelt. Die verbindliche Zusage verliert dann ihre Wirkung.

Jedoch nicht nur eine Modernisierung des vorhandenen BHKW, auch eine Umgestaltung des Bades kann die gleichen Konsequenzen nach sich ziehen. Bei den Änderungen kommt es maßgeblich auf den Umfang sowie die Art der Änderung an.

Wir möchten Ihnen mit unserem kostenfreien Querverbund-Check eine Hilfestellung bieten. In wenigen Schritten stellen Sie uns die wesentlichen Betriebsparameter zur Verfügung, wir werten diese aus und geben Ihnen zeitnah unsere Einschätzung, ob für Sie unseres Erachtens nach Handlungsbedarf besteht oder der steuerliche Querverbund auch weiterhin aufrechterhalten werden kann.

Den Link für die Dateneingabe „Querverbund-Check“ finden Sie hier: http://bit.ly/Querverbund-Check

Analog hierzu haben wir für den Themenkomplex „BHKW“ einen kostenfreien Online-Check entworfen, mit dem wir auf der Basis Ihrer Angaben eine Ersteinschätzung zu möglichen Chancen, Optimierungen und Risiken des Betriebs Ihres BHKW treffen können.

Den Link für die Dateneingabe „BHKW-Check“ finden Sie hier: http://bit.ly/BHKW-Check

KONTAKT FÜR WEITERE INFORMATIONEN

Benjamin Hufnagel
M.A. Europäische Energiewirtschaft,
B.Eng. Wirtschaftsingenieur,
Energiewirtschaftsmanager
T +49 911 9193 3570
E benjamin.hufnagel@roedl.com

Marcel Reinke
Rechtsanwalt
T +49 911 9193 3685
E marcel.reinke@roedl.com

Manuel Maul
Steuerberater, Geprüfter Bilanzbuchhalter int. (IHK)
T +49 911 9193 3563
E manuel.maul@roedl.com

→ IT/Datenschutz

Erleichterungen bei der Führung des Nachweises durch unabhängige Bescheinigungen zur Konformität des Datenschutz-Managements

von Christoph Naucke

Mit Einführung der DSGVO sowie der Neufassung des BDSG und zahlreicher Landesdatenschutzgesetze wurde das Datenschutzrecht wesentlich novelliert. Auch für die Gebietskörperschaften und die Unternehmen des öffentlichen Sektors ist es wesentlich anspruchsvoller geworden, sich rechtskonform zu verhalten.

Zwar läuft die Bundes- und Landesgesetzgebung darauf hinaus, dass gegen Behörden und öffentliche Stellen keine Bußgelder verhängt werden. Trotzdem sollte man sich nicht voreilig in Sicherheit wiegen. Denn dieser Schutz gilt in der Regel nicht für Leistungen, mit denen die Körperschaften am Wettbewerb teilnehmen. Hinzu kommt: Im Falle einer Panne wird dem Betroffenen ein Recht auf Schadensersatz zugesichert, und gleichzeitig wird dem Verantwortlichen die Beweislast dafür auferlegt, rechtskonform gehandelt zu haben. Daher kommt dem Nachweis eines tatsächlich funktionierenden Datenschutz-Managements, möglichst in Form einer Referenz von unabhängiger Stelle, eine wachsende Bedeutung zu. Dafür eignen sich Bescheinigungen eines Wirtschaftsprüfers, beispielsweise eine IT-Prüfung außerhalb der Abschlussprüfung oder auch eine spezifische, fokussierte Prüfung der Datenschutz-Compliance.

Die gesetzlichen Vertreter einer Organisation sind dafür verantwortlich, Maßnahmen zu ergreifen, um das rechtskonforme Verhalten der Organisation zu gewährleisten. Anderenfalls besteht der Verdacht auf ein Organisationsverschulden. Viele wissen dabei gar nicht, dass die

Haftung auch solche gesetzlichen Vertreter trifft, die lediglich ehrenamtlich tätig sind. Es besteht also auch ein Risiko für den nebenamtlichen Vereinsvorstand! Dieser Grundsatz wurde in der EU-Datenschutz-Grundverordnung dadurch unterstrichen, dass in Art. 5 Absatz 2 der Verantwortliche die Pflicht auferlegt bekommt, die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen zu können (faktische Beweislastumkehr).

Ende Oktober wurde über das erste empfindliche Bußgeld berichtet, das in der EU wegen eines Verstoßes gegen die DSGVO ergangen ist. Es wurde in Portugal gegen ein Krankenhaus verhängt und betrug 400.000 Euro. Die Unternehmen des Öffentlichen Sektors verarbeiten, oft in großem Umfang, sog. „besondere", also besonders sensible Daten nach der Definition der DSGVO (u. a. Gesundheitsdaten, beispielsweise in Krankenhäusern, Pflegeeinrichtungen oder der Jugend- und Sozialarbeit). Es wäre kaum überraschend, wenn sich u. a. in diesem Bereich ein Tätigkeitsschwerpunkt der Landesdatenschutzbehörden entwickeln würde.

Der bayerische Landesbeauftragte für den Datenschutz schreibt beispielsweise schon in seinem Tätigkeitsbericht für das Jahr 2016 mit Bezug zum Art. 27 des Bayerischen Krankenhausgesetzes: „Gerade in Krankenhäusern entstehen zunehmend große Mengen an Daten, die die Gesundheit der Patientinnen und Patienten und damit deren intimsten Lebensbereich betreffen. Für diese Daten ist es durchaus angemessen, strengere Schutzmaßnahmen zu fordern. Durch die Beteiligung externer Stellen wird der Kreis derer größer, die mit sensiblen medizinischen Daten in Berührung kommen. Gleichzeitig sinken die direkten Einflussmöglichkeiten der Krankenhäuser auf den Umgang mit den Daten ihrer Patientinnen und Patienten. Das kann das Risiko von Datenmissbrauch und Datenverlust in einem besonders sensiblen Bereich erhöhen."

Angesichts einer sehr anspruchsvollen Regelungsdichte der DSGVO und der zahlreichen weiteren einschlägigen Rechtsnormen wird auch der Nachweis der Konformität für die betroffenen Unternehmen erheblich anspruchsvoller. Zum Anforderungskatalog zählen beispielsweise:

- Der Nachweis angemessener technischer und organisatorischer Maßnahmen nach dem aktuellen Stand der Technik,
- der umfassende Nachweis der Verarbeitungstätigkeiten einschl. des Nachweises, welchen Zweck diese erfüllen und auf welcher Rechtsgrundlage sie erfolgen,
- die zuverlässige Umsetzung der Auskunfts- und Löschungsrechte der Betroffenen,
- der Nachweis über die ggf. zuverlässige, fristgerechte Meldung einer Datenpanne,
- der Nachweis, dass Mitarbeiter zum Datenschutz verpflichtet und dass sie unterwiesen worden sind,
- die Vorlage der notwendigen Vereinbarungen zur Auftragsverarbeitung,
- der Nachweis, dass für die Datenweitergaben, für die Einwilligungserklärungen erforderlich sind, diese Einwilligungserklärungen systematisch eingeholt werden
- der Nachweis, dass die Mitarbeiter im Bedarfsfall schnell prüfen können, ob die betreffende Einwilligung tatsächlich vorliegt,
- die Ermittlung der wichtigsten Datenschutzrisiken aus Betroffenensicht zur Auswahl derjenigen Verarbeitungstätigkeiten, für die eine Datenschutzfolgenabschätzung zu erstellen ist und schließlich
- die Vorlage der erforderlichen Datenschutzfolgenabschätzungen.

