II. MASSNAHMENKATALOG technisch/organisatorisch (TOM)

INHALTSVERZEICHNIS

1. Grundsätzliches

Mit in Geltung treten der Datenschutzgrundverordnung (DSGVO) der Europäischen Union im Mai 2018, werden alle Verarbeiter von personenbezogenen Daten verpflichtet, insbesondere organisatorische sowie technische Maßnahmen zu treffen, um die Geheimhaltung der zu verarbeitenden personenbezogenen Daten zu gewährleisten; dazu bietet § 54 DSG idF DS-AG 2018 einen guten Anhaltspunkt.

Die in diesem Maßnahmenkatalog angeführten Maßnahmen beschreiben den aktuellen Stand der Technik und sollen einen Best-Practice Leitfaden bieten, um auch einen Grundschutz in Bezug auf Informationssicherheit für Verantwortliche und Auftragsverarbeiter im Sinne der DSGVO umzusetzen.

Da nicht jeder Verantwortliche und Auftragsverarbeiter über die gleiche IT-Infrastruktur verfügt, können Abweichungen vom Maßnahmenkatalog bei der konkreten Implementierung der vorgeschlagenen Maßnahmen notwendig sein. Sollte dies der Fall sein, so sind die Abweichungen von der zuständigen Person zu begründen und zu dokumentieren.

Die Reihenfolge der Implementierung der Maßnahmen hängt primär von bereits vorhandenen IT-Security-/Informationssicherheitsmaßnahmen ab und auch davon, ob zB die IT-gestützten Verarbeitungen selbst oder von einem IT-Dienstleister, der von sich aus Mindestabsicherungsmaßnahmen bereits implementiert hat, betrieben werden.

Eine empfohlene Reihenfolge der Maßnahmenumsetzung ist ausgehend von den DSGVO-Vorgaben wie folgt möglich:

- Zugriffskontrolle (Passwörter, Zutritt, Clean-Desk)
- Schutz vor unautorisierter Datennutzung und Datenverlust (Rollen/Rechte, Verwahrung/Transport/Vernichtung)
- Endgerätesicherheit (Zugriffsregelung, Benutzerrechte, Virenscanner, …)
- Firewall/IPS – Schutz Unternehmen/LAN gegenüber Internet, Unternehmen WLAN, Gäste-WLAN und HotSpots
- Remotezugriff (VPN) und Fernwartungszugänge
- Ausfallssicherheit: Sicherungskonzept (Backup/Recovery)
- E-Mail-Sicherheit
- Mobilgeräte (Smartphone, Laptop, BYOD)
- Sonstige Maßnahmen

Dieser Maßnahmenkatalog konkretisiert und ergänzt die im Datenverarbeitungsverzeichnis (Teil I des DKP) angegebenen Kategorien an Datensicherheitsmaßnahmen bei den einzelnen Verarbeitungskategorien.

2.Zugangs- und Zugriffskontrolle

Mithilfe von Zugangs- und Zugriffskontrolle soll gewährleistet werden, dass nur berechtigte Personen auf die zu verarbeitenden personenbezogenen Daten Zugriff haben und der Zugang zu Verarbeitungsanlagen für Unbefugte verwehrt wird.

2.1. Verwalten von Benutzern und Berechtigungsgruppen

2.1.1. Berechtigungskonzept

Die DSGVO (Art 5) normiert, dass personenbezogene Daten vertraulich zu behandeln sind, dh es ist ein Berechtigungskonzept nach **dem Least-Privilege Prinzip** zwingend erforderlich. Demnach sind Berechtigungen nur auf Ressourcen zu gewähren, zu denen der Benutzer notwendigerweise Zugriff benötigt (gilt für alle Arten von Informationsträger - auch Papier).

Laufende/wiederkehrende Prüfung
Die vergebenen Berechtigungen sind zumindest jährlich auf Notwendigkeit zu überprüfen und zu entziehen, wenn der Benutzer diese nicht mehr zur Erfüllung seiner Aufgaben benötigt.

