ToM der KSM Kommunalservice Mecklenburg Aör

Version 24.10.2017 (11:39:17)

Durchgeführt bei der Verbund SIS - Schweriner IT- und Servicegesellschaft mbH am 24.10.2017

Mandant: KSM Kommunalservice Mecklenburg AöR

Hier werden die Technisch-organisatorischen Maßnahmen der KSM Kommunalservice Mecklenburg AöR dokumentiert.

1. Präambel

Die EU-Datenschutzgrundverordnung (DSGVO) schreibt vor, dass unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Es ist ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzurichten. Diese Aufgabe wird durch die vorliegende Prüfung umgesetzt und dokumentiert.

Der vorliegende Bericht basiert auf den derzeitigen Einschätzungen und Aussagen der am Workshop teilnehmenden Mitarbeiter.

Version	**Bemerkungen**	**Stand**
24.10.2017 (11:39:17)	Audit	24.10.2017

(hier können die Versionen der Prüfung eingetragen werden)

2. Teilnehmer

Teilnehmer	Rolle
Parton, Claudia ITSiBe	Prüfer
Block, Marco DSB	Auskunftsperson

(hier können die an der Prüfung teilnehmenden Personen eingetragen werden)

Die vorliegenden Ergebnisse wurden gemeinsam mit den oben genannten Teilnehmern im Rahmen eines Workshops/einer online-Prüfung am 24.10.2017 erarbeitet.

3. Ergebnisse im Detail

3.1Zutrittskontrolle

Eine wirksame Zutrittskontrolle minimiert folgende Risiken:
- Verlust von Datenverarbeitungsanlagen (auch durch Zerstörung)
- Beschädigung von Datenverarbeitungsanlagen
- unberechtigte Beeinträchtigung / Kompromittierung von Datenverarbeitungsanlagen
- Unterbrechungen der Unternehmenstätigkeit

Eine wirksame Zutrittskontrolle hält unbefugte Dritte von Datenverarbeitungsanlagen physisch fern. Sie stellt sicher, dass nur autorisierte Personen Zutritt zu den Datenverarbeitungsanlagen erhalten. Auf diese Weise erlangen Unbefugte keine Kenntnis von personenbezogenen Daten.
Vgl. auch ISO 27001, Annex A.9.1.2 "Zutrittskontrolle"

3.1.1 Zutrittskontrolle baulich

In diesem Unterkapitel sind die baulich-technischen Maßnahmen zur Unterstützung einer wirksamen Zutrittskontrolle aufgeführt.

Dokumentation Zutrittskontrollmaßnahmen

(Zutrittskontrolle / Zutrittskontrolle baulich)

Liegt eine Beschreibung / Dokumentation der gesamten am Standort eingesetzten Zutrittskontrollmaßnahmen vor?

Erläuterung: Unter Zutrittskontrolle versteht man alle Maßnahmen, die geeignet sind, Unbefugten das Eindringen in geschützte Bereiche zu erschweren. Die Spannweite reicht von einer einfachen Schlüsselvergabe bis zu aufwändigen Identifizierungssystemen mit Personenvereinzelung, wobei auch die Nutzung eines mechanischen Schlüssels nebst Schloss eine Zutrittsregelung darstellt.
Zutrittskontrollen sind nur dann wirksam, wenn es keine ungesicherten Zu- / Ausgänge oder andere Zutrittsmöglichkeiten gibt, z.B. über die Kantine etc.

Kommentar: Regelungen vorhanden. Gesonderte Regleungen für den RZ-Bereich.
(Doku: OR_107_1.1_SIS-KSM Zutrittsregelung)

Ergebnis: **Ja** 20 Punkt(e) (100%)

Existenz maschineller Zutrittskontrollsysteme

(Zutrittskontrolle / Zutrittskontrolle baulich)

Existieren maschinelle Zutrittskontrollsysteme?

Erläuterung: Gibt es am Standort maschinelle Zutrittskontrollsysteme zur Überwachung des Betretens und evtl. auch Verlassens eines Gebäudes / eines Gebäudeteils?
Werden eventuell biometrische Kontrollsysteme (Handflächen, Iris-Scanner, Fingerabdruck-Leser) eingesetzt, die durch die Überprüfung eines Personenmerkmals eine höhere Sicherheitsstufe darstellen?

Kommentar: Vorhanden. Keine biometrischen Systeme im Einsatz.
(Doku: OR_107_1.1_SIS-KSM Zutrittsregelung)

Ergebnis: **Ja** 4 Punkt(e) (100%)

Wartung und Verwaltung maschineller Zutrittskontrollsysteme

(Zutrittskontrolle / Zutrittskontrolle baulich)

Ist die Verwaltung und Wartung der maschinellen Zutrittskontrollsysteme geregelt und dokumentiert?

Erläuterung: Die verantwortliche Stelle soll folgende Fragen geregelt und dokumentiert haben:
- Wer ist für die Verwaltung (z.B. Durchführung von Berechtigungsänderungen) verantwortlich?
- Wer ist für die Wartung (Überprüfung der Funktionsfähigkeit) verantwortlich?
- Liegt die Wartung und Verwaltung innerhalb der verantwortlichen Stelle?
- Gibt es externe Dienstleister für die Verwaltung und Wartung?
- In welchen Abständen führt die verantwortliche Stelle die Wartung durch?
- Protokolliert die verantwortliche Stelle die Ergebnisse der Wartung?

Kommentar: Doku: OR_107_1.1_SIS-KSM Zutrittsregelung

Ergebnis: **Ja** 4 Punkt(e) (100%)

Protokollierung der Zugänge / Abgänge

(Zutrittskontrolle / Zutrittskontrolle baulich)

Werden in den Zutrittskontrollanlagen personenbezogene Daten gespeichert, so dass nachvollziehbar ist, wer wann einen bestimmten räumlichen Bereich betreten und ggf. auch wieder verlassen hat?

Erläuterung: Die Protokollierung der Zugänge und Abgänge erlaubt es der verantwortlichen Stelle nach einem Zwischenfall Rückschlüsse auf etwaige unberechtigte Zutritte zu ziehen und gegebenenfalls den Täter zu ermitteln.

Kommentar: Im Verantwortungsbereich ZD und bei den Stadtwerken für die gemieteten Gebäude. Einsicht in die Protokolle nur mit DS, BR,PR

Ergebnis: **Ja** 4 Punkt(e) (100%)

An- u. Ablieferungen Sicherheitssystem

(Zutrittskontrolle / Zutrittskontrolle baulich)

Wird durch die An- und Ablieferung von Datenträgern, Belegen, Listen usw. das Sicherheitssystem nicht durchbrochen?

Erläuterung: Übergabepunkte und Ladezonen sollten von den Räumen, in denen die Datenverarbeitungsanlagen untergebracht sind, möglichst separiert werden. Vgl. ISO 27001, Annex A.9.1.6 „Öffentlicher Zugang, Anlieferungs- und Ladezonen“

Kommentar: Regelungen in den einzelnen Bereichen vorhanden. (z.B. Datenschutztonnen für Papier, verschlossener Behälter für HD´s, usw.)

Ergebnis: **Ja** 4 Punkt(e) (100%)

Umfang Gebäude-Sicherheitskonzept

(Zutrittskontrolle / Zutrittskontrolle baulich)

Gibt es ein ausreichendes Gebäude-Sicherungskonzept, welches auf die Zutrittsmöglichkeiten eingeht?

Erläuterung: Bei dem Gebäude-Sicherheitskonzept zu berücksichtigende Punkte sind insbesondere:
- Bebauungsart: freistehender Gebäudekomplex, geschlossene Bebauung
- Werksgelände vorhanden oder nicht vorhanden?
- Grundstück umzäunt (eingezäunt) oder offen zugänglich?
- Evtl. Zutrittsmöglichkeiten über Aufzüge, Treppen, Versorgungsschächte und Notausgänge?

Das IT-Sicherheitskonzept ist das "zentrale" Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen.
Das Gebäude-Sicherungskonzept sollte entweder ein Unterkapitel des IT-Sicherheitskonzepts oder ein eigenständiges Dokument sein, auf welches im IT-Sicherheitskonzept verwiesen wird.
In der aktuellen Version des Gebäude-Sicherheitskonzepts sollten mindestens die o.g. Punkte zu den Zutrittsmöglichkeiten adressiert werden.

