



INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

Sascha Kuhrau

Erstellung von Informations- sicherheitskonzepten für Kommunen

nach Art. 8 Abs. 1 S. 2 BayEGovG

ARBEITSHILFE

Sascha Kuhrau

Erstellung von Informationssicherheits- konzepten für Kommunen nach Art. 8 Abs. 1 S. 2 BayEGovG

Arbeitshilfe

Sascha Kuhrau
Schulstr. 16a
91245 Simmelsdorf-Hüttenbach/Bayern

INNOVATIONSSSTIFTUNG BAYERISCHE KOMMUNE

Stiftungsvorstand

Alexander Schroth, AKDB

Rudolf Schleyer, AKDB

Kuratorium

Dr. Franz Dirnberger, Bayerischer Gemeindetag

Bernd Buckenhofer, Bayerischer Städtetag

Dr. Johann Keller, Bayerischer Landkreistag

Stefanie Krüger, Bayerischer Bezirketag

IMPRESSUM

Herausgeber

Innovationsstiftung Bayerische Kommune

c/o Anstalt für Kommunale Datenverarbeitung in Bayern – AKDB

Hauptverwaltung

Hansastraße 12-16

80686 München

Postfach 150140

80042 München

© Innovationsstiftung Bayerische Kommune, München 2016

www.bay-innovationsstiftung.de

Einleitung / Anwendung

Herzlich willkommen zur Arbeitshilfe zur Erstellung eines Konzepts zur Informationssicherheit für Kommunen nach Artikel 8 „Informationssicherheit und Datenschutz“ des Gesetzes über die elektronische Verwaltung in Bayern (BayEGovG). Um Ihnen die Einführung und Anwendung dieses Sicherheitskonzepts zu erleichtern, erhalten Sie in diesem Abschnitt alle notwendigen Informationen als Fragen-Antworten-Katalog (FAQ). Im Rahmen dessen klären wir ebenfalls alle weiteren Fragen zur Anwendbarkeit und Einordnung der vorliegenden Arbeitshilfe.

Mittels dieser Arbeitshilfe installieren und betreiben Sie ein Informationssicherheitskonzept in vier Schritten im sogenannten Plan-Do-Check-Act-Zyklus oder auch Plan-Do-Check-Adjust-Zyklus (PDCA):



Abbildung 1: PDCA-Zyklus

Inhaltsverzeichnis

EINLEITUNG / ANWENDUNG	3
MANAGEMENT SUMMARY FÜR DIE BEHÖRDENLEITUNG	6
1 (GESETZLICHE) GRUNDLAGEN	10
1.1 WIESO BENÖTIGT MEINE KOMMUNE EIN INFORMATIONSSICHERHEITSKONZEPT?	10
1.2 BIS WANN IST EIN SOLCHES INFORMATIONSSICHERHEITSKONZEPT EINZUFÜHREN?	10
1.3 WAS IST INFORMATIONSSICHERHEIT?	11
1.4 WAS IST EIN INFORMATIONSSICHERHEITSKONZEPT?	12
1.5 WAS UNTERSCHIEDET EIN INFORMATIONSSICHERHEITSKONZEPT VON EINEM ISMS?	13
1.6 WAS HAT ES MIT DEN TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN AUF SICH?	14
2 HINTERGRÜNDE ZU DIESER ARBEITSHILFE	15
2.1 WER STEHT HINTER DER ARBEITSHILFE?	15
2.2 IST DIE ARBEITSHILFE EINE NEUENTWICKLUNG?	15
2.3 WAS IST DIE ZIELRICHTUNG?	15
2.4 KONKURRIERT DIESER ARBEITSHILFE MIT VORHANDENEN ISMS WIE BSI IT-GRUNDSCHUTZ ODER ISIS12?	15
2.5 FÜR WEN IST DIESER ARBEITSHILFE GEEIGNET?	16
3 UMSETZUNG DER ARBEITSHILFE	16
3.1 WIE WENDE ICH DIESER ARBEITSHILFE KONKRET AN?	16
3.1.1 ERSTE BESTANDSAUFNAHME	17
3.1.2 ÜBERSICHT SCHWACHSTELLEN, RISIKEN UND LÖSUNGSVORSCHLÄGE ERSTELLEN	17
3.1.3 MAßNAHMENPLAN ERSTELLEN	18
3.1.4 BETRIEB DES INFORMATIONSSICHERHEITSKONZEPTS	19
3.2 WIE IST DER AUFBAU DER ARBEITSHILFE?	20
3.3 WELCHE THEMENBEREICHE DECKT DIE ARBEITSHILFE AB?	20
3.4 HANDELT ES SICH UM EIN FERTIG AUSFORMULIERTES KONZEPT FÜR MEINE ORGANISATION, DAS ICH AUF NACHFRAGE VORZEIGEN KANN?	20
3.5 WIE SIND DIE EINZELNEN KAPITEL DER ARBEITSHILFE AUFGEBAUT?	21
4 TIPPS & TRICKS	22
4.1 SEIEN SIE EHRlich	22
4.2 HALTEN SIE SICH AN DIE REIHENFOLGE	22
4.3 GEMEINSAM SIND SIE STARK	22
4.4 DOKUMENTIEREN SIE AUSFÜHRlich	22
4.5 EXTERNE UNTERSTÜTZUNG IST ERLAUBT	22
4.6 BEGREIFEN SIE INFORMATIONSSICHERHEIT ALS ORGANISATIONSÜBERGREIFENDES THEMA	22
4.7 MACHEN SIE SICH NICHT KLEINER, ALS SIE ES TATSÄCHlich SIND	23

KAPITEL 1 INFORMATIONSSICHERHEIT	25
KAPITEL 2 DATENSCHUTZ (OPTIONAL IM SINNE DES ART. 8 BAYEGOVG)	47
KAPITEL 3 GEBÄUDESICHERHEIT	59
KAPITEL 4 ZUGANG IT-SYSTEME	75
KAPITEL 5 BERECHTIGUNGSKONZEPTE UND PROTOKOLLIERUNG	85
KAPITEL 6 SYSTEMVERFÜGBARKEIT UND NOTFALLMANAGEMENT	95
KAPITEL 7 RICHTLINIEN / DIENSTANWEISUNGEN	115
KAPITEL 8 SCHULUNGEN UND SENSIBILISIERUNGEN	125
KAPITEL 9 EXTERNE DIENSTLEISTER / AUFTRAGSDATENVERARBEITUNG	141

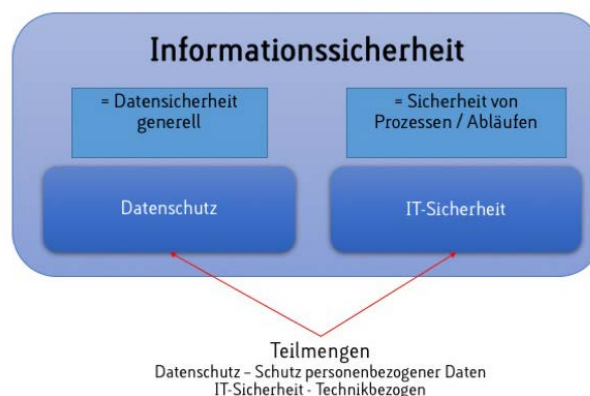
Management Summary für die Behördenleitung

Am 22.12.2015 wurde das „Gesetz über die elektronische Verwaltung in Bayern“ (BayEGovG) verabschiedet und trat zum 30. Dezember 2015 in Kraft. In Artikel 8 Absatz 1 BayEGovG heißt es konkret:

„¹Die Sicherheit der informationstechnischen Systeme der Behörden ist im Rahmen der Verhältnismäßigkeit sicherzustellen.²Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen im Sinn des Art. 7 des Bayerischen Datenschutzgesetzes (BayDSG) und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.“

Die Einführung und der Betrieb eines Informationssicherheitskonzepts sind somit verbindlich für alle bayerischen Kommunen. Artikel 10 Absatz 2 BayEGovG regelt zudem, dass ein solches Informationssicherheitskonzept bis zum 1. Januar 2018 vorzuliegen hat. Bayerische Kommunen müssen ab diesem Zeitpunkt den Nachweis führen können, einen systematischen Ansatz (= Konzept) zur dauerhaften Sicherstellung der Informationssicherheit eingeführt zu haben und zu betreiben.

Informationssicherheitskonzepte gibt es nicht von der Stange. Im Gegenteil sind dies Verfahrensweisen und Regeln, die organisationsindividuell langfristig Informationssicherheit sicherstellen sollen. Auch wenn sich die rechtliche Verpflichtung aus Art. 8 BayEGovG im engeren Sinn primär auf den Schutz informationstechnischer Systeme beschränkt, ist es in der Praxis sinnvoll, Informationssicherheit nicht hierauf zu beschränken, sondern unter Einbeziehung der sogenannten technischen UND organisatorischen Maßnahmen im Sinne des Artikel 7 BayDSG den Schutz aller analogen und digitalen Informationen einer Organisation in den Blick zu nehmen. Das beginnt beim Thema Gebäudesicherheit, setzt sich über Themen wie Datenschutz, Schulungen, Richtlinien, externe Dienstleister fort und endet nicht zwingend beim Thema IT-Sicherheit.



Ein funktionierendes Informationssicherheitskonzept hält mindestens bereit

- Vorgehensweisen zur Identifikation von (neuen und bestehenden) Risiken,
- Vorgehensweisen zur Planung von Maßnahmen zur Beseitigung oder Minimierung dieser Risiken,
- Vorgehensweisen zur kontinuierlichen Beschäftigung mit dem Thema in der Organisation („Sicherheitskultur“),
- verantwortliche Personen mit ausreichend Zeit und Mitteln zum Betrieb des Sicherheitskonzepts,
- Regeln, Richtlinien und Anweisungen für die Organisation und die Mitarbeiter zur Umsetzung und zum Betrieb des Konzepts,
- Maßnahmen zur kontinuierlichen Schulung und Sensibilisierung für Informationssicherheit.

Artikel 8 BayEGovG bezieht sich konkret auf die technischen und organisatorischen Maßnahmen des Artikel 7 BayDSG. Diese dienen in ihrer Gesamtheit dem Schutz der Informationen einer Organisation. Dabei ist es wichtig, eine angemessene und ausreichende Kombination an Maßnahmen für die Organisation zu entwickeln und einzuführen. Bildlich kann man sich dies wie eine Zwiebel vorstellen. Viele Lagen von außen nach innen schützen den weichen Kern der Zwiebel, der sinnbildlich für die schützenswerten Informationen in der Organisation steht. Diesen Kern gilt es zu schützen und hierfür wählt man aus einem großen Portfolio die geeigneten Maßnahmen aus.

Zu diesem Zweck können die unterschiedlichsten Maßnahmen als Schutzschichten kombiniert werden. Statt einer sehr teuren und aufwändigen Schutzschicht können mehrere kleinere und preiswerte Maßnahmen denselben Schutzzweck erreichen. Ist die Organisation leicht zugänglich, so wird ein sehr gut abgesicherter Serverraum schon fast Pflicht. Kann man sich jedoch nicht so ohne weiteres in dem Gebäude bis zum Serverraum bewegen, reicht vielleicht schon eine stabile, verschlossene Tür.

Eine pauschale Aussage, welche Maßnahmen Pflicht sind, lässt sich daher nicht treffen. Dies ergibt sich erst aus den individuellen Gegebenheiten vor Ort. Generell lässt sich sagen: Je geringer der Schutzwert äußerer Hüllen ist, umso höher muss dieser für die inneren Maßnahmen (= Zwiebelschichten) ausfallen.

Auf dem Markt gibt es bekannte Standards zur Informationssicherheit, wie die ISO27001, den BSI IT-Grundschutz, ISIS12 oder VDS3473. Diese bieten sehr umfangreiche Handbücher und Kataloge zur Einführung und zum Betrieb eines Informationssicherheitskonzepts im Rahmen des jeweiligen Standards. Gerade kleinere Einrichtungen können damit schnell überfordert sein. Dennoch besteht die Verpflichtung zur Informationssicherheit aus dem BayEGovG unabhängig von der Einrichtungsgröße.

Die nun vorliegende Arbeitshilfe zur Erstellung eines Informationssicherheitskonzepts nach Artikel 8 BayEGovG stellt eine Hilfe zur Selbsthilfe für kommunale Einrichtungen dar, die nicht über ausreichende Möglichkeiten zur Einführung und Umsetzung von anderen Standards zur Informationssicherheit verfügen. In vier angeleiteten Schritten wird damit ein Informationssicherheitskonzept eingeführt und betrieben:



Die Arbeitshilfe und das daraus resultierende Informationssicherheitskonzept decken die folgenden Punkte ab:

1. Informationssicherheit – Grundlagen zur Einführung und zur Aufrechterhaltung von Informationssicherheit
2. Datenschutz – Grundlegende Umsetzungen im Datenschutz (auf Basis des BayDSG) als elementarer Bestandteil der Informationssicherheit
3. Gebäudesicherheit
4. Zugang zu IT-Systemen
5. Berechtigungskonzepte und Protokollierung
6. Notfallmanagement (Vorsorge und Notfallplan)
7. Richtlinien und Dienstanweisungen
8. Schulungen und Sensibilisierung – Mitarbeiter als elementarer Bestandteil der Informationssicherheit
9. Externe Dienstleister – Anforderungen an externe Dienstleister, nicht nur im Rahmen einer Auftragsdatenverarbeitung

Für jedes Thema stehen ausführliche Checklisten zur Selbstüberprüfung, Mustervorlagen sowie Verweise auf weiterführende Informationen und Dokumente zur Verfügung. Ein Fragen-und-Antworten-Katalog führt durch die Anwendung der Arbeitshilfe und erklärt ausführlich die Hintergründe.

Die Arbeitshilfe kann intern oder auch mit externer Unterstützung durch kompetente Berater bearbeitet werden. Überlegenswert ist weiterhin der Ansatz, mit vergleichbaren Kommunen gemeinsame Lösungen zu suchen, einzuführen und zu betreiben. Dies kann sowohl technische Lösungen betreffen, aber eben auch das gemeinsame Durchführen von Schulungen.

1 (Gesetzliche) Grundlagen

1.1 Wieso benötigt meine Kommune ein Informationssicherheitskonzept?

Am 22.12.2015 wurde das „Gesetz über die elektronische Verwaltung in Bayern“ (BayEGovG) verabschiedet. In Artikel 8¹ Absatz 1 BayEGovG heißt es konkret:

„¹Die Sicherheit der informationstechnischen Systeme der Behörden ist im Rahmen der Verhältnismäßigkeit sicherzustellen.²Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen im Sinn des Art. 7 des Bayerischen Datenschutzgesetzes (BayDSG) und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.“

Die Einführung und der Betrieb eines Informationssicherheitskonzepts sind somit verbindlich für alle bayerischen Kommunen. Auch wenn sich die rechtliche Verpflichtung aus Artikel 8 BayEGovG im engeren Sinn primär auf den Schutz digitaler Informationen beschränkt, ist es in der Praxis sinnvoll, Informationssicherheit nicht auf die pure IT-Sicherheit zu reduzieren, sondern unter Einbeziehung der sogenannten technischen UND organisatorischen Maßnahmen im Sinne des Artikel 7 BayDSG den Schutz aller analogen und digitalen Informationen einer Organisation in den Blick zu nehmen. (Passagen in dieser Arbeitshilfe – speziell in den Prüfkatalogen -, die über die „informationstechnischen“ Anforderungen hinausgehen, sind entsprechend farblich gekennzeichnet.)

In der verabschiedeten und zum 25. Mai 2018 wirksam werdenden EU-Datenschutz-Grundverordnung (EU-DSGVO)² findet sich ebenfalls eine Verpflichtung zur Einführung und zum Betrieb eines Informationssicherheitskonzepts. Wie der Artikel 8 BayEGovG es vorsieht, wird auch hier die Leistungsfähigkeit der Organisation im Rahmen der Verhältnismäßigkeit zu berücksichtigen sein.

1.2 Bis wann ist ein solches Informationssicherheitskonzept einzuführen?

Dieser Punkt ist in Artikel 10 Absatz 2 BayEGovG³ sehr genau geregelt:

„¹Dieses Gesetz tritt am 30. Dezember 2015 in Kraft.²Abweichend von Satz 1 treten in Kraft: [...] 3. Art. 8 Abs. 1 Satz 2 am 1. Januar 2018.“

Sie sollten daher ab dem 1. Januar 2018 den Nachweis führen können, einen systematischen Ansatz (= Konzept) zur dauerhaften Sicherstellung der Informationssicherheit in Ihrer Kommune eingeführt zu haben und zu betreiben.

¹ <http://www.gesetze-bayern.de/Content/Document/BayEGovG-8>

² https://www.la-bayern.de/de/datenschutz_eu.html

³ <http://www.gesetze-bayern.de/Content/Document/BayEGovG-10>

Hinweis: Im Rahmen der Einführung eines Informationssicherheitskonzepts werden Sie auf Schwachstellen in Ihrer Kommune stoßen, die es möglichst zu beseitigen gilt. Die Beseitigung dieser Schwachstellen muss nicht zum 1. Januar 2018 abgeschlossen sein. Sie sollten diese jedoch bis dahin kennen und Systematiken eingeführt haben, um mit diesen Risiken entsprechend umzugehen („Risikobewältigung“).

1.3 Was ist Informationssicherheit?

Mit Informationssicherheit wird der Schutz von für die Organisation wichtigen oder durch Rechtsvorschriften zu schützenden Informationen vor Änderung, Missbrauch, Verlust und Zerstörung bezeichnet. Dabei wird kein Unterschied zwischen analogen oder digitalen, personenbezogenen oder nicht personenbezogenen Daten gemacht. Auch Informationen in den Köpfen der Mitarbeiter („Wissen“) gilt es für die Organisation zu schützen und zu sichern⁴. Der Schutzwert richtet sich nach der Bedeutung der Information für die Aufgabenerfüllung und Zielerreichung der jeweiligen Organisation oder einem durch ein Gesetz vorgegebenen Schutzwert (Datenschutz). Weiterhin können auch Verträge den Schutzwert von Informationen bestimmen.

Sofern es mit dem Schutz vor Zerstörung nicht geklappt hat, sollten geeignete Maßnahmen zur Wiederherstellung zur Verfügung stehen. Diese sind beispielsweise im technischen Bereich funktionsfähige und dem Stand der Technik entsprechende Sicherungen samt regelmäßiger Wiederherstellungstests (bis hin zu ganzen Servern / Systemlandschaften). Im analogen Bereich finden sich solche Maßnahmen beispielweise durch ein ausgelagertes Katastrophenarchiv wichtiger Originaldokumente in Verbindung mit einem Archiv der analogen Arbeitskopien im Hauptgebäude für die tägliche Nutzung.

Wer Informationssicherheit auf die Teilmengen IT-Sicherheit oder Datenschutz reduziert, vergisst dabei wesentliche Aspekte und erhöht sein Risiko erheblich. Nicht umsonst wird im Artikel 8 BayEGovG erneut Bezug auf die technischen (IT-Sicherheit) und organisatorischen Maßnahmen im Artikel 7 des Bayerischen Datenschutzgesetz (BayDSG)⁵ Bezug genommen. Hierbei wird explizit die digitale Welt verlassen und der gesamte Organisationsbereich (Gebäude, Mitarbeiter, Richtlinien etc.) miteinbezogen. Daher unser Tipp: Lösen Sie sich von der irrigen Annahme Informationssicherheit = IT-Sicherheit.

⁴ Innovationsstiftung Bayerische Kommune: Wissensmanagement in der öffentlichen Verwaltung, <http://www.bay-innovationsstiftung.de/index.php?id=71>

⁵ http://byds.juris.de/byds/009_1.1_DSG_BY_1993_rahmen.html

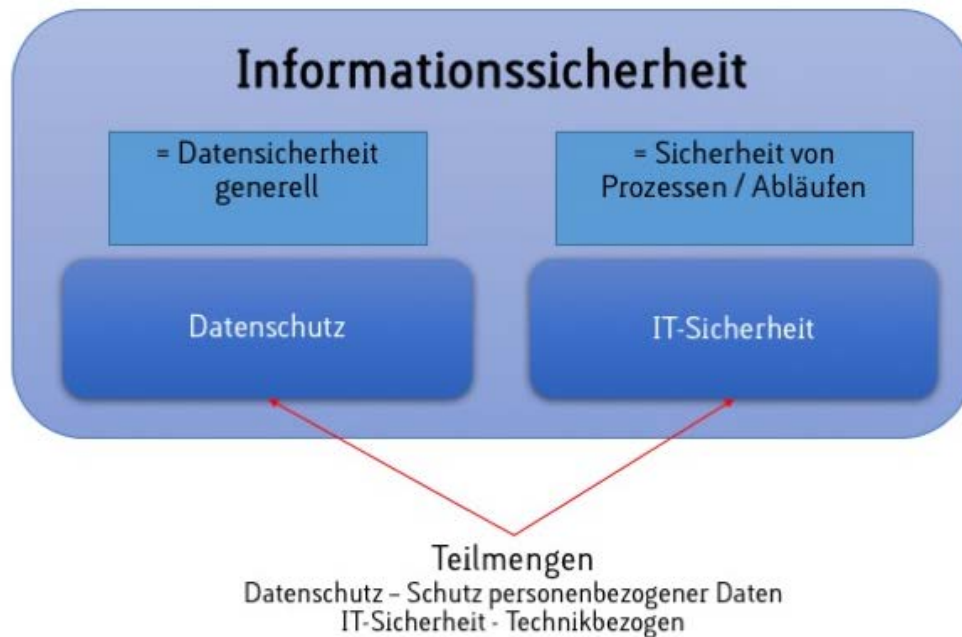


Abbildung 2: Informationssicherheit und Teilmengen

1.4 Was ist ein Informationssicherheitskonzept?

Ein Informationssicherheitskonzept beschreibt eine systematische und langfristig ausgelegte Vorgehensweise, welche die zuvor genannten Ziele der Informationssicherheit sowohl technisch als auch organisatorisch sicherstellt. Dabei muss ein Konzept darauf ausgelegt sein, jederzeit auftretende technische, organisatorische, personelle und auch rechtliche Veränderungen zu erkennen. Aus diesen Erkenntnissen leitet ein funktionierendes Konzept notwendige Maßnahmen aufgrund neuer Sicherheitsrisiken oder rechtlicher Auflagen ab, die es dann im weiteren Verlauf abzuarbeiten gilt. Beispiele für solche Änderungen:

- Technisch: Anschaffung neuer Server, Virtualisierung, Wechsel des Betriebssystems, neue Verfahren, aktuelle Bedrohungslagen (wie Kryptotrojaner) etc.
- Organisatorisch: Änderung von Raumnutzungen, Umzug, neue zusätzliche Gebäude/ Räume, Richtlinien etc.
- Personell: Umgang mit neuen Mitarbeitern (Einführung, Training), Umgang mit ausscheidenden Mitarbeitern (Deaktivierung von Accounts, Übergabe an neuen Mitarbeiter -> Wissenssicherung), Wechsel von Aufgaben, Verantwortlichkeiten, Schulungen, Anweisungen etc.
- Rechtlich: Auflagen im Datenschutz oder aus den Sozialgesetzbüchern oder weiteren Spezialgesetzen im Umgang mit Daten, Einführung neuer Gesetze wie BayEGovG im Jahr 2015 oder der EU-DSGVO zum Mai 2018.

Ein funktionierendes Informationssicherheitskonzept hält mindestens bereit

- Vorgehensweisen zur Identifikation von (neuen und bestehenden) Risiken,
- Vorgehensweisen zur Planung von Maßnahmen zur Beseitigung oder Minimierung dieser Risiken,

- Vorgehensweisen zur kontinuierlichen Beschäftigung mit dem Thema in der Organisation („Sicherheitskultur“),
- verantwortliche Personen mit ausreichend Zeit und Mitteln zum Betrieb des Sicherheitskonzepts (Informationssicherheitsbeauftragter, Team für Informationssicherheit, weitere Funktionen),
- Regeln, Richtlinien und Anweisungen für die Organisation und die Mitarbeiter zur Umsetzung und zum Betrieb des Konzepts,
- Maßnahmen zur kontinuierlichen Schulung und Sensibilisierung für Informationssicherheit.

Aus diesen Anforderungen wird ersichtlich, „*mal eben so Informationssicherheit*“ ist nicht möglich.