Vertreterregelung / Entzug von Berechtigungen
Werden die Tätigkeiten eines Mitarbeiters während seiner Abwesenheit unbedingt benötigt, so darf dieser seinen Account nicht einfach weitergeben. Dafür ist zuerst ein Vertreter für diese Tätigkeiten zu benennen. Dieser Vertreter hat dann beim dafür Verantwortlichen Berechtigungen, die für das Erfüllen der Tätigkeiten notwendig sind, einzufordern.
Sollte ein Mitarbeiter die Abteilung oder das Aufgabengebiet wechseln, so sind seine Berechtigungen erneut zu prüfen und gegebenenfalls zu berichtigen. Berechtigungen, welche nicht mehr benötigt werden, sind umgehend zu entfernen. Bei einem Austritt des Mitarbeiters sind diesem alle vergebenen Berechtigungen zu entziehen.
Sollte eine Berechtigung zwischen mehreren Mitarbeitern geteilt worden sein (zB: Gruppenbenutzer mit gemeinsamem Passwort), so ist das Passwort nach Ausscheiden eines Mitarbeiters sofort zu ändern.

2.1.2.Berechtigungsvergabe

Die Einrichtung von Benutzern und Berechtigungsgruppen geschieht durch den dafür Verantwortlichen. Dieser teilt den Benutzern Berechtigungen auf Ressourcen zu, beziehungsweise entzieht diese.
Außer dem Verantwortlichen darf niemand administrativen Zugang auf ein IT-System haben. Besonders ist darauf zu achten, dass sich Mitarbeiter nicht mit Administratoraccounts, in halb-öffentlichen Räumlichkeiten wie beispielsweise Vortrags- oder Besprechungsräumen einloggen können.

2.2. Elektronische Zugriffskontrolle - Passwörter

Der Zugang zu allen IT-Systemen und Diensten muss durch Identifikation und Authentisierung mittels Benutzerkennung und Passwort abgesichert sein. Bei der Passwortvergabe müssen die Passwortrichtlinien (Maßnahme - Passwortrichtlinie) eingehalten werden.

Bei der **Erstanmeldung** der Benutzer sollten Initialpasswörter verwendet werden, welche beim ersten Zugriff vom Benutzer geändert werden müssen. Die Passwörter dürfen nur dem jeweiligen Benutzer bekannt sein. Sollte das Passwort einer unautorisierten Person bekannt geworden sein, so muss das Passwort vom Benutzer sofort geändert werden.

Falls technisch möglich, sollte das Authentisierungssystem so konfiguriert werden, dass nach fünf aufeinanderfolgenden fehlerhaften Passworteingaben das jeweilige Benutzerkonto gesperrt wird.

Zurücksetzen von Passwörtern

Wird das Passwort vom Benutzer vergessen, muss beim Systemadministrator ein neues Passwort angefordert werden. Dieser hat dabei sicherzustellen, dass der anfordernde Benutzer auch wirklich derjenige ist, der er vorgibt zu sein. Diese Authentizitätsprüfung kann durch das Vorzeigen des Mitarbeiterausweises, oder bei telefonischer Rücksetzung durch einen Rückruf an die im Mitarbeiterverzeichnis angegebene Telefonnummer geschehen. Die Bekanntgabe des neuen Passworts hat ausschließlich persönlich oder verschlüsselt per E-Mail an den jeweiligen Benutzer zu erfolgen.

2.3. Physische Zugangskontrolle

2.3.1. Zulässige Schlüssel

Der Zutritt zu schutzbedürftigen Teilen des Gebäudes muss mithilfe von Zugangskontrolle abgesichert werden. Wie die Absicherung implementiert wird - ob mittels herkömmlichem physischem Schlüssel oder einem elektronischen Zugangskontrollsystem - ist dem Zuständigen überlassen. Dieser sollte bei der Planung (bei elektronischen, als auch bei physischen Schließanlagen) einen externen Berater zuziehen, welcher den aktuellen Stand der Technik abschätzen kann.[1]

2.3.2.Schlüsselverwaltung

Die Schlüsselverwaltung (Ausgabe, Herstellung, Aufbewahrung) hat durch den dafür Verantwortlichen zu erfolgen. Schlüssel dürfen nur an berechtigte Personen ausgegeben werden. Die Ausgabe/ Rückgabe aller Schlüssel ist schriftlich zu dokumentieren, um jederzeit nachvollziehen zu können, wer zu welchem Zeitpunkt Zutritt zu welchen Räumen hatte.