Kommentar: (Doku: OR_107_1.1_SIS-KSM Zutrittsregelung)

Ergebnis: **Ja** 20 Punkt(e) (100%)

Sicherheitszonen im Gebäude-Sicherheitskonzept

(Zutrittskontrolle / Zutrittskontrolle baulich)

Sind Sicherheitszonen unterschiedlicher Klassifizierung und Sensibilität vorgesehen? Sind diese im Gebäude-Sicherungskonzept ausreichend genau beschrieben?

Erläuterung: Da zu schützende Bereiche wie etwa Grundstücke, Gebäude, Serverräume, Räume mit Peripheriegeräten, Archive, Kommunikationseinrichtungen oder die Haustechnik unterschiedliche Sicherheitsanforderungen aufweisen, ist es sinnvoll, diese in sog. Sicherheitszonen aufzuteilen.
Nicht alle eingerichteten Sicherheitszonen sind gleichermaßen gefährdet. So sollte z.B. die Nutzung der firmeneigenen Besucherparkplätze kontrolliert werden, jedoch ist eine Kameraüberwachung und eine Speicherung der KFZ-Kennzeichen i.d.R. nicht erforderlich.

Kommentar: (Doku: OR_107_1.1_SIS-KSM Zutrittsregelung)

Ergebnis: **Ja** 4 Punkt(e) (100%)

Existenz nicht maschineller Zutrittskontrollen

(Zutrittskontrolle / Zutrittskontrolle baulich)

Existieren angemessene, nicht maschinelle Zutrittskontrollen zu dem Gebäude?

Erläuterung: Nicht maschinelle Maßnahmen zur Zutrittskontrollen sind solche Maßnahmen, die in der Regel mechanisch bedient werden, um den Zutritt zu einem Gebäude oder einem Raum zu erlangen.
Hierunter können folgende Maßnahmen fallen:
- Türen mit einfachen Schlössern
- Türen mit Sicherheitsschlössern
- per Hand ausgelöste elektro-mechanische Sperren (Öffnen einer Tür durch den Pförtner durch "Summer")

Kommentar: Alle Türen sind mit Sicherheitsschlössern versehen. (Computer-programmierbare Schlüssel.)

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.1.2 Zutrittskontrolle organisatorisch

In diesem Unterkapitel sind die organisatorischen Maßnahmen zur Unterstützung einer wirksamen Zutrittskontrolle aufgeführt.

Existenz Schlüssel- und Schließordnung

(Zutrittskontrolle / Zutrittskontrolle organisatorisch)

Existiert eine Schlüssel- und Schließordnung, die das Verschließen bestimmter Räume, die Hinterlegung von Ersatzschlüsseln (insbesondere nach Dienstschluss), die Führung einer revisionsfähigen Schlüsselliste und die Verwendung von Ersatzschlüsseln regelt?

Erläuterung: Liegt für alle Schlüssel des Gebäudes (von Etagen, Fluren und Räumen) ein Schließplan vor? Ist die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln zentral geregelt und dokumentiert? Sind Reserveschlüssel vorhanden und gesichert aufbewahrt? Das gleiche gilt auch für alle Identifikationsmittel wie Magnetstreifen- oder Chipkarten.

Kommentar: ZD und GF-Sekretariat, (Doku: OR_107_1.1_SIS-KSM Zutrittsregelung)

Ergebnis: **Ja** 20 Punkt(e) (100%)

3.1.3 Rechnerräume ("Closed Shop" - Betrieb)

Mit "Closed Shop" - Betrieb wird der Zustand bezeichnet, bei dem nur berechtigte Personen Zutritt zu den Räumlichkeiten haben, in dem sich die zentralen EDV-Systeme des Unternehmens befinden.

Anzahl Eingänge

(Zutrittskontrolle / Rechnerräume ("Closed Shop" - Betrieb))

Sind möglichst wenig Eingänge zum Rechnerraum / zu den Rechnerräumen vorhanden?

Erläuterung: Eine geringe Zahl von Eingängen führt zu einer besseren Kontrolle der Zugänge und Abgänge zu dem Rechnerraum.
Eingänge - wie beispielsweise Türen - bieten grundsätzlich eine Schwachstelle zum Eindringen in einen Raum. Sofern mehrere Eingänge vorhanden sind, muss die verantwortliche Stelle darauf achten, dass alle Zugänge das gleich hohe Schutzniveau bieten. Da sich ein Eindringling grundsätzlich die schwächste Stelle für einen Einbruchsversuch aussuchen wird, richtet sich die Beurteilung der Zutrittssicherung zum Rechnerraum nach dem am schwächsten gesicherten Eingang.

Kommentar: Betriebshandbuch RZ und Pläne RZ

Ergebnis: **Ja** 4 Punkt(e) (100%)

Existenz Raumüberwachung

(Zutrittskontrolle / Rechnerräume ("Closed Shop" - Betrieb))

Wurden Maßnahmen zur Raumüberwachung getroffen (Videokameras / Bewegungsmelder)?

Erläuterung: Unzulässige Zutritte zu Rechnerräumen sollten möglichst sofort feststellbar sein. Dies können bereits Bewegungsmelder leisten oder entsprechende Benachrichtigungen,

wenn die Tür(en) zum Rechnerraum geöffnet wird/werden. Sofern festgestellt werden soll, wer sich in den Rechnerräumen aufgehalten hat, kann hierfür ggfls. eine Videoüberwachung installiert werden.
Hinweis:
Wenn eine Videoüberwachung installiert ist, so ist diese auf Konformität zum Datenschutz zu überprüfen.
Die Videoüberwachung greift je nach Gestaltung der Anlage in die Rechte und Freiheiten der betroffenen Personen ein. Insbesondere das Recht auf freie Entfaltung der Persönlichkeit kann betroffen sein. Es ist daher vor der Inbetriebnahme einer Video-Überwachungsanlage zu prüfen, ob eine Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO erforderlich ist.

Kommentar: Betriebshandbuch RZ

Ergebnis: **Ja** 4 Punkt(e) (100%)

Aufstellungsort Server

(Zutrittskontrolle / Rechnerräume ("Closed Shop" - Betrieb))

Werden die Unternehmensserver in einem abgeschlossenen und zutrittsgesicherten Raum betrieben?

Erläuterung: Die Server bilden in der Regel das Herzstück des EDV-Betriebs eines Unternehmens. Eine Zerstörung oder Manipulation der Server kann zu einer erheblichen Unterbrechung des Geschäftsbetriebes führen. Ein Diebstahl führt in der Regel zu einem Bekanntwerden von personenbezogenen Daten bei unberechtigten Dritten. Dies kann zu einer Informationspflicht nach Artikel 33 und Artikel 34 DS-GVO führen.

Kommentar: RZ

Ergebnis: **Ja** 4 Punkt(e) (100%)

Regelung Zutritt Rechnerraum / Serverraum

(Zutrittskontrolle / Rechnerräume ("Closed Shop" - Betrieb))

Besteht Zutritt zum Rechnerraum / Serverraum nur für Befugte?

Erläuterung: Der Rechner- bzw. Serverraum ist ein sicherheitsrelevanter Bereich; daher sollten dort nur die Administratoren der dort aufgestellten IT-Systeme Zutritt haben. Durch eine darauf abgestimmte Zutrittsregelung muss für eigene Mitarbeiter und, wichtiger noch, für nur zeitweilig Beschäftigte, welche z. B. zu Wartungsarbeiten die Rechnerräume betreten, sichergestellt werden, dass sie keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten.
Technisch wird diese Anforderung durch Schließanlagen erfüllt. Ausschließlich Personen, die im Besitz des Schlüssels oder - bei elektronischen Schließanlagen - einer gültigen Codekarte sind, dürfen sich Zugang zu den Räumen verschaffen können.

Kommentar: OR 107 und Betriebshandbuch RZ

Ergebnis: **Ja** 4 Punkt(e) (100%)

Festlegung Zutrittsbefugter Personen
(Zutrittskontrolle / Rechnerräume ("Closed Shop" - Betrieb))

Erfolgt eine Festlegung der zutrittsberechtigten Personen?