Die jüngere Vergangenheit hat gezeigt, wie sinnvoll es ist, Informationssicherheitskonzepte im Einsatz und aktuell zu haben. Nehmen Sie nur die Bedrohung durch Kryptotrojaner, die ganze Verwaltungen über Monate in Mitleidenschaft gezogen haben. Oder stellen Sie sich einen Brand in Ihrer Verwaltung bis zur vollkommenen Unbrauchbarkeit inklusive weitreichender Beeinträchtigung der IT/TK-Struktur sowie Verlust umfänglicher Papierunterlagen und auch Räumlichkeiten vor. Hier kann im Vorfeld durch umfangreiche Maßnahmen im Rahmen der Informationssicherheit zeitnah ein funktionsfähiger Notbetrieb wieder aufgenommen werden.

Bitte beachten Sie bei den zahlreichen Angeboten „*Informationssicherheit von der Stange*“ mittels einiger Softwarelösungen Folgendes: Diese decken zumeist nur die technischen Aspekte ab. Informationssicherheit ist nicht mit der Anschaffung von zwei bis drei Programmen sowie Wartungs- und Lizenzverträgen getan. Diese können wichtige Hilfsmittel im Rahmen eines Konzepts darstellen, sind jedoch kein Ersatz. Details hierzu finden Sie auch in den dazugehörigen Kapiteln.

Bei all diesen Erklärungen sollte klar geworden sein, ein Informationssicherheitskonzept ist kein Stück Papier, das es lediglich mit dem Namen Ihrer Einrichtung auszufüllen und in den Schrank zu stellen gilt. Informationssicherheit ist auch keine einmalige Arbeit, sondern ein stetiger Prozess, der sich von Beginn der Einführung bis über die Aufrechterhaltung und Weiterentwicklung in der Zukunft Ihrer Organisation erstreckt. Diese Arbeit kann Ihnen niemand abnehmen, auch wenn der Wunsch danach weit verbreitet ist.

1.5 Was unterscheidet ein Informationssicherheitskonzept von einem ISMS?

Informationssicherheitsmanagementsysteme (ISMS) bieten eine fertige und in vielen Organisationen bewährte Systematik zur Einführung und Aufrechterhaltung von Informationssicherheit in Organisationen an. Dies umfasst nicht nur Maßnahmen zur Risikoidentifikation und Maßnahmenplanung, sondern es werden gleichzeitig Verfahrensweisen in der Organisation etabliert, die einen kontinuierlichen Betrieb der Systematik sicherstellen. Weiterhin sind diese zertifizierbar, sprich sie können von unabhängiger Stelle auf praxistaugliche und den Standards entsprechende Umsetzung geprüft werden. Bei erfolgreicher Prüfung erhalten Sie darüber einen zeitlich befristeten Nachweis und werden regelmäßigen, meist jährlichen Nachprüfungen unterzogen. So können Sie jederzeit ohne große Diskussion belegen, was Ihre

Organisation für die Informationssicherheit getan hat. Bei einer eigenen Konzeptlösung ist eine Zertifizierung nicht möglich und der Beleg entsprechend aufwendiger zu führen.

Ein großer Vorteil dieser ISMS und Sicherheitsstandards wie dem BSI IT-Grundschutz, ISIS12 oder auch VDS3473 sind die umfangreichen Prüfkataloge, mit denen Risiken in der Organisation identifiziert und zugleich geeignete Maßnahmen zu deren Bewältigung ermittelt, geplant und überprüft werden. Dieses Angebot an fertigen Katalogen führt zu einem mehr oder weniger großen Umfang an Hilfsmitteln, die der Organisation zur Verfügung stehen. Diese sollten jedoch nicht als Last, sondern als Chance verstanden werden, Informationssicherheit auf einem hinreichenden Niveau in der Organisation umzusetzen.

Allen Managementsystemen aber auch Konzepten ist eines gemein, sie erledigen sich nicht von selbst. Es ist – egal welche Lösung Sie anstreben – stets ein nicht zu unterschätzender interner Zeit-, Personal- und Budgetanteil einzuplanen. Je weniger Sie interne Ressourcen zur Verfügung haben, umso mehr können und sollten Sie auf externe Unterstützung zurückgreifen. Jedoch ist es utopisch anzunehmen, man könne das Thema Informationssicherheit komplett auslagern. ISMS wie der BSI IT-Grundschutz oder auch ISIS12 sind für kleine Organisationen genauso gut geeignet wie für große Einrichtungen. In kleinen Einrichtungen fehlt es jedoch meist an Personal, Zeit und Geld für die Umsetzung.

1.6 Was hat es mit den technischen und organisatorischen Maßnahmen auf sich?

Technische und organisatorische Maßnahmen (TOM) dienen in Ihrer Gesamtheit dem Schutz der Informationen in Ihrer Organisation. Dabei ist es wichtig, eine angemessene und ausreichende Kombination an Maßnahmen für Ihre Organisation zu entwickeln und einzuführen. Bildlich können Sie sich das wie eine Zwiebel vorstellen. Viele Lagen von außen nach innen schützen den weichen saftigen Kern der Zwiebel, der sinnbildlich für die schützenswerten Informationen in Ihrer Organisation steht. Diesen Kern gilt es zu schützen und Sie wählen dafür aus einem großen Portfolio die geeigneten Maßnahmen aus.

Zu diesem Zweck können die unterschiedlichsten Maßnahmen als Schutzschichten kombiniert werden. Statt einer sehr teuren und aufwändigen Schutzschicht können mehrere kleinere und preiswerte Maßnahmen denselben Schutzzweck erreichen. Ist die Organisation leicht zugänglich, so wird ein sehr gut abgesicherter Serverraum mit Innenraumüberwachung (Betreten, Video, Öffnungsdauer der Tür) schon fast Pflicht. Kann man sich jedoch nicht so ohne weiteres in Ihrem Gebäude bis zum Serverraum bewegen, reicht vielleicht schon eine stabile, verschlossene Tür.

Eine pauschale Aussage, welche Maßnahmen Pflicht sind, lässt sich daher nicht treffen. Dies ergibt sich erst aus den individuellen Gegebenheiten vor Ort. **Es gibt hierfür leider kein Schema F.** Generell lässt sich sagen: Je geringer der Schutzwert äußerer Hüllen ist, umso höher muss dieser für die inneren Maßnahmen (=Zwiebelschichten) ausfallen.

2 Hintergründe zu dieser Arbeitshilfe

2.1 Wer steht hinter der Arbeitshilfe?

Initiiert wurde die Entwicklung dieser Arbeitshilfe von der Innovationsstiftung Bayerische Kommune mit Sitz in München zusammen mit den Bayerischen Kommunalen Spitzenverbänden. Das Projekt zur Erstellung wurde an das Unternehmen a.s.k. Datenschutz, Sascha Kuhrau mit Sitz im Nürnberger Land vergeben. Im Rahmen von Workshops und Nutzung einer gemeinsamen Kollaborationsplattform wurden die Inhalte und Vorgehensweisen mit Praktikern aus allen kommunalen Ebenen erarbeitet.

2.2 Ist die Arbeitshilfe eine Neuentwicklung?

Ja und nein. Einerseits wurde der bereits 2014 für die Stiftung entwickelte „*Quick Check Datenschutz und Datensicherheit*“ herangezogen und überarbeitet, andererseits sind zahlreiche Erweiterungen eingeflossen, die dem Thema Informationssicherheit und den rechtlichen Vorgaben Rechnung tragen. Hinzu kamen eine neue Struktur, Rahmendokumente zur Einführung und zum kontinuierlichen Betrieb sowie diverse Mustervorlagen samt aktuellen Web-links zu weiterführenden Mustern und Informationen mit Tipps und Tricks zur Umsetzung.

Bei der Erstellung wurde Wert auf Berücksichtigung von Bewährtem und Bekanntem gelegt. So finden sich zahlreiche Hinweise auf Elemente des BSI IT-Grundschutzes oder auch von ISIS12 (als Ableger des BSI IT-Grundschutzes) in dieser Arbeitshilfe wieder. Zusätzlich sind praxistaugliche Quellen wie die Archive und Webseiten der Landesdatenschutzbehörden mit Stellungnahmen und Mustervorlagen berücksichtigt.

Wie bereits beim Quick Check wurde dabei Wert auf die umfängliche Betrachtung der Anforderungen aus den technischen und organisatorischen Maßnahmen aus den Datenschutzgesetzen gelegt, da diese im BayEGovG als Maßstab / Grundlage benannt sind.

2.3 Was ist die Zielrichtung?

Diese Arbeitshilfe soll eine Hilfe zur Selbsthilfe für kommunale Einrichtungen sein, die nicht über ausreichende Möglichkeiten zur Einführung und Umsetzung von Standards zur Informationssicherheit wie BSI IT-Grundschutz oder ISIS12 verfügen, um den Anforderungen des Artikel 8 BayEGovG zu genügen.

2.4 Konkurriert diese Arbeitshilfe mit vorhandenen ISMS wie BSI IT-Grundschutz oder ISIS12?

Definitiv nein. Es hätte keinen Sinn ergeben, neben den bereits bekannten Standards ein weiteres Managementsystem zu entwickeln. Vielmehr verfolgt die Arbeitshilfe den Ansatz, den Mindestanforderungen aus Artikel 8 BayEGovG gerecht zu werden. Also denjenigen kommunalen Einrichtungen ein Hilfsmittel zur Entwicklung und Einführung eines eigenen Informationssicherheitskonzepts an die Hand zu geben, die aus zeitlichen, personellen oder monetären Gründen eines der oben genannten ISMS nicht umsetzen können.

Aus diesem Grund erhalten Sie mit der Arbeitshilfe auch nur einen begrenzten Fragen- und Maßnahmenkatalog zur Selbstüberprüfung und Hilfsmittel zur anschließenden kontinuierlichen Weiterentwicklung in Ihrer Organisation. Die Anwendung dieser Arbeitshilfe ist weiterhin nicht zertifizierbar. Wobei Sie natürlich jederzeit den Umsetzungsstand in Ihrer Organisation durch fachlich kompetente Berater für Informationssicherheit prüfen und dokumentieren lassen können. (Bitte seien Sie sorgfältig bei der Auswahl des Dienstleisters. Im Zweifel fragen Sie Kolleginnen und Kollegen anderer Einrichtungen, welche Erfahrungen diese gemacht haben.)

2.5 Für wen ist diese Arbeitshilfe geeignet?

Da die hier vorgestellte Arbeitshilfe keinen Ersatz für ein ISMS darstellt, ist sie von der Detailtiefe und Vorgehensweise eher für mittlere und kleine Einrichtungen geeignet. Letztendlich ist die Eignung jedoch an den vorhandenen Mitteln und Möglichkeiten sowie dem bereits aktuellen Stand der Informationssicherheit in der Organisation festzumachen.

Hat sich in Ihrer Organisation noch niemand mit dem Thema Informationssicherheit systematisch beschäftigt, ist die Arbeitshilfe ein geeigneter Einstieg. In kleineren Einrichtungen wird diese auch bereits vollkommen ausreichend sein, um den Anforderungen des Artikel 8 BayEGovG zu genügen. In mittleren und größeren Einrichtungen kann die Arbeitshilfe jedoch im Zweifel nur der erste Schritt – quasi ein Einstieg ins Thema - sein, der in nachgelagerten Phasen ein „Upgrade“ in Richtung ISIS12 oder je nach Organisationsgröße und Kritikalität zum BSI IT-Grundschutz erfährt.

Eine Einrichtung, die sich bisher schon stark am BSI IT-Grundschutz orientiert hat, wird den Teil der Arbeitshilfe zur Selbstüberprüfung (Kapitel 1-9) für eine interne Kontrolle gut heranziehen können.

3 Umsetzung der Arbeitshilfe

3.1 Wie wende ich diese Arbeitshilfe konkret an?

Im ersten Schritt machen Sie sich mit den Komponenten und Inhalten dieser Arbeitshilfe vertraut. Dazu dient unter anderem die Lektüre dieses Dokuments. Es ist jedoch ebenfalls sehr hilfreich, im Kreis vergleichbarer Kommunen ähnlicher Größe, zu denen Sie Kontakt haben (beispielsweise aufgrund gemeinsam besuchter Schulungen / Veranstaltungen), Informationen einzuholen, wer sich mit dem Thema bereits befasst und welche Erfahrungen gesammelt worden sind. Die Anwendung dieser Arbeitshilfe findet im Rahmen eines PDCA-Zyklus statt:



Abbildung 3: Plan - Do - Check - Act Zyklus der Arbeitshilfe

3.1.1 Erste Bestandsaufnahme

Beginnen sollten Sie stets mit den ersten beiden Kapiteln „*Informationssicherheit*“ und „*Datenschutz*“. Hier legen Sie den Grundstein für eine erfolgreiche Einführung und Umsetzung eines Informationssicherheitskonzepts. Nehmen Sie diese beiden Kapitel bitte sehr ernst. Alles, was Sie hier auslassen oder versäumen, wird Sie im weiteren Verlauf unangenehm einholen bis hin zum Scheitern des Projekts.

Haben Sie die beiden ersten Kapitel erfolgreich bearbeitet, machen Sie sich an die Bearbeitung der weiteren Kapitel. Sollten Sie bereits Erkenntnisse über größere Schwachstellen / Lücken in den einzelnen Themen gewonnen haben, ziehen Sie die Kapitel mit den größten Schwachstellen zur Bearbeitung vor. Auf diese Art erzielen Sie im Zweifel am schnellsten Fortschritte in der Informationssicherheit.

Es empfiehlt sich, ein Kapitel nach dem anderen zu bearbeiten. Sobald Sie Schwachstellen identifiziert und im Rahmendokument (siehe nächsten Abschnitt) dokumentiert haben, bearbeiten Sie die Prüffragen und Kapitel weiter. Maßnahmenplanung und Umsetzung startet erst nach der Selbstüberprüfung.

3.1.2 Übersicht Schwachstellen, Risiken und Lösungsvorschläge erstellen

Identifizierte Schwachstellen beschreiben Sie kurz in den Kapiteln unter „*Ergebnis(se)*“ und ausführlich im Übertrag in das Rahmendokument „*Übersicht identifizierte Schwachstellen und mögliche Lösungen*“. Dieses Rahmendokument dient der weiteren Bearbeitung nach Durchlauf der Selbstüberprüfung mit den Fragen aus den Kapiteln.

Sobald Sie ein Kapitel durchlaufen und das Dokument „*Übersicht identifizierte Schwachstellen*“ gefüllt haben (es wird sich füllen, das ist ganz normal), beschreiben Sie konkret die sich

aus der Schwachstelle ergebenden Risiken für Ihre Organisation (Spalte 2). Denken Sie dabei daran, dass die Risiken ganz unterschiedlicher Natur sein können (Datenverlust / Kompromittieren, finanzielle Schäden, Rechtsverstöße, Vertragsverstöße, Verletzung der Betroffenenrechte / Datenschutz, aber auch Imageschäden / negative Außenwirkungen). Versuchen Sie die Risiken möglichst detailliert zu beschreiben, damit die Behördenleitung eine Grundlage hat, über den Umgang mit diesen Risiken zu entscheiden. In Spalte 1 tragen Sie in der ersten Zeile die Kapitelnummer ein und in die zweite Zeile die Nummer des Prüfpunkts in dem jeweiligen Kapitel. So bleibt stets der Bezug zur Bestandsaufnahme erhalten.

Für das Ausfüllen der Spalte 3 „*Mögliche Maßnahmen zur Beseitigung*“ sollten Sie sich mit den betroffenen Sachbereichen auseinandersetzen und versuchen, möglichst mehr als einen Lösungsvorschlag zur Beseitigung der Schwachstelle anzubieten. Denken Sie dabei in Alternativen. Beispiel: Im Serverraum laufen wasserführende Leitungen und darüber befinden sich schlimmstenfalls Sanitärräume? Dann kann eine der Maßnahmen zur Beseitigung „*Umgang des Serverraums in anderes Gebäudeteil*“ sein, verbunden mit hohen finanziellen Aufwendungen. Eine Alternative könnte jedoch sein, Wassermelder im Serverraum zu installieren. Eine Maßnahme, die mit geringem finanziellen Aufwand durchaus eine zulässige alternative Schutzschicht im Mix (denken Sie an die Zwiebelschichten) darstellt.

In Spalte 4 „*Budget intern / extern in Euro*“ tragen Sie die voraussichtlichen Kosten für die geplanten Maßnahmen ein beispielsweise auf Basis vorliegender Angebote. Spalte 5 dient der Erfassung interner Zeitaufwendungen zur Bearbeitung der Maßnahmen. Im Zweifel werden Sie hier schätzen müssen (schätzen Sie lieber mehr als weniger, hat die Praxis gezeigt). In der letzten Spalte tragen Sie den oder die Verantwortlichen für die Beseitigung der Schwachstellen ein.

Haben Sie dieses Dokument für ein oder mehrere Kapitel mit Details befüllt, ist die Grundlage für die weitere Umsetzung geschaffen.

3.1.3 Maßnahmenplan erstellen

Mit dem vollständig ausgefüllten Dokument „*Übersicht identifizierte Schwachstellen und mögliche Lösungen*“ gehen Sie nun zur Behördenleitung und stellen die Inhalte vor. Ziel ist es, nun die konkret zu ergreifenden Maßnahmen zur Beseitigung der identifizierten Schwachstellen zeitlich und monetär zu planen. Sie können dabei gerne Ihre Vorstellungen und Vorschläge einfließen lassen, entscheiden muss jedoch letztendlich die Behördenleitung. (Dieser obliegt nämlich die organisatorische Verantwortung für das Thema, die auch nicht auf Sie als Bearbeiter des Themas übertragen werden kann.)

Bitte beachten Sie: Für den Nachweis eines Informationssicherheitskonzepts zum 01.01.2018 ist es nicht notwendig, bis dahin alle identifizierten Schwachstellen beseitigt zu haben! Sie müssen lediglich interne Verfahrensweisen etabliert haben, mit denen Sie heutige und zukünftige Schwachstellen identifizieren und bearbeiten können. Nichtsdestotrotz muss die Beseitigung der Schwachstellen das Ziel sein.

Die Ergebnisse tragen Sie in die konkrete Maßnahmenplanung im Dokument „*Übersicht Maßnahmenplan*“ ein. Wie bereits im vorherigen Rahmendokument verweisen Sie in Spalte 1 auf das dazugehörige Kapitel und den Prüfpunkt. In Spalte 2 „*Beschlossene Maßnahmen*“

beschreiben Sie nun sehr konkret, was beschlossen wurde und was zu tun ist. In Spalte 3 „*Umzusetzen durch*“ weisen Sie die einzelnen Aktivitäten den handelnden Personen zu, wohingegen Sie in Spalte 4 „*Verantwortlich*“ die Person benennen, die für den Punkt und dessen erfolgreiche Umsetzung hauptverantwortlich ist. (Dies muss nicht unbedingt eine der handelnden Personen aus Spalte 3 sein.)

Damit das Projekt zeitlich nicht aus dem Ruder läuft, schreiben Sie in Spalte 5 realistische Umsetzungstermine fest. Machen Sie den Beteiligten bitte klar, dass bei absehbarer Nichteinhaltung dieser Termine frühzeitig eine Information sowohl an den Verantwortlichen aus Spalte 4 aber auch an die Funktion ISB erfolgen sollte. Damit behalten Sie die Möglichkeit, auf aufgeplante Verzögerungen zu reagieren.

Nutzen Sie die Spalte 6 „*Kommentar*“ zur ausführlichen Beschreibung der ergriffenen / umgesetzten Aktivitäten. Ebenso beschreiben und begründen Sie im Kommentarfeld ausführlich, wenn geplante Maßnahmen zurückgestellt oder gar nicht umgesetzt werden. Diese zurückgestellten Maßnahmen sowie die Maßnahmen mit Status „*Offen*“ und „*In Arbeit*“ stellen Ihr sogenanntes „*Risikoinventar*“ dar.

Die Spalte 7 „*Status*“ dient der vereinfachten Darstellung des Umsetzungsstatus. „*Offen*“, „*in Arbeit*“, „*beendet*“ oder „*zurückgestellt*“ sollten hier genutzt werden.

Dieses Dokument und das vorherige Rahmendokument sollten Sie stets aktuell halten und bei Bedarf um weitere notwendige Maßnahmen ergänzen, wenn sich ein Änderungsbedarf ergibt oder sich Rahmenbedingungen ändern, die weitere Maßnahmen notwendig machen. Weiterhin sollten Sie dieses Dokument regelmäßig mit der Behördenleitung abstimmen, damit diese über das aktuelle Risikoinventar informiert ist.

Weitere Hinweise zum Umgang mit diesen Dokumenten finden Sie stets am jeweiligen Dokumentenende unter „*Hinweise*“.

3.1.4 Betrieb des Informationssicherheitskonzepts

Wenn Sie an diesem Schritt angelangt sind, befinden Sie sich bereits mitten in einem aktiven Informationssicherheitskonzept. Herzlichen Glückwunsch! Nach der erstmaligen Selbstüberprüfung, Risikoidentifizierung, Maßnahmenplanung und Umsetzung gilt es nun, sich auch weiterhin mit dem Thema Informationssicherheit regelmäßig zu beschäftigen.

Dies erfolgt einerseits durch das aktive Überwachen und Kontrollieren der geplanten und offenen Maßnahmen aus Ihrer Planung. Legen Sie sich diese Termine doch in dem in der Organisation im Einsatz befindlichen Kalenderprogramm an, damit Sie diese nicht aus den Augen verlieren.

Zusätzlich sollten Sie nun Einrichtungen schaffen, die eine kontinuierliche Weiterentwicklung ermöglichen. Haben Sie ein Team für Informationssicherheit eingerichtet? Dann legen Sie feste Termine für gemeinsame Besprechungen und Abstimmungen fest (z.B. 1 x Quartal). Planen Sie diese Termine fest und verbindlich ein und legen Sie diese bereits jetzt für zwölf Monate im Voraus fest. Denken Sie rechtzeitig an die Folgetermine.

Es gibt kein Team für Informationssicherheit? Dann sollte zumindest der Verantwortliche für Informationssicherheit sich feste Termine einplanen, um sich selbst als Verantwortlicher des Themas anzunehmen. Dazu gehören Termine für regelmäßige Begehungen aller Räumlichkeiten inklusive der Außenstellen, Schulungstermine, Termine zur Bearbeitung und zum Überprüfen offener Maßnahmen, Abstimmungen mit den Sachbereichen, Identifikation geänderter Rahmenbedingungen und Planung daraus entstehender weiterer Maßnahmen etc. Sie sehen schon, Informationssicherheit ist keine einmalige Sache. Sie brauchen zwingend Verantwortlichkeiten, Zeit und Mittel für dieses Thema. Auch hier erneut der Hinweis: Schauen Sie über den Tellerrand Ihrer eigenen Organisation und tauschen Sie sich mit vergleichbaren Kommunen aus. Informationssicherheit ist kein Thema für Einzelkämpfer.

3.2 Wie ist der Aufbau der Arbeitshilfe?

Die Arbeitshilfe besteht aus neun Kapiteln plus Rahmendokumenten (wie beispielsweise dieser Einleitung / Erklärung). Rahmendokumente befinden sich im vorangestellten Kapitel 0. Jedes Kapitel befasst sich mit einem wichtigen Thema der Informationssicherheit ausgehend von den Anforderungen der technischen und organisatorischen Maßnahmen der Datenschutzgesetze sowie den einschlägigen Normen zur Informationssicherheit.

