Datenschutzkonzept

incl. der technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO

Verantwortliche Stelle:	Niedling & Partner Grondahlsmühle 10 53881 Euskirchen-Kuchenheim
Leiter der verantwortlichen Stelle:	Guido Niedling Joachim Kontny
Datenschutzbeauftragter:	Reinhold Goetz Dipl. Ing. Nachrichtentechnik Kampstr.6 50374 Erftstadt Tel.: 02235 - 99 47 99 7 E-Mail.: rgoetz@wimas.de
Stand:	02.02.2018

Inhaltsverzeichnis

1. Organisationskontrolle

1.1. Organisation des Datenschutzes

Wie ist die Umsetzung des Datenschutzes organisiert?
(interner/externer Datenschutzbeauftragter, Schulung der Mitarbeiter, Dokumentation des Sicherheitskonzeptes etc.)

Istzustand:

- Als externer Datenschutzbeauftragter (DSB) wurde Herr Reinhold Goetz bestellt. Herr Goetz verfügt über eine Ingenieurausbildung im IT-Bereich und hat seine datenschutzrechtliche Qualifikation über entsprechende Zertifikate nachgewiesen. [1] [2]
- Der Datenschutzbeauftragte ist mit seinen Kontaktdaten allen Mtarbeitern bekannt. [1]
- Die verantwortliche Stelle hat seine TOM's (Technisch Organisatorischen Maßnahmen) gemäß Artikel 32 Abs. 1 in einem schriftlich geführten Datenschutzkonzept dokumentiert.
- Die Einhaltung der Dienstanweisungen wird durch die Geschäftsführung oder durch eine von der Geschäftsführung beauftragten Person stichprobenartig überprüft.
- Die Mitarbeiter der verantwortlichen Stelle werden bei Bedarf, mindestens jedoch einmal jährlich durch den Datenschutzbeauftragten im Rahmen einer Präsenzschulung auf die datenschutzrechtlichen Anforderungen hingewiesen. Die Unterweisungen werden dokumentiert. [3] [4] [5]
- Der Datenschutzbeauftrage überprüft bei Systemveränderungen die einen Einfluss auf die Verarbeitung personenbezogener Daten haben, spätestens jedoch nach Ablauf eines Jahres, im Rahmen einer Bestandsaufnahme die Einhaltung aktueller Datenschutzbestimmungen.
- Der Datenschutzbeauftragte wird vor der Beauftragung von Servicedienstleistern (Reinigungsfirmen, Wartungsdienst Kopierer etc.) und Auftragnehmern (IT-Systempartner, Cloud-Anbieter etc.) einbezogen, um die datenschutzrechtlichen Anforderungen zu prüfen (Verpflichtung auf das Datengeheimnis, Vereinbarung zur Auftragsverarbeitung etc.).

2. Zugangskontrolle

2.1. Lage der Betriebstätte

Wo befindet sich die Betriebsstätte und gibt es noch andere Mieter?
(Wohngebiet, Gewerbegebiet, Mischgebiet, Untermieter etc.)

Istzustand:

- Die Betriebsstätte befindet sich in einem Mischgebiet in Euskirchen-Kuchenheim. Im Gebäude selber befindet sich auch eine Privatwohnung eine(s/r) Mitarbeiter(s/rin). Das eingezäunte Grundstück wird ganztags von zwei Wachhunden bewacht.
- In der Betriebsstätte befinden sich keine betriebsfremden Untermieter.

2.2. Schutz- und Sicherungsmaßnahmen

Welche zusätzlichen Schutz- und Sicherungsmaßnahmen für den Schutz des Geschäftsbereiches vor unbefugtem Zutritt sind vorhanden?
(Schließsysteme, Alarmanlagen, Wachdienst, Videoüberwachung, Serverraum etc.)

Istzustand:

- Die Außentüren sind einbruchsicher und mit doppelten Schließzylindern ausgestattet, die Schließzylinder sind aufbohr- und ausziehsicher [6] [7] [8]
- Die Schließzylinder der Haupteingangstür und der Zugangstüren zum Geschäftsbereich entsprechen der Klasse „erhöht einbruchhemmend“ mit Sicherheitszertifikat, damit können Schlüsselkopien nur beim Hersteller unter Vorlage des Zertifikates erstellt werden. Zugang zum Schlüssel-Zertifikat hat nur die Geschäftsleitung. [9]
- Alle Türen und Fenster im Erdgeschoß sind vergittert. [6] [8]
- Die Zentralrechner (Server) befinden sich in einem verschlossenen und klimatisierten Schrank und sind nur einem autorisierten Personenkreis zugänglich, die Schlüsselinhaber werden in einer Schlüsselliste geführt. [9]
- Im Serverraum befinden sich keine weiteren leicht brennbaren Stoffe, d. h. keine Aktenlagerung. [10]
- Im Gebäude sind verknüpfte Rauchmelder installiert, die einen Innenalarm auslösen. [11] [12]

2.4. Zutritt zum Geschäftsbereich

Wie ist der Zutritt zum Geschäftsbereich organisiert?
(Türöffnung, Nebeneingänge, Einsichtmöglichkeiten, Schlüsselinhaber etc.)

Istzustand:

- Der Einblick von außen auf sensible Bereiche des Geschäftsbereiches ist nicht möglich. Unbefugte Personen haben von außen keinen Einblick auf schutzwürdige oder personenbezogene Unterlagen. [13] [14]
- Sensible Bereiche wie z. B. Serverraum, Datenträgerarchiv und Verteilungen der Stromversorgung tragen keinen Hinweis auf ihre Nutzung (Türschilder wie z. B. SERVERRAUM oder ARCHIV). [13]
- Es gibt keine unverschlossenen Nebeneingänge zum Geschäftsbereich. [9]
- Die Eingangstür zum Geschäftsbereich ist auch während der Geschäftszeiten grundsätzlich verschlossen. Die Türöffnung erfolgt durch einen Mitarbeiter, der den Besucher empfängt und in ein Besprechungszimmer begleitet. [15]
- Es befinden sich keine Schlüssel bei betriebsfremden Personen. [16]
- Alle Schlüsselinhaber zum Geschäftsbereich werden in einer aktuellen Schlüsselliste geführt. [17]
- In einer Dienstanweisung werden Verhaltensrichtlinien im Umgang mit den Schlüsseln gegeben. Darin ist unter anderem auch festgelegt, dass ein Schlüsselverlust der Geschäftsleitung unverzüglich angezeigt werden muss und die Schlüssel keine Kennzeichnung tragen dürfen, die Rückschlüsse auf das Objekt ermöglicht. [17]
- Die Reinigung erfolgt durch eine angestellte Reinigungskraft. Die Vertretung wird intern

organisiert, d. h. auch im Vertretungsfall erfolgt die Reinigung durch eigenes Personal. [18]
- Alle betriebsfremden Servicedienstleister (Fensterreinigung etc.) arbeiten nur bei Anwesenheit von min. einem Mitarbeiter und haben eine schriftliche Verpflichtungserklärung zum Datenschutz abgeben. [18]
- Der Geschäftsbereich erstreckt sich über mehrere Etagen, die über ein gemeinsam genutztes Treppenhaus mit anderen Mietern verbunden sind. Alle Etagentüren sind verschlossen.

2.5. Zutritt zu den Büros

Wie ist der Zutritt zu den Büros organisiert?
(Besucher, Aufbewahrung von Akten etc.)

Istzustand:

- Die Mitarbeiter werden regelmäßig im Rahmen einer Datenschutzschulung darauf hingewiesen, dass sie verpflichtet sind, personenbezogene und vertrauliche Daten vor unberechtigten Zugriff zu schützen und Unbefugte nicht unbeaufsichtigt zu lassen. Eine Kontrolle der Einhaltung erfolgt regelmäßig durch die Geschäftsleitung. [3]
- Die Mitarbeiter wurden in einer Dienstanweisung verpflichtet, Besucher nur in den dafür vorgesehenen Besprechungszimmern zu empfangen. Sollte das nicht möglich sein, z. B. bei belegten Besprechungszimmern, werden die Besucher vom Sekretariat dem Mitarbeiter telefonisch angekündigt, damit dieser die Möglichkeit hat alle schutzwürdigen Unterlagen zu verschließen. [19]
- Die Büros werden nur von eigenen Mitarbeitern betreten. [20]
- In den Besprechungszimmern werden keine vertraulichen oder personenbezogenen Daten gelagert. [19]
- Büros die beim Verlassen nicht abgeschlossen werden verfügen über abschließbare Aktenschränke. Die Schüsselinhaber zu den Schränken mit vertraulichen Inhalt, z.B. Personalunterlagen, Vertragsunterlagen etc., werden in einer Schlüsselliste geführt. [21]

2.6. Anforderungen an Home Office Arbeitsplätze

Wie wird sichergestellt, dass die Verarbeitung personenbezogener Daten in einer privaten Arbeitsumgebung vertraulich erfolgt?
Risiken bei Telearbeit sind bei sensiblen und daher besonders schützenswerten personenbezogene Daten nur dann vertretbar, wenn deren Schutz durch angemessene technisch-organisatorische Maßnahmen und entsprechende Kontrollmöglichkeiten des Arbeitgebers vor Ort gewährleistet ist.