Erläuterung: Gibt es schriftliche Dokumentationen darüber, wer eine Zutrittsbefugnis zum Rechenzentrum/ Rechnerraum hat?
Sind auch die Gründe für die Zutrittsbefugnis dokumentiert?
Zutrittsberechtigungen erlauben der betroffenen Person, bestimmte IT-Systeme bzw. System-Komponenten physisch zu erreichen. Dies ist für jede zutrittsberechtigte Person auf Grund ihrer Funktion, möglichst unter Beachtung der Funktionstrennung, im Einzelnen festzulegen.
Ergänzend hierzu muss sichergestellt sein, dass personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.

Kommentar: Zutrittsregelung in OR 107

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.2Zugangskontrolle

Die Zugangskontrolle soll die unbefugte Nutzung von Datenverarbeitungssystemen verhindern.
Die Zugangskontrolle knüpft an das Datenverarbeitungssystem an, während die Zutrittskontrolle an die Datenverarbeitungsanlage anknüpfte.
Bei der Zugangskontrolle geht es um den Zugang unberechtigter Personen zu dem Datenverarbeitungssystem, wohingegen es bei der Zugriffskontrolle (nächster Fragenblock) um den Zugriff grundsätzlich berechtigter Personen mit Zugang zu dem System außerhalb ihrer Berechtigungsstufe geht.

3.2.1 Zugangskontrollmaßnahmen

Dieses Unterkapitel enthält Fragen zu den übergreifenden Richtlinien und Verfahren der Zugangskontrolle.
Die Zugangskontrolle knüpft an das Datenverarbeitungssystem an. Daher ist auch der Zugang zu dem Datenverarbeitungssystem über Fernkommunikation in die Betrachtung einzubeziehen. Hierdurch unterscheidet sich die Zugangskontrolle durch die Zutrittskontrolle, welche an die physische Datenverarbeitungsanlage anknüpft.
Beispiel: Die Reinigungskraft hat Zutritt zu Rechnerräumen aber keinen Zugang zu dem Datenverarbeitungssystem.

Regelwerk zur Zugangskontrolle
(Zugangskontrolle / Zugangskontrollmaßnahmen)

Benutzerregistrierung
(Zugangskontrolle / Zugangskontrollmaßnahmen)

Gibt es für alle Informationssysteme und Dienste eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen?

Erläuterung: Vgl. ISO 27001, Annex A.11.2.1: "Benutzerregistrierung"

Kommentar: Im Bereich ZD

Ergebnis: **Ja** 20 Punkt(e) (100%)

Zugriffskontrolle

Die verantwortliche Stelle muss angemessene Maßnahmen treffen, um sicherzustellen, dass Nutzer ausschließlich auf solche personenbezogenen Daten zugreifen können, die ihrer Zugriffsberechtigung unterliegen.
Eine wirksame Zugriffskontrolle minimiert das Risiko, dass personenbezogene Daten bei der Verarbeitung und Nutzung unbefugt gelesen, kopiert, verändert oder entfernt werden.

3.2.2 Zugriffsschutzmaßnahmen

Dieses Unterkapitel enthält Fragen zu den anwenderseitigen Zugriffsschutzmaßnahmen und zum Zugriffsschutz durch kryptographische Maßnahmen.

Cleen Desk / Clear Screen Policy

(Zugriffskontrolle / Zugriffsschutzmaßnahmen)

Wird der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms gelebt?

Erläuterung: Weder in Papierform vorhandene noch auf Datenträgern abgelegte personenbezogene Informationen sollten längere Zeit auf dem Schreibtisch des Nutzers verbleiben. Sobald die Unterlagen nicht mehr benötigt werden, sollten die Unterlagen und Datenträger - je nach Sensibilität - in Schränken oder Safes weggeschlossen werden. Das Prinzip lässt sich auch auf den digitalen "Desktop" des Nutzers übertragen. Vgl. ISO 27001, Annex A.11.3.3 „Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms“

Kommentar: Merkblatt und Datenschutzbegehungen

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.2.3 Sichere Entsorgung oder Weiterverwendung von Datenträgern / Sichere Löschung von Dokumenten

Zu den Maßnahmen der Zugriffskontrolle zählt auch die datenschutzgerechte Entsorgung von nicht mehr benötigten oder defekten Datenträgern.

Entsorgung von Papierdokumenten und Datenträgern

(Zugriffskontrolle / Sichere Entsorgung oder Weiterverwendung von Datenträgern / Sichere Löschung von Dokumenten)

Gibt es eine Anweisung darüber, wie mit nicht mehr benötigten Datenträgern umzugehen ist (dazu gehört auch beschriebenes oder bedrucktes Papier)?

Erläuterung: Vgl. ISO 27001, Annex A.10.7.2 „Entsorgung von Medien“:
Entsprechende verschließbare Tonnen sollten für Papierdokumente und Datenträger vorhanden sein und regelmäßig geleert werden. Die Mitarbeiter sind über die Notwendigkeit der ordnungsgemäßen Entsorgung und das Vorgehen zu informieren.

Kommentar: Merkblatt, OR 101 Netzsicherheit

Ergebnis: **Ja** 12 Punkt(e) (100%)

Sichere Entsorgung oder Weiterverwendung von mit Speichermedien ausgestatten Geräten

(Zugriffskontrolle / Sichere Entsorgung oder Weiterverwendung von Datenträgern / Sichere Löschung von Dokumenten)

Gibt es eine Anweisung darüber, wie bei der Entsorgung oder Weiterverwedung von Geräten vorzugehen ist, die mit Speichermedien ausgerüstet sind?

Erläuterung: Auch Multifunktionsgeräte wie Scanner-, Fax- und Druckereinheiten können über eingebaute Speichermedien verfügen, auf denen sich noch Dokumente befinden. Vor der Entsorgung oder Weiterverwendung ist sicherzustellen, dass hierdurch keine personenbezogene Daten an unberechtigte Dritte weitergegeben werden.
Vgl. ISO 27001, Annex A.9.2.6 „Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln“

Kommentar: OR_101_Sicherheitsrichtlinie Netzwerk

Ergebnis: **Ja** 12 Punkt(e) (100%)

Beachtung von Aufbewahrungsfristen

(Zugriffskontrolle / Sichere Entsorgung oder Weiterverwendung von Datenträgern / Sichere Löschung von Dokumenten)

Ist sichergestellt, dass Dokumente und Datenträger, deren Aufbewahrungsfrist abläuft, nachhaltig vernichtet bzw. gelöscht werden?

Erläuterung: Dokumente und / oder Datenträger sind erst nach Ablauf, aber dann zuverlässig, zu löschen oder zu vernichteten. Wird das nicht konsequent umgesetzt, so können vorgefundene veraltete Daten und Dokumente z.B. bei Betriebsprüfungen oder Ermittlungsverfahren als Beweismittel verwertet werden.

Kommentar: Überprüfung durch den DSB

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.3Weitergabekontrolle

Die Weitergabekontrolle hat zwei Ziele:
1.
Es soll verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder entfernt werden können.
2.
Es soll überprüfbar dokumentiert werden, welche Empfänger personenbezogene Daten durch Einrichtungen zur Datenübertragung erhalten sollen.
Typische Fälle der Weitergabekontrolle im betrieblichen Alltag sind:
- Die Weitergabe von Gehaltsdaten an ein externes Steuerbüro
- Die Weitergabe von Unternehmensdaten an einen externen Archiv-Dienstleister
- Die Übergabe von Datenträgern an einen externen Dienstleister zwecks Wartung oder Fehleranalyse

3.3.1 Datenschutzbeauftragter (Artikel 37 bis 39 DS-GVO + nationales Recht)

Während die bisher abgefragten Themengebiete Zutritts, Zugangs- und Zugriffskontrolle rein technisch betrachtet und vom Unternehmen relativ stringent vorgegeben werden können, spielen die organisatorischen Maßnahmen und die Verantwortung der Mitarbeiter eine ungleich größere Rolle.
Jeder Mitarbeiter, der umfassende Zugriffsmöglichkeiten auf technische und personenbezogene Daten im Unternehmen hat und wohlmöglich über einen Internet-Zugang verfügt, kann mit einem unbedachten Mausklick wesentliche Informationswerte aus dem Unternehmen (unfreiwillig) preisgeben und damit unter Umständen einen schwerwiegenden Gesetzesverstoß begehen.
Der Datenschutzbeauftragte kontrolliert nicht nur die Einhaltung der für das Unternehmen einschlägigen Datenschutzvorschriften und die ordnungsgemäße Anwendung der Datenverarbeitung, er schult und sensibilisiert die Mitarbeiter zudem auf die Belange des Datenschutzes. Daher geht der Fragenkatalog an dieser Stelle auf den Datenschutzbeauftragten und seine Stellung innerhalb der Organisation ein.