3.3 Welche Themenbereiche deckt die Arbeitshilfe ab?

Dies ist gut aus der Kapitelstruktur ersichtlich:

1. Informationssicherheit – Grundlagen zur Einführung und zur Aufrechterhaltung von Informationssicherheit
2. Datenschutz – Grundlegende Umsetzungen im Datenschutz (auf Basis des BayDSG) als elementarer Bestandteil der Informationssicherheit
3. Gebäudesicherheit
4. Zugang zu IT-Systemen
5. Berechtigungskonzepte und Protokollierung
6. Notfallmanagement (Vorsorge und Notfallplan)
7. Richtlinien und Dienstanweisungen
8. Schulungen und Sensibilisierung – Mitarbeiter als elementarer Bestandteil der Informationssicherheit
9. Externe Dienstleister – Anforderungen an externe Dienstleister, nicht nur im Rahmen einer Auftragsdatenverarbeitung

Wenn Sie diese Punkte mit den technischen und organisatorischen Maßnahmen (TOM) vergleichen, werden Sie die Inhalte darin wiederfinden. Hinzu sind sogenannte Rahmendokumente gekommen, die es nach der Selbstüberprüfung und Feststellung des Status Quo ermöglichen, Informationssicherheit in Ihrer Organisation zu überprüfen, weiter zu entwickeln und auf geänderte Rahmenbedingungen zu reagieren (siehe auch Abschnitt 1.4)

3.4 Handelt es sich um ein fertig ausformuliertes Konzept für meine Organisation, das ich auf Nachfrage vorzeigen kann?

Die vorliegende Arbeitshilfe stellt kein fertig ausformuliertes Konzept für Ihre Organisation dar. Informationssicherheit ist Arbeit und eine organisationsspezifische Angelegenheit. Vom

Aufbau her ähneln sich Sicherheitskonzepte inhaltlich nur bedingt (siehe auch Abschnitt 1.4 und 1.6)

Sie erhalten mit dieser Arbeitshilfe jedoch das Handwerkzeug, um geführt ein Informationssicherheitskonzept für Ihre Organisation zu entwickeln, einzuführen und zu betreiben. Das können Sie in kompletter Eigenleistung erbringen oder bei Bedarf externe Unterstützung heranziehen (Achtung bei der Auswahl der Anbieter!). Ob und inwieweit Sie externe Unterstützung benötigen, hängt von den internen Gegebenheiten (Zeit, Know-how etc.) ab.

3.5 Wie sind die einzelnen Kapitel der Arbeitshilfe aufgebaut?

Der Aufbau aller Kapitel ist identisch, um die Bearbeitung zu erleichtern. Eingangs finden sich Erläuterungen und Erklärungen sowie teilweise Beispiele zum jeweiligen Thema des Kapitels (Notwendigkeit, Risiken, Möglichkeiten),

In der anschließenden Tabelle finden Sie ausgewählte Prüfpunkte und Fragen in der Spalte „*Erläuterungen / Fragen*“, die eine konkrete Beschäftigung mit dem Thema fördern und bei korrekter Bearbeitung mögliche Schwachstellen in der Informationssicherheit in Ihrer Organisation identifizieren helfen. Um den Umfang möglichst übersichtlich zu halten, implizieren die meisten Prüffragen bereits eine mögliche Lösung, sollten Sie bisher für diesen Punkt keine Maßnahmen ergriffen haben.

Beispiel: Die Frage „*Enthält Ihr Notfallplan einen Netzplan mit der Infrastruktur Ihrer technischen Einrichtungen?*“ impliziert bei einer Nein-Antwort, dass Sie diesen Netzplan erstellen sollten (ein Beispiel dafür ist in den Mustervorlagen beigelegt).

Die Spalte „*Ergebnis(se)*“ dient dazu, den Status Quo konkreter zu beschreiben. Was ist bereits umgesetzt, was fehlt möglicherweise noch. In der Spalte „*Bewertung*“ finden Sie ein vereinfachtes Schema zur Beurteilung und dem Umsetzungsgrad des Prüfpunkts. Das Schema unterteilt sich in „*Erfüllt*“, „*Nicht erfüllt*“, „*Nicht anwendbar*“ und „*In Arbeit*“.

Am Ende eines jeden Kapitels besteht die Möglichkeit, eine Gesamtbewertung nach dem zuvor genannten Schema vorzunehmen und eine formulierte Einschätzung abzugeben. Dahinter befinden sich Sammlungen an Weblinks zu ausgewählten Informationen und Vorlagen zum jeweiligen Themenbereich.

Ein Kapitel schließt jeweils mit einem Hinweis auf beiliegende Mustervorlagen und Dokumente ab.

4 Tipps & Tricks

4.1 Seien Sie ehrlich

Wenn Sie sich im Rahmen der Konzepterstellung etwas vormachen, wird Sie das zu einem unerwarteten oder auch absehbaren Zeitpunkt unangenehm einholen.

4.2 Halten Sie sich an die Reihenfolge

Beginnen Sie wirklich mit den Kapiteln 1 und 2. Erst nach deren erfolgreichen Bearbeitung – und in diesem Fall auch Umsetzung – sollten Sie sich mit den weiteren Kapiteln beschäftigen. Lassen Sie die ersten beiden Kapitel aus oder nehmen diese nicht ernst, können Sie sich den weiteren Aufwand eigentlich sparen.

4.3 Gemeinsam sind Sie stark

Suchen Sie mit umliegenden vergleichbaren Kommunen gemeinsame Lösungen für Ihre Probleme. So hat sich das Modell Interkommunale Zusammenarbeit (IKZ) in vielen Fällen bereits gut bewährt. Kommunen im Landkreis teilen sich einen Datenschutzbeauftragten, organisieren gemeinsam Schulungen für ihre Mitarbeiter, erwerben gemeinsam „Landkreislizenzen“ und viele positive Beispiele mehr. Die Vorteile liegen klar auf der Hand: transparente Kostenaufteilung, niedrigere Kosten und die Beteiligten sind stets aktuell im Thema.

4.4 Dokumentieren Sie ausführlich

Nutzen Sie die jeweiligen Dokumente und Eingabemöglichkeiten ausführlich zur Beschreibung und für Erläuterungen. Ziel muss sein, dass jederzeit andere fachlich geeignete Personen anhand der Unterlagen Ihres Konzepts den Status Quo der Informationssicherheit in Ihrer Organisation erkennen und bei Bedarf das Konzept fortführen können.

4.5 Externe Unterstützung ist erlaubt

Gerade in kleinen Organisationen wird es schwierig sein, das Know-how zur Einführung und zum Betrieb eines Informationssicherheitskonzepts mit allen Unterthemen vollständig im eigenen Haus vorzuhalten. Schauen Sie sich nach kompetenten Dienstleistern um, die Sie einmalig oder regelmäßig bei den Themen unterstützen, bei denen Sie Lücken haben. Stimmen Sie sich mit umliegenden Kommunen ab. Vielleicht lassen sich auch beim Einsatz von externen Dienstleistern Synergieeffekte erzielen (z.B. gemeinsame Schulungen etc.)

4.6 Begreifen Sie Informationssicherheit als organisationsübergreifendes Thema

Lösen Sie sich von der Annahme Informationssicherheit = IT-Sicherheit. IT-Sicherheit ist neben Datenschutz eine Teilmenge der Informationssicherheit. Sicherlich kommt dieser eine elementare Bedeutung zu, doch eine Reduktion des Themas auf IT-Sicherheit greift zu kurz. Bedenken Sie, über 50% aller Datenpannen⁶ werden aufgrund von Unkenntnis und Fahrlässigkeit verursacht. Dies können Sie nicht mit Technik abfangen, dazu sind organisatorische Maßnahmen notwendig.

⁶ http://www.zdnet.de/88157277/symantec-fehler-sind-ursachen-der-meisten-datenpannen-nicht-hacker/?utm_source=rss&utm_medium=rss&utm_campaign=rss

4.7 Machen Sie sich nicht kleiner, als Sie es tatsächlich sind

In einem ersten Schritt mag es praktisch erscheinen, mit der eigenen Organisation tief zu stapeln und somit die Anforderungen an die interne Informationssicherheit möglichst gering zu halten. Widerstehen Sie bitte dieser Versuchung! Die Folgen können für Sie katastrophal sein. Kleine Organisationen betreiben mittels dieser Vorlage Informationssicherheit auf einem ausreichenden Niveau. Mittlere Einrichtungen können damit vielleicht gerade noch so hinkommen. Große Einrichtungen sollten sich den Anforderungen eines ISMS stellen, um ausreichende Sicherheit – auch im Hinblick auf die Kritikalität – zu gewährleisten. Diese können jedoch durchaus diese hier vorliegende Arbeitshilfe als Einstieg nutzen, um darauf weiter aufzubauen.

Viel Erfolg bei der Umsetzung!

Abkürzungen der Arbeitshilfe

BayEGovG	Gesetz über die elektronische Verwaltung in Bayern
BayDSG	Bayerisches Datenschutzgesetz
EU-DSGVO	EU-Datenschutz-Grundverordnung
FAQ	Frequently asked questions – Fragen und Antworten
IKZ	Interkommunale Zusammenarbeit
ISMS	Informationssicherheitsmanagementsystem oder auch Managementsystem für Informationssicherheit
PDCA	Plan-Do-Check-Act oder auch Plan-Do-Check-Adjust: Management-Methode zur kontinuierlichen Verbesserung von Leistungen und Produkten
TOM	Technische und organisatorische Maßnahmen
ZD	Zentrale Dienste

Kapitel 1 Informationssicherheit

Im Rahmen dieses Kapitels legen Sie den Grundstein für alle weiteren Kapitel und die erfolgreiche Einführung von Informationssicherheit in Ihrer Organisation. Je leichter es Ihnen fällt, die Punkte aus diesem Kapitel in Ihrer Einrichtung zu etablieren, um so leichter werden Sie es in den nachfolgenden Kapiteln haben. Stoßen Sie jedoch bereits in diesem Kapitel auf unüberwindbare Widerstände, um so höher ist die Wahrscheinlichkeit des Scheiterns des Informationssicherheitskonzepts in Ihrer Organisation.

Sollten Sie bei der Behördenleitung kein Gehör für diese Themen finden, so kann das Hinzuziehen eines externen Beraters mit Erfahrung im Projektmanagement sehr hilfreich sein. Dieser kann aufgrund seiner Erlebnisse in der Praxis der Leitung sehr plakativ darstellen, wieso dieses Kapitel als Basis für das Projekt „Informationssicherheitskonzept“ unabdingbar ist.

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1. Informationssicherheit	Haben Sie die grundlegenden Anforderungen an Verfahren und Abläufe zur Einführung und kontinuierlicher Aufrechterhaltung von Informationssicherheit sichergestellt? Diese dienen als Basis, um Informationssicherheit als kontinuierlichen Prozess in Ihrer Organisation nicht nur einzuführen, sondern auch aufrechtzuerhalten. Tipp: Nehmen Sie sich diesen Punkt als Erstes vor, bevor Sie mit weiteren Maßnahmen aus diesem Konzept weitermachen. Hinweis: Sofern Sie die Punkte aus Schritt 1 „<i>Informationssicherheit</i>“ in Ihrer Organisation nicht umsetzen können, sollten Sie der Behördenleitung die Frage stellen, ob eine Fortführung überhaupt noch Sinn ergibt. Denn Ihnen wird im weiteren Verlauf der Umsetzung die notwendige Basis und Unterstützung fehlen, die Sie mit diesem Schritt aufbauen.		

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.1. Leitlinie / Dienstanweisung zur Informationssicherheit	Ihre Sicherheitsstrategie sollte in einer Leitlinie zur Informationssicherheit zusammengefasst werden, um die zu verfolgenden Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter zu dokumentieren (und diese einzufordern!). Mit der Sicherheitsleitlinie bekennt sich die Behördenleitung klar zu ihrer Verantwortung für Informationssicherheit. Idealerweise erfolgt die Umsetzung der Leitlinie mittels Inkraftsetzung durch eine Dienstanweisung. Wie jede andere Leitlinie sollte auch die Leitlinie Informationssicherheit regelmäßig, spätestens jährlich, auf notwendige Anpassungen hin geprüft und bei Bedarf aktualisiert werden.		Dokumente / Anlagen:
1.1.1. Verantwortung der Behördenleitung	Informationssicherheit hat in Ihrer Einrichtung keine Chance, wenn die Behördenleitung nicht im vollen Umfang hinter den Zielen der Informationssicherheit und den dafür notwendigen Maßnahmen steht. Hat sich die Behördenleitung zu ihrer Gesamtverantwortung für Informationssicherheit bekannt? Wurde die Leitlinie von der Behördenleitung unterschrieben?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

1.1.2. Geltungsbereich	Ist schriftlich festgelegt, für welche Einrichtungen (Verwaltung, Kindergarten, Bauhof, Außenstellen, Eigenbetriebe etc.) die Leitlinie gelten soll? Wurde dabei klar festgestellt, dass sich Informationssicherheit auf analoge und digitale Daten sowie die gesamte organisatorische Tätigkeit bezieht und sich eben nicht auf IT-Systeme beschränkt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
1.1.3. Sicherheitsziele	Welche Ziele sollen mittels Informationssicherheit erreicht werden (Erfüllung rechtlicher Auflagen, Sicherung der Aufgabenerfüllung, Vermeidung von Umsatz-/Gewinnausfällen [bspw. bei Eigenbetrieben] etc.)? Sind diese Ziele klar formuliert?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.1.4. Kernelemente der Sicherheitsstrategie	Sind folgende Punkte klar aufgeführt? 1. Verantwortlichkeit aller Mitarbeiter zur Sicherstellung von Informationssicherheit 2. Verbindlicher Appell an Mitarbeiter mit Zusicherung der Unterstützung durch Leitung 3. Schaffung einer Verantwortlichkeit für Informationssicherheit bspw. Informationssicherheitsbeauftragter (ISB) – siehe auch Abschnitt 0 4. Einführen von Methoden und Richtlinien zur aktiven Umsetzung von Informationssicherheit 5. Regelmäßige Überprüfung der umgesetzten Maßnahmen auf Wirksamkeit und auf umzusetzende Maßnahmen aufgrund technischer, rechtlicher oder organisatorischer Änderungen 6. Umfassende und regelmäßige Schulungen und Sensibilisierungsmaßnahmen für ALLE Mitarbeiter 7. Ausdehnung der Anforderungen zur Informationssicherheit auf mögliche externe Dienstleister (z.B. durch Einbindung der Leitlinie für Informationssicherheit in den Dienstleistungsvertrag sowie Bekanntmachung relevanter technischer und organisatorischer		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Richtlinien im Anhang, welche den Dienstleister im Rahmen seiner Tätigkeit betreffen werden) Schriftlich festgehalten werden diese Punkte u.a. in der Leitlinie zur Informationssicherheit.		
1.1.5. Verpflichtung zur Umsetzung	Sichert die Behördenleitung die notwendige Unterstützung zur Einführung und Aufrechterhaltung von Informationssicherheit zu in Form von Zeit, Mitteln und Personal? Ist festgeschrieben, dass identifizierte Schwachstellen durch geeignete Maßnahmen beseitigt werden, sofern deren Umsetzung im Rahmen der Abwägung zumutbar ist?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.1.6. Verbesserung	Sichert die Behördenleitung im Rahmen der Verhältnismäßigkeit und Angemessenheit ihre eigene Unterstützung und Teilhabe zur kontinuierlichen Verbesserung der Informationssicherheit klar zu? Ist klar geregelt, dass der Verantwortliche für Informationssicherheit regelmäßig und bei Akutfällen umgehend die Behördenleitung über bestehende Risiken informiert und hierfür ein direktes Vortragsrecht hat? Ist die rechtzeitige Einbindung des Verantwortlichen für Informationssicherheit (oder ISB) in Neuerungen oder Änderungen vorgeschrieben, damit dieser geeignete Maßnahmen zur Sicherstellung der Informationssicherheit entwickeln kann? Ist die Pflicht zur Unterstützung des Verantwortlichen für Informationssicherheit durch Bereichsleiter und Mitarbeiter zugesichert / vorgeschrieben? Sind die Mitarbeiter gehalten, mögliche Verbesserungen aber auch erkannte Schwachstellen an den Verantwortlichen zu kommunizieren?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

1.1.7. Verstöße / Sanktionen	Die Leitlinie (oder Dienstanweisung zur Inkraftsetzung) sollte klare Aussagen dazu treffen, mit welchen Konsequenzen ein Mitarbeiter bei Nichteinhaltung von Maßnahmen zur Informationssicherheit zum Beispiel bei • unberechtigtem Zugriff und Änderung von Daten • unberechtigter Weitergabe von Daten • Missbrauch von Daten • Gefährdung der Informationssicherheit zu rechnen hat. Immerhin wird die Leitlinie zur Informationssicherheit mittels Dienstanweisung herausgegeben, weshalb ein Verstoß zumindest dienstrechtliche Konsequenzen nach sich ziehen kann. Sind mögliche Verstöße und deren Sanktionen in der Leitlinie aufgeführt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
1.1.8. Aktualisierung	Sind Verantwortlichkeit und Intervall für die Überprüfung und Aktualisierung der Leitlinie festgeschrieben?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.1.9. Inkraftsetzung und Unterzeichnung	Ist der Startzeitpunkt für die Leitlinie klar benannt, ab wann diese gültig sein wird (mit Unterzeichnung, ab bestimmten Termin etc.)? Wurde die Leitlinie von der Behördenleitung unterzeichnet?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
1.2. Verantwortlicher für Informationssicherheit / Informationssicherheitsbeauftragter (ISB)	Informationssicherheit ist kein einmaliges Projekt. Es gilt, regelmäßig zu prüfen, ob die aktuellen Schutzmaßnahmen noch wirksam sind oder auf technische, organisatorische oder rechtliche Änderungen reagiert werden muss. Das geht nicht, ohne eine verantwortliche Person zu benennen, die sich dieser Aufgabe regelmäßig widmet. Dabei ist es unerheblich, ob diese Person nun „Verantwortlicher für Informationssicherheit“ oder „Informationssicherheitsbeauftragter“ genannt wird. Deren Aufgabe ist es, sich zu Beginn und in Zukunft um die Belange der Informationssicherheit in Ihrer Organisation zu kümmern. Der Zeitaufwand dieser Person ist unter anderem abhängig von der Organisationsgröße, aber auch von weiteren Faktoren wie technischer Ausstattung, Wirksamkeit vorhandener Richtlinien oder dem Schulungsgrad der Mitarbeiter. Pauschale Aussagen hierzu fallen dementsprechend schwer. In einer Einrichtung von 100 Mitarbeitern und mehr hat diese Person zur Aufrechterhaltung der Informationssicherheit durchaus einen Zeitaufwand von 20% Vollzeit oder mehr. In kleineren Organisationen fällt die Belastung sicher niedriger aus und vor allem auch nicht kontinuierlich an. Hier kann es ausreichen, wenn eine Person auf aktuelle Änderungen bei Bedarf reagiert, ansonsten in einem Turnus von drei Monaten einen oder mehrere Tage für Informationssicherheit investiert. Eine Faustformel gibt es hierzu leider nicht. Eine Rechtsvorschrift zur Bestellung / Benennung einer solchen Funktion gibt es – im Gegensatz zum Datenschutzbeauftragten – nicht. Sollte Ihre Organisation		Dokumente / Anlagen: Muster Stellenbeschreibung und Bestellung ISB

	jedoch entscheiden, hierfür weder personelle noch zeitliche und monetäre Mittel bereitzustellen, dann fangen Sie mit dem Thema Informationssicherheit am besten erst gar nicht an. Alles, was Sie jetzt einmalig an Zeit und Geld investieren, ist verloren, sofern keine kontinuierliche Betreuung durch einen Verantwortlichen erfolgt. Alle Anforderungen an eine solche Funktion sind aus Normvorschriften wie der ISO 27001, dem BSI IT-Grundschutz oder ISIS12 entnommen, da sich diese in der Praxis bewährt haben.		
1.2.1. Bestellung	Wurde eine verantwortliche Person für Informationssicherheit benannt oder ein ISB bestellt? Liegt hierzu eine entsprechende schriftliche Bestellung / Benennung vor? Sind die Aufgaben, Rechte und Pflichten klar benannt (Stellenbeschreibung)?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.2.2. Interessenskonflikte	Eine Vermeidung von Interessenskonflikten ist anzustreben. Somit sind wegen möglicher Interessenskonflikte • Leitungsebene • Datenschutzbeauftragter • IT-Leitung (jedoch immer noch besser als gar keine Verantwortlichkeit) • IT-Mitarbeiter • Auszubildende und Praktikanten nicht optimal. Generell bleibt jedoch festzuhalten, lieber ein aktiver Verantwortlicher mit Interessenskonflikten als kein oder nur pro forma benannter Verantwortlicher! Sind die Voraussetzungen zur Vermeidung von Interessenskonflikten gegeben?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
1.2.3. Stellung	Generell sollte die verantwortliche Person in dieser Funktion direkt der Behördenleitung unterstellt sein, bzw. ein direktes Vortragsrecht haben. Idealerweise wird diese Funktion als Stabsstelle eingeführt. Die Vorteile liegen auf der Hand • Direkte Berichterstattung • Kurze Wege • Betonung des Themas Informationssicherheit innerhalb der Organisation		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Ist der Verantwortliche für Informationssicherheit / Informationssicherheitsbeauftragte in dieser Funktion direkt der Behördenleitung unterstellt?		
1.2.4. Beratend / Weisungsbefugt	Da es keine Rechtsgrundlagen zu Bestellung und Aufgaben eines ISB / Verantwortlichen für Informationssicherheit gibt, stehen mehrere Wege der Umsetzung zur Verfügung. Die Funktion kann – analog zum Datenschutzbeauftragten – lediglich beratend eingesetzt werden. Alternativ kann die Funktion mit Weisungsbefugnissen ausgestattet werden. Darf der Verantwortliche den sprichwörtlichen „Stecker ziehen“, wenn ein klar ersichtliches Risiko besteht oder nicht? Die Befugnisse können z.B. auf hohe Risiken (monetär, rechtlich, Image) beschränkt werden. Wie ist die notwendige Unterstützung der Funktion durch Behördenleitung, Sachbereichsleiter und Mitarbeiter geregelt? Die Ausgestaltung sollte auf jeden Fall zusammen mit der Gestaltung der Leitlinie (1.1) erfolgen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.2.5. Ressourcen (Zeit und Mittel)	Der Informationssicherheitsbeauftragte / Verantwortliche benötigt ausreichend Zeit und Ressourcen für seine Arbeit. Diese sind durch die Organisation zur Verfügung zu stellen / sicherzustellen. Mittel / Zeit für – Ausübung der Tätigkeit generell – Grundausbildung – regelmäßige Weiterbildung – Reisekosten – Softwarelösungen – Literatur – Awareness-Maßnahmen – uvm. Die Zusicherung der Zeit und Mittel sollte erfolgen in der – Bestellung – Stellenbeschreibung – Leitlinie Informationssicherheit Ist dies erfolgt? Unabhängig von der Organisationsgröße werden Sie jemanden benötigen, der Informationssicherheit aktiv betreut, begleitet und auch weiterentwickelt. Das geht nicht ohne entsprechende Ressourcen. Klar ist, nicht jede Orga-		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	nisation benötigt dafür eine Vollzeitstelle. Bedenken Sie jedoch: Bei Teilzeitausübung der Tätigkeit ist die Person nicht stets im Thema (Aktualitätsproblem), oftmals sind andere Themen stets wichtiger (Prioritätenproblem). Idee: Suchen Sie eine gemeinsame Lösung mit umliegenden oder vergleichbaren Kommunen im Rahmen der interkommunalen Zusammenarbeit (IKZ).		
--	---	--	--

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.2.6. Ausbildung / Kompetenzen / Nachweise	Notwendige Qualifikationen zur Ausübung dieser Funktion: Kompetenzen und Nachweise zu • Informationssicherheit (Schulung / Ausbildung z.B. Informationssicherheitsbeauftragter BVS) • IT-Kenntnisse, zumindest IT-Affinität • Projektmanagement • Organisatorische Zusammenhänge (BWL, Verwaltungsfachwirt etc.) Persönliche Qualifikationen • Blick über den Tellerrand, für die ganze Organisation interdisziplinäres Denken • Kommunikationsfähigkeit und soziale Kompetenz (Teampayer, Coach und Motivator) • Analytische Fähigkeiten • Führungskompetenz • Diplomatisches Geschick • Prozessorientiertes Denken Bringt der Kandidat für diese Funktion oder die bereits aktive Person diese Qualifikationen mit?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