NACHWEISPFLICHT DER DSGVO HEISST NICHTS ANDERES ALS DATENSCHUTZ-COMPLIANCE-MANAGEMENT

Damit entsteht im Bereich Datenschutz die Notwendigkeit, ein funktionierendes Compliance-Management, also ein Datenschutz-Compliance-Management, belegen zu können. Denn der Inhalt des Begriffs Compliance ist durch die (nachgewiesene) Einhaltung gesetzlicher und interner Regelungen und Standards definiert. Bei der Übersetzung der allgemein gehaltenen Anforderungen der DSGVO in die Praxis spielen die für die Körperschaft und ihre Prozesse angemessenen TOMs, die technischen und organisatorischen Maßnahmen also, eine zentrale Rolle. Hier gibt es branchen- und risikospezifische Anhaltspunkte, die man berücksichtigen sollte. Eine funktionierende Datenschutz-Compliance bedeutet, dass die tatsächliche Einhaltung der unternehmensbezogen definierten Standards nachgewiesen werden kann.

Die Bescheinigung eines Wirtschaftsprüfers über die Wirksamkeit eines Compliance-Management-Systems (CMS) bedeutet wertvolle Anhaltspunkte nach außen hin für den Fall, dass trotz aller Maßnahmen dennoch einmal etwas schiefläuft und eine Datenpanne geschieht. Das Institut der Wirtschaftsprüfer (IDW) hat mit dem Prüfungsstandard 980 einen Standard gesetzt, anhand dessen die Fragestellung nach der Wirksamkeit eines CMS beantwortet und als Ergebnis eine entsprechende Bescheinigung erlangt werden kann.

Die Prüfung des CMS nach diesem Prüfungsstandard 980 kann auf bestimmte Unternehmensfunktionen eingeschränkt werden. Deshalb eignet sich der Standard u. a. gut dafür, eine gezielte Prüfung des Datenschutz-Compliance-Management-Systems mit anschließender Bescheinigung durchzuführen. Die Prüfung kann als Konzeptions-, als Angemessenheits- oder als Wirksamkeitsprüfung definiert werden. Ziel einer umfassenden Wirksamkeitsprüfung ist es festzustellen, ob die

definierten Grundsätze und Maßnahmen gemäß der Konzeption des CMS angemessen sind, ob sie zu einem bestimmten Zeitpunkt implementiert und in einem zu bestimmenden Prüfungszeitraum auch wirksam waren. Für den Fall einer spezifischen Datenschutz-CMS-Prüfung umfasst diese sowohl organisatorische als auch technische Aspekte eines Datenschutz-CMS.

BESCHEINIGUNG DER DATENSCHUTZ-COMPLIANCE IN EINEM ABGRENZBAREN IT-SYSTEM: PS 860 ALS ALTERNATIVE ZUM PS 980

Wenn eine Bescheinigung mit Bezug zu bestimmten IT-Systemen angestrebt wird, eignet sich eine Prüfung nach dem IDW-Prüfungsstandard 860 für IT-Prüfungen außerhalb der Abschlussprüfung. Die Prüfung kann als Angemessenheitsprüfung und als Wirksamkeitsprüfung gestaltet werden. Ziel einer Angemessenheitsprüfung ist es festzustellen, ob die angewandten Grundsätze, Verfahren und Maßnahmen geeignet sind, die durch das IDW erstellten Kriterien einzuhalten und ob sie zum relevanten Prüfzeitpunkt im Unternehmen implementiert sind. Ziel der Wirksamkeitsprüfung ist über die Angemessenheitsprüfung hinaus zu beurteilen, ob die in der Erklärung zum IT-System dargestellten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems in dem zu prüfenden Zeitraum wirksam gewesen sind.

Da sich das Datenschutz-Management-System des Unternehmens letztlich in der Gesamtheit dieser Grundsätze, Verfahren und Maßnahmen manifestiert, wird mit der Prüfung daher eine externe, unabhängige Aussage zur Angemessenheit, zum Stand der Implementierung sowie ggf. zur Wirksamkeit des Datenschutz-Management-Systems getroffen. Sie kann daher ebenfalls ein wertvoller Baustein bei der Führung des Nachweises sein, den die DSGVO vom Verantwortlichen fordert.

Aufgrund der Ausrichtung des zugrundeliegenden IDW PS 860 für IT-Prüfungen sind diese Prüfungen besonders dafür geeignet, Gewissheit über die Angemessenheit und den Implementierungsstand der notwendigen Schutzmaßnahmen (technische und organisatorische Maßnahmen, TOMs) zu erlangen. Damit steht ein zusätzliches Werkzeug mit ggf. besonderem Schwerpunkt auf die TOMs und zur Erlangung einer entsprechenden Bescheinigung zur Verfügung.

Die von den gesetzlichen Vertretern getroffenen Grundsätze, Verfahren und Maßnahmen sind den rechtlichen Kriterien gegenüberzustellen und auf ihre Angemessenheit und ggf. Wirksamkeit hin zu überprüfen. Diese Überprüfung kann durch eine geeignete Aufbau- und Funktionsprüfung erfolgen. Darüber hinaus ist eine Risikobeurteilung durchzuführen.

Bescheinigungen aufgrund von Prüfungen, die als CMS-Prüfungen (PS 980) oder auch als Systemprüfungen (PS 860) ausgestaltet sind, unterliegen, genau wie andere Testate und Bescheinigungen eines Wirtschaftsprüfers, der Berufspflicht der Unabhängigkeit. Gleichzeitig unterstützt der Prüfungsprozess oftmals beim Aufdecken und Beseitigen noch unbemerkter Schwachstellen und bietet damit im Anschluss an die Prüfung eine wesentlich verbesserte Ausgangslage, um den Nachweis der Einhaltung der Grundsätze der DSGVO zu führen.

KONTAKT FÜR WEITERE INFORMATIONEN

Christoph Naucke
Betriebswirt (BA), Compliance Officer,
zert. Datenschutzbeauftragter DSB
T +49 911 9193 3628
E christoph.naucke@roedl.com

→ IT/Datenschutz

Mit gutem Beispiel voran und doch versagt?