Istzustand:

- Home Office Arbeitsplätze sind nur für die Geschäftsführung und angestellte Mitarbeiter eingerichtet.
- Daten über Beurteilungen oder Erkrankungen werden grundsätzlich nicht über Telearbeitsplätze verarbeitet. [22]

- Sind im Rahmen einer konventionellen Verarbeitung besonders schutzbedürftige Daten betroffen, wird von der Wahrnehmung der Tätigkeit in Telearbeit abgesehen. [22] [23]
- Es ist sichergestellt, dass die Telearbeiter über entsprechende Räumlichkeiten verfügen (z. B. separates, abschließbares Arbeitszimmer), die eine vertrauliche Verarbeitung der Daten erlaubt. Eine Kontrolle durch den Arbeitgeber vor Inbetriebnahme des Telearbeitsplatzes und danach ist gegeben. Die Kontrolle wird zudem dokumentiert. [22] [24] [23]
- Es erfolgt eine strikte Trennung zwischen beruflichem und privaten (Internet-)Anschluss, z.B. durch getrennte Netzwerke im HomeOffice. [22]
- Falls erforderlich, gibt es eine sichere Anbindung eines lokalen Druckers (kein Netzwerkdrucker, kein WLAN-Drucker, kein online-Drucker!!!) in unmittelbarer Nähe des Arbeitsplatzes mit Protokollierung von häuslichen Druckvorgängen. [22]
- Die beruflich zur Verfügung gestellte IT-Ausstattung wird nicht privat genutzt. [22] [24] [23]
- Der Arbeitgeber kommt seiner Pflicht nach, was gleichzeitig auch sein Recht ist, vor und nach der Genehmigung der Telearbeit routinemäßig und in regelmäßigen Abständen den Telearbeitsplatz zu kontrollieren. [22] [24]
- Am Telearbeitsplatz wird keine private Hard- oder Software eingesetzt. [22] [24]
- Berufliche E-Mails und Telefonate werden nicht auf private Postfächer oder private Telefonanschlüsse/Handys der Telearbeiter umgeleitet. [22]
- Bei der Entscheidung über einen Telearbeitsplatz ist der Beauftragte für den Datenschutz des Arbeitgebers rechtzeitig beteiligt. [22]

2.7. Digitalkopierer

Sind Digitalkopierer im Einsatz?
(Welche Funktionen haben diese: Drucken / Faxen / Scannen / Archivieren etc.)

Istzustand:

- Um zu verhindern, dass Drucker, Kopierer oder Multifunktionsgeräte manipuliert werden oder die Druckausgabe von Unbefugten kopiert oder mitgelesen werden können, werden die Geräte so aufgestellt, dass nur berechtigte Mitarbeiter Zugang zu ihnen haben. [25]
- Fehldrucke werden durch die Mitarbeiter selbst entsorgt und nicht den Reinigungskräften überlassen. [25]
- Digitalkopierer werden im Rahmen der Wartung mit den aktuellen Sicherheitspatches des Herstellers ausgestattet.
  Generell wird darauf geachtet, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden.
- Falls Digitalkopierer über das Netzwerk administriert werden, ist sichergestellt dass Administratoren sich hierfür ebenfalls authentisieren müssen. Die Zugangsdaten sind nur der Leitung und dem Techniker bekannt. [25]
- Ausdrucke mit schutzwürdigem Inhalt werden direkt am Arbeitsplatz gedruckt oder Kennwort geschützt auf einem Zentraldrucker ausgegeben. [25]
- Die lokale Systemkonfiguration der Digitalkopierer ist passwortgeschützt. Das Passwort

ist nur der Leitung und dem Techniker bekannt. [25]
- Netztrennung - Die Sicherheitsgateways zwischen LAN und Internet sind so konfiguriert, dass Netzdrucker nicht auf das Internet zugreifen können und umgekehrt nicht aus dem Internet erreichbar sind. [25]
- Umgang mit Digitalkopierern beim Kunden:
  - Die Administrationspasswörter werden bei der Ersteinrichtung auf ein individuelles Passwort abgeändert, dass nur den Technikern und dem Kunden bekannt ist.
  - Auf den netzwerkfähigen Digitalkopierern sind nur die notwendigen Dienste und Protokolle, in der Regel nur TCP/IP, aktiviert.
  - Im Netzwerk angeschlossene Digitalkopierer werden im Rahmen der Wartung mit den sicherheitsrelevanten Updates des Herstellers ausgestattet, alle anderen Updates nur bei Bedarf bzw. auf Kundenwunsch.
  - Nicht flüchtige Speicher (Flash oder Festplatten) in den Geräten werden vor der Entsorgung mechanisch zerstört oder datenschutzkonform formatiert, so dass eine Wiederherstellung der Daten ausgeschlossen ist.

2.8. Faxgeräte

Wie werden die Faxgeräte gegen unbefugte Nutzung und unbefugte Einsichtnahme eingehender Faxe geschützt?
(Reinigungskräfte, unbefugte Mitarbeiter, Besucher etc.)

Istzustand:

- Das Faxgerät für die öffentlich bekannte Fax-Nr. ist nur einem befugten Personenkreis (Sekretariat/Empfang) zugänglich. [26] [27] [28]

2.9. Netzwerkverkabelung

Wie ist das Netzwerk verkabelt?
(Standort der Sternverteiler, Zugriff durch unbefugte Nutzung etc.)

Istzustand:

- Die Netzwerkverkabelung ist als CAT5/6/7-Verkabelung eingerichtet. Die Sternverteiler sind Eigentum der verantwortlichen Stelle und beinhalten nur eigene Geräte.

3. Datenträgerkontrolle

3.1. Vernichtung von Akten und Datenträgern

Wie wird die ordnungsgemäße Vernichtung von Akten und Datenträgern sichergestellt?
(vertrauliches und/oder personenbezogenes Schriftgut am Arbeitsplatz entsorgt oder zwischengelagert, zentrale Entsorgung über Entsorgungsunternehmen)

Istzustand:

- Damit keine Datenschutzpannen geschehen, sind die wesentlichsten Anforderungen an

die datenschutzgerechte Entsorgung von Datenträgern mit schutzwürdigen Daten und die dabei zu ergreifenden Sicherheitsmaßnahmen innerhalb eines Entsorgungskonzeptes festgehalten. [29] [30]
- Die verantwortlichen Entscheidungsträger, Administratoren und alle Mitarbeiter sind durch geeignete Information und Schulung zum Thema Datenträgerentsorgung sensibilisiert. Das Datenträgerentsorgungskonzept wurde auch den Mitarbeitern bekannt gegeben. [29] [30]
- Bei der internen Vernichtung von Akten und anderem vertraulichem Schriftgut mit einem Schredder bzw. Reißwolf wird darauf geachtet, dass die DIN 66399-2 Sicherheitsstufe P-4 (Fläche der Materialteilchen max. 160mm² und für gleichförmige Partikel: Breite des Streifens max. 6mm) eingehalten wird. [31] [32] [29] [33] [30]
- Das Vernichten von Datenträgern erfolgt nach Maßgabe der DIN 66399-2, Schutzklasse 3 bzw. Sicherheitsstufe 4 für besonders sensible Daten. Eine Reproduktrion ist damit nur mit außergewöhnlichem Aufwand möglich. Dementsprechend finden folgende Sicherheitsstufen Anwendung:
  - O-4 für CDs, DVD's,
  - T-5 für Magnetbänder,
  - H-5 für HDD-Festplatten (magnetischer Datenträger) und
  - E-4 für Speichersticks, SSD-Festplatten (Halbleiter) und andere mobile Datenträger.
  Das Löschen von Datenträgern erfolgt durch ein nach dem Maßnahmenkatalog M2.167 des BSI empfohlenes Verfahren zur Löschung von Datenträgern mit höherem Schutzbedarf. [31] [32] [33] [30]

3.2. Kopieren von Daten

Wie ist das Kopieren von Daten geregelt?
(Welche Daten werden kopiert, zu welchem Zweck, auf welchen Datenträgern, Schutz vor unbefugtem Zugriff, Dokumentation von Kopiervorgängen)

Istzustand:

- In einer IT-Nutzungsrichtlinie ist das Kopieren von Daten nur im Rahmen der Datensicherung und für die besonders geregelten Fälle der Datenweitergabe erlaubt, z. B. notwendiger Datenaustausch mit Kunden/Mandanten. [34]
- Die Datenübergabe an externe Stellen (Kunden, Servicepartner, Druckereien etc.) erfolgt über CDs und USB-Sticks. Die Datenträger werden mit einem Kennwort vor unbefugtem Zugriff geschützt. [35] [34]

3.3. Nutzung von Datenschnittstellen (USB u.a.)

Welche Maßnahmen werden für die Kontrolle der Datenschnittstellen eingerichtet? (Sperre der Schnittstellen, Endpoint-Protection u.a.)

Istzustand:

- Die USB-Schnittstellen und CD/DVD-Laufwerke werden über eine Endpoint-Protection überwacht bzw. gesperrt. Damit wird verhindert, dass Nutzer private Speichermedien im

Netzwerk oder an den Arbeitsplätzen anschließen können. [36]
- Die Nutzung der USB-Schnittstellen und der Schreibzugriff auf CD/DVD werden auf das Notwendige beschränkt. [36]

4. Speicherkontrolle

4.1. Löschkonzepte für interne Daten

Werden die gesetzlichen Löschfristen eingehalten? (Ausgeschiedene Mitarbeiter, Bewerberdaten etc.)

Istzustand:

- Bzgl. der Lösch- und Aufbewahrungsfristen wird keine Unterscheidung zwischen Papier und elektronischen Daten gemacht. Die Aufbewahrungs- und Löschfristen sind nicht auf elektronische Archivsysteme anwendbar, da hier ein partielles Löschen technisch und organisatorisch nicht umzusetzen ist. Die Archivsysteme sind nur einem eingeschränkten und berechtigtem Personenkreis zugänglich. Eine Manipulation (Löschen, Verändern) der Archivdaten ist nicht möglich. [37]
- Grundsätzlich werden personenbezogene Daten gelöscht, wenn der Zweck der Verarbeitung nicht mehr gegeben ist und keine gesetzlichen Aufbewahrungspflichten dem widersprechen. Ist eine Löschung nicht möglich werden die Daten vor einer weiteren Verarbeitung gesperrt. [38] [39] [40] [41]
- Jahresabschlüsse und Steuererklärungen werden nach 12 Jahren (10+2) wegen möglicher Fahndungsfälle für eine Weiterverarbeitung gesperrt. [42]
- Eigene Buchungsunterlagen (Belege) werden nach 12 Jahren vernichtet. [42]
- Arbeitsverträge, Dienstanweissungen und Einwilligungserklärungen von Mitarbeitern werden aufgrund von Nachweismöglichkeiten nicht vernichtet.
- Lohn- und Gehaltsnachweise von Mitarbeitern werden wegen Nachweismöglichkeiten gegenüber der Rentenversicherung nicht vernichtet, sondern lediglich für eine Weiterverarbeitung gesperrt.
- Bewerbungsunterlagen (Anschreiben, Zeugnisse, Lebenslauf etc.) werden bei Nichteinstellung spätestens nach 6 Monaten zurückgeschickt bzw. gelöscht. Begründung: Nachweis über die Einhaltung des Benachteiligungsverbotes. [43] [44] [45]
- Notwendige Gehaltsdaten und die Meldungen an das Finanzant und Sozialkassen der eigenen Mitarbeiter werden nach dem Ausscheiden wegen möglicher Lohnsteuerprüfungen erst nach 10 Jahren gelöscht. Sofern eine Löschung aus technischen Gründen nicht möglich ist, werden die Daten für eine Weiterverarbeitung gesperrt.
- Personalunterlagen ausgeschiedener Mitarbeiter die nicht für den Lohn- und Entgeltnachweis benötigt werden, z. B. Bewerbungsunterlagen, Zeugnisse etc. werden 3 Jahre nach dem Ausscheiden gelöscht oder sofern eine Löschung nicht möglich ist für eine Weiterverarbeitung gesperrt.