1.3. Team für Informationssicherheit	Es bietet sich stets die Einberufung eines Teams für Informationssicherheit an. Die Teilnehmer treffen sich bei Bedarf sowie in regelmäßigen Abständen zur Bewertung des Status Quo der Informationssicherheit, zur gemeinsamen Identifikation möglicher Schwachstellen sowie Entwicklung geeigneter Maßnahmen zu deren Beseitigung, zur Abstimmung technischer, organisatorischer und rechtlicher Entwicklungen und zur strategischen Weiterentwicklung des Themas. Aufgrund der Zugehörigkeit zu verschiedenen Sachbereichen ist sichergestellt, keine relevanten Sicherheitsthemen in der Organisation zu übersehen und notwendige Maßnahmen nicht zu treffen. Alleine schon aufgrund des notwendigen Blicks über den Tellerrand ist es wenig sinnvoll, relevante Funktionen wie IT-Leitung (oder Administration), Datenschutzbeauftragten und Informationssicherheitsbeauftragten auf einer Person zu vereinen. In Ausnahmen mag das akzeptabel sein, aber nicht als Dauerzustand. Idealerweise wird das Team aus folgenden Funktionen gebildet: • Informationssicherheitsbeauftragter / Verantwortlicher (festes Mitglied) • IT-Leiter (festes Mitglied) • Datenschutzbeauftragter (festes Mitglied) • Personalvertretung (Teilnahme bei Bedarf) • Behördenleitung (Teilnahme bei Bedarf) • Eventuell externer Berater (fest oder nach Bedarf)		Dokumente / Anlagen: keine
1.3.1. Team	Ist die Bildung eines solchen Teams in Ihrer Organisationsgröße sinnvoll? Existieren die o.g. Funktionen in Ihrer Einrichtung? Wurde ein entsprechendes Team gebildet und sind dessen Aufgaben klar beschrieben?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.4. Mitarbeiter Schulung / Sensibilisierung	Informationssicherheit ist kein Thema für Einzelkämpfer, genauso wenig wie ein reines IT-Thema. Erfolgreiche und wirksame Informationssicherheit benötigt die Mitarbeit und Unterstützung aller Mitarbeiter innerhalb der Organisation. Umso wichtiger ist es, die Mitarbeiter frühzeitig einzubinden, für das Thema zu begeistern und dazu zu motivieren, aktiv mitzuarbeiten und mitzugestalten. Dies ist kein einmaliger Vorgang, sondern Sie müssen Ihre Mitarbeiter „bei der Stange halten“. Dabei können Sie verschiedene Wege und Kanäle zur Kommunikation nutzen, es muss nicht immer der Vortrag vor versammelter Mannschaft sein. Wichtig: Informieren, schulen und sensibilisieren Sie zielgruppengerecht. Für das Kernteam sowie den IT-Bereich empfehlen sich Workshops zu Beginn zur Vorstellung und Einführung des Themas Informationssicherheit sowie der Vorgehensweise nach dieser Konzeption. Die Behördenleitung belasten Sie zu Beginn weniger mit Details, sondern stellen sinnvoll die Ziele der Informationssicherheit sowie in groben Zügen die vorliegende Sicherheitskonzeption vor, mittels der Sie das Thema umsetzen wollen. Sachbereichsleiter holen Sie mit Zusatzinformationen ins Boot, wo und wie deren Unterstützung im Ablauf der Konzeptbearbeitung notwendig sein wird. Und den Mitarbeitern machen Sie zu Beginn klar (beispielsweise am Thema „Kryptotrojaner und deren Auswirkungen“), warum Informationssicherheit kein IT-Thema ist, sondern jeder Einzelne zur Informationssicherheit an seinem Arbeitsplatz beitragen kann und muss. Im weiteren Verlauf informieren Sie über den jeweiligen Projektstatus (kurze Erfolgs-/Zwischenberichte) und natürlich auch über aktuelle Bedrohungen und Risiken. Nutzen Sie dazu die jeweils geeigneten Kommunikationskanäle. Weitere Informationen zu Schulung und Sensibilisierung entnehmen Sie bitte Kapitel 8 dieses Konzepts.		Dokumente / Anlagen: keine

1.4.1. Erstinformation	Wurde eine Erstinformation mit allen Beteiligten zielgruppengerecht durchgeführt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
1.4.2. Fahrplan	Steht der weitere Fahrplan zur Kommunikation über das Projekt sowie weitere mögliche Schulungen und Sensibilisierungen fest? Sind Termine (Datum) / Ereignisse (bspw. bei Abschluss jeder Einzelphase) hierfür fest vorgesehen und geplant?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.4.3. Auswahl Kommunikationskanäle	Haben Sie sich Gedanken über die geeigneten Kommunikationskanäle gemacht und diese je nach Inhalt der Kommunikation passend ausgewählt? Mögliche Kanäle • Schulung • Kurzvortrag Personalversammlung • Online-Schulung • Rundmail • Aushänge • Intranet • Kurzvideos • Beitrag Mitarbeiterzeitung • Plakate • Flyer Jeder Kanal hat seine Vor- und Nachteile. Eine Schulung bietet sich an für eine tiefergehende Vorstellung oder die Vermittlung von Inhalten. Rundmail ist wiederum (der kurzen Aufmerksamkeitsdauer des Mediums geschuldet) meist nur für Warnungen vor aktuellen Bedrohungen geeignet. Ist ihr schwarzes Brett verwaist und der letzte Aushang darauf schon zwei Jahre alt? Dann sollte das kein Kanal Ihrer bevorzugten Wahl sein. Wurden mögliche Kommunikationskanäle ge-		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	prüft und eine entsprechende Strategie zur Kommunikation im Rahmen der Informationssicherheit (einmalig bei Einführung und wiederholend für die Zukunft) festgelegt? Sind die Verantwortlichkeiten für die Kommunikation festgelegt?		
1.5. Klassifizierung von Daten	Datenverluste sind oft nur einen Mausklick oder einige Sekunden des Nicht-Schredderns entfernt. Umso wichtiger ist es, Mitarbeitern Informationen zum Schutzbedarf und zur Verwendung von Daten mitzugeben, die jederzeit ersichtlich sind.		Dokumente / Anlagen: Muster Klassifizierung
1.5.1. Schema zur Klassifizierung	Gibt es ein gültiges organisationsweites Schema zur Klassifizierung von Daten (beispielsweise „frei verfügbar“, „nur zum internen Gebrauch“, „vertraulich“, „streng vertraulich“)? Ist dieses Schema durchgehend in den Metadaten von Dokumenten und bei Datensätzen umgesetzt und die Klassifizierung ersichtlich (beispielsweise Angabe in Fußzeile eines Dokuments, schriftliche Einstufung von Daten innerhalb eines Verfahrens etc.)?		
1.5.2. Umgang mit klassifizierten Daten	Sind organisationsweite Regelungen umgesetzt und den Mitarbeitern bekannt, wie mit Daten in der jeweiligen Klassifizierung umzugehen ist?		

Abschlusskommentar zu Kapitel 1 Informationssicherheit

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 1 Informationssicherheit

BSI M 2.192 – Maßnahme „Erstellung einer Leitlinie zur Informationssicherheit“

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02192.html

BSI Webkurs IT-Grundschutz 2.5 „Sicherheitsleitlinie“

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Sicherheitsmanagement/Sicherheitsleitlinie/sicherheitsleitlinie_node.html;jsessionid=0140138633FB567D57B8E0219AAD3F63.2_cid368

Leitlinie IT-Planungsrat

http://www.it-planungsrat.de/DE/Projekte/Steuerungsprojekte/InfoSic/InfoSic_node.html

Weitere Möglichkeit

Handreichung ISIS12 für Kommunen. Für öffentliche Stellen kostenfrei als PDF zu bestellen unter

<https://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12/isis12-fuer-kommunen.html>

Leitlinie Sächsische Staatsregierung (Seite 3-7 im PDF), leicht anpassbar

http://www.sachsen-gesetze.de/shop/saechsabl/2011/38/read_pdf

Dokumente / Anlagen

Muster Stellenbeschreibung und Bestellung Informationssicherheitsbeauftragter

Muster Klassifizierung von Daten

Kapitel 2 Datenschutz (optional im Sinne des Art. 8 BayEGovG)

Datenschutz kümmert sich von Gesetz wegen lediglich um personenbezogene Daten. Als Untermenge der Informationssicherheit kommt diesem Punkt jedoch eine nicht unerhebliche Bedeutung zu. Dabei spielen sowohl der technische als auch der organisatorische Datenschutz eine wichtige Rolle. Dessen Schutzmaßnahmen streuen weit über den Schutz personenbezogener Daten hinaus.

Maßnahmen, die ein Datenschutzbeauftragter vornimmt, sind zwar im Sinne des Artikel 8 BayEGovG nicht zwingend vorgeschrieben, jedoch aus den Anforderungen des BayDSG (1993) rechtlich verbindlich.

Bitte beachten Sie: Zu allen Fragen rund um den behördlichen Datenschutz ist die Webseite vom Bayerischen Landesbeauftragten für Datenschutz eine gute Anlaufstelle.

Mit der EU-Datenschutz-Grundverordnung und der noch zu erfolgenden Formulierung der nationalen Öffnungsklauseln stehen in diesem Bereich einige Änderungen an. Diese sollten Sie bei der ganzen Aufgabenflut rund um die Einführung eines Informationssicherheitskonzepts nicht aus den Augen verlieren. Denn beide Themen sind zeitnah umzusetzen (Januar und Mai 2018).

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
2. Datenschutz	Betrachten wir den nicht unerheblichen Anteil (> 50%) des Fehlverhaltens von Mitarbeitern als Ursache für Datenpannen, so wird schnell klar, warum der Gesetzgeber Schulungen und Sensibilisierungen in Verbindung mit Richtlinien und Dienstanweisungen im Datenschutzrecht zwingend vorschreibt. Doch auch Prozesse innerhalb der Organisation beispielsweise bei der Einstellung von neuen Mitarbeitern oder Positionswechseln beeinflussen maßgeblich die Informationssicherheit. Sind hier keine nachvollziehbar dokumentierten Arbeitsabläufe (möglichst formularisiert) vorhanden, so führt das schnell zu unzulässigen Zugriffen auf Daten – woher soll die IT denn beispielsweise wissen, welche Zugriffsrechte der Mitarbeiter haben soll? Gesetzlich vorgeschriebene Dokumentationen im Datenschutz wie beispielsweise das Führen eines Verfahrensverzeichnisses unterstützen im Rahmen der Informationssicherheit bei der Analyse und Bewertung kritischer Verfahren und Applikationen im Haus. Diesen muss besonderes Augenmerk geschenkt werden, nicht nur im Rahmen eines funktionierenden Notfallmanagements.		

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
2.1. Beschäftigte / Mitarbeiter	Ein nicht unerhebliches Risiko für Datensicherheit und Datenschutz geht – bewusst oder unbewusst – von den eigenen Mitarbeitern aus. Neben der Entwicklung und Bekanntmachung von Richtlinien und Anweisungen sind daher weitere Maßnahmen zur Sensibilisierung und Umsetzung rechtlicher Anforderungen notwendig.		Dokumente /Anlagen: • Musterprozess Einstellen / Aus-scheiden • Anforderung IT Arbeitsplatz
2.1.1. Schulungen Datenschutz und Datensicherheit	Werden Mitarbeiter bei der Einstellung im Rahmen einer Präsenzveranstaltung oder eines Online-Trainings (möglichst mit Zertifikat) auf die Themen Datenschutz und Datensicherheit sensibilisiert? Wie werden die Mitarbeiter sensibilisiert, wenn nicht im Rahmen des zuvor genannten Online-Trainings? Finden regelmäßig, spätestens alle zwei Jahre, besser häufiger, Auffrischungen statt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
2.1.2. Prozess Einstellen / Wechsel / Aus-scheiden von Mitarbeitern	Existiert ein nachvollziehbarer Prozess für alle Beteiligten (Personal, IT, Verwaltung etc.) für neue, wechselnde und ausscheidende Mitarbeiter? Sind darin auch enthalten - Anforderung IT-Arbeitsplatz? - Zugriffsberechtigungen (Einrichtungen / Entzug)? - Ausgabe / Rücknahme von IT-Equipment? - Sicherheitsunterweisung?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	- Schulung Datenschutz und Datensicherheit? - Verpflichtungen? Ist der Datenschutzbeauftragte in die Entwicklung und Pflege dieses Prozesses aktiv involviert?		
2.2. Datenschutzbeauftragter	Ein aktiver Datenschutzbeauftragter ist ein wichtiger Beitrag zur Datensicherheit, nicht nur zum Datenschutz. Seine Maßnahmen beschränken sich in der Praxis nicht auf personenbezogene Daten, sondern beinhalten jedwede Art von schützenswerter Information.		Dokumente / Anlagen: • Stellenbeschreibung DSB • Bestellurkunde DSB
2.2.1. Bestellpflicht	Öffentliche Stellen sind verpflichtet, einen Datenschutzbeauftragten (DSB) zu bestellen (siehe auch Artikel 25 BayDSG). Mehrere öffentliche Stellen können sich einen DSB teilen, sofern er seinen Aufgaben als DSB nach wie vor im ausreichenden Maß nachkommen kann (Art. 25 Absatz 2 Satz 2 BayDSG). Dies wird bereits in der Praxis erfolgreich praktiziert. Tipp: Sprechen Sie mit Ihrem Landratsamt oder den umliegenden Gemeinden! Wurde ein Datenschutzbeauftragter bestellt? Ist dieser auch wirklich aktiv? (Seien Sie ehrlich!)		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
2.2.2. Bestellkunde	Wurde der Datenschutzbeauftragte korrekt schriftlich bestellt und seine Aufgaben klar definiert (z.B. Stellenbeschreibung)?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
2.2.3. Fachkunde	Hat der (zu bestellende) DSB ausreichend Fachkunde als Voraussetzung für die Tätigkeit als DSB? Die Fachkunde muss vor der Bestellung vorliegen. Hinweis: Bei der Auswahl der Qualifizierungskurse ist darauf zu achten, dass Crash-Kurse oft nicht das notwendige Grundwissen für die Ausübung dieser Tätigkeit vermitteln. Empfohlen sind mindestens drei Tage, besser fünf Tage.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
2.2.4. Ressourcen	Dem DSB müssen ausreichend zeitliche, finanzielle und räumliche Ressourcen zur Verfügung stehen. Ist dies (gerade in Anbetracht einer Bestellung zusätzlich zum eigentlichen Aufgabenbereich) gewährleistet? (Siehe auch Wilde / Ehmann / Niese / Knoblauch: Kommentar BayDSG, Art. 25 BayDSG Absatz 3 Satz 5 „Freistellung“)		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
2.2.5. Vermeidung einer Pro-forma-Bestellung	Sind die Grundlagen zur Vermeidung einer Pro-forma-Bestellung geschaffen und ist Ihr		☐ Erfüllt ☐ Nicht erfüllt

	Datenschutzbeauftragter aktiv tätig (eigeninitiativ)?		☐ Nicht anwendbar ☐ Aktuell in Arbeit
2.2.6. Interessenkonflikte	Ist der Datenschutzbeauftragte frei von Interessenkonflikten zu seinen anderen Tätigkeiten? Bei Mitarbeitern im Bereich IT, Personal, Marketing, Behördenleitung, Bereichsleitung kann in der Regel ein Interessenkonflikt angenommen werden. Diese Positionen sind für eine Bestellung daher nicht ideal.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
2.2.7. Reporting / Unterstützung	Hat der DSB ein exklusives Vortragsrecht an den Geschäfts-/Behördenleiter? (vgl. auch Wilde / Ehmann / Niese / Knoblauch: Kommentar BayDSG, Art. 25 BayDSG Absatz 3 „Unmittelbare Zuordnung zur Behördenleitung“) Erhält er von diesen die notwendige Rücken- deckung für seine Tätigkeit und die Umset- zung notwendiger Maßnahmen?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
2.2.8. Einbeziehung	Wird der DSB rechtzeitig von den Fachbereichen einbezogen, z.B. bei Änderung bestehender Verfahren oder Einführung neuer Verfahren? Hier besteht eine Bringschuld gegenüber dem DSB.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
2.2.9. Das datenschutzrechtliche Freigabeverfahren	Sowohl der erstmalige Einsatz als auch wesentliche Änderungen von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedürfen grundsätzlich gem. Art. 26 BayDSG der vorherigen schriftlichen Freigabe durch den behördlichen Datenschutzbeauftragten der das Verfahren einsetzenden öffentlichen Stelle. Die Freigabe des Verfahrens ist rechtzeitig vor dem Einsatz beim Datenschutzbeauftragten zu beantragen (siehe auch Wilde / Ehmann / Niese / Knoblauch: Kommentar BayDSG, Art. 26 BayDSG). Ist diese Vorgehensweise als fester Bestandteil der Arbeitsabläufe implementiert? AKDB-Verfahren werden gemäß Art. 26 Absatz 1 Satz 2 BayDSG als bereits freigegeben betrachtet. Hinweis: Aufgrund der ab Mai 2018 wirksamen Datenschutz-Grundverordnung und den natio-		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	nalen Umsetzungsgesetzen wird es hier zu Änderungen kommen!		
2.3. Verfahrensverzeichnis	Unsere Datenschutzgesetze (speziell Artikel 27 BayDSG für öffentliche Stellen im Freistaat Bayern) verpflichten jede Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt, zum Führen eines sogenannten Verfahrensverzeichnisses. Dieses muss auf Verlangen des Bayerischen Landesbeauftragten für den Datenschutz jederzeit vorgelegt werden können, kann jedoch auch von jedermann eingesehen werden (Art. 27 Absatz 3 BayDSG). Unterschätzen Sie den Zeitaufwand für dessen Erstellung und Pflege nicht. Wenn die Anforderung kommt, ist es für gewöhnlich zu spät, um das Verzeichnis fristgerecht noch erstellen und vorlegen zu können. Das Verfahrensverzeichnis wird im Rahmen der Datenschutz-Grundverordnung Änderungen erfahren. Bitte behalten Sie dies entsprechend im Auge (im Laufe des Jahres 2017 werden voraussichtlich konkrete und belastbare Handlungsanweisungen der Schutzbehörden vorliegen).		
	Dokumente / Anlagen: • Vorlage Tabelle Verfahrensverzeichnis • Formular Meldung neue / geänderte Verfahren an DSB		

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
2.3.1. „Verfahrensverzeichnis für jedermann“	Existiert eine grobe Übersicht der Aufgabenbeschreibung und betroffenen personenbezogenen Daten samt Kreis der Betroffenen? (Aufbau und Struktur siehe Art. 26 Absatz 2 BayDSG) Für gewöhnlich ist dies recht schnell und einfach zu erstellen. Auf Verlangen ist diese jedermann zur Verfügung zu stellen. Achtung: Detailgrad (gerade der Schutzmaßnahmen) darf kein Sicherheitsrisiko darstellen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
2.3.2. Detailliertes Verfahrensverzeichnis	Wurde eine umfangreiche Übersicht über ALLE IT-gestützten Verfahren, mit denen personenbezogene Daten verarbeitet werden und die dem Freigabeverfahren unterliegen, erstellt? Diese Übersicht enthält neben der Beschreibung der Verfahren detaillierte Angaben wie zum Beispiel - eingesetzter Hard- und Software, - Berechtigungskonzepte, - Schutzmaßnahmen, - Angaben zu den verarbeiteten Daten, - verantwortliche Mitarbeiter, - Löschfristen, - Angaben zu involvierten externen Dienstleistern, - Inkrafttreten des Verfahrens, - Nachweis der Aktualitätsprüfung.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

2.3.3. Zuständigkeiten	Die Datenschutzgesetze sehen vor, diese Verzeichnisse durch den DSB führen zu lassen. Die Meldung von Verfahren, das Einliefern aller relevanten Informationen sowie deren regelmäßige Aktualisierung obliegen jedoch den Fachbereichen als verantwortliche Stelle unter Einbeziehung des IT-Bereichs / -Verantwortlichen. Wurden zur Meldung neuer oder geänderter Verfahren entsprechende Meldeprozesse in der Organisation eingeführt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
-------------------------------	---	--	--

Abschlusskommentar zu Kapitel 2 Datenschutz:

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 2 Datenschutz

Verfahrensverzeichnis und Detailübersichten

Vorlage Beschreibung Einzelverfahren im Detail, Bayerischer Landesbeauftragter für den Datenschutz

<https://www.datenschutz-bayern.de/download/verfbes.pdf>

BSI Grundsatzkatalog M 2.508 „Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten“

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02508.html

Datenschutzbeauftragter / Freigabeverfahren

Orientierungshilfe „Der behördliche Datenschutzbeauftragte“ inklusive Musterformular einer Bestellurkunde (Schriftform ist erforderlich), Bayerischer Landesbeauftragter für den Datenschutz

<https://www.datenschutz-bayern.de/technik/orient/behDSB.htm>

Musterablaufplan für das datenschutzrechtliche Freigabeverfahren, Bayerischer Landesbeauftragter für den Datenschutz

https://www.datenschutz-bayern.de/verwaltung/20081009_freigabe-musterablaufplan.pdf

Mitarbeiterdatenschutz

Fragen und Antworten zum Personalwesen im öffentlichen Bereich, Bayerischer Landesbeauftragter für den Datenschutz

<https://www.datenschutz-bayern.de/nav/0609.html>

Verpflichtung auf das Datengeheimnis Art. 5 BayDSG, Bayerischer Landesbeauftragter für den Datenschutz

<https://www.datenschutz-bayern.de/faq/FAQ-technik-to/FAQ-datengeheimnis.html>

Kommentar zum BayDSG

www.rehmnetz.de/shop/Verwaltungsrecht/Bayerisches-Datenschutzgesetz-Loseblattwerk-zzgl-Aktualisierungslieferungen.html

Dokumente / Anlagen

Musterprozess Einstellen / Ausscheiden

Anforderung IT Arbeitsplatz

Stellenbeschreibung DSB

Bestellurkunde DSB

Vorlage Tabelle Verfahrensverzeichnis

Formular Meldung neue / geänderte Verfahren an DSB

Kapitel 3 Gebäudesicherheit

Gebäudesicherheit im kommunalen Bereich ist kein leichtes Thema. Aufgrund der Zutrittsmöglichkeiten für Bürger zu Bürgerbüro, Zulassungsstelle und den verschiedenen Ämtern ist eine Abschottung über die Außenhaut – zumindest während der Öffnungszeiten – nur schwer machbar. Umso wichtiger ist, diesen Punkt ausführlich zu betrachten. Der Zugang zum Bürgerbüro ist in der Regel frei zugänglich zu halten. Doch wie verhält es sich mit Nebeneingängen oder auch Zugängen aus Garagen mit Mitarbeiterparkplätzen? Stehen die Türen dort frei offen (der berühmte „Raucherkeil“) oder sind diese verschlossen und von außen nur mit Knauf zu öffnen? Bieten diese Türen Zugang zu internen Verwaltungsbereichen mit schützenswerten Informationen oder sind diese Zugänge Teil Ihres Sicherheitskonzepts und werden regelmäßig auf ihre Schutzwirkung hin überprüft?

Eine sinnvolle Auf- und Verteilung der Räumlichkeiten kann maßgeblich die Sicherheit in Ihrer Organisation erhöhen. Das kann je nach örtlichen Begebenheiten ganz pragmatisch sein. Eine dicke Kordel am Treppenaufgang zum ersten Stock, in dem sich vielleicht keine Ämter mit Publikumsverkehr befinden, signalisiert ganz klar „Bis hier und nicht weiter“. Es muss nicht immer die große Lösung mit Umbaumaßnahmen sein.

Die Maßnahmen aus diesem Kapitel können schnell kostenintensiv werden - in Zeiten knapper Budgets nicht immer sehr angenehm. Daher sollten Sie bei den zu treffenden Schutzmaßnahmen stets prüfen, ob es Alternativen gibt, die möglicherweise einen vergleichbaren Schutzwert liefern, aber keine Unsummen verschlingen. Fehlt eine Brand- oder Wassermeldeanlage im Serverraum, so kann man sich kurzfristig auch mit vernetzten Funkmeldern und einer Meldestrecke behelfen. Ziel ist schließlich, rechtzeitig von einem eingetretenen Notfall wie Feuer oder Wasser Kenntnis zu erlangen. Mit der Alternativlösung haben Sie dies zumindest für die üblichen Öffnungszeiten sichergestellt. Als langfristige Maßnahme wäre dann die Meldeanlage anzustreben. Generell sollten Sie bei der Planung von Schutzmaßnahmen den Nutzen gegen das Risiko, dessen Eintrittswahrscheinlichkeit, die Kosten und den Aufwand abwägen. Diese Abwägung kann jedoch für gewöhnlich nur zu einer milderer Maßnahme führen, die vielleicht weniger kostenintensiv ist.

Hinweis: optionale Punkte sind gelb hinterlegt.