Immer mehr Behörden mit Digitalisierungskonzept, jedoch mit fehlendem Informationssicherheits-Management-System

von Hannes Hahn, Bastian Schönnenbeck und Jonas Dikau

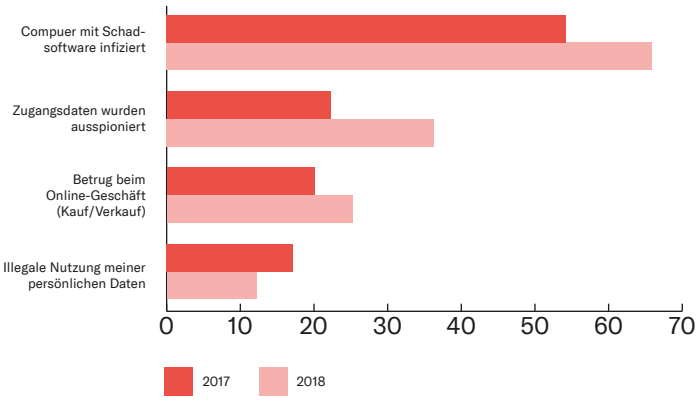
„Every business will be (is already) a digital business". Bedeutet nichts anderes, als dass alle Unternehmen, egal welcher Branche, zwangsläufig zu IT-Firmen werden. Das wachsende Aufkommen an Daten, Informationen, cloudbasierten Anwendungen, der Vormarsch künstlicher Intelligenz und die digitale Verknüpfung sämtlicher Prozesse macht es auch für Behörden unmöglich, diese Entwicklung zu ignorieren. Die Aufbruchstimmung ist spürbar und eine positive Entwicklung. Bei allen Digitalisierungsvorhaben kommt jedoch oft ein Thema zu kurz: ein stabiles Informationssicherheits-Management-System.

Die bayerische Landesregierung hat nach den zuletzt stattgefundenen Landeswahlen einen über 50-seitigen Koalitionsvertrag vorgelegt. Darin enthalten: Ganze 63-mal das Wörtchen „digital". Nicht nur Tourismus, öffentlicher Verkehr und Schulen sollen digitaler werden, sondern auch die Kommunen, Gemeinden, Behörden und Verwaltungsvorgänge. Die digitale Modellstadt Gelsenkirchen trumpft mit dem großflächigen Ausbau der Glasfaserinfrastruktur und Baden-Württemberg will für rund 800.000 Euro in die Ausbildung zum „Kommunalen Digitallotsen" der Verwaltungsangestellten investieren. Eine – wenn auch späte – Aufbruchstimmung in Sachen Digitalisierung ist im ganzen Land spürbar. Das ist vom Grundsatz her eine tolle Entwicklung und zeigt, dass auch das vermeintlich eingestaubte Thema „Verwaltung" daran teilnimmt. Bei aller Begeisterung erkennt man jedoch einen großen Nachteil:

DIE WACHSENDE CYBER-KRIMINALITÄT

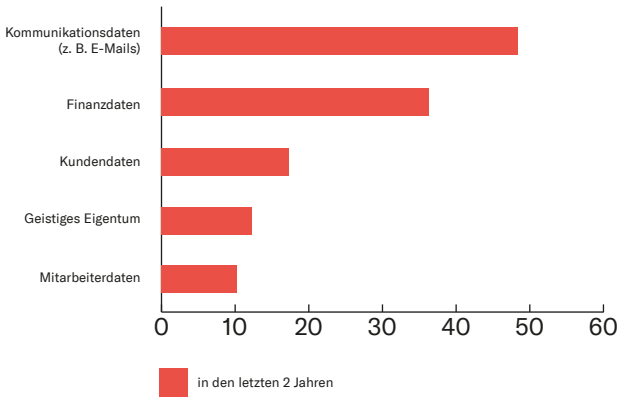
Straftaten im Umfeld der Cyber- und IT-Kriminalität sind das derzeit am stärksten wachsende Delikt, wohingegen die Tätergruppen relativ klein sind. Ein Täter kann auf diesem Gebiet nur weitaus größeren Schaden bewirken, als ein Täter in einem klassischen Deliktumfeld wie dem Ladendiebstahl. Angriffe auf Unternehmen, Einrichtungen und Behörden sind leider längst kein zufälliges Phänomen von einigen wenigen, sondern tatsächliche Realität. Was die wenigsten wissen ist, dass selbst das Installieren eines Virus bzw. Computersabotage im Strafgesetzbuch, in diesem Fall § 303b StGB, mit bis zu 5 Jahren Freiheitsentzug unter Strafe gestellt werden kann.

Welche kriminellen Erfahrungen haben Sie in den vergangenen 12 Monaten im Internet gemacht?



Bitkom Research, n=503

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?



Bitkom Research, n=178

Allein im Jahr 2017 hat IT-Kriminalität in Deutschland für einen geschätzten wirtschaftlichen Schaden von 55 Milliarden Euro gesorgt, Privathaushalte und Unternehmen zusammengerechnet. Da das Datenaufkommen täglich durch den simplen Gebrauch von Smartphones, Smart-Uhren, dem Surfen im Internet, durch das Nutzen von Apps etc. massiv steigt, steigt damit einhergehend leider auch das Interesse von Hackern und Datendieben. Dabei besonders im Fokus: Finanzdaten und personenbezogene Daten.

EINE BEHÖRDE IST GERN GENOMMENES ZIEL BEI HACKERANGRIFFEN UND DATENDIEBSTÄHLEN

Das zeigt nicht nur ein im November veröffentlichter Artikel des Landesbeauftragten für Informationssicherheit Sachsen, indem deutlich wird, dass der Freistaat mit rund 26.000 E-Mail-Viren zu kämpfen hat. Thomas Popp, ebengenannter Landesbeauftragter für Informationssicherheit drückt es so aus: „Das sei Cyberkrieg." Und damit hat er damit nicht Unrecht. Gemeinden und behördliche Einrichtungen arbeiten und verwalten im höchsten Maße vertrauliche Daten von Bürgern, auch Kindern, Kunden und Unternehmen. Elterngeld, Steuererklärungen, Beantragungen von Sozialleistungen oder die Gewerbeanmeldung sind nur einige Beispiele, die man anführen könnte. Kriminelle Hacker haben es genau auf derlei sensible Daten abgesehen.

WIE SIEHT EIN TYPISCHER HACKERANGRIFF AUS?

Eine klassische Vorgehensweise von Kriminellen: Über täuschend echt gestaltete E-Mails, wird der Mitarbeiter gebeten, den Anhang zu öffnen. Es wird eine säumige Rechnung oder ähnliches vorgetäuscht. Sobald ein Mitarbeiter den Anhang öffnet, installiert sich eine Schadsoftware auf dem lokalen PC. Ziel ist es, tiefer in das Netzwerk einzudringen und so Zugang zu sämtlichen Daten und Informationen zu erhalten. Nicht selten werden diese dann geklaut oder das Netzwerk so manipuliert, dass ein Weiterarbeiten für die Gemeinde, die Behörde oder das Unternehmen unmöglich ist. Zumeist wird ein Lösegeld von den Hackern gefordert, um die Systeme wieder freizugeben.