4.2. Löschkonzepte für externe Daten

Werden die gesetzlichen Löschfristen eingehalten? (Ausgeschiedene oder passive Kunden/Mandantendaten)

Istzustand:

- Bzgl. der Lösch- und Aufbewahrungsfristen wird keine Unterscheidung zwischen Papier und elektronischen Daten gemacht. Die Aufbewahrungs- und Löschfristen sind nicht auf elektronische Archivsysteme anwendbar, da hier ein partielles Löschen technisch und organisatorisch nicht umzusetzen ist. Die Archivsysteme sind nur einem eingeschränkten und berechtigtem Personenkreis zugänglich. Eine Manipulation (Löschen, Verändern) der Archivdaten ist nicht möglich. [37]
- Grundsätzlich werden personenbezogene Daten gelöscht, wenn der Zweck der Verarbeitung nicht mehr gegeben ist und keine gesetzlichen Aufbewahrungspflichten dem widersprechen. Ist eine Löschung nicht möglich werden die Daten vor einer weiteren Verarbeitung gesperrt. [38] [39] [40] [41]
- Verträge, Dauerakten und Einwilligungserklärungen von und mit externen Geschäftspartnern werden aufgrund von Nachweismöglichkeiten nicht vernichtet.

5. Benutzerkontrolle

5.1. Benutzeridentifikation und –authentifikation

Wie ist die Systemanmeldung grundsätzlich realisiert?
(Individuelle Anmeldung, Anmeldehierarchien, Need-to-know-Prinzip)

Istzustand:

- Jeder Nutzer kann jederzeit seine persönlichen Kennwörter auf Betriebssystemebene und in Anwendungsprogrammen selbst ändern.
- Die Systemanmeldung (Arbeitsplatz/Domain) ist individuell und geheim, d. h. die Anmeldeinformation ist keinem anderen Nutzer, auch nicht Ausnahmsweise für den Vertretungsfall der Geschäftsleitung oder dem Administrator bekannt. [46]
- Die Anmeldung am Terminalserver erfolgt über den Benutzernamen und einem persönlichen Kennwort. Mehrfachanmeldungen am Terminalserver führen zur Abmeldung der ersten Anmeldung mit einem entsprechendem Benutzerhinweis.

5.2. Passwortregelungen

Wie sind die Passwortkonventionen grundsätzlich umgesetzt?
(Geheim, kryptischer Zwang, Gültigkeitsdauer, Fehlversuche ...)

Istzustand:

- Es gibt im Rahmen der EDV-Nutzungsrichtlinien schriftlich fixierte Passwortkonventionen in der auch die Geheimhaltung und die Passwortänderung festgelegt ist. [46]
- Passworte bestehen aus mindestens 10 Zeichen, Groß- und Kleinbuchstaben, mindestens einem Sonderzeichen und einer Ziffer. Die Passworte enthalten keine

zusammenhängenden Worte oder Wortfragmente die aus einem Wörterbuch stammen. [46]
- Die Passwortkonventionen werden, sofern möglich, vom Betriebssystem bzw. der Applikation eingefordert.
- Die Passworte sind geheim und individuell. [46]
- Passworte werden an keiner Stelle im Klartext aufbewahrt oder gespeichert. [46] [47]
- Die Einrichtungspassworte müssen bei der ersten Systemanmeldung zwangsweise geändert werden. [46]
- Die Administrationspassworte sind kryptisch, einmalig und werden regelmäßig geändert.
- Administrationspassworte sind nur dem zuständigen Mitarbeiter bekannt. Für den Notfall werden diese verschlüsselt gespeichert und können nur von der Geschäftsleitung entschlüsselt werden.

5.3. Nutzung der Rechner

Wie werden die Rechner gegen eine unbefugte Nutzung geschützt?
(Bootschutz, individuelle Anmeldung etc.)

Istzustand:

- Die Systemnutzung ist hierarchisch aufgebaut. Jede Anmeldung, d.h. lokal, Domaine und CRM erfolgt über eine individuelle und geheime Anmeldung mit Name und verschiedenen Passwörtern.
- Die Zutrittskontrolle sowie die Benutzeridentifikation und Benutzerauthentifikation (Individuelle Anmeldung, SmartCard, etc.) verhindern eine unbefugte Nutzung der Rechner.
- Die BIOS-Einstellungen verhindern einen Start über eine Boot-Diskette, eine bootfähige CD oder einen bootfähigen USB-Stick, durch den die Sicherheitseinstellungen umgangen werden könnten. [48] [49]
- Der Zugang zum BIOS aller Rechner ist über ein Passwort geschützt, das nur der Geschäftsleitung und dem Administrator bzw. Systembetreuer bekannt ist. [50] [48] [49]
- Auf den fest installierten Arbeitsplätzen befinden sich keine schutzwürdigen oder personenbezogene Daten. Auf den Notebooks der Techniker befinden sich nur temporär Kundendaten. Aus diesem Grund sind die Notebooks alle vollständig verschlüsselt.

5.7. Internetzugang

Wie ist der Internetzugang realisiert?
(Absicherung, Nutzung, Contentfilter etc.)

Istzustand:

- Der Internetzugang erfolgt ausschließlich über eine UTM (Unified Threat Management) mit aktivem Contentfilter. Damit wird das Risiko Schadsoftware über den Besuch von Webseiten auf den lokalen Computer zu laden minimiert. Die Blacklisten der aktiven Contentfilter werden automatisch aktualisiert und Webseiten mit bekannten Bedrohungen werden automatisch gesperrt. [51]

- Es erfolgt keine automatisierte und individuelle Protokollierung der Internetverbindungen. Eine personenbezogene Auswertung erfolgt nur bei konkretem Missbrauchsverdacht unter Einbeziehung des Datenschutzbeauftragten.
- Es werden nur vom Hersteller aktuell gepatchte Browser eingesetzt (Microsoft IE 11,Microsoft Edge, Mozilla Firefox, etc.). [52]
- Die verwendeten Browser wurden entsprechend der BSI Empfehlung angepasst. Darunter zählen z.B.:

  Mozilla Firefox:
  - Master-Passwort ist aktiviert.

  Google Chrome:
  - Passwort-Manager samt Master-Passwort wurde per Add-on installiert; alternativ wird auf einen Passwort-Manager verzichtet.

  Microsoft Internet Explorer:
  - Maßnahmen zur Aktualisierung von Erweiterungen beziehungsweise deren Sperrung.
  – Passwort-Manager samt Master-Passwort wurde per Add-on installiert; alternativ wird auf einen Passwort-Manager verzichtet.
  – Es steht ein zweiter Browser zur Verfügung beziehungsweise kann kurzfristig verfügbar gemacht werden; alternativ kann ein zweiter, virtualisierter Internet Explorer genutzt werden. [53] [52] [54]

5.8. Sicherheitseinstellungen für PC und LAN

Welche Sicherheitsmaßnahmen sind für den Internetzugang auf den Arbeitsplätzen (PCs) und im Netzwerk (LAN) eingerichtet?
(Firewall, Browser, Änderungsschutz etc.)

Istzustand:

- Die Konfiguration der lokalen Sicherheitsgateways (Firewall) inkl. aller Filterregeln ist mit Angabe des Gerätetyps und dem verantwortlichen Techniker dokumentiert, d. h. freigegebene Dienste und Ports, WLAN und eingerichtete VPN-Zugänge und ggfs. Contentfilter. [55]
- Die Browsereinstellungen sind unter Berücksichtigung der Anwendungen auf die höchst mögliche Sicherheitsstufe eingestellt. [56] [52]
- Die Büroangestellten haben keine Administrationsrechte. Damit wird verhindert, dass ein Nutzer selbst einen Browser und andere Programme installieren und die Sicherheitseinstellungen selbst verändern kann. [57]
- Die Sicherheitspatches für das Betriebssystem und die verwendeten Browser werden auf allen Geräten (Terminalserver und ggfs. auch lokale Arbeitsplätze) aktuell und automatisch installiert. Die Aktualisierung erfolgt nicht in festen Abständen, sondern werden nach Erforderlichkeit durchgeführt. Das bedeutet, dass relevante Updates, die ein hohes Sicherheitsrisiko darstellen zeitnah installiert werden. Neben den Microsoft Updates ist auch die zeitnahe Aktualisierung der Anwendungen:

- Adobe Flash-Player
- Acrobat-Reader und
- Java-Modul

organisiert. [58]

- Die Konfiguration der lokalen Firewall ist nur einem autorisierten Personenkreis möglich.

5.9. Einsatz von Smartphones

Wie werden die dienstlich genutzten Smartphones geschützt?
(Passworte, Verschlüsselung, Sicherheitssoftware, Ortung etc.)