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
3. Gebäudesicherheit	Art und Beschaffenheit des Gebäudes stellen einen nicht unerheblichen Beitrag zur Sicherheit dar. Das Gebäude ist die äußerste Schutzschicht.		
3.1. Zutritt	Je einfacher sich Zutritt ins Gebäude verschafft werden kann, umso höher das Sicherheitsrisiko. Im kommunalen Bereich nicht einfach durch Abschottung zu lösen. Daher mit besonderem Augenmerk und Pragmatismus zu betrachten.		Dokumente / Anlagen: keine
3.1.1. Zutrittsmöglichkeiten	Welche Zutrittsmöglichkeiten in das Gebäude bestehen? Ist die genaue Lage und Anzahl bekannt? Sind diese Türen stets verschlossen? Welche müssen zwingend für den öffentlichen Zugang zu den Bürozeiten geöffnet sein, z.B. Bürgerbüro? Welche Eingänge sollten verschlossen bleiben, um einen unbefugten Zutritt in Verwaltungsbereiche zu verhindern? Wie sind die Türen gesichert? Schlüssel, Code-Eingabe, Code-Karte, biometrische Systeme? Sind Türen nach Möglichkeit von außen nicht mit Türklinke ausgestattet, sondern mit einem nicht drehbaren Knauf? Existieren weitere zu sichernde Zugänge durch Nebengebäude oder Tiefgarage? Wie		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	sind diese gesichert? Existieren Notausgänge und wie sind diese gegen unbefugtes Öffnen gesichert? Geben diese Ausgänge Alarm, wenn sie betätigt werden?		
--	--	--	--

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
3.1.2. Besucher Empfang / Pforte	Unberechtigte Besucher sollten frühzeitig am tieferen Eindringen in das Gebäude gehindert werden. Existiert ein zentraler Empfang, der Besucher auf den richtigen Weg leitet? Sind Pforte / Empfang durchgehend zu den Öffnungszeiten besetzt? Wie ist sichergestellt, dass Personen nicht in sensible Bereiche wie Verwaltung, IT oder Personalbereich gelangen? Existieren Richtlinien für Mitarbeiter, worauf sie zu achten haben und wie mit auffälligen Personen umzugehen ist? Wenn Pforte / Empfang nicht möglich sind, existieren klare und eindeutige Beschilderungen für den öffentlich zugänglichen Bereich, damit Besucher ohne Umwege den Weg finden? (Denken Sie bitte daran, dieselbe „Sprache“ wie Ihre Besucher zu verwenden. Unter „ZD“ Zentrale Dienste versteht nicht gleich jeder „Personalbereich“ oder „IT“).		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

3.1.3. Schlüsselvergabe und Behandlung bei Verlust	Sind Ausgabe, Rücknahme, Tausch und Ersatz von Schlüsseln, Code-Karten, PINs nachvollziehbar dokumentiert und existieren hierfür feste Verfahrensweisen? Ist den Mitarbeitern diese Verfahrensweise bekannt? Wird deren Einhaltung regelmäßig überprüft? Sind Regelungen klar kommuniziert, was im Falle des Verlusts von Schlüsseln, Code-Karten etc. durch die Mitarbeiter und die ausgebende Stelle zu tun ist?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.1.4. Zusätzliche Schutzmaßnahmen	Sind weitere Maßnahmen, welche die Gebäudesicherheit signifikant erhöhen können, vorhanden: - Bewegungssensoren für Außenbeleuchtung? - Alarmanlage? - Bewegungsmelder? - Glasbruchmelder? - Kontrollgänge, z.B. durch Wachschutz außerhalb der Öffnungszeiten? Denken Sie daran, jede Einzelmaßnahme fügt Ihren technischen und organisatorischen Maßnahmen eine weitere Schutzschicht hinzu und leistet einen aktiven Beitrag zur Informationssicherheit.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
3.2. Sicherheitszonen	Eine interne Einteilung des Gebäudes in Sicherheitszonen unterstützt bei der Risikobewertung und Planung der notwendigen Schutzmaßnahmen. Auch wenn das im aktuellen Betrieb nachträglich nicht einzurichten ist, so sollte das Thema für zukünftige Umbauten / Umzüge / Raumänderungen stets auf Wiedervorlage liegen.		Dokumente / Anlagen: keine
3.2.1. Planung	Ist das Gebäude in verschiedene Sicherheitszonen unterteilt? Z.B. - Bürgerbüro - Verwaltung - IT-Bereich - Archiv Alternativ (wenn auch weniger differenziert): - Zwingend öffentlich zugänglicher Bereich - Teilweise öffentlich zugänglicher Bereich - Interner Bereich ohne öffentlichen Zugang Da Sie in der kommunalen Verwaltung Bereiche mit Zugang für Bürger vorhalten, ist eine durchdachte Raumplanung und Trennung der Schutzbereiche von frei zugänglichen Bereichen umso wichtiger.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

3.2.2. Schutzmaßnahmen Über- tritte	Wie ist sichergestellt, dass Unbefugte nicht aus den öffentlich zugänglichen Bereichen in die internen Bereiche gelangen? Dies können sein: Absperrungen, Gitter, Kordeln (Treppe), Türen (außen Knauf) etc. Sind Ihre Mitarbeiter entsprechend geschult und angewiesen, Personen in üblicherweise nicht für den Publikumsverkehr gedachten Bereichen aktiv anzusprechen, um eine Durchbrechung der Schutzmaßnahmen zu verhindern: „Guten Tag, darf ich Ihnen helfen? Zu wem möchten Sie bitte?“		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.2.3. Signalisation	Sind nicht öffentlich zugängliche Bereiche entsprechend gekennzeichnet und diese Signalisation leicht zu erkennen? (nur sinnvoll, wenn es keine Schutzmechanismen wie verschlossene Tür zwischen öffentlichem und nicht öffentlichem Bereich gibt) Wurde auf eine gesonderte Kennzeichnung sensibler Bereiche bewusst verzichtet? Schilder wie „Serverraum“, „Technikraum“ oder „Zutritt nur für Befugte“ sind eine Einladung.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
3.2.4. Vermeidung	Ist durch die gezielte Anlage der Sicherheitszonen gewährleistet, dass in Bereichen mit höherer Schutzstufe kein oder nur so wenig wie möglich Publikumsverkehr herrscht?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.3. Serverraum	In der heutigen Zeit ist der Serverraum oder der Bereich mit der Netzwerkverteiltertechnik der Bereich, den es besonders zu schützen gilt. Hier gilt, je mehr desto besser. Eine regelmäßige Überprüfung und Anpassung der Schutzmaßnahmen ist Pflicht. Und beachten Sie: Es gibt nicht umsonst Spezialisten für die Planung und Konzeption von Serverräumen (nicht nur in Bezug auf Lage, sondern auch technische Ausstattung, Verkabelung etc.). Auch wenn deren Beauftragung Geld kostet, sollten Sie sich nicht einfach auf Aussagen von Architekten oder „Baufachleuten“ verlassen. Nachträgliche Anpassungen oder Umbauten kosten ein Vielfaches dessen, was der Profi zu Beginn der Planungsphase gekostet hätte. Es hilft auch überhaupt nichts, im Anschluss an eine unzureichende Baudurchführung auf einen anderen Verantwortlichen zeigen zu können. Der Aufwand zur Beseitigung der Mängel kostet Geld und Zeit – in dieser Zeit trägt die Kommune weitere unnötige Sicherheitsrisiken mit sich herum.		Dokumente / Anlagen: keine
3.3.1. Lage	Liegt der Serverraum geschützt im Inneren des Gebäudes? Verfügt er über möglichst nur eine Zugangstür? Generell sollten keine Fenster vorhanden sein,		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	auch nicht ins Gebäudeinnere		
3.3.2. Fenster	Sofern doch Fenster vorhanden sind, wie sind diese gesichert? - Bruchfestes Glas - Sicherheitsglas - Fenstergitter - Glasbruchmelder		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.3.3. Türen	Sind Türen mit ausreichend hoher Schutzklasse verbaut (Metall, Zargen, Sicherheitsschlösser, Aushebelschutz etc.)? Sind diese mit separaten Schlüsseln oder Kreisen innerhalb des Schließsystems zu öffnen?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.3.4. Alarmierung	Sind für alle relevanten Vorfälle Alarmierungen eingerichtet? - Glasbruch - Tür steht zu lange offen oder nicht abgeschlossen - Bewegungsmelder - Videoüberwachung im Innenbereich		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
3.3.5. Schutz vor Feuer / Wasser	Liegt der Serverraum in einem eigenen Brandabschnittsbereich? Sind brandschutztechnische Belange berücksichtigt? Schwer brennbare Bodenbeläge, Vermeidung von Brandbrücken durch Kabelschächte, keine zusätzliche Nutzung als Lager (Papier, Putzmittel etc.) oder Archiv Sind Brand- und Wassermelder installiert und wird deren Funktion regelmäßig geprüft? (Im Zweifel sind bereits im Handel erhältliche Melder ohne Anschluss an eine Hausmeldeanlage eine gute Lösung.) Führen keine Wasserzu- und -ableitungen durch den Serverraum? Ist der Serverraum nicht unter wasserführenden Räumen wie Küche / Sanitär im Stockwerk darüber eingerichtet? Ist es möglich, den Serverraum nicht im Keller als wassersammelnden, tiefsten Punkt zu betreiben? Denken Sie pragmatisch. Es ist unverhältnismäßig, aufgrund wasserführender Leitungen den Serverraum in einen anderen Gebäudeteil		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	zu verlagern. Wassermelder aus dem Fachhandel können für weniger Geld ein ebenso guter Schutz sein. Mit Augenmaß betrachten.		
3.3.6. Verschlussache	Ist sichergestellt, dass diese Elemente stets verschlossen sind und nur ein beschränkter Mitarbeiterkreis Zugang hat? - Netzwerkverteiler (auch im Gebäude) - Serverschränke - Patch-Schränke		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.3.7. Serverraum ist IT-Raum, kein Abstellplatz	Ein Serverraum beherbergt ausschließlich IT- und TK-Komponenten wie Serverschränke, Serverhardware, TK / Kommunikationselemente, Patch-Felder, USV, Klimageräte etc. Ist sichergestellt, dass der Serverraum nicht als Lager für Papier, Toner, Kartonagen oder andere Brandbeschleuniger dient und auch nicht die Garage für die Putzwagen der Reinigungskolonie ist?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
3.4. Registratur/Schriftgutlager (nicht Archiv im Sinne des Archivgesetzes)			Dokumente / Anlagen: Keine
3.4.1. Lage	Ist der Archivraum an einem Ort im Gebäude untergebracht, der die Risiken durch Wasser und Brand minimiert? Also möglichst weder Keller noch Dachstuhl. Wurde darauf geachtet, dass weder im Archivraum noch darüber wasserführende Leitungen verlaufen? Sofern sich wasserführende Leitungen nicht vermeiden lassen: • Keine Lagerung direkt auf dem Boden oder in Bodennähe (Regale zum Beispiel aufgebockt)? • Wassermelder installiert? • Möglichkeit des Wasserablaufs vorhanden?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.4.2. Verschluss	Ist der Archivraum ausreichend gegen unbefugtes Betreten gesichert? • Tür stets verschlossen • Öffnen nur mit wenigen Schlüsseln, spezieller Code-Karte • Keine Fremdnutzung (Lager, Kopierer etc.)		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.4.3. Dimension	Wurde der Archivraum ausreichend groß konzipiert / geplant, um dem Umfang an Doku-		☐ Erfüllt ☐ Nicht erfüllt

	menten und Datenträgern im Rahmen der gesetzlichen Aufbewahrungsfristen über die Jahre hinweg gerecht zu werden?		☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.4.4. Ausstattung	Auch innerhalb des Archivs dürfen nur jeweils Berechtigte auf die unterschiedlichen Informationen zugreifen. So müssen z.B. Personaldaten getrennt und geschützt von anderen Informationen gelagert werden. Sind für die unterschiedlichen Daten entsprechende Schutzschränke / Lagervorrichtungen vorgesehen? • Getrennt voneinander? • Stabil? (Stahlschrank) • Feuerfestigkeit für wichtige Unterlagen? • Datenschutztresor (S60/S120DIS) für Datenträger, Medien, Lizenzen etc.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.4.5. Melde-/Warnsysteme	Sind Meldevorrichtungen installiert und funktionsfähig und werden regelmäßig getestet für • Brand, Feuer, Rauch • Wasser • Luftfeuchtigkeit (denken Sie an Papierunterlagen in feuchter Umgebung) • Unberechtigtes Betreten (Bewegungsmelder, Videoüberwachung, Alarmanlage)		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
3.5. Lieferanten/ Externe Dienstleister	Der unregelmäßige Zutritt durch Lieferanten und externe Dienstleister stellt eine Bedrohung für die Sicherheit dar.		Dokumente / Anlagen: keine
3.5.1. Anlieferung / Abholung	Werden die getroffenen Schutzmaßnahmen durch entsprechende organisatorische Regelungen bei Anlieferung und Abholung nicht unterbrochen?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.5.2. Bewegungsfreiheit	Dürfen sich Lieferanten und externe Dienstleister nur unter Aufsicht in den höheren Sicherheitszonen, z.B. nicht-öffentlichen Bereichen, bewegen?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
3.5.3. Identitäts- / Auftragsprüfung	Werden die Identität des Externen und die Richtigkeit des Auftrags vor Zugriff auf Informationen (unabhängig ob elektronisch oder in Papierform) überprüft? Werden Zugriff oder Übergabe protokolliert? Wo werden diese Protokolle aufbewahrt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Abschlusskommentar zu Kapitel 3 Gebäudesicherheit:

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 3 Gebäudesicherheit

Checkliste Zutrittskontrolle Landesamt für Datenschutz Niedersachsen (LfD Niedersachsen)

http://www.lfd.niedersachsen.de/download/60708/Orientierungshilfe_Zutrittskontrolle_LfD_Niedersachsen_.pdf

BSI Grundschutzkatalog M 1 Infrastruktur

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/M1Infrastruktur/m1infrastruktur_node.html

Dokumente / Anlagen

Keine. Relevante Dokumente sind über die Weblinks erreichbar.

Kapitel 4 Zugang IT-Systeme

Ein Kapitel, das sowohl bei Verantwortlichen als auch Anwendern oft Skepsis hervorruft. „*Nicht schon wieder Passwort-Richtlinie!*“ Der Einwand ist verständlich, wurde hier doch viele Jahre nach dem Motto „je mehr, desto besser“ verfahren. Es fällt schwer, Nutzer von IT-Systemen bei diesem Thema auf die Seite der Sicherheit zu ziehen. Umso mehr sind Sie gefragt, hier durch eine ausgewogene Balance an Schutzmaßnahmen sicherzustellen, dass kein Unbefugter Zugang zu den IT-Systemen in Ihrer Organisation erhält. Denn hat sich ein Unbefugter erst einmal Zutritt zu Ihren Räumlichkeiten verschafft, dann sind die Maßnahmen aus diesem Kapitel Ihre letzte Bastion, um Informationssicherheit noch sicherzustellen. Zumindest im Hinblick auf die IT-Systeme.

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
4. Zugang zu IT-Systemen	Hat sich jemand unbefugt Zutritt zu den Räumlichkeiten verschafft, stellen die Schutzmaßnahmen der IT- Systeme eine weitere, oftmals die letzte Hürde dar. Hier kann bereits mit wenigen Maßnahmen ein hohes Maß an Sicherheit gewährleistet werden. Und es besteht auch die Notwendigkeit dazu.		Dokumente / Anlagen: • Anleitung manueller Logout unter Windows-Systemen als Handout für Mitarbeiter
4.1. Passwortsicherheit	Muss ein Nutzer sowohl beim Login an seinem PC-Arbeitsplatz als auch in den einzelnen Verfahren ein sicheres Passwort eingeben? Existieren Richtlinien, wie ein sicheres Passwort auszusehen hat (Mindestlänge, Zusammensetzung, Lebensdauer)? Sind diese Richtlinien allen Mitarbeitern bekannt? Werden diese Richtlinien durchgängig beim Login (Gruppenrichtlinie und in den Verfahren) technisch erzwungen? Sind die Mitarbeiter angewiesen, die Richtlinien eigenverantwortlich einzuhalten, wenn es keinen technischen Zwang innerhalb des Verfahrens gibt? Sind die Mitarbeiter für die Notwendigkeit entsprechend sensibilisiert, z.B. im Rahmen einer Schulung Datenschutz und Datensicherheit?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Beachten Sie: Es ist nicht immer zwingend erforderlich, für jede Anwendung ein separates Passwort zu nutzen. Wenn das aus Sicherheitsgründen so wäre, hätten Techniken wie Single-Sign-On keine Chance (und diese werden vom BSI sogar empfohlen). Auch die Länge eines Passworts kann negativ zum angedachten Schutzzweck wirken. Schreibt sich Ihr Mitarbeiter dieses nämlich auf (der berühmte Zettel unter der Tastatur), ist der Schutz dahin. Nutzen Sie die „<i>Musterdienstanweisung zum Einsatz von Informationstechnologie in Kommunen</i>“ der Innovationsstiftung Bayerische Kommune. Diese enthält weitere Empfehlungen zum Umgang mit Passwörtern.		

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
4.2. Geräteschutz	Sind folgende Maßnahmen an den Arbeitsgeräten ergriffen? - Bootreihenfolge auf Festplatte als erstes Medium eingestellt - Auswahl der Bootreihenfolge beim Systemstart abgeschaltet - BIOS-Passwort gesetzt - Wenn vorhanden, Schutz vor Gehäuseöffnung eingerichtet bzw. Warnmeldung aktiviert - USB-Ports wenn möglich deaktiviert (hierfür gibt es Möglichkeiten via Gruppenrichtlinie, externen Softwaretools oder auch als fertiges Konzept diverser Dienstleister)		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
4.3. Umgang mit sowie Speicherung und Lagerung von Administrations- und Diensteknwörtern	Es existieren personenbezogene Administrations-Accounts zwecks Nachvollziehbarkeit? Der eigentliche Administrations-Account „Admin“ wird nur im Notfall genutzt? Voreingestellte Admin-Passwörter (Auslieferungszustand) werden direkt bei der ersten Nutzung geändert? Alle wichtigen Kennwörter sind in einem besonders geschützten Passwortcontainer abgelegt (mit eingeschränktem Zugriff) und in ausgedruckter Form im Datenschutztresor hinterlegt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Für Dienste sind separate Admin-Accounts eingerichtet, diese laufen nicht auf dem allgemeinen „Admin“ oder auf personenbezogenen Accounts?		
4.4. Erzwungener Login	Ohne Anmeldedaten (Nutzername und Kennwort) ist weder der System-Login noch der Zugriff auf relevante Verfahren möglich? Dies gilt sowohl für den ersten Start des Geräts als auch für das Aufwecken aus dem Ruhezustand oder dem Beenden des Bildschirmschoners!		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
4.5. Manueller Logout	Alle Mitarbeiter sind gehalten, sich bei Verlassen des Arbeitsplatzes (auch für kurze Zeit) manuell vom System abzumelden? Dies wurde schriftlich kommuniziert, sinnvollerweise mit einer Erklärung, z.B. Windows-L auf Windows Geräten? Zusätzlich kann über die IT ein Logout-Icon auf dem Desktop der Anwender eingerichtet werden? Prüfen Sie, ob es sinnvoll ist, die Abmeldung auch aus den Fachverfahren vorzuschreiben bei Abwesenheit von x Minuten. Dies kann jedoch nur ein Rettungsschirm sein, der zusätzlich zum manuellen Logout greift. Die automatisierte Abmeldung ersetzt NIE die Verpflichtung zum manuellen Abmelden.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
4.6. Bildschirmschoner mit Kennwortabfrage	In Kombination mit Punkt 1.5: Als zusätzliche Schutzmaßnahme sollte nach spätestens zehn Minuten der Bildschirmschoner mit Kennwortabfrage automatisch starten. Sofern das manuelle Logout nicht sichergestellt ist, ist die Startzeit des Bildschirmschoners entsprechend zu verkürzen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

4.7. Verschlüsselung / Signaturverfahren	Sind Dateien, Verzeichnisse und Laufwerke mit schutzbedürftigen Daten nach dem aktuellen Stand der Technik verschlüsselt? Sind mobile Datenträger (Sticks) und Geräte (Notebooks, Tablets, Smartphones) in die Verschlüsselung mit einbezogen? Kommen bei elektronischer Übertragung entsprechende Signatur- und Verschlüsselungsverfahren zum Einsatz (gerade bei Kommunikation außerhalb des bayerischen Behördennetzes)? Sind die Mitarbeiter für diese Maßnahmen sensibilisiert? Und wurden die Mitarbeiter im Umgang mit diesen Techniken geschult?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
---	--	--	--

Abschlusskommentar zu Kapitel 4 Zugang IT-Systeme:

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 4 Zugang IT-Systeme

BSI Grundschrutzkatalog M4 Hard- und Software

https://www.bsi.bund.de/DE/Themen/ITGrundschrut/ITGrundschrutKataloge/Inhalt/Massnahmenkataloge/M4HardwareundSoftware/m4hardwareundsoftware_node.html

Speziell

Passwortschrut (M 4.1)

https://www.bsi.bund.de/DE/Themen/ITGrundschrut/ITGrundschrutKataloge/Inhalt_content/m/m04/m04001.html

Bildschirmsperre (M 4.2)

https://www.bsi.bund.de/DE/Themen/ITGrundschrut/ITGrundschrutKataloge/Inhalt_content/m/m04/m04002.html

Änderung voreingestellter Passwörter (M 4.7)

https://www.bsi.bund.de/DE/Themen/ITGrundschrut/ITGrundschrutKataloge/Inhalt_content/m/m04/m04007.html

Zugriffsschrut am Laptop (M 4.27)

https://www.bsi.bund.de/DE/Themen/ITGrundschrut/ITGrundschrutKataloge/Inhalt_content/m/m04/m04027.html

Einsatz Verschlüsselungsprodukte für tragbare IT-Systeme (M 4.29)

https://www.bsi.bund.de/DE/Themen/ITGrundschrut/ITGrundschrutKataloge/Inhalt_content/m/m04/m04029.html

Passwörter aber richtig inkl. Hilfestellungen für Mitarbeiter, Landesamt für Datenschutz Niedersachsen (LfD Niedersachsen)

<http://www.lfd.niedersachsen.de/download/61775>

Für Teilnehmer am Bayerischen Behördennetz:

IT-Sicherheitsrichtlinien für die bayerische Staatsverwaltung - Sicherheit von IT-gestützten Endgeräten (BayITSiR-13)

Nur aus dem Bayerischen Behördennetz erreichbar:

<http://portal.bybn.de/portal/?quelle=jlink&query=2003.4-F-988-217-F&psml=fpbayernrechtprod.psml&max=true&uid=byp>

Verschlüsselung - Orientierungshilfe, 7/2010, Landesamt für Datenschutz Niedersachsen (LfD Niedersachsen)
<http://www.lfd.niedersachsen.de/download/59797>

Dokumente / Anlagen

Handout manueller Logout für Mitarbeiter

Kapitel 5 Berechtigungskonzepte und Protokollierung

Ein wichtiges Element in der Informationssicherheit ist das sogenannte „Need-to-Know-Prinzip“. Jeder Mitarbeiter soll nur auf die Informationen und Daten Zugriff haben, die er oder sie für die Ausführung der Tätigkeit zwingend benötigt. Das klingt einfach, ist aber eine große Herausforderung für jede Organisation. Seitens der IT werden Zugänge auf die IT-Systeme und Zugriffe auf bestimmte Laufwerke und Verzeichnisse mittels Berechtigungskonzepten (zumeist mit Gruppenberechtigungen) geregelt. Hat sich ein Benutzer an einem System angemeldet, so ist er aufgrund seiner Zuordnung in eine bestimmte Nutzergruppe (beispielsweise „Bürgerbüro“) zu Zugriffen auf allgemeine Arbeitslaufwerke des Sachbereichs Bürgerbüro berechtigt. Die Laufwerke und Verzeichnisse der Personalverwaltung sind ihm üblicherweise (im Idealfall) weder sichtbar noch im Zugriff.