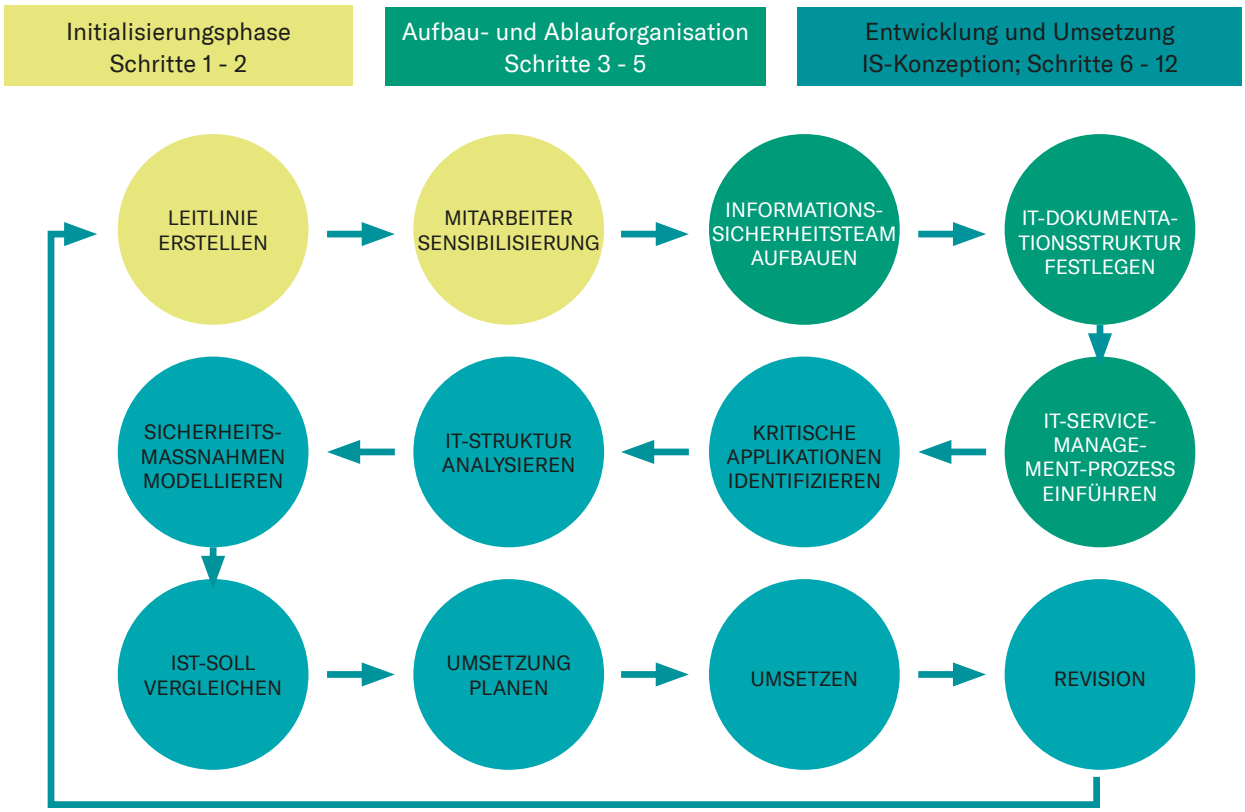
EIN STABILES INFORMATIONSSICHERHEITS-MANAGEMENT-SYSTEM IST DAHER ZWINGEND NOTWENDIG!

Und das alleine schon aus Sicht des Datenschutzes, dessen Gesetzeslage sich seit dem Inkrafttreten der EU-Datenschutz-Grundverordnung und des neuen Bundesdatenschutzgesetzes, deutlich verschärft hat. Die Erforderlichkeit eines Informationssicherheits-Management-Systems (ISMS) ergibt sich unter anderem aus Art. 32 DSGVO. Einfach ausgedrückt, handelt es sich um die Implementierung von technischen und organisatorischen Maßnahmen, die die Sicherheit der Verarbeitung von (personenbezogenen) Daten gewährleisten sollen. Einfache Beispiele dazu: die entsprechende Schulung jedes Mitarbeiters, das Verschlüsseln von E-Mails oder die zweifache Authentifizierung bei der Nutzung eines Rechners, der ebendiese sensiblen Daten verarbeitet. Aus Gesprächen mit unseren (potenziellen) Mandanten wissen wir, dass die Komplexität und die Verhältnismäßigkeit eines Informationssicherheits-Management-Systems in der Praxis nur schwer einzuschätzen sind. Oftmals scheitert es im ersten Schritt schon daran, dass eine saubere Dokumentation über Richtlinien, Anweisungen und Konzepte der jeweiligen Behörde, Einrichtung, Kommune oder Stadt bisher nicht vorgenommen wurde. Weiterhin scheitert es an dem technischen Verständnis eines ISMS. Und das, obwohl der Gesetzgeber Pflichten zur Einführung von Management-Systemen erlassen hat, wie man beim Betrachten der jeweiligen E-Government-Gesetze feststellen wird.

RÖDL & PARTNER IST ZERTIFIZIERTER BERATER BEI DER EINFÜHRUNG VON ISIS12

Ein Informationssicherheits-Management-System in 12 Schritten, das sich aufgrund seiner einfachen Zusammensetzung speziell in KMUs und Behörden sowie Kommunen etablieren lässt. Mit den 12 Schritten lässt sich ein zeitlicher Horizont zur Projektumsetzung abbilden und transparent umsetzen. Zum Beispiel beschäftigt sich Schritt 1 mit der Erstellung einer Leitlinie für Informationssicherheit. Die Leitlinie ist das zentrale Strategiepapier, in dem Ziele sowie die daraus abgeleiteten und abzuleitenden Konzepte und Maßnahmen festgehalten werden. Die Mitarbeiter müssen zur Einhaltung und Umsetzung motiviert werden, weshalb in Schritt 2 die Mitarbeitersensibilisierung erfolgt. Auf allen Organisationsebenen muss die Notwendigkeit des Projekts kommuniziert werden. In einem speziellen ISIS12-Vortrag, der sowohl von der internen Projektleitung wie durch einen Berater von Rödl & Partner gehalten werden kann, sollen alle Mitarbeiter über den ISIS12-Workflow und die spezifische Bedeutung der Informationssicherheit hingewiesen werden. In den folgenden 10 Schritten werden IST-Zustände und der strukturelle Aufbau der IT abgefragt, woraufhin eine SOLL-IST-Analyse zu Maßnahmen führt, deren Umsetzung Gegenstand der angestrebten Zertifizierung ist.

Die Erfahrungen bei unseren bisherigen Mandanten haben gezeigt, dass – vor allem bei Landkreisen – zunächst eine gesunde Skepsis bei den einzelnen Kommunen gegenüber der Einführung von ISIS12 herrschte. Nach einer allgemeinen Informationsveranstaltung, die zum Beispiel durch das Landratsamt kommuniziert wurde und wozu die Verantwortlichen aus den Kommunen eingeladen waren, ließ sich jedoch eine nahezu hundertprozentige Überzeugung resümieren.