Istzustand:

- Smartphones werden für dienstliche Zwecke von der Geschäftsführung und einigen fest angestellten Mitarbeitern (Technikern) genutzt. Alle Smartphones sind Eigentum der verantwortlichen Stelle.
- Es werden sichere Passwörter für das Entsperren der Smartphones verwendet, d. h. kryptisch oder biometrisch. Die Geräte werden nach einigen Minuten automatisch bei Nichtnutzung gesperrt. [59]
- Auf den Smartphones werden Kontakte, E-Mails und Termine über den Exchange-Server synchronisiert. Für diesen Fall ist eine Fernlöschung der E-Mails im Verlustfall eingerichtet. [60]
- Die Smartphones werden automatisch mit dem aktuellen Betriebssystem ausgestattet. [61] [59]
- Die mobilen Endgeräte (Smartphones, Tablets etc.) werden über ein zentrales "Mobile Device Management (MDM)" verwaltet. Darüber lässt sich die Synchronisation mit dem Exchange Server (Kalender, E-Mails, Aufgaben etc.) zentral verwalten, d. h. Sperren, Freigeben, Löschen. Über Benutzerprofile lassen sich bei Bedarf Funktionen sperren. Für die Endgeräte ist eine Ortung, Fernsperrung und Fernlöschung eingerichtet. Der Gerätestatus, z. B. installierte Apps, Betriebssystemversion etc., kann zentral abgerufen werden. Darüber hinaus kann die Installation von Apps zentral gesperrt bzw. freigeschaltet werden. [62]
- Der Instant-Messaging-Dienst "WhatsApp" wird nicht genutzt. [63] [64] [65]
- Der iCloud Dienst für die Apple-Geräte ist deaktiviert. [59]
- Bei der Neuanschaffung von iPhones wird auf aktuelle Hardware geachtet. Geräte, die vom Betriebssystemhersteller nicht mehr unterstützt werden, werden durch neue ersetzt. [59]

5.10. Telefonanlage

Welche Sicherheitsmaßnahmen sind für den Schutz der Telefonanlage vorgesehen?
(Administration, Kostenpflichtige Ruf-Nr., Notfallmanagement, Protokollierung etc.)

Istzustand:

- Die TK-Anlage wird automatisch mit dem aktuellen Sicherheitspatches ausgestattet.
- Die Administrationsanmeldeversuche an der TK-Anlage sind begrenzt, um ein

Ausspähen des Kennwortes zu verhindern.
- Der Notfall bzw. der Ausfall der TK-Anlage ist mit dem zuständigen TK-Dienstleister detailliert besprochen und dokumentiert. Dazu gehört auch die Datensicherung der TK-Anlage.
- Es erfolgt keine automatische bzw. regelmäßige Auswertung der Verbindungsdaten (Rufnummern, Gesprächsdauer) zur Profilbildung. Eine Auswertung der Protokolldateien erfolgt nur bei konkretem Missbrauchsverdacht im Einzelfall.
- Die TK-Anlage ist über ein CTI-Modul mit der Anwendersoftware, z. B. Outlook verknüpft. Die Verbindungsdaten sind nur dem Mitarbeiter zugänglich, der diese selbst löschen kann oder zu Abrechnungszwecken einem Mandanten zuordnen kann.
- Die TK-Anlage ist in einem separaten Sicherheitsbereich, wie zum Beispiel in einem abschließbaren Rechnerraum aufgestellt. Der Zutritt zu dem Raum beziehungsweise Zugriff auf die Anlage selbst ist geregelt. [66]

5.11. Zeitweises Verlassen des Arbeitsplatzes

Wie wird der Arbeitsplatz bei zeitweisem Verlassen gegen eine unbefugte Nutzung gesperrt?
(Zeitgesteuerter Bildschirmschoner mit Passwort, Screenkeeper o.ä.)

Istzustand:

- Auf allen Arbeitsplätzen ist ein passwortgeschützter Bildschirmschoner aktiviert, der sich spätestens nach 15min. automatisch einschaltet. Damit wird eine unbefugte Nutzung bei Abwesenheit des Mitarbeiters verhindert. [67] [68]

5.12. Zeiterfassung bzw. Zeitkonten der Mitarbeiter

Wie werden die Zeitkonten bzw. die Anwesenheit der Mitarbeiter verwaltet?
(Automatisierte Zeiterfassung, Zugriffsrechte etc.)

Istzustand:

- Keine EDV gestützte Zeiterfassung, nur handschriftliche Zeiterfassung der Mitarbeiter.

5.13. E-Mail Postfächer

Wie ist der Zugriff auf die E-Mail Konten organisiert?
(Einrichtung, Vertretungsregelung, Archivierung, etc.)

Istzustand:

- Alle ein- und ausgehenden E-Mails werden in Kopie in einem zentralen Mailarchiv abgelegt. Auf dieses Mailarchiv hat nur das Sekretariat für die Weiterleitung bei Abwesenheit eines Kollegen lesenden Zugriff. Schreibzugriff hat nur die Geschäftsleitung. [69]
- Alle Zugangsdaten zu den E-Mail Postfächern sind nur dem Administrator und der Geschäftsleitung bekannt.

- Die Mitarbeiter haben in einer IT-Nutzungsrichtlinie ihre Zustimmung für den Zugriff der Geschäftsführung auf die E-Mails gegeben. Hierin wird ausdrücklich darauf hingewiesen, dass systembedingt keine Unterscheidung zwischen dienstlichen und privaten E-Mails erfolgt. Eine Einsichtnahme auf den individuellen E-Mail-Account der Mitarbeiter ist aus organisatorischen Gründen (Vertretungsfall, Kontrollpflicht der Geschäftsleitung) nicht vermeidbar.
- In einer Organisationanweisung ist festgelegt, dass beim Ausscheiden eines Mitarbeiters auf dem Mailserver (Exchange) eine Weiterleitung der E-Mails auf die allgemeine E-Mail-Adresse der Kanzlei eingerichtet und eine Autoantwort für den Absender eingetragen wird. Auf diese Weise wird sichergestellt, dass auch die E-Mails ausgeschiedener Mitarbeiter bearbeitet werden.
- Scheidet ein Administrator aus, der eine Zugangsberechtigung auf den Mail-Provider (ISP) hat, werden alle Kennwörter für den Provider, den FTP-Server und die Kennwörter aller E-Mail Konten geändert. Damit wird verhindert, dass der ausgeschiedene Administrator unberechtigter Weise Zugang zum Webserver und zu allen E-Mail Postfächern hat.

5.14. IT-Nutzungsrichtlinie

Gibt es eine IT-Nutzungsrichtlinie?
(Dienstvereinbarung zur Internetnutzung, Nutzung des dienstlichen E-Mail-Accounts inklusive Zugriff und Vertreterregelung)

Istzustand:

- Die Nutzung des Bildschirmarbeitsplatzes wurde in einer IT-Nutzungsrichtlinie festgelegt. Darin ist auch die Internetnutzung und der Umgang mit dem dienstlichen E-Mail-Account geregelt. [70]

6. Zugriffskontrolle

6.1. Zugriffsberechtigungen

Wie sind die Zugriffsberechtigungen auf personenbezogene Daten organisiert?
(Anwendungsprogramme, Personaldaten, Benutzerberechtigungen etc.)

Istzustand:

- Die Zugriffsberechtigungen auf die Anwendungsprogramme werden in einer Verarbeitungsübersicht geführt. In dieser Liste ist eine Zuordnung ersichtlich, welche Personen auf welche Daten zugreifen können. Hierbei wird das Need-to-know-Prinzip beachtet. [71]
- Die Lohn- und Gehaltsbuchhaltung wurde an einen Steuerberater ausgelagert.
- Die Personalakten befinden sich in verschlossenen Aktenschränken, die nur der Personalverwaltung zugänglich sind.
- Es erfolgt keine Auftragsdatenverarbeitung nach Artikel 28 DSGVO oder § 80 SGB X in Telearbeit [22] [72]

- Bei Telearbeitsplätzen, dazu gehören HomeOffice-Arbeitsplätze und mobile Arbeitsplätze, ist der Zugriff des Berechtigten zu personenbezogenen Daten nur mit BenutzerID und PIN oder Zertifikat möglich (Zwei-Faktor-Authentifizierung). [22]

6.2. Systemadministration

Wie ist die Systemadministration geregelt?
(Personenkreis, Umfang der Berechtigung, Protokollierung der Tätigkeiten, Netzwerkdokumentation, Admin-Passworte)

Istzustand:

- Das Netzwerk ist in einer übersichtlichen Form aktuell dokumentiert. Dazu gehört:
  - Netzwerkstrukturplan (Grundsätzlicher Aufbau des LANeund eingerichtete Fernzugriffe)
  - Serverübersicht mit den darauf installierten Programmen
  - Benutzerverwaltung (Zugriffsrechte der eingerichteten Benutzer)
  - Browsereinstellungen (Eingerichtete Sicherheitsstufe)
  - Firewall-Konfiguration und Virenschutzschutzkonzept
  - Datensicherungskonzept mit Zugriffsrechten [73]
- Da die Netzwerkdokumentation schutzwürdige Informationen beinhaltet, wird sie sicher aufbewahrt und der Zugriff ist geregelt. [73]
- Alle administrativen Zugangsdaten sind der Geschäftsführung bekannt.
- Beim Wechsel oder Ausscheiden eines Administrators wird in einer Organisationsanweisung sichergestellt, dass alle Systempassworte umgehend geändert werden.

6.3. Fernzugriff

Sind die Kunden/Mandanten darüber informiert, dass der Systempartner sich über eine Remoteeinwahl auf die Server einwählen kann und wird der Fernzugriff überwacht bzw. protokolliert?