Doch mit der Anmeldung an den IT-Systemen ist es nicht getan. Jede Organisation betreibt eine Vielzahl von Verfahren und auch in diesen muss der Zugriff so geregelt sein, dass jeder Mitarbeiter nur auf die Daten zugreifen kann, die er für seine Arbeit benötigt. Werden Personalverwaltung und Personalabrechnung durch unterschiedliche Mitarbeiter in ein- und demselben Verfahren durchgeführt, so sind die Zugriffsrechte beider Mitarbeiter entsprechend zu beschränken. Der Mitarbeiter der Personalverwaltung benötigt üblicherweise keinen Zugriff auf die regelmäßigen Verdienstabrechnungen sowie der Mitarbeiter aus dem Abrechnungsbereich nur auf einen Teil an Informationen aus der Personalverwaltung angewiesen ist, um die Abrechnung durchführen zu können. Letzterer darf daher – als Beispiel – keinen Zugriff auf die vollständige Personalakte haben. Daher sind auch hier entsprechende Berechtigungskonzepte einzuführen und regelmäßig zu überprüfen.

Optional: Wir dürfen jedoch die analoge Welt nicht vergessen. Auch hier gilt das zuvor genannte Prinzip und ist mit entsprechenden Maßnahmen sicherzustellen. Schlüssel für den Bereich Personalverwaltung und die darin befindlichen Schränke haben nur Mitarbeiter aus genau dieser Abteilung. Auch das Papierarchiv darf nicht vergessen werden. Neben der Tatsache, dass dieses jederzeit verschlossen sein muss, sollte nicht jeder Mitarbeiter einfach Unterlagen einlagern und entnehmen können. Eine entsprechende Archivregelung (in kleineren Organisationen) oder ein Archivar (in größeren Einrichtungen) sollte dies sicherstellen. Die Unterlagen im Archiv sind ebenfalls entsprechend zu trennen. Zuvor in einem separaten Schrank im Personalbereich verwahrte Personalunterlagen können nicht im Archiv in friedlicher Eintracht neben Papierakten anderer Ämter im Regalfach stehen. Sie sind dort ebenfalls zu separieren (abschließbarer Schrank, Gitterbereich etc.).

Sie sehen also, das Thema Berechtigungskonzept zieht sich sowohl durch die digitale als auch die analoge Welt. Ein sehr aufwändiges Thema, aber unverzichtbar.

Hinweis: optionale Punkte sind gelb hinterlegt.

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
5. Berechtigungskonzept	Ein nachvollziehbares und administrierbares Berechtigungskonzept ist eines der Herzstücke eines funktionierenden Schutzkonzepts. Neueinstellungen, ausscheidende Mitarbeiter oder z.B. Aushilfen / Praktikanten, die mehrere Bereiche durchlaufen, stellen eine große Herausforderung für ein funktionsfähiges Berechtigungskonzept dar.		Dokumente / Anlagen: Keine, jedoch Vorlagen über Weblinks verfügbar
5.1. Gruppen- versus Einzelberechtigungen	Existieren nachvollziehbare Gruppen, mittels derer Nutzer ihre Zugriffsrechte zugeteilt bekommen? Wird auf die Nutzung von Einzelberechtigungen weitestgehend verzichtet? Sind möglichst wenig rekursive Gruppen vorhanden (Gruppen, die im schlimmsten Fall mehrmals ineinander verschachtelt sind)? Wurde das Berechtigungskonzept seit Einführung regelmäßig auf Aktualität und Sicherheit geprüft (z.B. auch mittels externer Tools für das Active Directory)?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

5.2. Berücksichtigung Fachverfahren	Sind Verantwortliche in der Organisation definiert, die für die Planung und Einrichtung von Berechtigungen in den Fachverfahren verantwortlich sind? (Dies ist üblicherweise jemand aus dem anwendenden Sachbereich, nicht die IT!) Sind diese Personen in den Freigabeprozess für Zugriffsberechtigungen mit einbezogen (siehe auch 5.3) und führen die Einrichtung von Benutzerfreigaben selbst durch? Werden die Berechtigungen in einem regelmäßigen Intervall (üblicherweise jährlich) geprüft und bei Bedarf entsprechend angepasst? Werden die Prüfung und Anpassung schriftlich dokumentiert?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
5.3. Zugriffsvergabe	Gibt es ein festes Verfahren, mittels dessen Zugriffsrechte vergeben und entzogen werden, z.B. bei Anforderung eines Arbeitsplatzes, Wechsel eines Mitarbeiters, Ausscheiden etc.? Existiert hierfür ein Formular (Papierform oder elektronisch), auf dem alle relevanten Informationen und Arbeitsschritte festgehalten werden (Anforderung, Grund, Prüfung, Freigabe, Bestätigung der Umsetzung)?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
5.4. Umgang bei zeitweisen Beschäftigungen oder bei Ausscheiden	Ist auch der Rechteentzug für zeitweise Beschäftigungsverhältnisse oder bei Ausscheiden klar geregelt? In der Praxis zeigt sich, der IT-Bereich erfährt mit als Erstes, wenn ein neuer Arbeitsplatz benötigt wird, ist jedoch das letzte Glied in der Kette, wenn es um die Information über einen ausgeschiedenen Mitarbeiter geht. Risiko: weiterhin bestehende Zugriffsmöglichkeiten, z.B. von außen auf die Systeme durch den ehemaligen Mitarbeiter etc.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
5.5. Systemprotokolle	Ist bekannt, welche Systemprotokolle aktiviert sind und was konkret aufgezeichnet wird (Login, Logout, Fehlversuche, Sicherheitsverstöße etc.)? Wann werden diese durch wen, wie oft ausgewertet? Ist geregelt, was beim Feststellen von Verstößen konkret erfolgt? Wie wird mit identifizierten Sicherheitsproblemen umgegangen? Für welche Dauer werden diese Protokolle vorgehalten?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Wie ist das Löschen dieser Protokolle sichergestellt?		
5.6. Zugriff, Änderung, Löschung	Kann in den Systemen und Verfahren die datenschutzkonforme Protokollierung von Zugriffen auf Daten, deren Änderung und Löschung sichergestellt werden? Wird diese umgesetzt? Wer kontrolliert dies wann, wie oft? Was passiert mit diesen Protokollen im Anschluss? Wer ist für die manuelle / automatisierte Löschung verantwortlich?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
5.7. Dokumentation	Sind die Berechtigungskonzepte (Laufwerke, Verzeichnisse, Fachverfahren) schriftlich dokumentiert und aktuell?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
5.8. Registratur / Schriftgutlager	Ab und zu wird bei der Betrachtung des Themas Informationssicherheit die analoge Welt vergessen. Doch auch hier müssen ausreichende Schutzmaßnahmen ergriffen werden. Einer der regelmäßigen Schwachpunkte ist der Archivraum.		Dokumente / Anlagen: keine
5.9. Schriftgutordnung	Existieren klare Regelungen („Schriftgutordnung“), welche Unterlagen eingelagert werden sollen / dürfen? Wenn ja, sind diese klar dokumentiert und den beteiligten Mitarbeitern kommuniziert?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
5.10. Zutritt	Ist sichergestellt, dass nur ein kleiner Kreis an Mitarbeitern Zutritt zu den Räumen hat? Und sind die berechtigten Personen in der Ordnung klar benannt? Möglichkeiten der Sicherstellung: Zugang stets verschlossen, keine Mehrfachnutzung der Räumlichkeit als Lager oder Kopierraum etc., restriktive und dokumentierte Ausgabe von Schlüsseln oder Code-Karten		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
5.11. Verwalter	Für größere Lager empfiehlt sich die Einsetzung eines Verwalters. Ist ein solcher vorhanden und mit seinen Aufgaben vertraut?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
5.12. Protokolle der Einlagerung und Entnahme, sowie Bestandskontrolle	Erfolgt die Einlagerung oder Entnahme von Dokumenten oder Datenträgern ausschließlich durch befugte Mitarbeiter?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar

	Werden Einlagerung und Entnahme zwecks Nachvollziehbarkeit protokolliert (Wer hat was wann eingelagert / entnommen?) Ist eine Bestandskontrolle (Soll/Ist) des Bestands in regelmäßigen Abständen (mindestens 1 x jährlich) sichergestellt? Wer führt diese durch? Wurden Auftrag und Verantwortlichkeit schriftlich festgehalten, z.B. in Stellenbeschreibung des zuständigen Mitarbeiters?		☐ Aktuell in Arbeit
5.13. Löschfristen	Sind die Löschfristen für eingelagerte Daten klar definiert, schriftlich festgehalten und kommuniziert? Wird die Einhaltung der Löschfristen regelmäßig überprüft (mindestens 1 x jährlich)? Wer ist für die Einhaltung der Fristen verantwortlich (einlagernder Sachbereich, Verwalter)? Werden Daten nach Erreichen der Löschfrist rechtskonform entsorgt? Entsorgungsunternehmen (zertifiziert), Schredder (mind. Sicherheitsstufe 3, Partikelschnitt) etc.? Wer ist für die Entsorgung zuständig / verantwortlich? Werden Nachweise über die Entsorgung schriftlich geführt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Abschlusskommentar zu Kapitel 5 Berechtigungskonzepte und Protokollierung:

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 5 Berechtigungskonzepte und Protokollierung

BSI – G 3 Gefährdung durch unzureichendes Berechtigungs- und Rollenkonzept

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02191.html

BSI – M 2.8 Maßnahmen Vergabe von Zugriffsrechten

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02008.html

BSI – M 2 Maßnahmen Geregelte Benutzer- und Berechtigungsverwaltung im Cloud Computing

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02519.html

Muster Berechtigungskonzept (Landesdatenschutzbeauftragter Hamburg)

www.hamburg.de/contentblob/3994566/data/anlage-10-4-muster-berechtigungskonzept.docx

Hinweise und Musterkonzept Umsetzung Berechtigungskonzept Deutsche Krankenhausgesellschaft

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/07/DKG-Hinweise_OHKIS_06-06-2013.pdf

Schriftgutordnung Kitzingen

http://www.kitzingen.info/fileadmin/files_rathaus_buergerservice/PDF_Ortsrecht/X-7_Schriftgutordnung.pdf

Dokumente / Anlagen

Muster und Vorlagen sind über die Linkliste verfügbar.

Kapitel 6 Systemverfügbarkeit und Notfallmanagement

Notfallmanagement wird im Alltag gerne auf den berühmt-berüchtigten „*Notfallplan*“ reduziert. Das greift allerdings deutlich zu kurz. Der Notfallplan ist eine reaktive Vorrichtung für den Fall, dass ein Notfall eingetreten ist. Zuvor gilt es, sich dem Notfallvorsorgekonzept zu widmen. Also den Maßnahmen und Vorkehrungen, die das Eintreten eines Notfalls verhindern oder zumindest die Eintrittswahrscheinlichkeit verringern. Sowohl die Vermeidung als auch die Behandlung von Notfällen variieren von Organisation zu Organisation. Von daher kann es nicht „das“ Konzept oder „den“ Plan geben, sondern es sind stets die individuellen Gegebenheiten zu berücksichtigen. IT-seitig ist es ein himmelweiter Unterschied, ob alle Komponenten inhouse betrieben und betreut werden, ob Wartung und Betreuung an einen externen IT-Dienstleister ausgelagert sind oder vielleicht im Rahmen der Risikoübertragung / Risikoreduzierung alle Verfahren bei einem externen Anbieter im Rechenzentrum gehostet und betreut werden. Entsprechend unterschiedlich fallen dann auch die technischen Vorsorgekonzepte und Notfallmaßnahmen (sprich Notfallplan) aus. Aber auch organisatorische Aspekte wie Lage, Beschaffenheit und Anzahl der Gebäude, bauliche Gegebenheiten und viele mehr wirken sich auf Inhalt und Umfang des Notfallmanagements aus.

Das Bundesamt für Sicherheit in der Informationstechnik stellt mit dem Standard 100-4 im Rahmen des IT-Grundschutzes eine systematische und leicht verständliche Vorgehensweise zur Einführung eines Notfallmanagements zur Verfügung. Die Informationen dazu sind auf den Seiten des BSI frei verfügbar. Es empfiehlt sich, die Phasen der Analyse, Planung und Konzeption, durchaus aber auch der Überprüfung durch einen externen Dienstleister begleiten zu lassen, wenn das interne Know-how hierzu an seine Grenzen stößt. Die Bayerische Verwaltungsschule (BVS) bietet zur Intensivierung und Unterstützung einen 2,5-tägigen Workshop „Notfallmanagement“ nach BSI Standard 100-4 an.

Für den Einstieg und eine erste Absicherung können die folgenden Punkte herangezogen werden. Eine vertiefende Bearbeitung im Anschluss wird dringend empfohlen.

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
6. Notfallvorsorge	Erst im Fall einer gravierenden Störung oder eines Notfalls zeigt sich, ob die Maßnahmen aus diesem Prüfpunkt erfolgreich umgesetzt wurden. Dies lässt sich auch durch ausführliche Tests teilweise nicht ausreichend simulieren. Umso wichtiger ist eine konsequente Prüfung und Umsetzung identifizierter Schwachstellen.		Dokumente / Anlagen: keine
6.1. Firewall	Wird eine dem Stand der Technik entsprechende Firewall-Lösung zum Schutz vor Zugriffen von außen eingesetzt, entweder als Hard- oder Softwarelösung? Sind die Funktionen der Firewall bekannt und dokumentiert? Wer überprüft die Firewall und deren Konfiguration auf Aktualität? Achtung: Firewall ist nicht gleich Firewall. Minimallösungen wie beispielsweise in DSL-Routern für den Heimgebrauch sind kein Ersatz für professionelle Firewall-Lösungen!		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
6.2. Virenschutz	Sind sowohl client- als auch serverseitig geeignete Virenschutzmaßnahmen installiert? Werden Updates sowohl auf dem Server als auch auf Clients sichergestellt? Wie wird dies getan? Sind mobile Geräte (Notebook, Smartphone,		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Tablet) in das Virenschutzkonzept eingebunden und ist die Versorgung mit Updates ebenfalls sichergestellt? Funktionieren die Updates auch außerhalb des internen Netzes? Werden Mitarbeiter über außerordentliche, aktuelle Bedrohungen informiert? Wenn ja, wie? Wenn nein, warum nicht?		
6.3. WLAN	Sofern WLAN eingesetzt wird: - Existiert eine Übersicht über alle Zugangspunkte / Hotspots? - Wurde auf ausreichend sichere Verschlüsselung (zurzeit mindestens WPA2) geachtet? - Sind weitere Schutzmechanismen im Einsatz wie MAC-Filter etc.? Es empfiehlt sich, WLAN in einem separaten Netz zu betreiben und nicht direkt im internen Organisationsnetz mit vollem Zugriff auf die internen Funktionen. Sollte dieser Zugriff notwendig sein, so richten Sie diesen mittels VPN o.ä. aus dem WLAN-Netz auf das interne Netz ein.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
6.4. Backup / Recovery	Nicht nur die Sicherung an sich ist wichtig. Die zu sichernden Daten müssen nach Dringlichkeit der Wiederherstellung klassifiziert, geeignete Backupverfahren und Zyklen ausgewählt sein sowie regelmäßig Wiederherstellungstests durchgeführt werden.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
6.4.1. Sicherungs-konzept	Existiert ein Sicherungskonzept, aus dem hervorgeht: - Wichtigkeit der Verfahren und Daten? - Sicherungsart? - Sicherungsrhythmus? - Verantwortlichkeiten? Der BSI IT-Grundschutz enthält zu diesem Thema einen gut beschriebenen Baustein und dazugehörige Maßnahmen (siehe Linkliste). Die Bearbeitung ist dringend angeraten. Sofern Sie Ihre IT ausgelagert haben, lassen Sie bitte Ihren Dienstleister die konforme Umsetzung prüfen und bestätigen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
6.4.2. Technik	Ist die Art der Sicherung noch zeitgemäß? Ist mittels der eingesetzten Sicherungstechnik ein zeitnahes Recovery möglich? Sind ausreichend Schutzmaßnahmen wie Verschlüsselung, Brandschutz etc. berücksichtigt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	sichtigt? (Ungeeigneter Klassiker: Tapelader im Serverraum in Endlosschleife) Bei Sicherung auf Wechselmedien: Werden diese regelmäßig ausgetauscht, um Ausfällen vorzubeugen?		
6.4.3. Lagerung der Datensicherung	Werden die Sicherungsmedien (Tape, Wechselplatte, NAS) außerhalb des Serverraums gelagert? Möglichst in einem anderen Brandabschnitt? Ist ein Datensicherungstresor vorhanden nach Norm S 60 / 120 DIS? Bei Online-Backup: Sind die Datenübertragung und der Online-Speicher nach aktuellem Stand verschlüsselt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
6.4.4. Beschreibung	Existiert eine genaue Beschreibung des Backups und der Maßnahmen für ein erfolgreiches Recovery für den Fall der Nichtverfügbarkeit der Hauptverantwortlichen für das Backup? Ohne eine solche Beschreibung wird das Zurückspielen zum unkalkulierbaren Risiko, z.B. bei Ausfall der verantwortlichen Mitarbeiter bei Krankheit, Dienstreise oder Ausscheiden. Wird diese Beschreibung zeitnah angepasst, wenn sich etwas am Sicherungskonzept verändert? Wer ist dafür verantwortlich? Und wer prüft die Aktualisierung nach?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
6.4.5. Recovery-Tests	Die Erfolgsmeldungen der Datensicherungssoftware können täuschen. Trotz positiver Meldung sind durchaus Backups nicht mehr les- und wiederherstellbar im Ernstfall. Werden regelmäßige (Intervall drei bis sechs Monate) Überprüfungen der Backups auf Funktionsfähigkeit durchgeführt? Beschränkt sich der Recovery-Test nicht auf einzelne Dateien, sondern werden auch komplette Verzeichnisstrukturen und Server-		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Umgebungen getestet? Wird das Ergebnis entsprechend dokumentiert? Werden Fehlversuche analysiert und deren Ursache zeitnah abgestellt? Werden auch diese Maßnahmen schriftlich dokumentiert? Wer ist für die Durchführung der Tests und die weitere Bearbeitung verantwortlich? Ist diese schriftlich dokumentiert und dem Verantwortlichen bekannt?		
6.4.6. Umgang mit älteren Sicherungen	Im Laufe der Zeit finden Wechsel der Sicherungssysteme (Hardware und Software statt). Ist sichergestellt, dass ältere Sicherungen (z.B. Jahressicherungen) auch nach einem Wechsel noch verfügbar sind, z.B. durch Überspielen auf neue Sicherungstechnik? Dies ist gerade im Hinblick auf Aufbewahrungsfristen wichtig, sofern keine anderweitige elektronische Archivierung stattfindet.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
6.5. Brandschutzgeräte	Existieren ausreichend Brandschutzgeräte gerade im IT-Bereich / Serverraum? Sind diese frei zugänglich angebracht? (nicht hinter Türen, zugestellt mit Material etc.) Existieren deutliche und ausreichend viele Hinweisschilder auf die Standorte der Brandschutzgeräte? (Im Zweifel sind das mehr Hinweise als sie der Brandschutz rechtlich vorsieht.) Werden die Brandschutzgeräte regelmäßig gewartet / geprüft? Sind nachvollziehbar ALLE Geräte in den Wartungszyklus integriert (Problem Einzelanschaffungen)? Sind Mitarbeiter in die Brandbekämpfung eingewiesen oder dafür speziell ausgebildet? Werden diese Einweisungen mindestens jährlich wiederholt? Ist klar gekennzeichnet, welche Löschgeräte zu welchem Zweck eingesetzt werden können? Es bringt wenig bis nichts, mit einem normalen Löscher einen Elektrobrand im Serverraum bekämpfen zu wollen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

6.6. Brandmeldesystem	Wird das Brandmeldesystem regelmäßig geprüft und das Ergebnis dokumentiert? Sind ausreichend Brandmelder vorhanden (in der Praxis werden meist mehr benötigt als der Brandschutz vorschreibt)? Ist die automatisierte Benachrichtigung der richtigen Ansprechpartner im Falle eines Auslösens sichergestellt? Wenn kein Brandmeldesystem in Form einer kompletten Anlage vorhanden ist, sind Alternativen geprüft und im Einsatz?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
------------------------------	---	--	--

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
6.7. Unterbrechungsfreie Stromversorgung	Sind relevante Systeme vor Stromausfällen mittels unterbrechungsfreier Stromversorgung (USV) gesichert? Werden die USV regelmäßig gewartet (Akkuprüfung, Austausch)? Werden diese Arbeiten protokolliert? Melden die USV kritische Zustände nicht nur per Leuchtanzeige, sondern ebenfalls für Meldesysteme wie E-Mail / SMS? Werden lediglich einfache USV eingesetzt oder intelligente Systeme, die entsprechende Notaktivitäten einleiten (Information an Nutzer, Schließen der Datenbanken, Herunterfahren der Systeme etc.)? Wer ist für die Betriebssicherheit und Funktionsfähigkeit der USV konkret verantwortlich? Sind ausreichend Netzersatzgeräte, z.B. Katastrophenschutzeinrichtungen, vorhanden?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
6.8. Überwachung / Monitoring	Sind alle verfügbaren Monitoring-Systeme im IT-/Server-Bereich installiert / aktiviert wie: - Temperatur? - Feuchtigkeit? - Unbefugter Zutritt / Einbruch?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	- Fehlerhafte Backups? - Fehlermeldungen der USV? - Verstöße gegen Sicherheitsrichtlinien auf den Systemen? Ist sichergestellt, dass der Empfänger von Alarm-SMS/-E-Mail mit den eingehenden Informationen handlungsfähig ist? Wie ist der Einsatz außerhalb der Öffnungszeiten geregelt? Sind die Empfänger aktuell oder laufen die Meldungen eventuell ins Leere? Wer ist für die Einrichtung und Konfiguration des Monitorings verantwortlich? Sind die informierten Mitarbeiter ausreichend geschult und eingewiesen, was im Meldefall zu tun ist?		