KONTAKT FÜR WEITERE INFORMATIONEN

Hannes Hahn
CISA, CSP, DSB, IT-Auditor IDW
T +49 221 949 909 200
E hannes.hahn@roedl.com

Bastian Schönnenbeck LL.M.
B. Sc. Betriebswirtschaft
T +49 221 949 909 426
E bastian.schoennenbeck@roedl.com

Jonas Dikau
B.Sc. Informationsmanagement
T +49 221 949 909 424
E jonas.dikau@roedl.com

→ IT/Datenschutz

Licht in den dunklen Cyberraum

Ein Cybersecurity-Rating hilft Verantwortlichen in den Kommunen, die eigene Cybersecurity-Resilienz beurteilen zu können.

von Hannes Hahn

Ein Cybersecurity-Rating kann allen helfen, die Sicherheitsschwächen der eigenen Institution zu erkennen, um entsprechende Gegenmaßnahmen ergreifen zu können. Aber nicht nur das. Auch die Resilienz wesentlicher Kooperationspartner kann damit beurteilt werden. Dabei bedient sich das Rating bewusst aus Quellen verfügbarer Daten und Informationen aus dem Internet und kann daher auch auf Dritte angewendet werden. Wie dieses System die vorhandenen Sicherheitsinstrumente sinnvoll ergänzt und was es langfristig für Vorteile bietet, soll dieser Beitrag klären.

Zugegeben, die Beurteilung, ob das eigene IT-System vor Angriffen Dritter sicher ist, ist vor dem Hintergrund der Komplexität von digitalisierten Verwaltungsprozessen und Informationstechnologie nur schwer bis gar nicht möglich. Im Idealfall befindet man über das einhergehende Risiko, ist aber weit davon entfernt, die Sicherheit absolut beurteilen zu können. Verschiedene Instrumenten verhelfen sich die Verantwortlichen (kommunaler Behördenleiter, IT-Verantwortliche, Informationssicherheitsbeauftragte, Datenschutzbeauftragte, Rechnungsprüfer etc.), die Grundlage für die Einschätzung zur eigenen Sicherheit abzuleiten. Generell gehören zu diesen Instrumenten

- Hinweise aus den eingeführten Sicherheitsmaßnahmen wie Firewalls, Virenschutzprogrammen, Sandbox-Systemen etc.
- Fallweise durchgeführte Penetrationstests (z. B. technische Server- oder Web-Tests, Social Engineering-Tests, etc.)
- Stichprobenbasierende IT-Audits (Prüfung vorhandener Dienstanweisungen, Nachweise über die Wirksamkeit von Rechtekonzepten, etc.)
- Sicherstellung über entsprechende Sicherheitskonzepte im Idealfall nach gängigen Rahmenwerken wir ISO IEC 27001 oder ISIS12®

Die Daten und Informationen aus diesen Instrumenten sind alle wichtig. Einzeln betrachtet beinhalten sie jedoch in der Regel eine von folgenden Schwachstellen:

Erste Schwachstelle: Sie beziehen nur einen Bruchteil des „Cyberraums“ in die Betrachtung mit ein!
Zweite Schwachstelle: Sie beziehen sich in der Regel nur auf einen Stichtag und liegen nicht kontinuierlich vor!

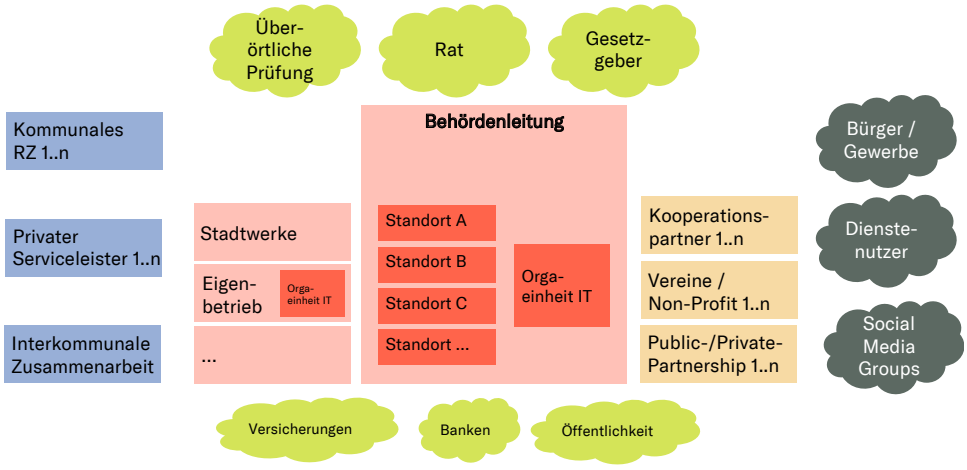
Dabei ist festzuhalten, dass diese obigen Instrumente enorm wichtig sind. Die Auseinandersetzung jedoch mit den vermeintlichen Mängeln sollte Ansätze zu deren Lösung liefern.

Daher zunächst ein paar einführende Worte, was mit dem „Cyberraum“ gemeint ist und warum in der Regel die heutigen Instrumente Lücken haben.

DAS CYBERSECURITY-ÖKO-SYSTEM AUS SICHT EINER BEHÖRDE

Vereinfachend blickt man in der Regel bei dem Begriff von Informations- oder IT-Sicherheit auf die eigene Verwaltung bzw. sogar nur auf die eigene IT. Das ist nachvollziehbar, ist dies doch der Bereich, den man selbst verantwortet und auf den man einen Einfluss hat.

Stellt man sich aber die Frage, mit wem sich die Verwaltung in digitalem Austausch befindet und wer alles bei digitalen Verwaltungsprozessen eine Rolle spielt, dann weitet sich der Blick auf ein sehr komplexes Öko-System aus.



Werden heute die Verwaltungsprozesse digital umgesetzt, so sind diese von der Sicherheit einer Vielzahl von Akteuren abhängig. Stellt man sich die Frage, ob der digitale Wertschöpfungsprozess (also der Verwaltungsprozess) sicher im Sinne von

- Vertraulichkeit,
- Integrität und
- Verfügbarkeit

ist, so muss man schnell feststellen, dass die Antwort sich immer nur auf den eigenen Verantwortungsbereich beziehen kann.

Hier setzt ein Cybersecurity-Rating an. Durch die vielen Spuren, die heute Anwender wie Unternehmen, Behörden und andere Institutionen im „Netz", also im Cyberraum hinterlassen, ist eine Beurteilung der Cybersecurity schon allein von außen durchaus möglich! Und zwar ohne in die IT von innen Einblick zu haben.