Istzustand:

- Der Fernzugriff zu Wartungszwecken auf die Kundennetze erfolgt je nach Zweck auf unterschiedliche Weise.
- Jeder Fernzugriff ist über eine User-ID mit Zeitstempel für die Ein- und Auswahl identifizierbar. Ein vom Auftraggeber unbemerkter Fernzugriff ist ausgeschlossen. [74] [5]
- Für die Zugriffs- und Eingabekontrolle sind geeignete Maßnahmen vorgesehen, die es dem Auftraggeber ermöglichen, die durchgeführten Tätigkeiten lückenlos nachzuvollziehen. Alle unbeobachteten Bedienungen einer Fernwartungssitzung werden zu diesem Zweck als Mitschnitt aufgezeichnet und 12 Monate zu Kontrollzwecken aufbewahrt. [74] [5]
- Einzelne Aufzeichnungen bzw. Mitschnitte der Fernwartungssitzungen werden dem Auftraggeber oder dem Datenschutzbeauftragten des Auftraggebers auf Nachfrage zur

Verfügung gestellt. Die Auswahl trifft der Auftraggeber. Dabei werden mindestens vier Aufzeichnungen pro Kalenderjahr dem Auftraggeber in einem Standardvideoformat für eine Stichprobenkontrolle zur Verfügung gestellt. [5] [75]
- Für den Fernzugriff ist eine Zwei-Faktor-Authentifizierung vorgesehen. [74]
- Eine Fernwartung erfolgt grundsätzlich nur über eine VPN-Verbindung. [74] [5]
- Die Fernsteuerung eines Arbeitsplatzes (Host) erfolgt nur nach Anmeldung und Zustimmung des Auftraggebers oder einer von dieser autorisierten Person. Der ferngesteuerte Host hat jederzeit die Möglichkeit die Verbindung über ein Menü zu beenden. Alle Bedienungen durch das Systemhaus (Client) können auf dem ferngesteuerten Host visuell mitverfolgt werden. [74]
- Die Routerkonfiguration ist nur einem autorisierten bzw. eingeschränktem Personenkreis möglich. Alle Änderungen werden mit Zeitstempel und Name des verantwortlichen Technikers protokolliert. [74]

6.4. Verpflichtung zur Wahrung der Vertraulichkeit

Sind die Mitarbeiter im Rahmen ihres Arbeitsverhältnisses auf die Wahrung der Vertraulichkeit personenbezogener Daten verpflichtet worden und haben alle Dienstleister eine Verpflichtungserklärung zur Wahrung der Vertraulichkeit personenbezogener Daten abgegeben? (Systemhaus, Reinigungskräfte, Servicedienstleister für die Kopierer, Sicherheitsdienst)

Istzustand:

- Die Mitarbeiter wurden im Rahmen ihres Arbeitsvertrages auch auf die Wahrung der Vertraulichkeit personenbezogener Daten verpflichtet.
- Die interne Reinigungskraft hat eine Verpflichtungserklärung zur Wahrung der Vertraulichkeit personenbezogener Daten abgegeben.
- Die Fensterreinigungsfirma hat eine Verpflichtungserklärung zur Wahrung der Vertraulichkeit personenbezogener Daten abgegeben.

7. Übertragungskontrolle

7.1. Kommunikation über das Internet

Die Übertragungskontrolle über das Internet soll die Vertraulichkeit der elektronischen Datenübertragung sichern (Verschlüsselung der Daten, VPN-Tunnel, Firewall, Virenschutz, Intrusion Detection, Content-Filter u.a.)

Istzustand:

- In den Browsereinstellungen ist die "Do not track" Option aktiviert. [76]

7.2. Externe Anbindungen

Wie werden externe Anbindungen, z.B. Homeoffice, Mobile Arbeitsplätze, betriebfremde Einrichtungen etc.) vor unberechtigtem Zugriff geschützt?

(VPN, Vertschlüsselung der Daten, Firewall etc.)

Istzustand:

- Alle extern genutzten Geräte für die Telearbeit sind Eigentum der verantwortlichen Stelle (Unternehmen). Damit wird sichergestellt, dass auf den Geräten die notwendigen Sicherheitseinstellungen (Virenschutz, Sicherheitspatches usw.) vorhanden sind und das Gerät auch nur für dienstliche Zwecke genutzt werden kann.
- Die Anbindung externer Arbeitsplätze erfolgt ausschließlich über ein sogenanntes Virtual Private Network (VPN). [22]
- Eine Datenübertragung zwischen Zentrale und externen Anbindungen, z.B. zum Zweck eines Remotezugriffs durch einen Hotline-Mitarbeiter erfolgt grundsätzlich nur verschlüsselt (Ende-zu-EndeSicherheit). [22]
- Die Telearbeitsplätze nutzen den privaten DSL-Zugang für den Zugang zum Firmennetzwerk. Aus Sicherheitsgründen (Malware, Mithören etc.) ist der Telearbeitsplatz jedoch vom Heimnetzwerk des Mitarbeiters getrennt. [22]
- Die VPN-Verbindung zum Unternehmen wird von einer UTM (Unified Threat Management) überwacht, damit sich hierüber keine Schadsoftware unbemerkt auf den Terminalserver übertragen kann.
- Mitarbeiter, die extern bei Kunden arbeiten nutzen für die Anbindung an das Firmennetzwerk einen separaten UMTS/LTE Router oder eine RED-Box für die Anbindung an das LAN beim Kunden.

8. Eingabekontrolle

8.1. Protokollierung der Dateneingabe

Werden die Nutzung der Anwendungsprogramme und die Veränderungen an den Datensätzen und Dokumenten mit Name und Zeitstempel protokolliert?

Istzustand:

- Jeder Mitarbeiter hat eine eigene E-Mail Adresse über die er seine E-Mails versendet. Ausgehende E-Mails lassen sich damit immer einer bestimmten Person zuordnen.
- Veränderungen in den Datensätzen zur Finanz, Lohn- und Gehaltsbuchhaltung werden mit Zeitstempel und Benutzername protokolliert.
- Mobile Datenträger (USB-Sticks etc.) werden zentral überwacht bzw. der Datenverkehr wird protokolliert.
- Das eingesetzte CRM-System, das von allen Mitarbeitern für die Kundenbeziehungen genutzt wird, protokolliert alle Änderungen mit Name und Zeitstempel revisionssicher
- Alle Bedienhandlungen im Rahmen eine Fernwartungssitzung werden revisionssicher als Mitschnitt aufgezeichnet.

9. Transportkontrolle

9.1. E-Mail Versand

Welche Maßnahmen zum Schutz der E-Mails gegen Manipulation bzw. Veränderung wurden umgesetzt?
(Virenprüfung, digitale Signatur etc.)

Istzustand:

- E-Mails werden vor dem Versand vom installierten Antivirenprogramm automatisch auf Schadsoftware geprüft.

9.2. E-Mail Verschlüsselung

Wie werden E-Mails mit personenbezogenen oder anderen schutzwürdigen Daten gegen unbefugten Zugriff geschützt?
(Verschlüsselung der Inhalte, Anhänge etc.)

Istzustand:

- Jeder Mitarbeiter besitzt für seinen Email-Account eine SmartCard der DATEV mit Zertifikat, das für eine Verschlüsselung und digitale Signatur verwendet werden kann. [77]
- Die Verschlüsselung erfolgt mit einem DATEV-Zertifikat auf einer Smartcard. Für die Entschlüsselung sind zwei Varianten implementiert.

  1. Empfänger besitzt kein S/MIME-Zertifikat
  Die Entschlüsselung erfolgt in diesem Fall über das DATEV Entschlüsselungsportal. Der E-Mail Empfänger enthält dazu einen Link in einem Anhang (secure-email.html) auf das Entschlüsselungsportal. Auf dem Portal registriert sich der Empfänger indem er sich selbst ein Passwort vergibt (min. 8 Zeichen). Die Registrierung am Entschlüsselungsportal ist nur einmalig erforderlich und wird mit der ersten verschlüsselt empfangenen E-Mail durchgeführt.
  Nach der Registrierung kann die verschlüsselte E-Mail auf das Entschlüsselungsportal hochgeladen und entschlüsselt werden. Anschließend besteht die Möglichkeit die entschlüsselte E-Mail über eine Download-Funktion herunterzuladen.

  2. Empfänger besitzt ein S/MIME-Zertifikat
  In diesem Fall erfolgt keine Entschlüsselung über das Portal, da die E-Mail direkt beim Empfänger mit seinem privaten Schlüssel entschlüsselt wird.

9.6. Datenübertragung an die Finanzämter

Wie erfolgt die Datenübertragung an die Finanzämter?
(Lohnsteuer, Umsatzsteuer etc.)

Istzustand:

- Die Umsatzsteuer- und Lohnsteuermeldungen werden vom Steuerberater initiiert von der DATEV an das Finanzamt übertragen.

9.7. Meldungen der Sozialversicherungen

Wie erfolgt die Datenübertragung an die Krankenkassen?
(Sozialversicherungsbeiträge, elektronischer Medlung über SV.net etc.)

Istzustand:

- Die Sozialversicherungsmeldungen werden vom Steuerberater initiiert von der DATEV an die Krankenkassen übertragen.

9.8. Online-Banking (eigene Zwecke)

Wie wird das Online-Banking vor unbefugtem Zugriff geschützt?
(Individuelle Zugangsdaten, HBCI-Zertifikate etc.)

Istzustand:

- Für das Online-Banking kommt grundsätzlich das aktuellste HBCI-Sicherheitsverfahren der Bank zur Anwendung.
- Das Online Banking für das eigene Unternehmen erfolgt direkt über die verschlüsselte (SSL) Webseite der Bank.

9.9. Kontenzugriff auf Konten Dritter

Wie wird der Zugriff auf die Bankkonten von Kunden/Mandanten vor unbefugter Nutzung geschützt?
(Zertifikate, individuelle Zugangsdaten etc.)

Istzustand:

- Für einige Kunden/Mandanten gibt es ein SEPA-Lastschriftmandat für den Einzug fälliger Rechnungen. Der Lastschrifteinzug kann nur von einem berechtigtem Personenkreis ausgeführt werden. Die dafür notwendigen Authentifizierungsdaten werden verschlossen aufbewahrt.

9.10. Wahrung des Briefgeheimnisses

Gibt es klare Regeln, wie mit der Wahrung des Briefgeheimnisses umgegangen wird?
(Persönlich adressierte Post, Inhalt von Infobriefen)

Istzustand:

- Ausgangspost mit schutzwürdigem Inhalt wird grundsätzlich nicht als Infopost deklariert.

9.11. Umgang mit eingehenden Daten

Wie ist der Umgang mit eingehenden Daten geregelt?
(Externe Datenträger, E-Mails inkl. Anhänge etc.)