Datenschutzbeauftragter

(Weitergabekontrolle / Datenschutzbeauftragter (Artikel 37 bis 39 DS-GVO + nationales Recht))

Wurde ein Datenschutzbeauftragter bestellt?

Erläuterung: Der Datenschutzbeauftragte ist eine Person, die beauftragt wurde, sich um die Einhaltung der Regeln und Gesetze des Datenschutzes zu kümmern und im Unternehmen in erster Linie beratend und überwachend tätig wird.
Die Voraussetzungen zur Bestellung sowie die Aufgaben des oder der Datenschutzbeauftragten ergeben sich aus den Artikeln 37 bis 39 der Datenschutz-Grundverordnung und können durch das nationale Recht der Mitgliedsstaaten ergänzt und ausgestaltet werden.

Kommentar: .

Ergebnis: **Ja** 4 Punkt(e) (100%)

Interessenskonflikte

(Weitergabekontrolle / Datenschutzbeauftragter (Artikel 37 bis 39 DS-GVO + nationales Recht))

Bestehen zwischen der Tätigkeit als Datenschutzbeauftragter und weiteren Tätigkeiten keine Interessenkonflikte?

Erläuterung: Interessenskonflikte treten beispielsweise auf, wenn der Datenschutzbeauftragte gleichzeitig IT-Leiter ist. Ungünstig sind alle Positionen, in denen sich der Datenschutzbeauftragte selbst überwachen müsste.

Kommentar: .

Ergebnis: **Ja** 4 Punkt(e) (100%)

Fachkunde und Zuverlässigkeit

(Weitergabekontrolle / Datenschutzbeauftragter (Artikel 37 bis 39 DS-GVO + nationales Recht))

Besitzt der Datenschutzbeauftragte die notwendige Fachkunde und Zuverlässigkeit?

Erläuterung: Ein/e Datenschutzbeauftragte/r muss Kenntnisse haben
- zur Anwendung des Datenschutzrechts
- über Informationstechnologie
- über Betriebsorganisation

Das Maß der erforderlichen Fachkunde richtet sich nach den Erfordernissen der jeweiligen Stelle.

Kommentar: .

Ergebnis: **Ja** 4 Punkt(e) (100%)

Schriftform

(Weitergabekontrolle / Datenschutzbeauftragter (Artikel 37 bis 39 DS-GVO + nationales Recht))

Ist der Datenschutzbeauftragte schriftlich bestellt/benannt worden?

Erläuterung: Gemäß Artikel 37 muss der Verantwortliche eine/n Datenschutzbeauftragte/n für den Datenschutz benennen. Eine bestimmte Form ist in der DS-GVO nicht vorgeschrieben. Es ist im Hinblick auf die Nachweisbarkeit allerdings dringend zu empfehlen, die Benennung des oder der Datenschutzbeauftragten in Schriftform vorzunehmen.

Kommentar: Bestellurkunde liegt vor. 1.1.2016/25.05.2018

Ergebnis: **Ja** 4 Punkt(e) (100%)

Veröffentlichung der Kontaktdaten des/der Datenschutzbeauftragten

(Weitergabekontrolle / Datenschutzbeauftragter (Artikel 37 bis 39 DS-GVO + nationales Recht))

Hat der Verantwortliche die Kontaktdaten des oder der Datenschutzbeauftragten veröffentlicht?

Erläuterung: Eine Veröffentlichung kann etwa über die Homepage des Unternehmens, oder Unternehmens-Kontaktlisten usw. erfolgen.

Kommentar: .

Ergebnis: **Ja** 4 Punkt(e) (100%)

Benennung gegenüber der zuständigen Aufsichtsbehörde

(Weitergabekontrolle / Datenschutzbeauftragter (Artikel 37 bis 39 DS-GVO + nationales Recht))

Hat der Verantwortliche die Kontaktdaten des oder der Datenschutzbeauftragten gegenüber der zuständigen Aufsichtsbehörde mitgeteilt?

Erläuterung: Der Verantwortliche ist verpflichtet, die Kontaktdaten des oder der Datenschutzbeauftragten gegenüber der zuständigen Aufsichtsbehörde für Datenschutz mitzuteilen.

Kommentar: .

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.3.2 Verpflichtung der Mitarbeiter auf das Datengeheimnis

Beschäftigte dürfen personenbezogene Daten nur dann erheben, verarbeiten oder nutzen, wenn dies in Einklang mit den Datenschutzgesetzen geschieht. Eine unzulässige Erhebung, Verarbeitung und Nutzung kann Bußgelder nach sich ziehen, zu Schadenersatzansprüchen oder gar zu einer strafrechtlichen Sanktion führen.
Die Beschäftigten sind darauf zu verpflichten, Daten nur zulässig zu erheben, zu verarbeiten oder zu nutzen (Verpflichtung auf das Datengeheimnis).
Die Verpflichtung auf das Datengeheimnis geht über eine bloße Verschwiegenheitsverpflichtung hinaus. Die wirksame Verpflichtung auf das Datengeheimnis muss mit einem Hinweis auf mögliche Konsequenzen einhergehen.
In der Regel wird die Verpflichtung durch eine unterzeichnete Erklärung des Beschäftigten dokumentiert. Auch wenn in der DS-GVO die Pflicht zur Verpflichtung auf das Datengeheimnis nicht mehr ausdrücklich geregelt ist, ist es im Hinblick auf die Schulung und Sensibilisierung der Mitarbeiter empfehlenswert, diese bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Verpflichtung

(Weitergabekontrolle / Verpflichtung der Mitarbeiter auf das Datengeheimnis)

Wurden alle Personen, die mit der Verarbeitung/Nutzung personenbezogener Daten beschäftigt sind, zur Einhaltung auf das Datengeheimnis verpflichtet?

Erläuterung: Existieren von allen Mitarbeitern, die mit der Verarbeitung von personenbezogenen Daten befasst sind, Verpflichtungserklärungen zur Wahrung des Datengeheimnisses? Ist ein Verfahren etabliert, wie vorzugehen ist, wenn sich ein Beschäftigter weigert, die Verpflichtungserklärung zu unterzeichnen?
Vgl. ISO 27001, Annex A.6.1.5 „Vertraulichkeitsvereinbarungen“

Kommentar: Bei Einstellung, Durchführung von Schulungen

Ergebnis: **Ja** 4 Punkt(e) (100%)

Informationsmaterial

(Weitergabekontrolle / Verpflichtung der Mitarbeiter auf das Datengeheimnis)

Werden allen neuen Mitarbeitern bei der Verpflichtung auf das Datengeheimnis Informationen zum Datenschutz ausgehändigt?

Erläuterung: Ohne eine entsprechende Informationsschrift ist die Wahrscheinlichkeit sehr hoch, dass die Verpflichtung nicht wirksam vorgenommen wird und den Mitarbeitenden die Reichweite des Datengeheimnisses nicht bekannt ist.
Der Beschäftigte muss über seine Obliegenheiten und Pflichten informiert werden.

Kommentar: .

Ergebnis: **Ja** 4 Punkt(e) (100%)

Erläuterung

(Weitergabekontrolle / Verpflichtung der Mitarbeiter auf das Datengeheimnis)

Wurden allen Beteiligten die Belange der Datensicherheit und des Datenschutzes erläutert?

Kommentar: .

Ergebnis: **Ja** 4 Punkt(e) (100%)

Datenschutzschulungen

(Weitergabekontrolle / Verpflichtung der Mitarbeiter auf das Datengeheimnis)

Sind die Mitarbeiter, die personenbezogene Daten verarbeiten/nutzen, durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz geschult worden?