Verlust von Schlüsseln

Mitarbeiter haben den Verlust eines Schlüssels unverzüglich dem Verantwortlichen der Schlüsselverwaltung zu melden. Der Zuständige hat dafür Sorge zu tragen, dass bei einem Verlust eines Schlüssels, keine unautorisierten Personen Zutritt zu den durch den Schlüssel gesicherten Räumlichkeiten hat. In Abhängigkeit des verwendeten Zutrittssystems (elektronisch oder physisch), sind zumindest folgende Schritte durchzuführen:

Bei elektronischen Systemen

- Den gestohlenen oder verlorenen Schlüssel sperren
- Neuen Schlüssel für den Mitarbeiter im System hinterlegen

Bei physischen Systemen

- Austauschen aller Schlösser, bei dem der verlorene Schlüssel sperrt.

[1]So entspricht beispielsweise das weit verbreitete System „MIFARE Classic“ nicht mehr dem aktuellen Stand der Technik und gilt somit als unsicher.

- Ausgabe der neuen Schlüssel an alle berechtigten Personen.

2.4. Endgeräte

Werden in einem IT -System oder einer Anwendung Passwörter zur Authentisierung verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig. Dafür ist folgende Regelung zum Passwortgebrauch einzuführen und die Benutzer von IT-Systemen sind diesbezüglich zu unterweisen:

- Passwörter **müssen mindestens zwölf Zeichen lang** sein.
- Passwörter müssen jeweils mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen oder eine Zahl enthalten.
- Passwörter müssen mindestens alle sechs Monate geändert werden.
- Ein bereits verwendetes Passwort darf bei einer Passwortänderung nicht mehr erneut verwendet werden.

Für Smartphones oder Geräte mit der Möglichkeit zu alternativen Authentisierungsverfahren gilt für die Gerätesperre:

- Verwendung eines PIN-Codes mit mindestens vier Ziffern oder biometrisches Merkmal (zB Fingerabdruck oder Gesichtserkennung)
- Einfache Authentisierungsverfahren, wie zB **Wischmuster sind unzulässig**.

Passwörter sind persönlich sicher zu verwahren, insbesondere ist darauf zu achten, dass diese nicht zB mit Post-It am Bildschirm oder unter der Tastatur angebracht werden.

2.5. Physische Räume

Der Schutzbedarf von Räumen in einem Gebäude hängt von der jeweiligen Nutzung ab. Die erforderlichen Sicherheitsmaßnahmen müssen diesem Schutzbedarf angepasst sein. Entsprechend muss die bauliche Ausführung von Wänden, Fenstern und Türen sein.
Es empfiehlt sich, die einzelnen Räume gemäß ihres Schutzbedarfs in einem Raumplan zu kennzeichnen (zB Rot für Räume mit erhöhtem Schutzbedarf, Gelb für nicht öffentliche Räume und Grün für öffentliche Räume), um die Einteilung der Räume zu dokumentieren.

2.5.1. Öffentliche Räumlichkeiten

Bei Räumlichkeiten, die externes Publikum anziehen, oder halb-öffentliche Räume wie Besprechungs-, Schulungs- oder Veranstaltungsräume bedarf es keiner sicheren Absperrung, aber es ist wichtig, nach einem Treffen beim Verlassen dieser Räume, die verwendeten Unterlagen sowie Grafiken oder Schriften auf Tafeln/Whiteboards gemäß einer Clean-Desk Policy (siehe Maßnahme 3.2.1 - Clean-Desk Policy/ Clear-Screen Policy) zu entfernen. Zusätzlich ist sicherzustellen, dass kein Zugriff auf das interne Netzwerk (LAN) möglich ist. Frei zugängliche Netzwerkanschlüsse in solchen Räumlichkeiten sind zu vermeiden oder gegebenenfalls mit geeigneten Sicherheitsmaßnahmen, wie zum Beispiel mechanische Versperrung oder Network Access Control (IEEE 802.1X), abzusichern.