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
7. Notfallbehandlung	Die Notfallbehandlung, also die Planung und Beschreibung von Maßnahmen für den Fall des trotz aller Vorsorge eingetretenen Notfalls, baut zwingend auf den Erkenntnissen aus dem Notfallvorsorgekonzept auf. Von daher sollten Sie stets die vorherigen Punkte dieses Kapitels bearbeitet haben und bitte nicht direkt zu diesem Bereich springen. Im Zweifel ersparen Sie sich damit a) Daten- und Zeitverluste, b) Kosten und c) Frust und Ärger (u.a. Imageschaden). Sofern Sie in Ihrer Organisation Teile der IT oder die IT im Ganzen an einen externen Dienstleister ausgegliedert haben, so ist es bei diesem Thema nicht damit getan, auf eine vorhandene Rufnummer und bestehende Service Level Agreements mit dem Dienstleister zu verweisen. Sie sollten die beim Dienstleister getroffenen Maßnahmen zur Notfallvorsorge und Bewältigung stets prüfen und die Prüfung regelmäßig wiederholen. Ihr Dienstleister muss in der Lage sein, Ihnen die entsprechende Dokumentation zur Verfügung zu stellen. Sollte dies nicht zeitnah möglich sein, denken Sie bitte über einen Wechsel des Dienstleisters nach.		Dokumente / Anlagen: • Muster Netzwerkplan • Muster Gliederung und Aufbau Notfallplan
7.1. Definition	Ist klar geregelt, wie sich ein Notfall von einer Störung abhebt? Ist dies dokumentiert? Ist klar definiert, für welche Art Notfall externe Hilfe notwendig ist?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
7.2. Initiator und Verantwortlicher in der Bearbeitung von Notfällen	Sind die Kompetenzen geklärt, wer einen bestimmten Notfall in der Organisation ausrufen und auch wieder aufheben kann? Ist für jeden betrachteten Notfall dokumentiert, wer für dessen Bearbeitung zuständig ist und wer von den verantwortlichen Personen für		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	den jeweiligen Notfall weisungsberechtigt ist? Je nach Art des Vorfalls muss das nicht zwingend immer die Leitung der Organisation sein. Das ist anfangs etwas ungewöhnlich in streng hierarchisch geführten Organisationen und daher entsprechend zu betonen UND zu üben.		
--	--	--	--

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
7.3. Dokumentation	Eine ausführliche Dokumentation ist das A und O für die erfolgreiche Umsetzung eines Notfallkonzepts. Ohne diese Informationen kann nicht gewährleistet werden, kritische Verfahren zeitnah wieder anfahren zu können. Folgende Informationen sollten mindestens verfügbar und aktuell sein: - Netzwerkübersichten der eingesetzten Technik und Systeme - Leitungsübersicht (interne Verkabelung) und externe Leitungen, inkl. Beschreibung der Patchfeld-Systematiken - Verzeichnis der im Einsatz befindlichen Hard- und Software sowohl für Server als auch Arbeitsplätze - Übersicht über auf den Geräten installierte Standardsoftware und darüber hinaus installierte Zusatzsoftware - Detailliertes Verfahrensverzeichnis (Übersicht aller relevanten Verfahren im Haus mit genauer Beschreibung der Verantwortlichkeiten, Funktionen, Daten, Berechtigungen, Schutzmaßnahmen etc.) – im Zweifel fragen Sie Ihren Datenschutz-beauftragten - Klassifizierung der eingesetzten Systeme und Verfahren nach Dringlichkeit für eine Wiederherstellung - Übersicht über externe Zulieferer (Strom, Wasser, TK, Datenleitungen, Hardware, Software etc.) mit Ansprechpartnern, Rufnummern, (Rah-		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	men-)Vertragsdaten, Leistungsbeschreibung in Kurzform - Übersicht über externe Dienstleister, z.B. für Installation, Wartung, Konfiguration, Support, Fehlerbehebung etc. mit Ansprechpartnern, Rufnummern, Vertragsdaten und Leistungsbeschreibung Tipp: Für einige dieser Punkte gibt es elektronische Tools zur Unterstützung beispielsweise zur automatisierten Inventarisierung von Hard- und Software, Lizenzen, Konfigurationen etc. Bei entsprechender Konfiguration sind einige dieser Tools auch in der Lage, Netzwerkpläne zu erstellen.		
--	---	--	--

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
7.4. Notfallplan	Wurde ein Notfallplan auf Basis der Erkenntnisse aus den Prüfpunkten dieses Konzepts erstellt und bekanntgemacht? Wo wird dieser Notfallplan aufbewahrt? Empfehlenswert: elektronische Kopie sowie stets aktuelle Papierversion z.B. im Datenschutztresor. Es bieten sich auch stand alone fähige WIKI-Versionen (bspw. TiddlyWiki – siehe Link) mit entsprechenden Sicherungskopien auf Stick / externer HDD im Datenschutztresor statt Papier an. Sind alle notwendigen Handlungsabläufe nachvollziehbar dokumentiert, auch für z.B. externe Kräfte oder Personen, die nicht an der Erstellung beteiligt waren? Sind die Organisationsstruktur und die Verantwortlichkeiten für die Wiederanlaufmaßnahmen klar vorgegeben, um eine reibungs- und konfliktlose Umsetzung zu gewährleisten? Denken Sie bitte daran, dass ein Notfallplan stets mehrere Phasen abdeckt: • Eintritt des Notfalls • Meldung des Notfalls • Beschreibung erste Sofortmaßnahmen • Maßnahmen zum Wiederanlauf		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	• Maßnahmen zum Erreichen eines Notbetriebs (kein 100% Betrieb, bspw. 1 von 5 Arbeitsplätzen im Bürgerbüro etc.) • Maßnahmen zum Erreichen des Normalbetriebs • Nachbearbeitung des Notfalls: Analyse, was lief gut, was nicht, was muss verbessert / geändert werden, aber auch: Dokumentation des kompletten Notfalls und dessen Bekämpfung Sind für die identifizierten Risiken die zuvor genannten Punkte klar und nachvollziehbar beschrieben?		
7.5. Übungen / Tests	Werden die Notfallmaßnahmen regelmäßig getestet und mit den Mitarbeitern Notfallübungen abgehalten? Hierbei kann es sich um reine Besprechungen der geplanten Maßnahmen zur Notfallbeseitigung im Team handeln (Plan-/ Dokumentenbesprechungen), aber auch um Einzelfall- und Vollübungen. Letztere sollten gewissenhaft vorbereitet werden, nicht einfach „Stecker ziehen“.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
7.6. Schulungen	Wichtiges Element ist, Mitarbeiter mit den Inhalten und den Vorgehensweisen des Notfallplans vertraut zu machen. Dies sollte zielgruppenorientiert geschehen. Das Bürgerbüro hat im Falle eines Notfalls im Zweifel andere Aufgaben als die IT. Werden solche Schulungen und Sensibilisierungen durchgeführt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Abschlusskommentar zu Kapitel 6 Systemverfügbarkeit und Notfallmanagement:

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 6 Systemverfügbarkeit und Notfallmanagement

BSI Elementare Gefährdungen G 0

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g00/g00.html

BVS Kurs Notfallmanagement

<http://www.bvs.de/fortbildung/seminare/seminarsuche/yca/c/show/informationstechnologie/datenschutz-und-it-sicherheit/datenschutz-und-it-notfallmanagement/index.html>

BSI - B 1.4 Datensicherungskonzept

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01004.html

BSI – M 6.32 Regelmäßige Datensicherung

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m06/m06032.html

Stand alone WIKI TiddlyWiki (kostenfrei)

<https://de.m.wikipedia.org/wiki/TiddlyWiki>

Alternativen zu MS Visio (Netzwerkplan / Netzplan)

http://praxistipps.chip.de/microsoft-visio-3-gute-alternativen_42641

BVS Kurs Notfallmanagement

<http://www.bvs.de/fortbildung/seminare/seminarsuche/yca/c/show/informationstechnologie/datenschutz-und-it-sicherheit/datenschutz-und-it-notfallmanagement/index.html>

Dokumente / Anlagen

Muster Netzwerkplan vereinfacht (mit Schwachstellen)

Muster Grobgliederung Notfallhandbuch (PDF)

Kapitel 7 Richtlinien / Dienstanweisungen

Richtlinien und Dienstanweisungen bilden die Leitplanken innerhalb einer Organisation und dienen sowohl der Absicherung der Mitarbeiter ALS AUCH der Organisation. Steht für die Organisation üblicherweise die Risikominimierung im Vordergrund, so erhält der Mitarbeiter im Zuge dessen die Zusicherung seines Arbeitsgebers, bei Einhaltung der Richtlinien nicht für Sicherheitsverstöße belangt zu werden („Richtung einhalten, kein Risiko für Dich, lieber Mitarbeiter“). Das Problem mit Richtlinien in einer Organisation ist dasselbe wie im Straßenverkehr: Es gibt bewusste oder unbewusste Geisterfahrer. Gegen unbewusste Geisterfahrer hilft Kapitel 8 Schulungen und Sensibilisierungen. Gegen Vorsatz jedoch ist bedauerlicherweise so gut wie kein Kraut gewachsen.

Richtlinien sind organisationsspezifisch zu erstellen und daher nur zum Teil per copy & paste oder aus Vorlagen zu entnehmen. Muster und Vorlagen können jedoch einen guten Anhaltspunkt für eine eigene Richtlinienlösung bilden. Klassische Themen für Richtlinien sind beispielsweise die Private Nutzung E-Mail / Internet, der Umgang mit Hard- und Software, organisationsweite Passwortvorgaben für Systeme ohne technisch umgesetzte Komplexität, das Verhalten im Notfall (Virus, Defekt, Brand, Wasser etc.), der Umgang mit mobilen Geräten bis hin zu Mobile Device Management (Sicherheitsmaßnahmen, Apps, Synchronisierung etc.), die Entsorgung von Papierakten / Datenträgern, die Schließordnung der Verwaltung, der Umgang mit Datenpannen oder auch eine Social Media Policy. Das sind lediglich einige Beispiele, die geregelt werden müssen / können, je nach Gegebenheit vor Ort.

Haben Sie das Richtlinienpaket für Ihre eigene Organisation geschnürt, geht die eigentliche Arbeit erst los. Sie müssen Ihre Mitarbeiter mit den Inhalten und Verfahrensweisen vertraut machen. Dieser Aufgabe stellt sich das Kapitel 8 Schulungen und Sensibilisierungen dieses Konzepts. Sie können es natürlich bei der bewährten Verfahrensweise belassen und einfach jedem Mitarbeiter die Richtlinien in Papierform oder per E-Mail zusenden. Dazu die Anweisung, diese Richtlinien zwingend einzuhalten. Eine bequeme Lösung („*Ich habe ja drauf hingewiesen. Was kann ich dafür, wenn der Mitarbeiter sich nicht daran hält*“), schafft aber keine Sicherheit und motiviert Ihre Mitarbeiter auch nicht zur Umsetzung / Unterstützung.

Bitte nutzen Sie das Muster der **Dienstanweisung für die Nutzung der Informationstechnologie** der Bayerischen Kommunalen Spitzenverbände zur Bearbeitung des hier vorliegenden Kapitels.

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
7. Richtlinien / Dienststanweisungen			Dokumente / Anlagen: Keine, dafür entsprechende Verweise auf Richtlinien in den Web-links
7.1. Bestandsaufnahme	Verfügen Sie über eine Übersicht über die Richtlinien und Dienststanweisungen (DA) zur Informationssicherheit (inklusive Datenschutz und IT-Sicherheit) in Ihrer Organisation? Können Sie eindeutig die jeweils aktuelle Version dieser Richtlinien/DA bestimmen / nachvollziehen? Wenn nein, sollten Sie zukünftig allen Dokumenten sogenannte Metadaten beispielsweise in der Fußzeile mitgeben (Datum, Autor, Version, Freigabe, Titel etc.). Sind Verantwortlichkeiten und Prozesse in Ihrer Organisation definiert, Richtlinien / DA in regelmäßigen Abständen auf Wirksamkeit und Aktualität (Änderung der Rahmenbedingungen wie Recht, Technik, Organisation und Bedrohung) hin zu überprüfen? Und werden diese wirklich konsequent eingehalten (Kontrollfrage: „Wann wurde die älteste Richtlinie / DA zuletzt und durch wen aktualisiert?“)? Wenn nein, sollten Sie sich bereits jetzt zu dem Thema Gedanken machen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung

7.2. Themenauswahl	Nach erfolgter Bestandsaufnahme sollten Sie sich Gedanken darüber machen, welche Richtlinien / DA Ihnen in Ihrer Organisation noch fehlen oder welche aus Aktualitätsgründen zeitnah überarbeitet gehören. Die Themen stimmen Sie sinnvollerweise innerhalb des Informationssicherheitsteams und mit der Organisationsleitung ab. Bitte denken Sie dabei auch an den ganzen organisatorischen Bereich und machen Sie nicht den weit verbreiteten Fehler, sich rein auf Technik / IT zu beschränken. Weitere mögliche Themen können neben den in der Einleitung genannten sein (kein Anspruch auf Vollständigkeit): Vorgehensweise Beschaffung technischer Geräte, Beantragung und Vergabe von Zugriffsrechten, Arbeitsschritte beim Einstellen / Ausscheiden von Mitarbeitern in Ihrer Organisation, Umgang mit Passwörtern (Aufbau, keine Weitergabe etc), Vorgehensweisen und Verhaltensweisen bei geplanter / ungeplanter Abwesenheit von Mitarbeitern, Klassifizierung von Daten und Informationen und wie damit umzugehen ist, Umgang mit mobilen Datenträgern, Beauftragung und Kontrolle von externen Dienstleistern, generelle frühzeitige Einbindung des ISB und DSB, Telearbeitsplatz		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	/ Home Office etc. Bitte beachten Sie auch die Vorschläge aus dem Muster Dienstanweisung für die Nutzung der Informationstechnologie. Wenn Sie mit der Themenauswahl fertig sind, sollten Sie deren Umsetzung priorisieren. Es wird nicht möglich sein, alle Themen gleichzeitig zu bearbeiten und in Richtlinien / DA zu formulieren. Implementieren Sie bereits jetzt Prozesse und Verantwortlichkeiten, wer für identifizierte oder zukünftige Themen die Aktualisierung übernimmt.		
--	--	--	--

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
7.3. Inhaltliche Abstimmung	Stehen die Themen fest, sollten Sie sich mit den Verantwortlichen für die Themen wie IT-Leitung, Gebäudeverwaltung, Leitung Personal, aber auch bei Bedarf weitere Sachbereichsleiter und Personalvertretung zu folgenden Punkten abstimmen: • Geltungsbereich • Erläuterung der Notwendigkeit und der Ziele • Konkrete Maßnahmen • Ansprechpartner für Detailfragen der Mitarbeiter • Bei Bedarf / Empfohlen: Konsequenzen bei Nichtbeachtung • Personalvertretung mit einbinden • Verantwortlichkeit für Aktualisierung und Intervall der Aktualisierung festschreiben		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
7.4. Tipps für Richtlinien und Dienstanweisungen	In der Kürze liegt die Würze (Aufmerksamkeitsspanne nutzen!) Vermeiden Sie umfangreiche technische Beschreibungen (oder erwähnen sie diese im Anhang) Sprechen Sie dieselbe Sprache der Zielgruppe!		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Erläutern Sie Motivation und Hintergrund der Regelung (Verständnis schaffen!) Keine Kommunikation einer Richtlinie / Dienstanweisung ohne vorherige Vorstellung bei den Mitarbeitern (Akzeptanz erhöhen!)		
--	---	--	--

Abschlusskommentar zu Kapitel 7 Richtlinien / Dienstanweisungen:

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 7 Richtlinien / Dienstanweisungen

Eine gute Zusammenstellung an Richtlinien und Orientierungshilfen zu verschiedenen Themen finden Sie auf den Webseiten des Sächsischen Datenschutzbeauftragten u.a. Nutzung E-Mail / Internet, private Nutzung, Organisation der Informationssicherheit und des Datenschutzes

<https://www.saechdsdb.de/informationen-oeb/arbeitshilfen-oeb>

Auch das BSI hält zahlreiche Muster und Vorlagen zum Thema bereit, u.a. Unberechtigte Nutzung externer IT Services, Entsorgung von Datenträgern, Telearbeitsplatz, Verhalten bei Sicherheitsvorfällen, Änderung von Berechtigungen

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/muster/muster.html

Ein schönes Beispiel für eine Dienstanweisung mit Erklärungen für den Anwender (am Ende des Dokuments unter Tipps)

www.sakd.de/fileadmin/recht/musterdienstanweisungen/Muster-DA_IT.doc

Haus- und Gebäudeordnung Stadt Solingen

[http://www2.solingen.de/C12572F800380BE5/files/2009_haus-_und_gebaeudeordnung_der_stadt_soling.pdf/\\$file/2009_haus-_und_gebaeudeordnung_der_stadt_soling.pdf](http://www2.solingen.de/C12572F800380BE5/files/2009_haus-_und_gebaeudeordnung_der_stadt_soling.pdf/$file/2009_haus-_und_gebaeudeordnung_der_stadt_soling.pdf)

Muster / Anleitung zur Erstellung von Social Media Guidelines

<https://www.wbs-law.de/internetrecht/muster-fuer-social-media-guidelines-5718/>

Leitfaden zur Erstellung einer Datenschutzrichtlinie des Hessischen Landesdatenschutzbeauftragten

https://www.datenschutz.hessen.de/_old_content/tb25/k20p3.htm

Umgang mit E-Mail und Internet inklusive Abwesenheit der Stadt Kitzingen

http://www.kitzingen.info/fileadmin/files_rathaus_buergerservice/PDF_Ortsrecht/Dienstanweisung_E-Mail_und_Internet.pdf

Kategorisierung und Schutzbedarf von Daten (Beitrag der Computerwoche) / Richtlinie der Rheinhausen-Gruppe (sehr gut!)

<http://www.computerwoche.de/a/datenschutz-durch-datentransparenz,3071049>
www.reinhausen.com/XparoDownload.ashx?raid=51753

Sammlung relevanter IT-Richtlinien des BSI

<https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/content/hilfmi/muster/musterrichtlinien/musterrichtlinien.html?nn=6610706>

Dokumente / Anlagen

Keine

Bitte beachten Sie die geplante Veröffentlichung des Musters der **Dienstanweisung für die Nutzung der Informationstechnologie** der Bayerischen Kommunalen Spitzenverbände im Rahmen eines Stiftungsprojekts der Innovationsstiftung Bayerische Kommune.

Veröffentlichung voraussichtlich im 1. Quartal 2017 unter <http://www.bay-innovationsstiftung.de/index.php?id=37>

Kapitel 8 Schulungen und Sensibilisierungen

Konrad Lorenz († 1989), ein bekannter Verhaltensforscher, sagte recht zutreffend:

„Gesagt heißt nicht immer gehört, gehört heißt nicht immer verstanden, verstanden heißt nicht immer einverstanden, einverstanden heißt nicht immer angewendet, angewendet heißt nicht immer beibehalten.“

Aus regelmäßigen Studien ist bekannt, dass über die Hälfte der Datenpannen aufgrund von Unkenntnis und Fahrlässigkeit von Mitarbeitern entstehen. Jetzt könnte man meinen, mit dem Entwickeln und Herausgeben von Dienstanweisungen und Richtlinien hat die Organisation ihre Schuldigkeit getan. Doch das greift zu kurz. Sicherlich ist dadurch der Nachweis erbracht, zumindest die Formalitäten erledigt zu haben. Im Zweifel auf dem gesetzlich minimal zulässigen Niveau. Doch ist deswegen Ihre Organisation jetzt „sicher“ geworden im Hinblick auf Informationssicherheit und Datenschutz? Oder haben Sie damit lediglich unbequeme Fragen in punkto Haftung reduziert, sich also selbst als Organisationsleiter abge-“sicher“-t?

Richtlinien sind daher nur ein Schritt für eine systematische Einführung und Aufrechterhaltung von Informationssicherheit in Ihrer Organisation. Es ist stets zu empfehlen, die Inhalte (Gründe, Umsetzung in der eigenen Organisation, Tipps und Tricks für den Alltag) den Mitarbeitern in geeigneten Schulungseinheiten (Präsenz, Online) vorzustellen und zu erklären. Analog zum Zitat weiter oben: Erklären – Verstehen – Leben / Umsetzen.

Da sich Richtlinien, Anweisungen, Rechtsgrundlagen und Bedrohungslagen ändern, sollten Sie die Themen Schulung und Sensibilisieren nicht als einmalige Angelegenheit betrachten. Bedenken Sie: Ihre Mitarbeiter haben den Kopf voll mit den nicht wenigen Sachaufgaben und Verfahren im Tagesgeschäft. Noch dazu sind nicht alle IT-Profis, ausgebildete Juristen noch Informationssicherheits- oder Datenschutzbeauftragte. Von daher ist die Organisation gefordert, regelmäßig in geeignetem Umfang, ausreichender Dauer und unter Berücksichtigung des geeigneten Mediums ihre Mitarbeiter für die Themen zu interessieren und mit geeigneten Handlungsanweisungen sowie Tipps und Tricks auszustatten. Ganz wichtig: Sprechen Sie dieselbe Sprache wie Ihre Zielgruppe (keine IT-Fachsprache, keine juristischen Ausarbeitungen).

Die Erfahrung hat gezeigt, dass über Schulungen oder Sensibilisierungsmaßnahmen transportierte Inhalte besser in den Köpfen der Mitarbeiter verankert sind – und somit eine Chance auf Auswirkungen in der Praxis haben -, als die pure Bekanntgabe in Form eines Aushangs oder einem bei Einstellung zu unterschreibenden 150-seitigen Dienstanweisungspaket. Probieren Sie es aus!

Hinweis: optionale Punkte sind gelb hinterlegt.

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
8. Schulungen und Sensibilisierungen	Bereits im Kapitel 1 „Informationssicherheit“ dieses Konzepts haben wir uns mit dem Thema Schulung befasst. Neben der geeigneten Auswahl des Kommunikationskanals gilt es, weitere Punkte zu berücksichtigen. Wichtig: Nur ein nachhaltiges und langfristiges Schulungskonzept hat Erfolg. Oder erinnern Sie sich heute noch an die konkreten Inhalte Ihres Erste-Hilfe-Kurses zum Führerschein und können diese fehlerfrei und sicher anwenden? In diesem Kapitel betrachten wir verschiedene Kommunikationskanäle etwas konkreter.		
8.1. Grundlagen			Dokumente / Anlagen: Keine
8.1.1. Verantwortlichkeit / Zuständigkeit	Gibt es einen Verantwortlichen für die Durchführung oder Koordination von Schulungsmaßnahmen in Ihrer Organisation? Ist dieser Verantwortliche aktiv?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.1.2. Zeit und Mittel	Verfügt dieser Verantwortliche über ausreichend Zeit und Mittel a) zur Planung b) zur Durchführung von kurz-, mittel- und langfristigen Schulungsmaßnahmen?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.1.3. Schulungsplanung	Haben Sie einen langfristigen Fahrplan über Ihre Schulungsmaßnahmen erstellt, aus dem Zeitrahmen und Inhalte sowie die dazugehörige Zielgruppe hervorgeht? Nicht jede Schulung muss sich stets an alle Mitarbeiter wenden. So können z.B. Schulungen zur Daten-		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	weitergabe ihren Schwerpunkt im Bürgerbüro haben, wohingegen das Bauamt sich mehr mit dem Thema „Sichere elektronische Übertragung großer Datenmengen“ befassen kann. Ein konkreter Fahrplan hilft zusätzlich bei der Budget- und Zeitplanung und dient als Nachweis der regelmäßigen Beschäftigung mit dem Thema Informationssicherheit in der Organisation.		
--	---	--	--

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
8.1.4. Externe Unterstützung	Kann und wird bei Bedarf externe Unterstützung für Planung und Durchführung von Schulungsmaßnahmen herangezogen? Sind die hierfür erforderlichen Mittel bereitgestellt? Bestehen hierzu ausreichende Kontakte zu geeigneten Anbietern, die über entsprechende Erfahrung mit Schulungsmaßnahmen im kommunalen Bereich verfügen? Konkret: Vermeiden Sie im Zweifel den Rufer im eigenen Haus. Externe Trainer sind zumeist fitter im Thema und in der praktischen Anwendung und werden oft eher „gehört“ als der Mahner aus den eigenen Reihen. Beachten Sie bitte, dass Ihr Trainer / Berater über die kommunalen Besonderheiten in der praktischen Anwendung von Informationssicherheit (und auch Datenschutz) Bescheid wissen sollte. Stimmen Sie sich mit anderen kommunalen Organisationen ab zwecks Empfehlungen geeigneter Trainer / Berater oder führen Sie diese doch gleich gemeinsam durch (cost sharing).		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.1.5. Zertifikate / Bestätigung der Teilnahme	Erhalten Ihre Mitarbeiter bei erfolgreicher Teilnahme an Schulungsveranstaltungen ein Zertifikat oder eine Teilnahmebestätigung?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar

	Konkret: Belohnen Sie die Teilnahme mit einem Lob, in diesem Fall einer schriftlichen Bestätigung. Dieser Faktor wird gerne unterschätzt.		☐ Aktuell in Arbeit
8.2. Präsenzs Schulung	Präsenzs Schulungen sind in unterschiedlicher Dauer sehr gut für die Vermittlung von Inhalten geeignet. Der Fokus liegt hier nicht auf dem Vortrag, sondern auf dem Erklären von Inhalten, dem Vermitteln von Verständnis und der Diskussion mit den Teilnehmern. Die Dauer der Schulung sollte sich stets am gewünschten Ziel, aber auch an der Aufmerksamkeitsspanne Ihrer Mitarbeiter orientieren. Grundlagenschulungen dürfen gerne etwas länger dauern (2 Stunden). Richtlinien sollten Sie in Einheiten von 30-60 Minuten vorstellen und erklären (BEVOR Sie diese schriftlich kommunizieren). Auffrischungsschulungen sollten 15-30 Minuten nicht überschreiten. Akute Bedrohungslagen sollten in maximal 5-15 Minuten (z.B. als erstes Thema auf einer Personalversammlung) angesprochen werden. In diesen Kurzveranstaltungen können Sie auch gut über den Status Quo des Projekts Informationssicherheit berichten und Werbung machen. Geeignete Themen - Rechtliche Grundlagen (Datenschutz und Informationssicherheit) - Anwendung des Datenschutzrechts (z.B. zulässige Datenweitergaben) - Richtlinien Vorstellung und Besprechung - Vermitteln von Basiswissen		Dokumente / Anlagen: keine
8.2.1. Status Quo	Wurden bereits in der Vergangenheit (regelmäßig) Präsenzs Schulungen zu Informationssicherheit, IT-Sicherheit und Datenschutz durchgeführt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
8.2.2. Fahrplan	Sind für die kommenden 24 Monate mindestens zwei Präsenzs Schulungen für alle Mitarbeiter und bei Bedarf weitere Schulungen für Teilbereiche geplant? Dabei ist die Informationsveranstaltung aus Kapitel 1 nicht zu berücksichtigen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.2.3. Atmosphäre	Sorgen Sie bei Ihren Präsenzs Schulungen für eine lockere und entspannte Atmosphäre. Dies hilft bei der Informationsrezeption ungem. Es hilft, wenn Ihre Mitarbeiter nicht dauernd auf die Uhr schauen, weil sie zurück zum Arbeitsplatz müssen. Belohnen Sie gute Beiträge und Fragen der Teilnehmer (verbal, mit Süßigkeiten etc.) Lassen Sie ausreichend Zeit für Fragen und Diskussionen. Vermeiden Sie das reine Able sen / Vortragen von Präsentationsfolien. Ist dies sichergestellt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.2.4. Teilnahme	Sie haben für die Organisation wichtige Inhalte zu vermitteln (siehe auch Leitlinie Informations sicherheit aus Kapitel 1). Von daher sollte es selbstverständlich sein, dass Ihre Schulungen Pflichtveranstaltungen sind. Ebenso selbstverständlich sollte es bei wichtigen und organisationsweiten Themen sein, dass die Behördenleitung zu Beginn ein kur-		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	zes Statement zur Einführung abgibt und die Unterstützung der Mitarbeiter einfordert.		
8.3. Online-Schulung	Online-Schulungen sind ein bewährtes Mittel zur Unterstützung der Schulungsstrategie. Über Online-Schulungen können Sie sowohl in kurzen Einheiten (max. 30 Minuten) Basiswissen vermitteln, aber auch konkrete Handlungsanweisungen und Empfehlungen schulen. Geeignete Themen - Sicherheit am eigenen Arbeitsplatz - Sicherheit Umgang mobile Datenträger / Geräte (für Zielgruppe) - Aktuelle Bedrohungslage wie Kryptotrojaner - Auffrischung Zulässigkeitstatbestände im Datenschutz - Datenweitergaben (Art.18-21BayDSG) Online-Schulungen sind ebenfalls gut geeignet, neuen Mitarbeitern einen ersten Überblick oder eine Einführung in die Schutzmechanismen der Organisation zu geben.		Dokumente / Anlagen: keine
8.3.1. Schulungsplattform	Setzen Sie Online-Schulungen im Rahmen Ihrer Schulungsstrategie ein? Konkret: Wenn nicht, sollten Sie sich auf jeden Fall nach einer geeigneten Plattform umschaun (siehe auch Kapitel 2 Datenschutz). Dabei sollten Sie die Möglichkeit haben, beliebig viele Schulungen selbst anzulegen und nicht nach Schulung und Anzahl der Nutzer abrechnen zu müssen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
8.3.2. Wissenstest	Da Sie bei einigen Formen der Online-Schulung kein direktes Feedback Ihrer Teilnehmer erhalten, sollten diese am Ende mit einem kurzen Wissenstest zum Verständnis abgeschlossen werden. Ansonsten haben Sie zumeist nur den Nachweis, dass Ihre Teilnehmer sich durch die Schulung „geklickt“ haben. Sie wissen jedoch nicht, ob die Teilnehmer die zu vermittelnden Informationen empfangen und verstanden haben. Ist dies sichergestellt? Hinweis: Sollte die gewählte Plattform dies nicht unterstützen, ist dies kein Drama. Besser wäre es jedoch aus didaktischen Gründen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.3.3. Zertifikat	Der erfolgreiche Abschluss der Online-Schulung sollte stets mit einem Zertifikat für die Mitarbeiter belohnt werden. Ist dies bei Ihrer (angedachten) Lösung – möglichst automatisiert – sichergestellt?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.3.4. Nachweis	Ist sichergestellt, dass Sie jederzeit eine Übersicht / einen Schulungsnachweis über Ihre Online-Schulungen nach Mitarbeitern belegen / führen können? Bitte beachten Sie, dass Sie diese Nachweise auch noch nach einem möglichen Wechsel		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	der Schulungsplattform durchführen können.		
8.4. Rundmails	Auch Rundmails können Bestandteil einer Schulungsstrategie sein. Dabei sollten Sie jedoch einige Aspekte berücksichtigen wie Themenauswahl, Aufmerksamkeitsspanne des Lesers sowie auch Zuständigkeiten.		Dokumente / Anlagen: keine
8.4.1. Zuständigkeiten	Ist klar festgelegt, wer in Ihrer Organisation im Rahmen der Schulungsstrategie E-Mails verfassen und versenden darf? Sie sollten dies auf einen kleinen Kreis an Verantwortlichen beschränken (siehe auch Informationssicherheitsteam im Kapitel 1).		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.4.2. Themenauswahl	Ist sichergestellt, dass nur für E-Mail geeignete Themen auch per E-Mail an die Mitarbeiter im Rahmen der Schulungsstrategie kommuniziert werden? Dies können beispielsweise sein - Akute Bedrohungslagen (Kryptotrojaner, Hoaxes, Viren, Phishing etc.) - Kurze Sicherheitshinweise (wie „Tipp: Manuelles Ausloggen mit Windows-Taste + L“)		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
8.4.3. Aufmerksamkeit	E-Mail ist ein schnelles Medium. Nutzer erwarten hier für gewöhnlich kurze und knappe Aussagen und Handlungsanweisungen. Ist sichergestellt, dass Sie in Rundmails im Rahmen der Schulungsstrategie kurz und knapp auf den Punkt kommen? Konkret: Sie sollten in der Lage sein, Ihre Kernbotschaft im Rahmen von ein bis zwei Minuten Lesedauer an den Empfänger gebracht zu haben. E-Mails, die sich über mehrere Bildschirmseiten (oder ausgedruckte Seiten) ziehen, haben zumeist eine geringe Akzeptanz. Sollten Sie doch weiterführende Informationen mitliefern wollen, dann gilt: Kernbotschaft kurz und knapp in der E-Mail formulieren, weiterführende Details in den Anhang oder Verweis auf Dokumente im Intranet / auf Netzlaufwerken. Unbedingt vermeiden: In der E-Mail lediglich auf den Anhang zu verweisen.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.4.4. Intervall / Häufigkeit	Wenn Sie aufgrund zu häufiger Aussendung von Rundmails bereits im gedanklichen Spam-Ordner Ihrer Mitarbeiter gelandet sind, dann haben Sie wenig bis nichts erreicht. Achten Sie daher auf eine angemessene Häufigkeit Ihrer Aussendungen und übertreiben Sie es nicht.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Konkret: Sofern keine akuten Bedrohungslagen vorliegen, sind ein bis zwei Rundmails im Monat vollkommen ausreichend, um in Erinnerung zu bleiben und für das Thema zu sensibilisieren. Achten Sie auch hier auf die Wahl der richtigen Sprache Ihrer Zielgruppe und vermeiden Sie unnötige technische / rechtliche Fachbegriffe. Ihre Empfänger sind Anwender, keine Vollprofis.		
--	---	--	--

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
8.5. Awareness-Kampagne	Um Informationssicherheit auch langfristig in Ihrer Organisation zu etablieren, werden Sie um langfristige Maßnahmen nicht herumkommen. Es gilt, Ihre Mitarbeiter auch über einen längeren Zeitraum mit den relevanten Themen zu konfrontieren und Hilfestellungen anzubieten. Bewährt haben sich hierzu sogenannte Awareness-Kampagnen („Aufklärungskampagnen“). Mögliche Themen, z.B. einer zwölfmonatigen Kampagne: - Soziale Medien - Virenschutz - USB, externe Geräte - Umgang mit Passwörtern - Aufmerksamkeit / Social Engineering - Abwesenheit - Kommunikation mit Externen - Sparsame Datenhaltung - Speicherorte - Das Büro – der Arbeitsplatz - Mobile Devices - Rechtliches (DSG, BayEGovG etc.) Da deren Planung und Umsetzung recht umfangreich sein kann, ist diese im Rahmen des Konzepts nur bedingt darstellbar. Eine frei verfügbare Mustervorlage einer erfolgreichen Kampagne der Stadt Oldenburg aus dem Jahr 2013 finden Sie mit allen Inhalten, Druckvorlagen etc. online. Link siehe Linkliste am Ende dieses Kapitels.		Dokumente / Anlagen: keine

8.5.1. Planung / Umsetzung	Haben Sie bereits eine langfristige Kampagne durchgeführt? Wenn nein, ist eine solche zumindest in Planung und ein zeitnaher Start vorgesehen? Konkret: Es bietet sich an, die Einführung von Informationssicherheit (die ja bekanntermaßen über einen längeren Zeitraum andauert) neben der reinen Projektkommunikation mit einer solchen Kampagne zu begleiten.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.5.2. Zusammenarbeit	Ihre Organisation ist zu klein für eine eigene Kampagne? Was spricht dagegen, diese mit anderen Gemeinden oder dem Landkreis durchzuführen? Auf die Art kostet eine solche Kampagne schnell nur einige wenige Euro oder sogar nur Cent pro Mitarbeiter – und zwar für die ganze Kampagne!		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
8.6. Handzettel / Merkblätter	Kurze und prägnante Handzettel sind ebenfalls ein unterstützendes Instrument im Rahmen einer Schulungsstrategie. Die Betonung liegt dabei auf Handzettel, nicht Handbuch! Ein Blatt (Vor- und Rückseite) mit kurzer prägnanter Darstellung der zu vermittelnden Inhalte sollte der Maximalumfang eines solchen Handzettels sein. Diese können beispielsweise bei der Einarbeitung neuer Mitarbeiter oder auch als kurze Anleitungen zu Schutzmaßnahmen zum Einsatz kommen. Formulieren Sie dabei bitte kurz und knapp. Visualisieren Sie, wo möglich.		Dokumente / Anlagen: Muster Sensibilisierung / Einweisung neue Mitarbeiter

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
8.6.1. Zuständigkeiten	Ist klar festgelegt, wer in Ihrer Organisation im Rahmen der Schulungsstrategie E-Mails verfassen und versenden darf? Sie sollten dies auf einen kleinen Kreis an Verantwortlichen beschränken (siehe auch Informationssicherheitsteam im Kapitel 1).		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Abschlusskommentar zu Kapitel 8 Schulungen und Sensibilisierungen:

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 8 Schulungen und Sensibilisierungen

Awareness-Kampagne „Wolfi“ der Stadt Oldenburg (alle Materialien – bis auf Bildrechte – stehen frei zur Verfügung)

<http://www.oldenburg.de/microsites/wolfi/wolfi.html>

BSI – M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit

<https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/content/m/m02/m02198.html>

BSI - M 3.45 Planung von Schulungsinhalten zur Informationssicherheit

<https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/content/m/m03/m03045.html>

Sicherheit beginnt im Kopf – Mitarbeiter erfolgreich sensibilisieren (Computerwoche)

<http://www.computerwoche.de/a/sicherheit-beginnt-im-kopf-mitarbeiter-erfolgreich-sensibilisieren,3068472>

Security Awareness Infopaper – mit zahlreichen Hintergrundinfos, Tipps und Tricks

<http://www.it-informationssicherheit.de/files/Security-Awareness-ISFOX-Tools-PDFs/1-Security-Awareness-Infopaper.pdf>

Dokumente / Anlagen

Muster Sensibilisierung / Einweisung neue Mitarbeiter

Kapitel 9 Externe Dienstleister / Auftragsdatenverarbeitung

Der Einsatz externer Dienstleister für Teilaufgaben oder auch die Auslagerung ganzer Aufgaben / Funktionen / Sachbereiche sind ein durchaus probates Mittel, will jedoch gut geplant sein. Einfach mal auslagern, ist in vielen Fällen die schlechteste Vorgehensweise. Mal abgesehen von entstehenden Abhängigkeiten von einem oder mehreren Dienstleistern muss das Schutzniveau des oder der Anbieter zum Schutzbedarf der betroffenen Daten passen. Dabei ist nicht nur das Datenschutzrecht im Umgang mit personenbezogenen Daten zu beachten. Darüber hinaus sind auch zahlreiche weitere Daten / Informationen schutzbedürftig. Deren Auslagerung zu oder Zugriff durch einen externen Dienstleister muss daher wohl überlegt und geplant sein. Auch wenn das Stichwort „Cloud“ heute auf viele eine magische Anziehungskraft ausübt, sind neben den rechtlichen Anforderungen zahlreiche weitere Aspekte zu prüfen.

Die Datenschutzgesetze sehen für ein Outsourcing von personenbezogenen Daten eine restriktive Vorgehensweise vor, an die Sie sich konsequent halten sollten, um Rechtsverstöße zu vermeiden. Diese Vorgehensweise findet jedoch auch auf Dienstleister Anwendung, die im Rahmen ihrer Tätigkeit für Ihre Organisation auf personenbezogene Daten zugreifen können. Damit sind Vorgänge wie Fernwartung für Hard- und Software, aber auch Vor-Ort-Wartung, das Einspielen von Updates aber auch Fehleranalyse und Support betroffen. Das Datenschutzrecht spricht beim Outsourcing von einer Auftragsdatenverarbeitung, sofern es um personenbezogene Daten geht.

Aber auch die Informationssicherheit stellt Anforderungen an den Outsourcing-Prozess. Das beginnt bei der Planung und Ausschreibung, geht über den Betrieb oder die Nutzung der Dienstleistung und endet mit der Vertragsauflösung samt Rückholung oder Löschung von Daten / Informationen.

Somit ist klar, eine strategische Vorgehensweise zur Planung, Konzeption, Prüfung und Auswahl von Dienstleistern, aber auch zur Beendigung solcher Services ist Pflicht.

Zwei gute Informationsquellen für das Thema sind die „Orientierungshilfe Auftragsdatenverarbeitung“ des Bayerischen Landesbeauftragten für Datenschutz inklusive Checkliste sowie der Baustein 1.11 Outsourcing des BSI IT-Grundschutzes. Die wichtigsten und häufigsten Punkte haben wir Ihnen hier zusammengefasst. Zur detaillierten Bearbeitung sollten Sie sich jedoch unbedingt mit diesen beiden Dokumenten beschäftigen. Die Links dazu finden Sie am Ende dieses Kapitels in der Linkliste.

Denken Sie daran: Sie bleiben für die Informationen und Daten verantwortlich, egal an wen Sie was und wieviel auslagern!

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
9. Externe Dienstleister und Auftragsdatenverarbeitung	Das bayerische Landesdatenschutzgesetz (Art. 6 BayDSG) aber auch die Verfahrensweisen zur Informationssicherheit schreiben eine besondere Vorgehensweise <u>VOR</u> dem Einsatz externer Dienstleister vor. Diese gilt nicht nur, wenn deren Tätigkeit direkt personenbezogene Daten betrifft oder durch deren Tätigkeit der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (z.B. IT-Support, Fernwartung etc.). Generell sind externe Dienstleister auf ihre Zuverlässigkeit und ihr Schutzniveau (in Bezug auf Informationssicherheit) bei Ausführung der beauftragten Leistungen für Ihre Organisation hin zu überprüfen. Dabei gilt es, zahlreiche Aspekte zu Datenschutz und Datensicherheit zu prüfen, noch bevor mit der Zusammenarbeit begonnen wird. Diese Prüfungen sind im Rahmen der sogenannten technischen und organisatorischen Maßnahmen – kurz TOM - (siehe auch Art. 7 BayDSG sowie §§ EU-DSGVO) durchzuführen. Hinweis: Die AKDB gilt als sorgfältig ausgewählt im Sinn des Art. 6 Absatz 2 Satz 1 BayDSG, vgl. Vollzugsbekanntmachung zum BayDSG vom 28.02.2001. Bitte prüfen Sie dies im Hinblick auf die zum Mai 2018 wirksam werdende EU-DSGVO, ob sich hier Änderungen ergeben.		Dokumente / Anlagen: • Vorlage Übersicht Dienstleister • Prüfliste TOM • Nachprüfung TOM

9.1. Übersicht Dienstleister	Existiert eine Übersicht der beauftragten Dienstleister für die Organisation? Bei Verfahren mit personenbezogenen Daten sollte der DSB entsprechende Übersichten haben. Für Verfahren und Leistungen ohne Bezug zu personenbezogenen Daten sind die Sachbereiche zu befragen. Ergebnis: vollständig ausgefüllte Übersicht aus Mustervorlage		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
9.2. Zulässigkeit der Auslagerung / Beauftragung	Bei allen Dienstleistungen und Services, die Sie teilweise oder ganz auf externe Dienstleister übertragen wollen, sollten Sie vorab die Sensibilität und Kritikalität der betroffenen Daten prüfen und sich Klarheit darüber verschaffen, ob die Auslagerung überhaupt rechtlich zulässig ist. Die (Nicht-) Zulässigkeit einer Auslagerung ergibt sich beispielsweise aus folgenden Gesetzen: - § 30 Abgabenordnung (AO) für Finanzdaten - § 80 Sozialgesetzbuch X (SGB) für Sozialdaten - Art. 34 Bayerisches Meldegesetz (BayMeldeG) für Meldedaten - § 203 Strafgesetzbuch (StGB) usw.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
9.3. Technische und organisatorische Maßnahmen	Wurde der externe Dienstleister vor Vertragsabschluss auf ein ausreichend hohes Niveau im Bereich Datenschutz und Datensicherheit geprüft? Konkret: Hat Ihnen der Dienstleister schriftlich dokumentiert sein Schutzniveau nachgewiesen? Alternativ haben Sie ihm die Prüfliste TOM aus diesem Konzept zur Bearbeitung und Darstellung seiner internen Schutzmaßnahmen zur Verfügung gestellt und zurückerhalten?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
9.4. Dokumentation der Prüfung	Wurden die Prüfungen und die Ergebnisse schriftlich dokumentiert? Sofern es Nachfragen an den Dienstleister gab, sind diese der Dokumentation beigelegt? Sofern das Schutzniveau nicht ausreichend nachgewiesen und belegt werden kann, muss von einer Beauftragung und Zusammenarbeit abgesehen werden!		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
9.5. Wiederholung der Prüfung	Die Prüfung aktueller technischer und organisatorischer Maßnahmen ist in regelmäßigen Abständen zu wiederholen (üblicherweise alle ein bis zwei Jahre).		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	Wird dies durchgeführt und das Ergebnis ebenfalls protokolliert? Sollten sich Verschlechterungen am Schutzniveau ergeben, sollte der Dienstleister diese zeitnah beheben. Ansonsten ist der Anbieter zu wechseln. Je sensibler die betroffenen Daten, desto kürzer sollten die Intervalle zur Nachprüfung ausfallen.		
9.6. Vereinbarung zur Auftragsdatenverarbeitung	Für die rechtskonforme Umsetzung ist eine schriftliche Vereinbarung notwendig, die über die übliche vertragliche Regelung der Zusammenarbeit wie Tätigkeit und Honorar hinausgeht. Früher übliche Klauseln wie <i>„Die Parteien vereinbaren, sich an die jeweils gültigen Datenschutzgesetze zu halten.“</i> sind nicht ausreichend. Konkret: Wurde eine der aktuellen Rechtslage entsprechende Vereinbarung mit dem Dienstleister <u>VOR</u> Aufnahme der Zusammenarbeit geschlossen?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
9.7. Überprüfen bestehender Vereinbarungen	Wurden langfristig bestehende Vereinbarungen jeweils der aktuellen Rechtslage z.B. nach Novellierungen angepasst? Sollte dies versäumt worden sein, holen Sie dies bitte nach.		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
9.8. Umfang der Vereinbarung (bei personenbezogenen Daten gesetzlich vorgeschrieben)	Regelt die Vereinbarung zur Auftragsdatenverarbeitung alle vorgeschriebenen Punkte wie z.B. - Bezeichnung des Verfahrens, - Zweck und Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung, - Art der gespeicherten Daten, - Kreis der Betroffenen, - Art der regelmäßig zu übermittelnden Daten und deren Empfänger, - Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung, - verarbeitungs- und nutzungsberechtigte Personengruppen, - im Fall des Art. 6 Abs. 1 bis 3 die Auftragnehmer, [Auftragsdatenverarbeitung], - Empfänger vorgesehener Datenübermittlungen in Drittländer?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
9.9. Einbindung in Strategie zur Informations-sicherheit	Haben Sie den Dienstleister (unabhängig von einer Auftragsdatenverarbeitung) zur Einhaltung der Vorschriften zur Informationssicherheit Ihrer Organisation unterworfen, ihm die		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar

	notwendigen Vorschriften bekanntgemacht und ihn in den Geltungsbereich der Leitlinie eingebunden?		☐ Aktuell in Arbeit
9.10. Verhaltensrichtlinie intern / extern	Gibt es klare Anweisungen, wie der Dienstleister sich bei Vor-Ort-Tätigkeiten zu verhalten hat und wird deren Einhaltung durch Ihre Organisation überprüft? • Vorherige Anmeldung der Vor-Ort-Tätigkeit oder einer Fernwartung? • Bewegen innerhalb der Räumlichkeiten nur in Begleitung eines zuständigen Mitarbeiters? Keine unbeaufsichtigten Aktivitäten im Haus? • Protokollierung von Fernzugriffen und Tätigkeiten? Im Zweifel Beaufsichtigen der Remote-Sitzungen? • Abmelden nach Abschluss der Tätigkeiten? • Anfertigen eines Tätigkeitsprotokolls? • Bei Bedarf: Verpflichtungen auf Datengeheimnis und / oder zur Vertraulichkeit bei Betreten des Gebäudes? • Identitätsfeststellung vor Ort? Prüfen auf Vorliegen eines gültigen Auftrags für die Tätigkeit?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
9.11. Einbindung des Teams für Informations-sicherheit (sofern vorhanden)	Wurde das Team oder einzelne Mitglieder daraus in die Auswahl geeigneter Dienstleister herangezogen? Wenn nein, warum nicht?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
9.12. Ausschreibung	Wurde / wird bei Anforderung eines Angebots oder im Rahmen einer Ausschreibung auf die Notwendigkeit des Nachweises des Schutzniveaus und bei personenbezogenen Daten auf den Abschluss einer Vereinbarung zur Auftragsdatenverarbeitung hingewiesen? Sind diese Kriterien als KO-Punkte definiert? (Wer diese nicht erfüllen kann / will, scheidet aus der Runde der Anbieter automatisch aus.)		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
9.13. Leistungsfähigkeit des Anbieters	Haben Sie sich im Vorfeld von der Leistungsfähigkeit des Anbieters überzeugt? Ist dieser überhaupt in der Lage, die vereinbarten und zugesagten Leistungen zu erbringen? Verfügt der Anbieter über ausreichend personelle, materielle und zeitliche Ressourcen für die Erbringung der Dienstleistung?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit
9.14. Abhängigkeit	Gerade bei der Auslagerung ganzer Verfahren oder Bereiche (beispielsweise IT-Support) entstehen große Abhängigkeiten für Sie als Auftraggeber. Haben Sie diese Abhängigkeiten bei Ihrer Outsourcing-Strategie entsprechend berücksichtigt? Und haben Sie bereits		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

	vor der Auslagerung Maßnahmen getroffenen und Bedingungen vereinbart, wie die Auslagerung wieder rückgängig gemacht werden kann? Denken Sie dabei bitte auch an Datenrückholung und / oder Migration zu anderen Anbietern.		
--	---	--	--

Abschlusskommentar zu Kapitel 9 Externe Dienstleister / Auftragsdatenverarbeitung:

Abschlussbewertung

- ☐ Ohne Mängel, kein Handlungsbedarf
- ☐ Wenige Mängel, es besteht Handlungsbedarf
- ☐ Zahlreiche Mängel, diese sollten zeitnah abgestellt werden
- ☐ Gravierende Mängel, akuter Handlungsbedarf

Linkliste 9 Externe Dienstleister / Auftragsdatenverarbeitung

Mustervordruck Auftragsdatenverarbeitung des Bayerischen Landesbeauftragten für Datenschutz

<https://www.datenschutz-bayern.de/technik/orient/m-vertr.htm>

Orientierungshilfe Auftragsdatenverarbeitung des Bayerischen Landesbeauftragten für Datenschutz inklusive Checkliste

https://www.datenschutz-bayern.de/technik/orient/oh_auftragsdatenverarbeitung.html

BSI IT-Grundschutz Baustein 1.11 Outsourcing

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01011.html

Artikel 6 BayDSG Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

http://byds.juris.de/byds/009_1.1_DSG_BY_1993_Art6.html

Heckmann, C3-Cloud Computing für Kommunen, <http://www.bay-innovationsstiftung.de/index.php?id=62>

Dokumente / Anlagen

Prüfliste technische und organisatorische Maßnahmen

Nachprüfung technische und organisatorische Maßnahmen beim Dienstleister nach x Monaten