Erläuterung: Zuständig für die Schulung der Mitarbeiter auf den Datenschutz ist der Beauftragte für den Datenschutz.

Kommentar: .

Ergebnis:	**Ja**	4 Punkt(e) (100%)
Ergebnis:	**Ja**	4 Punkt(e) (100%)

3.4Eingabekontrolle

Mit der Eingabekontrolle soll gewährleistet werden, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.
Um dieses gewährleisten zu können, müssen sicherheitsrelevante Abläufe und alle Vorgänge, die Personendaten betreffen, durch das System protokolliert (geloggt) werden.
Um später einwandfrei nachweisen zu können, wer personenbezogene Daten eingegeben, verändert oder entfernt hat, müssen Log-Dateien so aufgebaut sein, dass ein späteres Verändern sofort auffällt. Zudem müssen die Log-Dateien gegen unbefugtes Löschen geschützt werden.
Zu den Bestandteilen von Log-Dateien gehören Aufzeichnungen aller Login-Versuche, egal ob erfolgreich oder nicht, alle Logouts, Veränderungen oder Erneuerungen bei Passwörtern, Zugriffe auf Dateien und die Installation oder Deinstallation von Software.
Da die Protokollierung selbst wiederum den datenschutzrechtlichen Bestimmungen entsprechen sollte, ist im Verfahrensverzeichnis zu dokumentieren, wo und was protokolliert wird (Webserver, Proxy-Server, Mail-Server usw.), zu welchem Zweck protokolliert wird (Zugriffskontrolle, Eingabekontrolle usw.), wer die Protokolle einsehen darf und wie lange die Protokolle aufbewahrt werden müssen (Löschfristen).

3.4.1 Protokolle

Die verantwortliche Stelle muss Richtlinien für die Protokollierung der Zugriffe auf die Dateien mit personenbezogenen Daten erstellen. In diesen Richtlinien muss geregelt sein,

- welche Daten protokolliert werden,
- wo protokolliert wird,
- zu welchem Zweck protokolliert wird,
- wer die Protokolle einsehen darf und
- wie lange die Protokolle aufbewahrt werden sollen.

(Eingabekontrolle / Protokolle)

Zweckbestimmung von Protokolldateien

(Eingabekontrolle / Protokolle)

Unterliegen diese Daten einer strengen Zweckbestimmung?

Erläuterung: Zweckbestimmungen regeln die Verwendung der gesammelten Daten. Die protokollierten Daten dürfen nicht für die anlasslose Leistungs- und Verhaltenskontrolle der Mitarbeiter herangezogen werden.

Kommentar: Gesetzliche Vorgaben und interne Anweisungen dazu werden hier beachtet. Teilweise auch Vorgaben von Kundenseite.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Auswertungen nach Sicherheitsverstößen

(Eingabekontrolle / Protokolle)

Gibt es Anweisungen oder dokumentierte Vorgehensweisen für über das übliche Maß hinausgehende Auswertungen nach Sicherheitsverstößen?

Erläuterung: In besonderen Fällen (z.B. nach dem Bekanntwerden von Sicherheitsverstößen) kann es erforderlich werden, dass das Anwenderverhalten eines Einzelnen oder einer Gruppe von Mitarbeitern temporär über das übliche Maß hinaus geloggt und ausgewertet wird.
Hierfür sollten Vorgehensweisen dokumentiert und ggf. mit der Mitarbeitervertretung abgestimmt werden.
Beispiele für Sicherheitsverstöße sind:

- Menschliche Fehler (z.B. ein Benutzerfehlverhalten, welches zu Datenverlusten führt)
- Nichteinhaltung von Leitlinien, Regelungen und Verfahren
- Verstöße gegen physische Sicherheitsmaßnahmen
- unkontrollierte Änderungen an Systemen
- Zugriffsverletzungen

Kommentar: Gesetzliche Vorgaben und interne Regelungen (z.B. OR 101)

Ergebnis: **Ja** 12 Punkt(e) (100%)

3.5Auftragskontrolle

Die Auftragskontrolle gemäß Nr. 6 der Anlagen zu § 9 BDSG und § 78a SGB X soll die Umsetzungen der Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag (§ 11 BDSG; § 80 SGB X) sicherstellen.
Die Auftragskontrolle betrifft daher zum einen die Erteilung des Auftrags selbst als auch die spätere praktische Umsetzung der vertraglich geregelten oder vom Gesetzgeber vorgegebenen Pflichten.
Die Fragen dieses Abschnitts betreffen sowohl den Auftraggeber als auch den Auftragnehmer.
Die Auftragskontrolle greift stets, wenn personenbezogen Daten im Auftrag von Dritten erhoben, verarbeitet oder genutzt werden. Das bedeutet, dass jeder Auftrag, bei welchem dem Auftragnehmer personenbezogene Daten übermittelt werden, gemäß diesen vereinbarten Regelungen durchzuführen ist und auch vom Auftraggeber zu kontrollieren ist.

3.5.1 Vertragliche Verpflichtung

Gemäß Artikel 28 Abs. 3 DS-GVO muss der Verantwortliche mit dem Auftragsverarbeiter einen Vertrag über die Auftragsverarbeitung schließen. Verantwortlicher und Auftragsverarbeiter können dabei wählen, ob Sie den vertrag schriftlich oder elektronisch schließen wollen.
Vgl. ISO 27001, Annex A.6.2.3 „Adressieren von Sicherheit in Vereinbarungen mit Dritten“

Vertragliche Verpflichtung Auftragsverarbeiter

(Auftragskontrolle / Vertragliche Verpflichtung)

Sind alle Auftragsverarbeiter (z.B. der Steuerberater oder ggf. der Betreiber eines externen Archivs) vollständig vertraglich verpflichtet?

Erläuterung: Gemäß Artikel 28 DS-GVO müssen für alle Auftragsverarbeitungen die entsprechenden Verträge geschlossen werden.

Kommentar: AVV für alle bekannten neuen Verfahren/Anwendungen

Ergebnis: **Ja** 12 Punkt(e) (100%)

3.5.2 Weisungen

Das Auftragsverhältnis zeichnet sich dadurch aus, dass es sehr stark weisungsgebunden ist. Unklare Kompetenzregelungen zur Erteilung von Weisungen bergen grundsätzlich die Gefahr, dass unautorisierte Weisungen durch den Auftragnehmer ausgeführt werden.
Die verantwortliche Stelle muss daher für Weisungen klare Regelungen schaffen.

Weisungsberechtigte des Auftraggebers

(Auftragskontrolle / Weisungen)

Ist klar festgelegt, welche Mitarbeiter des Auftraggebers gegenüber dem Auftragnehmer weisungsbefugt sind? Sind dem Auftragnehmer diese Personen bekannt?

Erläuterung: Weisungsbefugte Mitarbeiter sollten gegenüber dem Auftragnehmer namentlich benannt werden, um zu verhindern, dass entweder nicht berechtigte Personen des Auftraggebers oder Dritte unberechtigt Weisungen an den Auftragnehmer erteilen.

Kommentar: Ansprechpartner werden im AVV benannt.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Weisungsempfänger bei dem Auftragnehmer

(Auftragskontrolle / Weisungen)

Verfügt der Auftraggeber über eine Liste der befugten Weisungsempfänger bei dem Auftragnehmer?

Erläuterung: Der Auftragnehmer muss die Weisungen des Auftraggebers schnell und effektiv umsetzen - etwa um einen entdeckten Datenschutzverstoß schnell abzustellen. Weisungen müssen daher die Personen erreichen, die dazu ermächtigt sind, die Weisungen umzusetzen. Daher sollten die Weisungsempfänger schriftlich festgelegt werden.

Kommentar: Im AVV benannt.

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.6Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle minimiert das Risiko, dass personenbezogene Daten zufällig zerstört werden oder "verloren" gehen. Eine wirksame Verfügbarkeitskontrolle stellt sicher, dass personenbezogene Daten, welche verfügbar sein sollen, zu den erforderlichen Zeiten auch tatsächlich verfügbar sind.
Die Verfügbarkeitskontrolle spielt bei der Auslagerung von Datenverarbeitungsvorgängen eine erhebliche Rolle. Die Aspekte der Verfügbarkeitskontrolle sollten daher etwa bei der Inanspruchnahme von Cloud-Diensten oder externen Rechenzentren thematisiert werden. Probleme bei der Verfügbarkeit führen in der Regel zu Unterbrechungen der Unternehmenstätigkeit und ziehen daher große wirtschaftliche Konsequenzen nach sich.