2.5.2. Nicht öffentliche Räumlichkeiten

Nicht öffentliche Räumlichkeiten wie Büroräume oder Räume der Gebäudetechnik müssen mit einer Zugangskontrolle (Schlüssel, Chipkarte,...) abgesichert werden (siehe Kapitel 2.3),

da in diesen Räumen im Regelfall vertrauliche Unterlagen oder Unterlagen mit personenbezogenen Daten verwahrt werden.

2.5.3. Räumlichkeiten mit erhöhtem Schutzbedarf

Bei Räumen mit erhöhtem Schutzbedarf, ist bei der Verwendung von elektronischen Zugangskontrollsystemen darauf zu achten, dass der Zugang nur über eine doppelt gesicherte sogenannte **Zwei-Faktor-Authentifizierung** (zB Chipkarte + PIN-Code) ermöglicht wird. Räume mit erhöhtem Schutzbedarf sind zB IT-Serverräume oder Räume, wo besondere Kategorien personenbezogener Daten (Art 9 DSGVO) ohne weitere Schutzmaßnahmen verwahrt werden und wo ein Datenverlust oder -diebstahl zu gravierenden Auswirkungen für die Betroffenen oder massiven finanziellen Schäden führen kann.

Kritische IT-Komponenten wie beispielsweise **Server oder Netzwerkkomponenten** (Switches, Firewalls, etc.) müssen vor unbefugtem Zugriff geschützt werden. Es ist somit zwingend erforderlich, diese Komponenten in einer gesicherten Umgebung aufzustellen. Dies kann entweder in einem eigenen Serverraum oder in verschließbaren Schränken (Racks) geschehen. Wichtig ist hierbei, zu beachten, dass die Zugangsschlüssel sicher verwahrt (beispielsweise in einem Schlüsselsafe) werden und die Räume und Schränke immer verschlossen sind.
Des Weiteren muss über eine Vertreterregelung sichergestellt werden, dass auch im Falle einer Abwesenheit des Zugangsberechtigten weiterhin der Zugang zu den Räumen beziehungsweise Schränken möglich ist.

Für einen Serverraum / IT-Raum sind besondere Merkmale zu beachten (BSI Grundschutzkatalog B 2.4):
„In einem Serverraum ist kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als zum Beispiel in einem Büroraum."
Eine ausführliche Auflistung von Gefährdungen und Maßnahmenempfehlungen finden sich im BSI IT-Grundschutz Katalog, Baustein B 2.4 – Serverraum und die empfohlenen Maßnahmen samt Kontrollfragen zur Prüfung finden sich im BSI IT-Grundschutz Katalog, Maßnahme M 1.58 - Technische und organisatorische Vorgaben für Serverräume.[2]

[2]M 1.58 - Technische und organisatorische Vorgaben für Serverräume: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m01/m01058.html?nn=6604958. B 2.4 – Serverraum: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b02/b02004.html

3. Speicher- und Datenträgerkontrolle

Im Kapitel Speicher- und Datenträgerkontrolle werden Maßnahmen beschrieben, welche die Verhinderung der unbefugten Eingabe, Kenntnisnahme, Veränderung sowie Löschung von gespeicherten personenbezogenen Daten behandeln.

3.1. Umgang mit Informationsträgern

DSGVO Art 5 fordert einen angemessenen Schutz vor unbefugter Verarbeitung personenbezogener Daten, auch beim Umgang mit Informationsträgern (zB Festplatte, CD/DVD, USB-Stick, Smartphone, Papier, Akten).