DER CYBERRAUM ALS QUELLE EINES RATINGS

Wie soll das gehen? Ebenso wie jeder Anwender, der durch die Nutzung von Diensten und Services Spuren im Netz hinterlässt, ist auch eine Verwaltung mit ihren Endgeräten und Servern im Netz nicht unbekannt. Sie hat einen Web-Auftritt und bei jedem Besuch einer Web-Seite werden Basis-Informationen ausgetauscht. In der Regel handelt es sich hierbei um Informationen, die notwendig sind, um einen reibungslosen Besuch der Web-Seite zu gewährleisten. Sie sind also öffentlich verfügbar!

Darin sind üblicherweise Informationen enthalten, nach welchen Sicherheitsstandards der Server der Web-Seite kommunizieren will. Ist dieser veraltet, stellt das eine Sicherheitslücke dar. Ebenso verhalten sich Server für E-Mail-Kommunikation, Server für mobile Applikationen und so weiter.

Diese sogenannten Risikovektoren (also z. B. Verschlüsselung), die aus den öffentlichen Daten und Informationen zu gewinnen sind, lassen sich grob in 3 wesentliche Risiko-Kategorien einteilen:

KOMPROMITTIERTE SYSTEME

Ist erkennbar, dass Endgeräte oder Server aus der eigenen Verwaltung mit bekannten Botnetzen kommunizieren und somit das eigenen System kompromittiert ist? Werden Endgeräte oder Server für SPAM-Mails missbraucht? Werden eigene Systeme missbraucht, um Schadsoftware zu verteilen?

ANWENDERVERHALTEN

Kommunizieren Endgeräte über Kommunikationsprotokolle mit Dritten oder als gefährlich einzustufende Server (Tauschserver, etc.) außerhalb der eigenen Verwaltung? Liegt somit der Verdacht nahe, dass eigene Anweisungen und Regelungen missachtet werden? Ist die Gefahr gegeben, dass Daten und Informationen auf diesem Weg weitergeleitet werden? Gibt es in einschlägigen Datenbanken von Sicherheitsinstitutionen Informationen, dass Userkennungen offengelegt wurden?

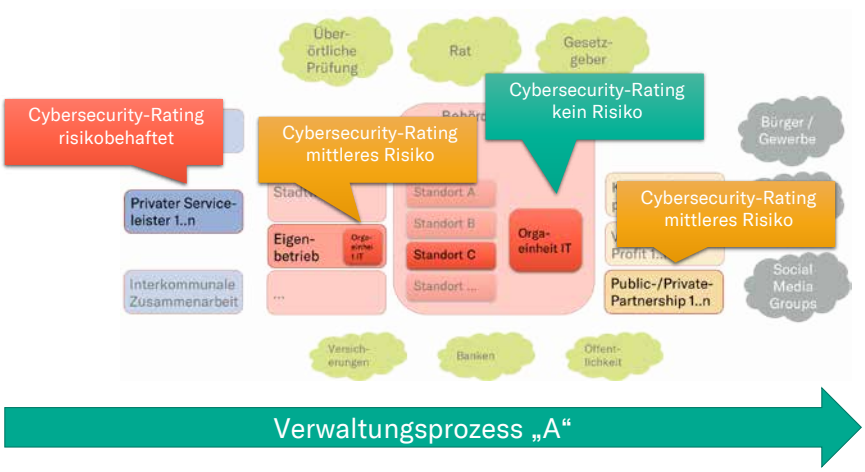
SORGFÄLTIGER BETRIEB VON SYSTEMEN

Sind die Systeme und Endgeräte, die offiziell mit Dritten kommunizieren (E-Mail-Server, etc.) so eingerichtet, dass auf einen sicheren oder eher unsicheren Betrieb geschlossen werden kann? Werden Best-Practice-Sicherheitsmechanismen (Verschlüsselung, Vermeidung von Man-in-the-Middle, etc.), die im Rahmen der Protokolle erkennbar sind, verwendet?

Alle diese Ergebnisse sind allein durch das Kommunikationsverhalten ableitbar und liefern Hinweise auf die gewählten Schutzmaßnahmen.

Diese Informationen sind nicht geheim, denn sie sind für die Kommunikation zwischen 2 Systemen notwendig, können aber Rückschlüsse auf die dahinter liegende Organisation von Sicherheitsmaßnahmen liefern. Und, sie liegen nicht nur für die eigene Verwaltung, sondern auch bezüglich der Partner, die im Verwaltungsprozess eine Rolle einnehmen (Kooperationspartner, Dienstleister, Eigen- und Beteiligungsgesellschaften etc.) vor.

Diese Einzelinformationen werden gewichtet und zu einem Cybersecurity-Rating zusammengeführt. Und sie liegen nicht nur für die eigene Verwaltung vor, sondern auch für alle anderen Partner.



Durch die Nutzung dieser Informationen ist die Beurteilung des gesamten Cybersecurity-Öko-Systems durch die Verantwortlichen möglich. Sie kommen hier in Verbindung mit den obigen Instrumenten ihrer Verantwortung näher, für die Überwachung der Wirksamkeit der Sicherheitsmaßnahmen Sorge zu tragen.

Aber noch viel bedeutsamer ist, dass im Rahmen des Ratings konkrete Handlungsbedarfe aus den obigen Kategorien an die Beteiligten formuliert werden können. So können die Verantwortlichen auch ihren Pflichten zur Steuerung nachkommen.

Es ergibt sich eine Vielzahl von Steuerungsmöglichkeiten aus Sicht der einzelnen Verantwortlichkeiten:

- Der Informationssicherheitsbeauftragte kann die eigenen Sicherheitsmaßnahmen beurteilen, aber auch im Rahmen der Auswahl und Überwachung Dritter einwirken.
- Der Datenschutzbeauftragte kann nachhalten, ob die technischen und organisatorischen Maßnahmen des Verantwortlichen und die der ausgewählten Auftragsdatenverarbeiter wirksam sind.
- Die Behördenleitung der Verwaltung kann das Rating zum Gegenstand von Dezernats- und Beteiligungssteuerung machen. Sie kann die Anforderungen an einen sicheren Betrieb von digitalen Verwaltungsprozessen an dem Rating orientieren.
- Die Rechnungsprüfung kann auf Basis der Ratings konkrete Handlungsbedarfe im Rahmen von großen Software-Projekten bzw. im laufenden Betrieb formulieren.