3.6.1 Planung

Dieses Unterkapitel untersucht, ob die verantwortliche Stelle bei der Planung Maßnahmen zur Verfügbarkeitskontrolle berücksichtigt hat.

Überschwemmungsschutz

(Verfügbarkeitskontrolle / Planung)

Ist das oder sind die Gebäude vor Überschwemmungen geschützt?

Erläuterung: Alle Bereiche, in denen sich Wasser sammeln und stauen kann oder in denen fließendes oder stehendes Wasser nicht oder erst spät entdeckt wird und in denen das Wasser Schäden verursachen kann, sollten mit geeigneten Maßnahmen abgesichert werden. Hierzu zählen u.a. selbsttätige Entwässerungsanlagen und Wassermelder.

Kommentar: Alle Geäude und Räume wurden unter diesen Aspekten betrachtet und z.B. das RZ unter Berücksichtigung von Überschwemmungen gebaut.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Technische Infrastruktur

(Verfügbarkeitskontrolle / Planung)

Wird in regelmäßigen Abständen überprüft, ob die Versorgung mit Fernmelde- und Datenleitungen, Strom, Wärme und Wasser noch ausreichend ist?

Erläuterung: Die Raumbelegung sowie die Anschluss- und Verbrauchswerte, die bei Einzug oder Neubau festgelegt wurden, stimmen erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist also unerlässlich, bei Änderungen der Raumnutzung und bei Änderungen und Ergänzungen der technischen Ausrüstung (IT, Klimatruhe, Beleuchtung etc.) die Kapazitäten zu prüfen und ggf. anzupassen.

Kommentar: Durch Auditierung.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Unterirdische Versorgungsleitungen
(Verfügbarkeitskontrolle / Planung)

Ist die Art der Versorgungsleitungen unterirdisch?

Erläuterung: Sind Fernmelde- und Datenleitungen, Stromversorgung sowie Leitungen für Wärme und Wasser unterirdisch bis zum Gebäude verlegt?

Kommentar: Soweit möglich, ja.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Größe und Ausstattung des Drucker-Raumes
(Verfügbarkeitskontrolle / Planung)

Genügt der Drucker-Raum den aktuellen Ansprüchen?

Erläuterung: Rahmenbedingungen und Anforderungen können sich über einen längeren Zeitraum verändern. Sind Mängel bekannt?

Kommentar: siehe Druckerkonzept. MFG´s befinden sich in separten Räumen oder getrennten Bereichen.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Vorrat an Printer-Verbrauchsmaterial
(Verfügbarkeitskontrolle / Planung)

Ist dafür gesorgt, dass stets genug Papier und Verbrauchsmaterial verfügbar ist, sodass keine Geschäftsprozesse durch Fehlen davon beeinträchtigt werden?

Kommentar: Etablierter Prozess. Abrufvereinbarung zur Papierlieferung.

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.6.2 Technische Beschaffenheit und Ausstattung DV-Bereich

Dieser Fragenkomplex prüft, ob die technische Beschaffenheit und die Ausstattung des IT-Bereichs eventuelle Risiken so beschaffen sind, dass Ausfallrisiken minimiert werden.

Zutrittsschutz im DV-Bereich
(Verfügbarkeitskontrolle / Technische Beschaffenheit und Ausstattung DV-Bereich)

Sind die Maßnahmen zum Zutrittsschutz so ausgeführt, dass hinsichtlich DV-Bereich von einem Sicherheitsbereich gesprochen werden kann?

Erläuterung: Folgende Bedingungen müssen dazu erfüllt sein:
- Die Anzahl der nach außen führenden Türen ist auf das unbedingt nötige Minimum zu beschränken.
- Die Türen sind ständig verschlossen zu halten und von außen nur mit einer Codekarte oder einem Schlüssel zu öffnen.
- Für den DV-Bereich sollte ein eigener Schließbereich mit besonderen Sicherheitsschlüsseln existieren.
- Fluchttüren dürfen sich nur von innen öffnen lassen.

Kommentar: Siehe Unterlagen neues RZ

Ergebnis: **Ja** 4 Punkt(e) (100%)

Fenster im DV-Bereich

(Verfügbarkeitskontrolle / Technische Beschaffenheit und Ausstattung DV-Bereich)

Sind die Fenster so ausgeführt, dass hinsichtlich DV-Bereich von einem Sicherheitsbereich gesprochen werden kann?

Erläuterung: Folgende Bedingungen müssen dazu erfüllt sein:
- Die Fenster müssen gegen unbefugtes Öffnen gesichert sein, z.B. durch in die Fenstergriffe integrierte Schlösser (Besonders wichtig bei klimatisierten Räumen).
- Das Material muss aus Panzerglas oder zumindest einbruchshemmender Verglasung bestehen.
- Falls die Fenster von außen leicht erreichbar sind, so müssen sie in die Außenhautsicherung mit einbezogen werden (d.h., es sind Glasbruch- und Öffnungsmelder zu installieren)
- Falls die Fenster von außen leicht einsehbar sind, so ist ein Sichtschutz zu installieren (z.B. durch aufgeklebte sog. Milchglasfolien)

Kommentar: Container ohne Fenster

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.6.3 Branderkennungs-, Brandbekämpfungsmaßnahmen, Überwachungsanlagen

Frühwarnsystem zur rechtzeitigen Branderkennung

(Verfügbarkeitskontrolle / Branderkennungs-, Brandbekämpfungsmaßnahmen, Überwachungsanlagen)

Ist ein Frühwarnsystem mit automatischen Brandmeldern (Ionisations- oder Rauchmelder) im Doppelboden, in der Decke sowie in den Zu- und Rücklaufkanälen der Klimaanlage installiert?

Kommentar: Siehe Betriebshandbuch neues RZ

Ergebnis: **Ja** 4 Punkt(e) (100%)

Anbringungsort Rauchmelder

(Verfügbarkeitskontrolle / Branderkennungs-, Brandbekämpfungsmaßnahmen, Überwachungsanlagen)

Wurde darauf geachtet, dass Rauchmelder leicht zugänglich und an Stellen optimaler Konvektion angebracht wurden?

Erläuterung: Die bestehenden Brandschutzvorschriften (z.B. DIN 4102) und die Auflagen der Bauaufsicht für Gebäude können nur von Fachleuten umgesetzt werden. Die Positionierung von Rauchmeldern gehört ebenfalls dazu.
Da mehr als 90 % aller Brandschäden in Rechenzentren durch Feuer im Umfeld verursacht werden, empfiehlt es sich, diese Bereiche in die Überwachung durch die Brandmeldeanlage zu integrieren. Zum Einsatz sollten Puls- bzw. Trendmelder (optisches Streulichtprinzip) kommen.
Die Identifikation des auslösenden Melders muss möglich sein. Zur Lokalisierung des Brandherdes und der Brandausbreitung ist diese Identifikation der Brandmelder ein besonders wichtiges Hilfsmittel.
Eine empfehlenswerte Mindestkonfiguration einer Brandmeldeanlage in der Infrastruktur besteht aus
- Kanalmeldern in den Klimakanälen für Zuluft und Abluft
- Meldern in der Frischluftansaugung, mit automatischer Sperrung der Frischluft, wenn Störgrößen erkannt werden.
Alle Meldungen der Brandmeldeanlage und auch Störmeldungen sollten, sofern möglich, auf einer ständig besetzte Stelle, z. B. der Pförtnerloge, auflaufen.
Nach Möglichkeit sollte eine direkte Aufschaltung zur Berufsfeuerwehr erfolgen.

Kommentar: Siehe Betriebshandbuch neues RZ

Ergebnis: **Ja** 4 Punkt(e) (100%)

Feuerlöscher und Flutungsanlagen

(Verfügbarkeitskontrolle / Branderkennungs-, Brandbekämpfungsmaßnahmen, Überwachungsanlagen)

Sind ausreichend geeignete Feuerlöscher/Flutungsanlagen sowie das richtige Löschmittel im Einsatz und wird dabei auf Einheitlichkeit geachtet (z.B. ausschließlich CO2 Löscher)?