3.1.1. Aufbewahrung von Informationsträgern

Informationsträger mit personenbezogenen Daten dürfen nicht öffentlich zugänglich sein und sind somit wegzusperren, sobald kein Mitarbeiter mehr vor Ort ist. Sollte es nicht möglich sein, die Informationsträger an öffentlich zugänglichen Orten zu verschließen (öffentlich zugänglicher Stand-PC mit gespeicherten personenbezogenen Daten), so sind diese zu verschlüsseln.
Externe Datenträger (USB-Sticks, externe Festplatten) **sind**, wie in Maßnahme 3.1.3 – Verschlüsselung von mobilen Datenträger und externen Geräten beschrieben, **zu verschlüsseln**.

3.1.2.Entsorgung von Informationsträgern

Es ist sicherzustellen, dass bei der Entsorgung von Informationsträgern ein angemessener Schutz gewährleistet wird, da ansonsten unbefugte Personen, beispielsweise beim Durchsuchen von Altpapiercontainern, unberechtigten Zugriff auf personenbezogene Daten erlangen könnten.

- Deshalb ist vom Zuständigen ein Entsorgungskonzept zu erstellen, indem definiert wird, wie die Entsorgung von Datenträgern mit personenbezogenen Daten zu erfolgen hat. Papierdokumente müssen mittels Aktenvernichter (Partikelschnitt maximale Partikelgröße 30 mm²) oder über ein nach ÖNORM 2109 zertifiziertes Entsorgungsunternehmen vernichtet werden.
- Elektronische Informationsträger müssen entweder sicher gelöscht oder physisch vernichtet werden (die physische Vernichtung elektronischer Informationsträger kann ebenfalls durch ein Entsorgungsunternehmen erfolgen). Geschieht die Entsorgung der Informationsträger über ein Entsorgungsunternehmen, so ist zu gewährleisten, dass die Informationsträger bis zur Abholung unter Verschluss gehalten werden.

Wichtig ist zu beachten, dass auch Kopierer meist eine Speichereinheit eingebaut haben, welche alle Kopiervorgänge speichert. Daher muss bei der Entsorgung eines Kopierers, diese Speichereinheit ausgebaut und wie andere elektronische Informationsträger sicher gelöscht oder physisch zerstört werden.
Alle Mitarbeiter sind vom Zuständigen über das Entsorgungskonzept zu informieren.

3.1.3. Verschlüsselung von mobilen Geräten und externen Datenträgern

Mobile Geräte und externe Datenträger (USB-Stick, USB-Festplatte), auf denen personenbezogene Daten gespeichert werden, sind zu verschlüsseln. Dadurch kann bei einem Verlust oder Diebstahl des Geräts verhindert werden, dass unbefugte Personen Zugriff auf die gespeicherten Daten erhalten. Es ist bei der eingesetzten Software darauf zu achten, dass **mindestens mit AES-128 verschlüsselt** wird.[3]
Für die Verschlüsselung können die betriebssysteminternen Boardmittel (Bitlocker, FileVault) verwendet werden. Bei der Vergabe des Verschlüsselungspasswortes gilt die Passwortrichtlinie aus Maßnahme - Passwortrichtlinie. Folgende Tools erfüllen derzeit die Mindeststandards hinsichtlich Verschlüsselungsstärke (mindestens AES-128):

- **Windows**: Bitlocker
- **MacOS**: FileVault
- **Android**: Systemverschlüsselung ab Android Version 5
- **iOS**: Systemverschlüsselung bei aktiver Pin- oder Biometriesperre

3.1.4. Umgang mit externen Wechseldatenträgern

Der Einsatz von betriebsfremden Wechseldatenträgern, wie beispielsweise USB-Sticks, externen Festplatten oder aber auch Smartphones, die von betriebsfremden Personen mitgebracht oder verwendet werden, bringt eine Reihe von Risiken mit sich. So ist es beispielsweise möglich, über einen USB-Stick Schadsoftware auf einem Computer auszuführen und Unternehmensdaten zu kopieren, wodurch die Vertraulichkeit personenbezogener Daten (DSGVO Art 5 Abs 1) gefährdet wird.
Es ist somit über eine organisatorische Maßnahme (zB verpflichtende Regelung) sicherzustellen, dass Mitarbeiter keine Wechseldatenträger von betriebsfremden Personen an ihre Computer anschließen.
Sollte ein schneller Datenaustausch mit einer betriebsfremden Person unbedingt notwendig sein, so wird empfohlen, die Daten via E-Mail auszutauschen und die empfangenen Daten mittels Virenscanner zu überprüfen, bevor diese weiterverwendet werden. Auch der Austausch via explizit freigegebener Datenaustauschplattformen (zB Cloud-Plattform des IT-Dienstleisters) ist möglich.