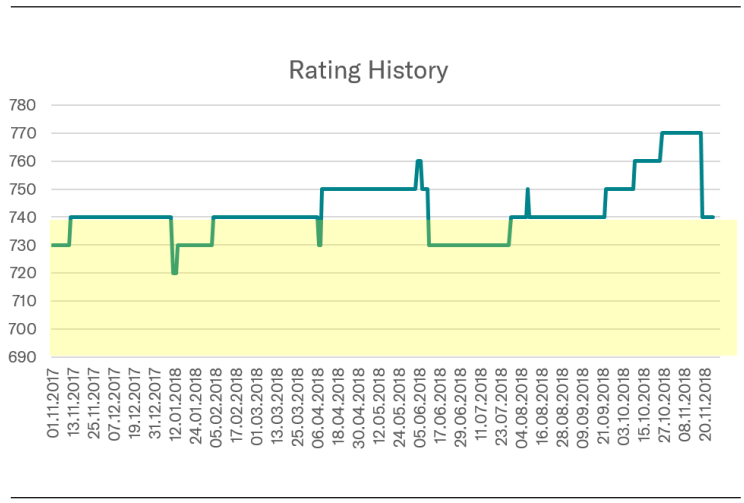
Die Ausdehnung des Rahmens der Steuerung und Überwachung über den eigenen Verantwortungsbereich hinaus ist ein enormer Gewinn.

CYBERSECURITY-RATING ALS KONTINUIERLICHER SERVICE

Ein Mangel steckt in den bisherigen Instrumenten jedoch nach wie vor. Nämlich die Zeitpunktbetrachtung. Fast jedes bisher bekannte Instrument (Audit, Penetrationstest, etc.) bezieht sich auf einen Zeitpunkt. Aussagen über einen Zeitraum sind nur bedingt möglich.

Die Daten und Informationen zu obig grob beschriebenen Risikovektoren können über einen größeren Zeitraum vorgehalten werden. Das heißt, dass die Information, an welchem Tag eine Kompromittierung eines Endgerätes in den eigenen Reihen stattgefunden hat und ab wann die eigenen Gegenmaßnahmen (Virenscanner, Intrusion Detection and Prevention System, etc.) gegriffen haben, auch erkennbar ist. Dies bedeutet, dass nicht nur eine Stichtagsbetrachtung, sondern eine Zeitraumbetrachtung greift. Und die Wirksamkeit der eigenen Maßnahmen wird messbar.

Wie so oft, werden auch im Sicherheitsbereich die Dienste Dritter in Anspruch genommen (Managed Security). Aber wer in den eigenen Reihen der Verwaltung kann beurteilen, ob diese Dienstleister und Instrumente die richtige Wahl waren und sind? Das Cybersecurity-Rating kann diese Dienste bewertbar machen und dient daher als wirksames Werkzeug der Verifizierung.



Geht man davon aus, dass die Handlungsempfehlungen zu den einzelnen Risikovektoren auch umgesetzt werden müssen, ist der Bedarf an „ständiger“ Beurteilung sowieso gegeben. So wird das Rating-System zu einem ständigen Monitoring-System, um die Resilienz im Cyberraum zu überwachen.

Dabei sind sogar neuralgische Zeitpunkte, die das Rating im Verlauf beeinflusst haben, erkennbar. Die sie auslösenden Ereignisse, z. B. eine Serverumstellung im Haus, können direkt mit dem Verlust an Sicherheit (Verwundbarkeit) in Verbindung gebracht werden.

Die Kenntnis hierüber beeinflusst auch nachhaltig das Management und fördert somit das Sicherheitsverständnis insgesamt.

CYBERSECURITY-RATING ALS INSTRUMENT NUTZEN

Die Nutzung eines solchen Systems ist einfach, der Umgang erfordert jedoch eine gewisse Methodik. Denn die Ergebnisse eines solchen Ratings und die hieraus verfügbaren Detailinformationen bedürfen einer behutsamen Nutzung.

Daher ist es ratsam, sich über folgende Schritte dem Cybersecurity-Rating zu nähern:

- Start eines Ratings über einen abgegrenzten Bereich für einen ersten Einstieg
- Ableitung des Nutzens des Ratingsystems in Bezug auf Umfang und Zeitpunkt. Nicht jede Verwaltung benötigt ein kontinuierliches Rating über das gesamte Öko-System. In vielen Fällen reicht eine Analyse z B. eines wichtigen Lieferanten einmal oder zweimal im Jahr aus. Die eigene Verwaltung sollte für sich selbst ein kontinuierliches Monitoring bevorzugen.
- Ableitung der Aufbau- und Ablauforganisation in Bezug auf die Nutzung des Systems. Wer übernimmt das Monitoring? Wer agiert bei Auffälligkeiten?
- Ableitung von Zuständigkeiten für erkannte Sicherheitslücken. Wer agiert wann bei erkannten Sicherheitsvorfällen?
- Integration des Systems in die vorhandenen Sicherheits- und Datenschutzkonzepte.
- Umsetzung eines Reportingsystems, das die verschiedenen Adressaten berücksichtigt.
- Sicherer und wirksamer dauerhafter Betrieb.

KONTAKT FÜR WEITERE INFORMATIONEN

Hannes Hahn
CISA, CSP, DSB, IT-Auditor IDW
T +49 221 949 909 200
E hannes.hahn@roedl.com

→ IT/Datenschutz

Kommunale Rechnungsprüfung und IT-Prüfung

Die Komplexität der IT und der digitalisierten Verwaltungsprozesse spiegelt sich leider nicht in der Kapazität und Kompetenz der kommunalen Rechnungsprüfer wider. Es ist Zeit zu handeln.

von Hannes Hahn

Die IT und die damit unterstützten Verwaltungsprozesse werden zunehmend komplexer. Die IT-Trends zeigen, dass sich die Situation verstärkt. Vereinfachungen sind kaum zu erkennen. Vor diesem Hintergrund ist die Entwicklung der IT-Kompetenz und Kapazität in den kommunalen Rechnungsprüfungsämtern besorgniserregend. Es ist Zeit für alle Verantwortlichen, der kommunalen Rechnungsprüfung mit Blick auf die Digitalisierung mehr Raum und Budget zu geben.

Am 26. April 2018 hat das Institut der Rechnungsprüfer e. V. das Gutachten zur „Optimierung der Prüfung der Informationstechnologie der örtlichen Rechnungsprüfung“ veröffentlicht. Über https://idrd.de/news/aktuelles/?tx_ttnews%5Btt_news%5D=130&cHash=5fbe7192974ffc681e2cc33b0d0fa128 kann das Gutachten heruntergeladen werden.

Bedenkt man, dass die kommunale Rechnungsprüfung einen wichtigen Bestandteil der öffentlichen Finanzkontrolle darstellt und im Sinne eines Internen Kontrollsystems (IKS) eine wesentliche Funktion einnimmt, muss sich folgerichtig die Kompetenz und Kapazität im Umfeld der IT den Entwicklungen laufend anpassen.

Mittels einer Online-Umfrage wurden Themen wie Organisationsmodelle, Personalausstattung und Prüfungsmethodik in den Rechnungsprüfungsämtern im Rahmen des Gutachtens abgefragt.