Istzustand:

- Den Mitarbeitern ist es im Rahmen einer schriftlich fixierten IT-Nutzungsrichtlinie nicht gestattet private Datenträger in jedweder Form am Arbeitsplatz oder im Netzwerk anzuschließen, dazu gehören insbesondere Notebooks, CDs, USB-Sticks und Smartphones.
- Der E-Mail Client ist so eingestellt, dass eingebettete Bilder in den E-Mails nicht automatisch geladen werden, um damit zu verhindern, dass sich Schadsoftware über eingebettete Bilder ausbreiten kann.
- Die Sicherheitseinstellungen in den Office-Programmen (MS-Word, MS-Excel etc.) sind so eingestellt, dass integrierte Makros nur nach Bestätigung durch den Anwender ausgeführt werden.
- Die Mitarbeiter wurden im Rahmen einer IT-Nutzungsrichtlinie angewiesen E-Mail Anhänge unbekannter Herkunft grundsätzlich nicht zu öffnen und E-Mails unbekannter Herkunft nur im Textformat zu lesen.
- Die Mitarbeiter wurden im Rahmen einer Datenschutzschulung im Umgang mit E-Mails geschult. Unter anderem wurde darauf hingewiesen, dass E-Mail Anhänge unbekannter Herkunft grundsätzlich nicht geöffnet werden sollen. Ferner sollen E-Mails unbekannter Herkunft nur im Textformat gelesen werden.
- Downloads werden automatisch mit dem lokalen Virenscanner auf Schadsoftware geprüft.
- Die Autovorschau im E-Mail Programm ist deaktiviert.
- Die Kommunikation mit dem Mailserver (Provider) erfolgt über den Einsatz eines Verschlüsselungsprotokolls SSL/TLS bzw. STARTTLS.
- Ausführbare Dateien (*.com; *.exe; *.bat) werden vom Mailserver geblockt und nicht zugestellt.

9.12. Mobile Datenträger

Wie ist die Handhabung von mobilen Datenträgern geregelt?
(Welche mobilen Datenträger sind im Einsatz, schutzbedürftige Daten, Auswirkungen eines Verlusts, Aufbewahrungsort, Schutz vor unbefugtem Zugriff/Diebstahl, Kennzeichnung, Virenscan bei ein- und ausgehenden Datenträgern)

Istzustand:

- Firmeneigene mobile Datenträger (USB-Sticks, Datensicherungsmedien u.a.) sind grundsätzlich verschlüsselt.
- Alle transportablen Datenträger werden eindeutig gekennzeichnet, um eine Verwechslungsgefahr auszuschließen. Bei Nichtbenutzung werden die Datenträger verschlossen aufbewahrt, z. B. beim zuständigen Mitarbeiter.
- Notebooks werden grundsätzlich verschlüsselt, sofern diese außer Haus transportiert werden und nicht ausgeschlossen werden kann, dass sich auf den Geräten personenbezogene Daten befinden.

9.13. Datenträger bei Telearbeitsplätzen

Wie werden Datenträger und Papierunterlagen bei den Telearbeitern vor unberechtigtem Zugriff geschützt? (verschlossene Behältnisse, Datenträgerverschlüsselung etc.)

Istzustand:

- Mobile Datenträger mit vertraulichen oder personenbezogenen Daten (CDs, USB-Sticks, Notebooks etc.) werden ausschließlich verschlüsselt transportiert. [22]
- Papierunterlagen werden nur in verschlossenen Behältern transportiert. [22]
- Datenträger und Unterlagen werden nie unbeaufsichtigt gelassen. [22]
- Arbeitsmittel zur sicheren Aufbewahrung von Personen bezogenen Daten wurden vom Arbeitgeber zur Verfügung gestellt. Dazu zählen z. B. verschließbare Einrichtungsgegenstände und datenschutzkonforme Aktenvernichter. [22]

10. Wiederherstellbarkeit

10.1. Datensicherung (lokale Server)

Wie wird die Zuverlässigkeit der Datensicherung sichergestellt? (Verantwortlichkeiten inkl. Vertretung, Sicherungsalgorithmus, Umfang der Datensicherung, Datensicherungsgeräte, Aufbewahrung der Datensicherung, Integritätsprüfung)

Istzustand:

- Für die Datensicherung sind verantwortliche Personen inkl. Vertreter benannt.
- Es wird wöchentlich eine Vollsicherung und täglich eine Differenzsicherung aller Bewegungsdaten durchgeführt. Zusätzlich werden besonders geschäftskritische Daten mehrmals täglich gesichert.
- Der genaue Umfang der Datensicherung, d. h. welche Daten von welchen Geräten (Arbeitsplätze, Server) gesichert werden ist dokumentiert.
- Alle Datensicherungsmedien werden verschlüsselt, um einen Zugriff durch Unbefugte zu verhindern.
- Das tägliche Datensicherungsprotokoll wird archiviert.
- Alle Server werden wöchentlich, jeweils am Wochenende, zusätzlich zur täglichen Datensicherung auf einer NAS (Network Attached Storage) in einem Image (1:1 Kopie) gesichert.
- Zum Schutz gegen Feuer, Wasser, Einbruch etc. wird täglich eine verschlüsselte Datensicherung auf eine NAS in das Home-Office des technischen Leiters übertragen.
- Alle Datensicherungsmedien sind im Netzwerk nicht sichtbar und können nur über eine separate Authentifizierung (Datensicherungsprogramm) erreicht werden. Damit sind die Datensicherungsmedien gegen Manipulationen und Schadsoftware (Verschlüsselungstrojaner etc.) geschützt. Zusätzlich sind die Datensicherungsmedien verschlüsselt.

10.5. Notfallszenario

Welche Maßnahmen sind für ein Notfallszenario vorgesehen?

(Ausfall zentraler Komponenten, Totalausfall der EDV-Anlage, Passwörter und Zugangsdaten im Unternehmen bekannt, Höhe des maximalen Schadens bei Datenverlust, Umfang des Arbeitsausfalls)

Istzustand:

- Das Notfallszenario beim Totalausfall des IT-Systems durch Feuer, Diebstahl etc. ist für jede zentrale Komponente (Router, Server, Sternverteiler, Telefonanlage etc.) separat dokumentiert, angefangen von der Hardwarelieferung, Datenrücksicherung bis zur vollständigen Wiederherstellung des Produktivsystems. Hierbei ist auch der zeitliche Faktor berücksichtigt, d. h. wie lange dauert es im Worst Case, bis das Produktivsystem wiederhergestellt ist und wie groß ist der maximale Ausfall und der maximale Datenverlust.
- Der Backupserver (NAS) befindet sich in einem anderen Brandschutzabschnitt.
- Um die Ausfallzeiten des Produktivsystems bei Serverausfall zu minimieren werden die Server unabhängig von der Datensicherung zusätzlich mindestens einmal pro Woche in einem Image gesichert.
- Alle Passwörter und Admin-Zugangsdaten (Server, Internetprovider, Banken etc.) werden auch außerhalb der Geschäftsräume an einem sicheren Ort in einem verschlossenen Briefumschlag aufbewahrt.
  Das gilt auch für die Daten die nur dem Inhaber oder Systembetreuer bekannt sind. [78]
- Für die Gewährleistung der Verfügbarkeit von Druckern, Kopierern und Multifunktionsgeräten wurden folgende Maßnahmen vorgesehen:
  - es stehen Ersatzgeräte bereit
  - in Wartungsverträgen ist eine angemessene Reaktionszeit vereinbart
  - es gibt eine Liste mit Fachhändlern, um schnell Ersatzgeräte oder -teile beschaffen zu können
  - ggf. werden wichtige Ersatzteile gelagert [25]

11. Zuverlässigkeit

11.1. Automatische Meldung von Fehlfunktionen

Wie werden Fehlfunktionen im System gemeldet?
(Monitoringsystem, Broadcastmeldungen etc.)

Istzustand:

- Die Server sind mit einem Monitoringsystem (z. B. LabTech, GfI etc.) ausgestattet. Damit werden mindestens folgende Komponenten überwacht und Warnmeldungen oder Störungen per E-Mail automatisch dem Systempartner gemeldet:
  - Überwachung der RAID-Festplatten
  - Überwachung der Servernetzteile
  - Lüfterüberwachung im Server
  - Notstromversorgung
  - Virenscanner
  - Windows-Updates

- notwendige Dienste
- Datensicherung

- Die Funktion der Serverüberwachung (Monitoring) sind beschrieben, d. h. welche Störungen werden an wen gemeldet und wann werden die Störungen behoben.
- Die Umschaltung auf die Notstromversorgung führt zu einer automatischen Meldung an den Arbeitsplätzen (Broadcastmeldung).
- Eine Nichtaktualisierung des Virenschutzes führt spätestens nach 4 Tagen zu einer automatischen Meldung an die Geschäftsleitung bzw. an den Administrator.
- Durch eine Advanced Threat Protection (Sophos) werden infizierte Rechner schnell entdeckt und isoliert und damit die Kommunikation mit bösartigen Command & Control Hosts verhindert.
- Jeder entdeckte oder vermutete Vireninfekt (Server und Arbeitsplatz) wird von der Virenschutzsoftware automatisch der Geschäftsleitung oder dem Administrator per E-Mail oder Broadcastmeldung angezeigt.

12. Datenintegrität

12.1. Datensicherung - Datenintigrität

Wie wird die Datenintigrität der Datensicherung sichergestellt? (Integritätsprüfung)

Istzustand:

- Die Integrität der Datensicherung wird mindestens einmal im Jahr überprüft. Dabei wird durch eine temporäre Rücksicherung die Vollständigkeit und Richtigkeit der Datensicherung festgestellt. Die Integritätsprüfung wird dokumentiert.

13. Auftragskontrolle

13.2. Zulässigkeit des Umgangs

Ist der Umgang mit personenbezogenen Daten zulässig?

Istzustand:

- Der Umgang mit personenbezogenen Daten von Auftraggebern ist zulässig gemäß Artikel 6 Absatz 1 lit. b zur Erfüllung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen.
- Der Umgang mit personenbezogenen Daten von Beschäftigten ist zulässig gemäß § 26 BDSG-neu Abs.1. Danach dürfen die Daten von Beschäftigten für Zwecke des Beschäftigtenverhältnisses verarbeitet werden. Dazu gehört auch die Datenverarbeitung, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses (etwa im Rahmen eines Bewerbungsverfahrens) oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Beschäftigte im Sinne des BDSG-neu sind u. a. Arbeitnehmer und zu ihrer Berufsbildung Beschäftigte. Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten ebenfalls als Beschäftigte.

13.3. Datensparsamkeit

Ist der Grundsatz der Datensparsamkeit und -vermeidung erfüllt?

Istzustand:

- Es wird nur mit den zur Erledigung der vertraglichen Aufgaben nötigen personenbezogenen Daten umgegangen
- Schutzwürdige Daten und personenbezogene Daten werden den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist.