Erläuterung: Die Sofortbekämpfung aufkommender Brände ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3) in ausreichender Zahl und Größe (Beratung durch die örtliche Feuerwehr) im Gebäude zur Verfügung stehen. Dabei ist die räumliche Nähe zu schützenswerten Bereichen und Räumen wie Serverraum, Raum mit technischer Infrastruktur oder Belegarchiv anzustreben.
Für elektronische Geräte sollten vorzugsweise Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen. Die Löschwirkung wird durch Verdrängung des Sauerstoffs erreicht, deshalb ist bei Anwendung in engen, schlecht belüfteten Räumen Vorsicht geboten
Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.
Wasserlöscher mit Eignung für Brandklasse A bis 1000 V sind durchaus für elektrisch betriebene Geräte geeignet.
Für elektronisch gesteuerte Geräte, z. B. Rechner, sollten vorzugsweise Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen. Die Löschwirkung wird durch Verdrängung des Sauerstoffs erreicht, deshalb ist bei Anwendung in engen, schlecht belüfteten Räumen Vorsicht geboten.
Pulverlöscher, die die Brandklassen A (feste Stoffe), B (brennbare Flüssigkeiten) und C (Gase) abdecken, sollten in Bereichen mit elektrischen und elektronischen Geräten nicht eingesetzt werden, weil die Löschschäden in der Regel unverhältnismäßig hoch sind.

Kommentar: ja.

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.6.4 Katastrophenvorsorge und IT-Notfallkonzept

Bei und nach Zwischenfällen muss die Verantwortliche Stelle schnell und koordiniert handeln, um weiteren Schaden zu vermeiden. Für ein strukturiertes Vorgehen bei Katastrophen oder gravierenden IT-Zwischenfällen sorgt das Katastrophenvorsorge- und IT-Notfallkonzept.

Untersuchung Katastrophenmöglichkeiten

(Verfügbarkeitskontrolle / Katastrophenvorsorge und IT-Notfallkonzept)

Wurden alle in Frage kommenden Katastrophenmöglichkeiten untersucht (Streik, Personalausfall, Sachbeschädigung, Feuer, Explosion, Erdbeben, Wassereinbruch, längere Störungen oder Ausfälle der Infrastruktur)?

Erläuterung: Wurden dabei besondere Risikofaktoren der Gebäudelage berücksichtigt, wie z.B.
- Lage des Gebäudes in einer Einflugschneise militärischer oder ziviler Flughäfen?
- Lage des Gebäudes in unmittelbarer Nachbarschaft zu Brennstofflagern wie z.B. Raffinerien, Tankstellen, Benzin- oder Heizöllager?
- Lage des Gebäudes an einem demonstrationsgefährdeten Ort?

Eine ausführliche Aufstellung und Erläuterung möglicher Katastrophenfälle findet sich auch im Grundschutzhandbuch des BSI - Bundesamt für Sicherheit in der Informationstechnik. Es ist über die Webseite (www.bsi.de) öffentlich zugänglich.

Kommentar: Untersuchung an Hand einer Risikoanalyse. Bereiche wurden betrachtet,

Ergebnis: **Ja** 12 Punkt(e) (100%)

Existenz aktuelles Notfallhandbuch

(Verfügbarkeitskontrolle / Katastrophenvorsorge und IT-Notfallkonzept)

Existiert ein Notfallhandbuch und wird dieses laufend aktualisiert?

Erläuterung: In einem Notfallhandbuch sind alle Maßnahmen, die nach Eintritt eines notfallauslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen dokumentiert. Das Notfallhandbuch ist so verfasst, dass ein sachverständiger Dritter in der Lage ist, die im Handbuch spezifizierten Notfallmaßnahmen durchzuführen.

Kommentar: Notfallhandbuch exisitiert.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Existenz Sicherheitsbeauftragter

(Verfügbarkeitskontrolle / Katastrophenvorsorge und IT-Notfallkonzept)

Wurde ein IT Sicherheitsbeauftragter bestellt?

Ergebnis: **Ja** 4 Punkt(e) (100%)

Dokumentation Mitarbeiterverhalten Katastrophenfall

(Verfügbarkeitskontrolle / Katastrophenvorsorge und IT-Notfallkonzept)

Gibt es schriftliche Festlegungen für das Verhalten der Mitarbeiter im Katastrophenfall?

Kommentar: Teil des Notfallhandbuchs.

Notfallübungen
(Verfügbarkeitskontrolle / Katastrophenvorsorge und IT-Notfallkonzept)

Finden regelmäßige Notfallübungen statt?

Erläuterung: Ob ein Notfallkonzept wirklich funktioniert, kann ausschließlich durch entsprechende Übungen verifiziert werden. Der Umfang der Übungen variiert zwischen gedanklicher Vorstellung eines Szenarios und der daraufhin einzuleitenden Maßnahmen („Table Top Testing“) bis zur lebensnahen Simulation.

Kommentar: Teil des Notfallhandbuchs

Ergebnis: **Ja** 20 Punkt(e) (100%)

3.6.5 Backupkonzept

Unter die Verfügbarkeitskontrolle fallen auch Maßnahmen zur Datensicherung, also die klassischen Backup- und Datenspiegelungslösungen.

Dokumentation der Anforderungen
(Verfügbarkeitskontrolle / Backupkonzept)

Sind die Anforderungen an das Backup in einem Backup-Konzept dokumentiert?

Erläuterung: Abhängig von der Art der Daten, der Veränderungshäufigkeit und der Wichtigkeit der Daten für das Unternehmen ergeben sich spezifische Anforderungen, welche im Backup-Konzept zu dokumentieren sind.

Kommentar: Abhängig vom Schutzbedarf

Ergebnis: **Ja** 4 Punkt(e) (100%)

Schutz vor Diebstahl oder Zerstörung
(Verfügbarkeitskontrolle / Backupkonzept)

Sind Die Backups ausreichend vor Diebstahl und Zerstörung geschützt?

Erläuterung: Sicherungskopien dürfen nie im gleichen Gebäude oder Brandabschnitt wie das DV-System aufbewahrt werden. Die Datensicherung muss entweder direkt auf einem Server an einem anderen Standort erstellt werden, oder Datenträger mit Datensicherungen sind entsprechend an einem ausgelagerten Ort aufzubewahren.

Kommentar: Teil des Notfallhandbuchs

Ergebnis: **Ja** 4 Punkt(e) (100%)

Verantwortlichkeiten
(Verfügbarkeitskontrolle / Backupkonzept)

Wurden die für die Sicherung verantwortlichen Personen namentlich benannt und wurde dieses dokumentiert?

Erläuterung: Es muss namentlich und schriftlich festgehalten werden, wer für welche Datensicherung verantwortlich ist. Operatoren müssen festgelegt werden.

Kommentar: Teil des Notfallhandbuchs und Schutzbedarfsfeststellung

Ergebnis: **Ja** 4 Punkt(e) (100%)

Funktionalitätstest
(Verfügbarkeitskontrolle / Backupkonzept)

Wird regelmäßig getestet, ob das Backup brauchbar ist?

Erläuterung: Es ist regelmäßig zu testen, ob sich aus dem Backup funktionsfähige Datensätze oder Systeme wiederherstellen lassen. Diese Tests sollen nicht auf dem Produktivsystem sondern in der Testumgebung stattfinden.

Kommentar: Test durch regelmäßige Rücksicherungen (Kundenanfragen.)

Ergebnis: **Ja** 20 Punkt(e) (100%)

3.6.6 Aufbewahrung von Geschäftsunterlagen

Archivraum
(Verfügbarkeitskontrolle / Aufbewahrung von Geschäftsunterlagen)

Existiert ein eigener Archivraum?

Erläuterung: Es ist grundsätzlich zu empfehlen, Datenträger sowie Akten (Kundendaten etc.) in einem Archiv zu lagern, dessen Zugang kontrolliert werden kann.
Es sollte geprüft werden, ob ein Archivraum eingerichtet werden kann.