So sind zwei Drittel der teilgenommenen Rechnungsprüfer der Meinung, dass derzeit der gesetzliche Aufgabenumfang nicht oder nur in geringem Umfang erfüllt werden kann. Zur Personalausstattung konnte festgestellt werden, dass erst ab der Größenklasse 3 (Gemeinden

größer 100 Tsd. Einwohner) verlässlich eine Person mit Zeitanteilen im Mittel von 0,88 Vollzeitäquivalenten (VZÄ) für IT-Prüfungen zur Verfügung steht. Bei Kreisen sind erst ab der Größenklasse 1 (mehr als 250 Tsd. Einwohner) Zeitanteile im Mittel von 0,34 VZÄ vorhanden. Dabei stehen der Rechnungsprüfung im Mittel lediglich 2.000 Euro pro Jahr für die Einbindung Dritter zur Verfügung.

Vor dem Hintergrund der erheblichen Beträge, die die kommunale IT jährlich bindet, sind das besorgniserregende Zahlen. Die finanzielle und personelle Situation führt in Folge laut Gutachten zu folgenden Detailsituationen:

Zusammenarbeit: IT ist komplex. Ein IT-Prüfer kann nicht alle sinnvollen Wissensbereiche abdecken. Der überwiegende Teil der Befragten gab an, dass eine verwaltungsübergreifende Zusammenarbeit im Rahmen der IT-Prüfung nicht stattfindet. Es gibt kaum IT-Prüfer.

Qualifikation: Nur in Ausnahmen haben die IT-Prüfer eine Ausbildung oder einen Hochschulabschluss im IT-Umfeld. Größtenteils haben sich die IT-Prüfer die IT-Kenntnisse über Weiterbildung angeeignet.

Change-Management: Veränderungen finden innerhalb einer Verwaltung laufend statt. Die Rechnungsprüfung kann hier im IT-Umfeld keine qualitätssichernde Rolle einnehmen. Der überwiegende Teil der Befragten ist der Meinung, nicht eingebunden zu werden.

Prüfungsmethodik: Ein beschriebenes Internes Kontrollsystem (IKS) ist elementar für die IT-Prüfung. Auf Basis eines solchen IKS kann effizient und verlässlich geprüft werden. Bei dem überwiegenden Teil der Befragten lag in der Verwaltung kein durch die Leitung beschriebenes IKS vor. Demzufolge gab auch die Mehrheit an, die Wirksamkeit eines IKS nicht zu prüfen.

Prüfwerkzeuge: Der überwiegende Teil der Befragten gab an, den Nutzen von speziellen IT-Tools für die Prüfung nicht realisieren zu können.

Prüfungsleitlinien und -hilfen: Wenige haben eigene Hilfen entwickelt oder nutzen Hilfen Dritter. Der Nutzen solcher Hilfen wurde aber überwiegend erkannt.

Outsourcing: Viele Verwaltungsprozesse sind entweder ausgelagert oder werden durch ausgelagerte Prozesse gestützt. Rechnungsprüfer nutzen dabei selten die Prüfungsergebnisse der Kollegen aus den ausgelagerten Einheiten.

Die Fragestellung nach einer optimalen Personalausstattung wurde mit einer merkmalbasierten Stellenbedarfsermittlung beantwortet. Grund für diese Empfehlung war, dass aufgrund von fehlenden Benchmark-Werten lediglich auf Erfahrungswerte aus IT-Organisationen Bezug genommen werden konnte. Die Herangehensweise soll eine sachliche Basis für eine individuelle Auseinandersetzung vor Ort bieten.

Das Gutachten macht aber auch deutlich, dass trotz „Stellenbedarfsermittlung“ insbesondere kleine und mittlere Verwaltungen sich schwer tun werden, die fachliche Breite in der IT-Prüfung abdecken zu können. Es wird zunehmend schwerer, am hart umkämpften Personalmarkt entsprechendes Personal zu finden. Daher erging die Empfehlung, dass die verwaltungsinternen und individuellen Vor-Ort-Maßnahmen eher darauf ausgerichtet sein sollten, eine verwaltungsübergreifende Zusammenarbeit zu ermöglichen.

So erging die Empfehlung, für ein Modell der interkommunalen Zusammenarbeit auf Ebene des IdR e. V. die Grundlage in Form einer Strategie sowie Regelungen in Form von Prüfungsleitlinien zu schaffen, um hieraus auch weitere Entwicklungspotenziale zu erschließen (Datenanalyseplattform, IT-Prüferpool, Schulungsangebote, etc.).

Vor diesem Hintergrund dürfen wir auf einen im Jahr 2015 erschienen Artikel mit einem kleinen Schmunzeln im Sinne „Beste Vorsätze zum Neuen Jahr!“ verweisen: https://www.roedl.de/themen/kommunales-rechnungswesen/it-audits-kommunale-rechnungspruefung. Als der Artikel verfasst wurde, war das Jahr 2020 noch in weiter Ferne.

Das Gutachten schließt insgesamt mit einem positiven Fazit zur Umsetzung der Handlungsbedarfe, da insbesondere der Wille für einen gemeinsamen Weg auf Ebene der kommunalen Rechnungsprüfer gegeben ist.

KONTAKT FÜR WEITERE INFORMATIONEN

Hannes Hahn
CISA, CSP, DSB, IT-Auditor IDW
T +49 221 949909 200
E hannes.hahn@roedl.com

→ Rödl & Partner intern

Veranstaltungshinweise

THEMA	Revisionssichere Archivierung durch digitale Dokumentensteuerung richtig umsetzen
TERMIN / ORT	29. Januar 2019 / Nürnberg

THEMA	Fachsymposium: Smart Mobility On-Demand-Lösungen für Städte & Landkreise
TERMIN / ORT	21. Februar 2019 / Köln

THEMA	§ 2b UStG & Tax CMS – die Praxis für die Zukunft
TERMIN / ORT	13. März 2019 / Köln 20. März 2019 / Eschborn 21. März 2019 / Leipzig 26. März 2019 / Stuttgart 27. März 2019 / München 28. März 2019 / Nürnberg 3. April 2019 / Hannover 10. April 2019 / Bielefeld

THEMA	Führungskräftetraining
TERMIN / ORT	9. April 2019 / Köln 10. April 2019 / Hannover 11. April 2019 / München

Alle Informationen zu unseren Seminaren finden Sie direkt im Internet unter: www.roedl.de/seminare.

KONTAKT FÜR WEITERE INFORMATIONEN:

Peggy Kretschmer
B.Sc. Wirtschaftswissenschaften
T +49 911 9193 3502
E peggy.kretschmer@roedl.com

Rödl & Partner

Impressum

HERAUSGEBER:
Rödl & Partner GbR
Äußere Sulzbacher Str. 100 | 90491 Nürnberg
T +49 911 9193 3504
pmc@roedl.com
www.roedl.com

VERANTWORTLICH FÜR DEN INHALT:
Martin Wambach – martin.wambach@roedl.com
Kranhaus 1, Im Zollhafen 18 | 50678 Köln

Heiko Pech – heiko.pech@roedl.com
Äußere Sulzbacher Str. 100 | 90491 Nürnberg

LAYOUT/SATZ:
Katharina Bühler – katharina.buehler@roedl.com
Äußere Sulzbacher Str. 100 | 90491 Nürnberg