14. Verfügbarkeitskontrolle

14.1. EMV-taugliche Stromversorgung

Absolut unverzichtbare Grundlage für die störungsfreie Funktion moderner IT-Systeme sowie der für deren Betrieb erforderlichen Supportsysteme (von der USV über die NEA bis hin zur Klimatechnik) ist eine EMV-taugliche Stromversorgung.
Wurden die Anforderungen Normgerecht umgesetzt?

Istzustand:

- Die Stromversorgung wurde den aktuell gültigen Normen entsprechend als TN-S-System mit ZEP (Zentralem Erdungspunkt) aufgebaut.
  Zur Erklärung:
  Übergabe vom Versorger: L1, L2, L3, PEN (4-Leiter-Netz)
  wird im Hausanschlussraum durch den Einsatz eines ZEP zu den Verbrauchern hin zu: L1, L2, L3, N, PE (5-Leiter-Netz). [79] [73] [80]

14.2. Notstromversorgung

Wie erfolgt die Notstromversorgung und die Überwachung der Klimaanlage im EDV-Raum? (Zentrale Systemkomponenten über eine USV abgesichert, Broadcast-Meldung im Falle eines Stromausfalls auf den Clients)

Istzustand:

- Alle zentralen Komponenten (Router, Switche, Server etc.) werden mit einer Notstromversorgung gegen Stromausfall und Netzschwankungen abgesichert.

14.3. Klimaanlage im EDV-Raum

Wird der EDV-Raum durch eine Klimaanlage gekühlt und wird diese überwacht?
(Meldung bei Ausfall der EDV-Klimaanlage)

Istzustand:

- Der Serverraum/Serverschrank wird durch eine Klimaanlage gekühlt. Der Ausfall der Klimaanlage führt zu einer zentralen Meldung.

14.4. Computer-Virenschutzkonzept

Wie ist das Virenschutzkonzept umgesetzt?
(Schutz aller Geräte vor Schadprogrammen, tägliche und automatische Aktualisierung des Virenschutzes, Dokumentation der durchgeführten Virenprüfung, automatische Meldung im Falle eines Infekts, Überwachung des aktiven Virenschutzes, Schutz des Virenschutzes gegen Manipulation, regelmäßiger vollständiger Virenscan)

Istzustand:

- Alle lokalen Server sind mit einer Antivirenschutzsoftware ausgestattet, die täglich aktualisiert wird.
- Auf allen lokalen Arbeitsplätzen ist ein Virenschutzprogramm eingerichtet, das täglich und automatisch aktualisiert wird.
- Es ist sichergestellt, dass alle angeschlossenen Speichermedien (USB-Sticks, CD/DVD etc.) automatisch einem Virencheck unterzogen werden. Entweder durch einen Komplettscan des Datenträgers nach dem er angeschlossen wurde oder durch einen Onlinescan bei dem die Dateien erst beim Zugriff gescannt werden.
- Die Autorun-Funktion mit der ausführbare Programme beim Anschluss oder beim Einlegen von Datenträgern automatisch gestartet werden ist deaktiviert.
- Durch eine Advanced Threat Protection werden infizierte Rechner schnell entdeckt und isoliert und damit die Kommunikation mit bösartigen Command & Control Hosts verhindert.
- In einer IT-Nutzungsrichtlinie sind die Mitarbeiter darauf hingewiesen worden, dass der im Hintergrund aktivierte Virenscanner nur einen oberflächlichen Schutz bietet. Aus diesem Grund führen die Mitarbeiter auf ihrem lokalen Arbeitsplatz regelmäßig, mindestens einmal pro Woche einen vollständigen manuellen Virenscan durch, sofern kein geplanter Virenscan eingerichtet ist.
- Die Konfiguration des Virenschutzprogramms auf den lokalen Arbeitsplätzen ist nicht vom Anwender änderbar, z. B. Deaktivierung des automatischen Scans externer Speichermedien.
- Das Netzwerk ist durch einen mehrstufigen Schutz gegen Schadsoftware abgesichert:
  1.) Network Protection
  2.) Enduser Protection
  3.) Server Protection

14.5. Wartung

Unterliegt die EDV einer regelmäßigen, vorbeugenden Wartung und wie sind die

Wartungstätigkeiten festgelegt und protokolliert?

Istzustand:

- Die gesamte IT-Infrastruktur unterliegt einer vorbeugenden Wartung, um das Risiko unvorhersehbarer Systemausfälle zu minimieren.

15. Trennbarkeit

15.1. Trennung der Verarbeitung

Wie erfolgt die Datentrennung für die Verarbeitung unterschiedlicher Zwecke? (Verarbeitung für eigene Zwecke und Verarbeitung im Auftrag, Trennung von privaten und geschäftlichen Daten auf mobilen Geräten bzw. Telearbeitsplätzen)

Istzustand:

- Für die Telearbeit werden keine privaten Geräte eingesetzt. Die Geräte werden ausschließlich dienstlich genutzt, eine private Nutzung ist untersagt.
- Auf den Telearbeitsplätzen erfolgt eine strikte Trennung von dienstlichen und privaten Daten. Sofern die Geräte auch privat genutzt werden erfolgt diese Nutzung in einer separaten Systemumgebung bzw. Partition.
- Das Prinzip der Funktionstrennung wird konsequent eingehalten, dabei erfolgt eine strikte Trennung zwischen auftragsbezogenen und internen Verarbeitungen und zwar organisatorisch und datentechnisch.
- Es ist gewährleistet, dass Daten zu unterschiedlichen Zwecken und für unterschiedliche Ordnungsbegriffe (z. B. Personal- Kunden/Mandantennummer) erhobene bzw. gespeicherte Daten getrennt verarbeitet werden können.
- Auf den dienstlich genutzten Smartphones ist eine MDM-App (Mobile Device Management) eingesetzt über die eine Datentrennung (Containerlösung) zwischen dienstlichen und privaten Daten eingerichtet ist.

17. E-Mail Kommunikation

17.1. E-Mail Signaturen

Erfüllen die E-Mail Signaturen die gesetzlichen Anforderungen? (Mitarbeiter unterrichtet, Vorgabe durch System, vom Absender editierbar)

Istzustand:

- Die E-Mail Signaturen für jeden E-Mail Account sind standardisiert und werden vom System automatisch generiert.
- Die Textsignatur in den E-Mails ist in maschinenlesbarer Form (Textformat) vorhanden. Bei einem ggfs. vorhandenen Logo mit den Firmenangaben als Grafik werden die Pflichtangaben zusätzlich als Text der E-Mail angehängt.
- Die E-Mail Signatur enthält die Pflichtangaben für eine GmbH:
  • Firmenbezeichnung wie im Handelsregister, Rechtsformzusatz "GmbH",

  - Ort der Handelsniederlassung,
  - zuständiges Registergericht, Handelsregisternummer,
  - Familienname und mindestens ein ausgeschriebener Vorname jedes Geschäftsführers.
- Der E-Mail Disclaimer enthält keine Haftungsreglungen für den Empfänger.

Literaturverzeichnis

[1] BfDI, INFO 4 - Die Datenschutzbeauftragten in Behörde und Betrieb, "INFO 4 - 1 Bestellung". http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO4.pdf?__blob=publicationFile, 2017-04.

[2] BfDI, , "Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f ". https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.html, 25.11.2010.

[3] BfDI, INFO 4 - Die Datenschutzbeauftragten in Behörde und Betrieb, "INFO 4 - 3.4 Schulung". http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO4.pdf?__blob=publicationFile, 2017-04.

[4] BSI, IT-Grundschutz-Kompendium, "ORP.3: Sensibilisierung und Schulung". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html, 05.11.2017.

[5] BStBK, Berufsrechtliches Handbuch, II Anhang, Anlage 1 zu 5.2.4, "Gefährdungspotential". https://www.bstbk.de/, 9.2017.

[6] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M22: Sichere Türen und Fenster". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 04.11.2017.

[7] BStBK, Berufsrechtliches Handbuch, II Anhang, Anlage 1 zu 5.2.4, "Gebäude- Und Raumabsicherung". https://www.bstbk.de/, 9.2017.

[8] DIN (Deutsches Institut für Normung e. V.), Vorschrift, "DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmu". https://www.beuth.de/de/norm/din-en-1627/116125567, 01.09.2011.

[9] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M27: Einbruchsschutz". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 05.11.2017.

[10] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M03: Einhaltung von Brandschutzvorschriften". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 04.11.2017.

[11] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M04: Branderkennung in Gebäuden [Planer]".

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 04.11.2017.

[12] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M34: Gefahrenmeldeanlage". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 05.11.2017.

[13] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M16: Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 04.11.2017.

[14] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M33: Anordnung schützenswerter Gebäudeteile". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 05.11.2017.

[15] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M26: Pförtner- oder Sicherheitsdienst". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 04.11.2017.

[16] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M07: Zutrittsregelung und -kontrolle [Leiter Organisation]". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 04.11.2017.

[17] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M12: Schlüsselverwaltung". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 04.11.2017.

[18] BSI, IT-Grundschutz-Kompendium Umsetzungshinweise, "INF.01.M39: Organisatorische Vorgaben für die Gebäudereinigung". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html, 05.11.2017.

[19] BSI, IT-Grundschutz-Kompendium, "INF.11: Besprechungs-, Veranstalltungs- und Schulungsräume". https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Besprechungsraum.html, 25.08.2017.

[20] BSI, IT-Grundschutz-Kompendium, "INF.07: Büroraum".

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Bueroraum.html, 25.08.2017.

[21] BOStB, BOStB § 5, Abs. 4, "Verschwiegenheitsverpflichtung". https://www.bstbk.de/, 9.2017.

[22] BfDI, Informationsflyer, "Telearbeit – Ein Datenschutz-Wegweiser ". https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html, 01.04.2017.

[23] BSI, IT-Grundschutz-Kompendium, "INF.09: Mobiler Arbeitsplatz". https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/UH_Mobiler_Arbeitsplatz.html, 21.06.2017.

[24] BSI, IT-Grundschutz-Kompendium, "INF.08: Häuslicher Arbeitsplatz". https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/UH_Haeuslicher_Arbeitsplatz.html, 15.12.2016.