Kommentar: Archivraum (mit Tresor)

Ergebnis: **Ja** 4 Punkt(e) (100%)

Archivordnung
(Verfügbarkeitskontrolle / Aufbewahrung von Geschäftsunterlagen)

Besteht eine Archivordnung?

Kommentar: Gesetzliche Vorgaben

Ergebnis: **Ja** 4 Punkt(e) (100%)

Zutritt zum Archiv
(Verfügbarkeitskontrolle / Aufbewahrung von Geschäftsunterlagen)

Ist der Zutritt zum Archiv auf einen genau festgelegten Personenkreis eingeschränkt?

Erläuterung: Eine Zutrittskontrolle kann z.B. durch eine entsprechende Schlüsselverwaltung/Schlüsselausgabe erfolgen. Voraussetzung ist, dass das Archiv verschlossen werden kann und muss.

Kommentar: Entsprechende Zutrittsmöglichkeiten sind über die programmierbaren Schlüssel gegeben.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Bestandskontrollen
(Verfügbarkeitskontrolle / Aufbewahrung von Geschäftsunterlagen)

Erfolgen regelmäßige Bestandskontrollen der Datenträger durch Soll/Ist Vergleich?

Erläuterung: Regelmäßige Bestandskontrollen sind erforderlich, um eventuelle Fehlbestände zu identifizieren.

Kommentar: Jährliche Inventarisierung

Ergebnis: **Ja** 4 Punkt(e) (100%)

Feuerfeste Schränke
(Verfügbarkeitskontrolle / Aufbewahrung von Geschäftsunterlagen)

Sind für besonders wichtige Unterlagen geeignete feuer- und einbruchssichere Schränke vorhanden?

Erläuterung: Wichtige Papiere, Dokumente und Datenträger sollten grundsätzlich in einem geprüften Schrank nach RAL-RG 626/7 aufbewahrt werden, der in der jeweiligen Güteklasse nach VDMA 24991 optimalen Feuerschutz kombiniert mit genau definiertem Einbruchschutz nach der Euro/VdS-Norm bietet. Die Prüfbedingungen der Schränke gegen Feuer sind im VDMA Einheitsblatt 24991 geregelt und umfassen eine Feuerwiderstandsprüfung (bis 860 Grad) sowie eine Feuerstoß- (bis 1080 Grad) und Sturzprüfung aus 9,15 m Höhe. Gesamtprüfzeit ca. 24 Stunden.
Bei zentralen Datenträgerarchiven und Datensicherungsarchiven ist die Nutzung von Datensicherungsschränken empfehlenswert, um den Brandschutz, den Schutz gegen unbefugten Zugriff und die Durchsetzung von Zugangsberechtigungen zu unterstützen. Es ist zu empfehlen, für das Archiv entsprechende Schränke mit einer Feuerwiderstandsklasse zu beschaffen.

Kommentar: Tresore oder spezielle Archivschränke sind vorhanden.

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.6.7 Sonstige Sicherheitsmaßnahmen

Rauch-, Ess- und Trinkverbot in Rechnerräumen
(Verfügbarkeitskontrolle / Sonstige Sicherheitsmaßnahmen)

Wurde im Rechnerraum ein Rauch-, Ess- und Trinkverbot verfügt?

Erläuterung: Es ist anzuraten, in Rechnerräumen ein Ess-, Trink- und Rauchverbot zu erteilen.

Kommentar: Vorgaben sind vorhanden, Mitarbieter werden vor dem ersten Betreten belehrt.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Zeitplan Reinigung Serverräume (Aufbewahrung Reinigungsmittel)
(Verfügbarkeitskontrolle / Sonstige Sicherheitsmaßnahmen)

Findet eine regelmäßige Reinigung der Serverräume einschließlich der Doppelböden statt und werden die Reinigungsmittel in sicherer Distanz zum IT-Equipment aufbewahrt?

Kommentar: Vorgaben sind vorhanden.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Regelung zur Mitnahme von Gegenständen in Rechnerräume

(Verfügbarkeitskontrolle / Sonstige Sicherheitsmaßnahmen)

Ist die Mitnahme von Taschen, Mänteln oder sonstigen Gegenständen in Rechnerräume verboten?

Kommentar: Regelungen dazu sind vorhanden.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Existenz schriftlicher Dienstanweisungen Sicherheitsmaßnahmen

(Verfügbarkeitskontrolle / Sonstige Sicherheitsmaßnahmen)

Wurden schriftliche Dienstanweisungen über die Art und den Zweck der eingeführten Sicherheitsmaßnahmen erlassen?

Kommentar: Umfangreiche Regelungen vorhanden. (Betriebshandbuch, Notfallhandbuch, usw.)

Ergebnis: **Ja** 4 Punkt(e) (100%)

Vergabe von Sicherheitshandbüchern an Personal

(Verfügbarkeitskontrolle / Sonstige Sicherheitsmaßnahmen)

Werden dem Personal Sicherheitshandbücher zum persönlichen Gebrauch ausgehändigt?

Kommentar: Elektronisch ist der Zugriff aller Mitarbeiter auf die Unterlagen gewährleistet.

Ergebnis: **Ja** 4 Punkt(e) (100%)

Existiert ein Störungslogbuch

(Verfügbarkeitskontrolle / Sonstige Sicherheitsmaßnahmen)

Werden Störungen und Maßnahmen zu deren Behebung in einem Störungslogbuch revisionsfähig (Datum, Uhrzeit, unternommene Aktion) dokumentiert?

Erläuterung: In einem elektronischen Störungslogbuch werden alle bekannten Störungen mit den eingeleiteten Maßnahmen zur Behebung dokumentiert und so gespeichert, dass eine nachträgliche Änderung nicht unbemerkt erfolgen kann.

Kommentar: Störungslogbuch für den Bereitschaftsdienst und im Benutzerservice

Ergebnis: **Ja** 4 Punkt(e) (100%)

Existenz Versicherungsschutz

(Verfügbarkeitskontrolle / Sonstige Sicherheitsmaßnahmen)

Besteht Versicherungsschutz gegen bestimmte IT Risiken: Feuer, Wasser etc.? Ausfall der Datenverarbeitung? Softwarefehler? DV Missbrauch?

Kommentar: Umfangreicher Versicherungsschutz. (z.B. auch Cyber-Schutz)

Ergebnis: **Ja** 4 Punkt(e) (100%)

Art Versicherungsschutz

(Verfügbarkeitskontrolle / Sonstige Sicherheitsmaßnahmen)

Wurden folgende Versicherungen abgeschlossen: Elektronikversicherung, Datenträger- und Softwareversicherung, Elektronikmehrkostenversicherung, Elektronikbetriebsunterbrechungsversicherung, Computermissbrauchsversicherung?

Kommentar: Umfangreicher Versicherungsschutz

Ergebnis: **Ja** 4 Punkt(e) (100%)

3.7 Trennungskontrolle

Die Trennungskontrolle setzt das Prinzip der Zweckbestimmung und Zweckbindung um.
Eine wirksame Trennungskontrolle gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden.

3.7.1 Trennung von Office-, Entwicklungs-, Test- und Produktivumgebungen

Netztrennung

(Trennungskontrolle / Trennung von Office-, Entwicklungs-, Test- und Produktivumgebungen)

Befinden sich Office-, Entwicklungs-, Test- und Wirksysteme in klar voneinander getrennten Netzsegmenten, vielleicht sogar physikalisch voneinander getrennt?

Erläuterung: Die Trennung dieser Netzsegmente empfiehlt sich schon aus technischen Gründen, z.B. aufgrund des Virenschutzes und des Patchmanagements.
Hinzu kommt, dass sich durch diese Trennung Zugriffskonzepte leichter umsetzen lassen. So wird dadurch z.B. von vornherein unterbunden, dass Anwender aus dem Office-Netz unkontrolliert auf Testsysteme zugreifen können.
Schnittstellen zwischen den Netzsegmenten (z.B. zur Administration von Produktivsystemen) sind zulässig, sollten aber wohlbegründet sein und restriktiv gehandhabt werden.

Kommentar: Umfangreiches Netzkonzept, dass in den letzten Jahren umgesetzt wurde.

Ergebnis: **Ja** 20 Punkt(e) (100%)