[25] BSI, IT-Grundschutz-Kompendium, "SYS.04.1: Drucker, Kopierer und Multifunktionsgeräte". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_1_Drucker,_Kopierer_und_Multifunktionsger%C3%A4te.html, 14.01.2018.

[26] BSI, IT-Grundschutz-Kataloge, "M 1.37: Geeignete Aufstellung eines Faxgerätes ". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m01/m01037.html, 07.01.2018.

[27] BSI, IT-Grundschutz-Kataloge, "M 2.048 Festlegung berechtigter Faxbediener". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02048.html, 05.11.2017.

[28] BSI, IT-Grundschutz-Kataloge, "M 2.053 Abschalten des Faxgerätes außerhalb der Bürozeiten". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02053.html, 05.11.2017.

[29] BSI, IT-Grundschutz-Kataloge, "M 2.515 Datenschutzgerechte Löschung/Vernichtung". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02515.html, 25.11.2017.

[30] LDA_Bayern, , "Orientierungshilfe - Datenträgerentsorgung". https://www.datenschutz-bayern.de/technik/orient/oh_datentraegerentsorgung.pdf , 14.02.2014.

[31] BSI, IT-Grundschutz-Kataloge, "M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02167.html?nn=6610630, 11.11.2017.

[32] BSI, IT-Grundschutz-Kataloge, "M 2.435 Auswahl geeigneter Aktenvernichter ". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/

_content/m/m02/m02435.html, 06.11.2017.

[33] DIN (Deutsches Institut für Normung e. V.), Vorschrift, "DIN 66399:2012 Vernichten von Datenträgern". 2012.

[34] BSI, IT-Grundschutz-Kataloge, "M 5.088 Vereinbarung über Datenaustausch mit Dritten". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05088.html, 01.12.2017.

[35] BSI, IT-Grundschutz-Kataloge, "M 2.045 Regelung des Datenträgeraustausches". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02045.html?nn=6610610, 25.11.2017.

[36] BSI, , "Mindeststandard des BSI für Schnittstellenkontrollen". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_4_Fernwartung.html, 16.11.2016.

[37] DIN (Deutsches Institut für Normung e. V.), Vorschrift, "DIN 66398:2016-05 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten". 08.04.2016.

[38] Bundesministerium, Gesetz, "BDSG (neu) § 35 - Recht auf Löschung". https://dsgvo-gesetz.de/bdsg-neu/35-bdsg-neu/, 8.12.2017.

[39] DSGVO, Artikel 05 Absatz 1 lit. e, "Art. 05 - Grundsätze für die Verarbeitung personenbezogener Daten". https://dsgvo-gesetz.de/art-5-dsgvo/, 8.12.2017.

[40] DSGVO, Artikel 06 Absatz 1, "Art. 06 - Rechtmäßigkeit der Verarbeitung". https://dsgvo-gesetz.de/art-6-dsgvo/, 8.12.2017.

[41] DSGVO, Artikel 17, "Art. 17 - Recht auf Löschung". https://dsgvo-gesetz.de/art-17-dsgvo/, 8.12.2017.

[42] Abgabenordnung (AO), , "§ 147 Ordnungsvorschriften für die Aufbewahrung von Unterlagen". https://www.gesetze-im-internet.de/ao_1977/__147.html, 01.12.2017.

[43] Allgemeines Gleichbehandlungsgesetz (AGG), , "§ 15 Entschädigung und Schadensersatz". https://www.gesetze-im-internet.de/agg/__15.html, 02.12.2017.

[44] Arbeitsgerichtsgesetz (ArbGG), , "§ 61b Klage wegen Benachteiligung". https://www.gesetze-im-internet.de/arbgg/__61b.html, 02.12.2017.

[45] Bundesministerium, Gesetz, "BDSG (neu) § 75 - Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung". https://dsgvo-gesetz.de/bdsg-neu/75-bdsg-neu/, 25.11.2017.

[46] BSI, IT-Grundschutz-Kataloge, "M 2.011 Regelung des Passwortgebrauchs". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html;jsessionid=514F9EDA5FC4C743C96E25C40762FA3B.1_cid341?nn=6610622, 10.12.2017.

[47] BSI, IT-Grundschutz-Kataloge, "M 4.306 Umgang mit Passwort-Speicher-Tools". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/

_content/m/m04/m04306.html?nn=6610622, 11.12.2017.

[48] BSI, IT-Grundschutz-Kataloge, "M 4.004 Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04004.html, 10.12.2017.

[49] BSI, IT-Grundschutz-Kataloge, "M 4.084 Nutzung der BIOS-Sicherheitsmechanismen". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04084.html?nn=6610622, 10.12.2017.

[50] BSI, IT-Grundschutz-Kataloge, "M 4.001 Passwortschutz für IT-Systeme". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04001.html?nn=6610622, 10.12.2017.

[51] BSI, IT-Grundschutz-Kataloge, "M 2.476 Konzeption für die sichere Internet-Anbindung". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02476.html, 06.01.2018.

[52] BSI für Bürger, , "Ihre Software sicher einrichten - Der Browser". https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/derbrowser_node.html, 07.01.2018.

[53] BSI, , "Mindeststandard des BSI für Sichere Web-Browser". https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/Sichere_Web-Browser/Sichere_Web-Browser_node.html, 07.01.2018.

[54] BStBK, Berufsrechtliches Handbuch, II Anhang, Anlage 1 zu 5.2.4, "Browsereinstellungen". https://www.bstbk.de/, 9.2017.

[55] BSI, IT-Grundschutz-Kataloge, "M 2.076 Auswahl und Einrichtung geeigneter Filterregeln". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html, 07.01.2018.

[56] BSI, IT-Grundschutz-Kataloge, "M 5.045 Sichere Nutzung von Browsern". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05045.html, 07.01.2018.

[57] BSI, IT-Grundschutz-Kataloge, "M 2.032 Einrichtung einer eingeschränkten Benutzerumgebung". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html, 07.01.2018.

[58] BSI, IT-Grundschutz-Kataloge, "M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02273.html, 07.01.2018.

[59] BSI, BSI-Veröffentlichungen zur Cyber-Sicherheit, "iOS - Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit".

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_074.pdf?__blob=publicationFile, 18.12.2015.

[60] BSI, , "Mindeststandard des BSI für Mobile Device Management". https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.pdf?__blob=publicationFile&v=5, 11.05.2017.

[61] BSI, BSI-Veröffentlichungen zur Cyber-Sicherheit, "Android - Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit". https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_109.pdf?__blob=publicationFile&v=8, 12.05.2015.

[62] BSI, IT-Grundschutz-Kompendium, "SYS.03.2.2: Mobile Device Management (MDM)". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_2_Mobile_Device_Management_(MDM).html, 21.01.2018.

[63] Amtsgericht Bad Hersfeld, , "Beschl. v. 15.05.2017, Az.: F 120/17 EASO". http://www.lareda.hessenrecht.hessen.de/lexsoft/default/hessenrecht_lareda.html#docid:7876045, 15.05.2017.

[64] intersoft consulting services AG, , "Abmahngefahr: WhatsApp-Nutzer müssen Einwilligung der Kontakte einholen". https://www.datenschutzbeauftragter-info.de/abmahngefahr-whatsapp-nutzer-muessen-einwilligung-der-kontakte-einholen/, 26.06.2017.

[65] intersoft consulting services AG, , "WhatsApp und Datenschutz – Antworten auf die wichtigsten Fragen". https://www.datenschutzbeauftragter-info.de/whatsapp-und-datenschutz-antworten-auf-die-wichtigsten-fragen/, 15.01.2015.

[66] BSI, IT-Grundschutz-Kataloge, "M 2.472 Erstellung einer Sicherheitsrichtlinie für TK-Anlagen". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02472.html, 27.01.2018.

[67] BSI, IT-Grundschutz-Kataloge, "M 4.002 Bildschirmsperre". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04002.html, 28.01.2018.

[68] BStBK, Berufsrechtliches Handbuch, II Anhang, Anlage 1 zu 5.2.4, "Bildschirmschoner". https://www.bstbk.de/, 9.2017.

[69] intersoft consulting services AG, , "Vorgaben für die E-Mail-Archivierung". https://www.datenschutzbeauftragter-info.de/vorgaben-fuer-die-e-mail-archivierung/, 08.03.2017.

[70] BStBK, Berufsrechtliches Handbuch, II Anhang, Anlage 1 zu 5.2.4, "Richtlinien zur Nutzung der betrieblichen EDV". https://www.bstbk.de/, 9.2017.

[71] BStBK, Berufsrechtliches Handbuch, II Anhang, Anlage 1 zu 5.2.4, "Zugriffsrechte". https://www.bstbk.de/, 9.2017.

[72] Bundesministerium, Gesetz, "SGB X § 80 - Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag". http://www.gesetze-im-internet.de/sgb_10/__80.html, 20.08.2017.

[73] BSI, IT-Grundschutz-Kompendium, "INF.04: IT-Verkabelung". https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/UH_IT_Verkabelung.html, 09.06.2016.

[74] BSI, IT-Grundschutz-Kompendium, "OPS.2.4: Fernwartung". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_4_Fernwartung.html, 05.11.2017.

[75] DSGVO, Art. 28 Abs.3 lit. h - Auftragsverarbeiter, DSGVO, "Protokollpflicht des Auftragnehmers". 26.9.2017.

[76] EU-Privacy Richtlinie, Artikel 8, "Cookie-Hinweis-Layer". 10.1.2017.

[77] BStBK, Berufsrechtliches Handbuch, II Anhang, Anlage 1 zu 5.2.4, "E-Mail Verschlüsselung". https://www.bstbk.de/, 9.2017.

[78] BSI, IT-Grundschutz-Kataloge, "M 2.022 Hinterlegen des Passwortes". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02022.html?nn=6610622, 10.12.2017.

[79] BSI, IT-Grundschutz-Kataloge, "M 1.74: EMV-taugliche Stromversorgung". https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m01/m01074.html, 05.11.2017.

[80] VDE Verlag, Norm, "DIN VDE 0100-444: Errichten von Niederspannungsanlagen". https://www.vde-verlag.de/normen/0100155/din-vde-0100-444-vde-0100-444-2010-10.html, 2010-10.