3.2. Verhindern unbefugter Kenntnisnahme

3.2.1. Clean-Desk Policy / Clear-Screen Policy

Mitarbeiter müssen bei Abwesenheit alle Informationsträger, welche personenbezogene Daten beinhalten, von ihrem Arbeitsplatz entfernen. Dadurch wird verhindert, dass unbefugte Personen Zugriff auf die Daten bekommen. Den Mitarbeitern muss dazu eine Möglichkeit bereitgestellt werden, die Informationsträger zu verschließen. Dies kann beispielsweise durch verschließbare Schränke gewährleistet werden.
Beim Verlassen der Büroräumlichkeiten ist auf jeden Fall dafür Sorge zu tragen, dass alle Informationen ihrem Schutzbedarf entsprechend physisch weggesperrt werden (falls andere nicht autorisierte Personen Zugang zu den schützenswerten Informationen erlangen könnten)

[3] BSI-TR-02102:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf

oder der Raum so versperrt wird, dass unautorisierte Personen keinen Zutritt zum Raum erlangen können.[4]
Computer oder andere Geräte mit Benutzer-Login sind bei jedem Verlassen des Arbeitsplatzes zu sperren (auch bei kurzen Pausen). Der Zuständige hat die Mitarbeiter über diese Maßnahme zu informieren und die Durchsetzung der Maßnahme regelmäßig zu überprüfen.[5]

3.2.2. Zweckgebundenheit - Reduzierung von unbefugten Verarbeitungsschritten

Zweckbindungsoll sicherstellen, dass Daten nur für den Zweck verarbeitet werden, für den sie erhoben worden sind. Der Zweck der Datenverarbeitung folgt aus der jeweiligen Fachaufgabe, zu deren Erfüllung die Daten erhoben wurden. Eine Datenverarbeitung zu einem anderen als dem ursprünglich festgelegten Zweck ist als Zweckänderung oder Zweckdurchbrechung nur auf gesetzlicher Grundlage oder mit Einwilligung des Betroffenen zulässig. Dies gilt auch dann, wenn die Daten an eine andere Stelle mit einer anderen, über bloße Hilfsfunktionen hinausgehenden Aufgabenstellung weitergegeben werden sollen.[6]

Sofern bei Anwendungen verknüpfbare Sammlungen von personenbezogenen Daten entstehen, muss besonders darauf geachtet werden, dass diese Daten wirklich nur für die Zwecke verwendet werden, für die sie erhoben und gespeichert wurden. Nur in für den Betroffenen klar überschaubaren Grenzen, nämlich aufgrund einer ausdrücklichen gesetzlichen Erlaubnis oder mit dessen Einwilligung, dürfen diese Daten auch für andere Zwecke verwendet werden. Die Zweckbindung muss vorsorglich durch organisatorische und technische Maßnahmen gesichert werden.

- Sicherstellung des alleinigen Zuganges zu den Daten durch berechtigte Personen mit geeigneter Identifizierung und Authentisierung (siehe Maßnahme 2.2 - Elektronische Zugriffskontrolle - Passwörter und Maßnahme 2.3 - Physische Zugangskontrolle
- Benutzer-, Datei- und Programm-bezogene Rechtevergabe (siehe Maßnahme 2.2 - Elektronische Zugriffskontrolle - Passwörter) für den zweckgebundenen Zugriff nach fachlichem Anforderungsprofil und Arbeitsaufgabe des jeweiligen Benutzers
- Kennzeichnung der für besondere Zwecke erhobenen Daten zur Spezifizierung des Zwecks ihrer Erhebung, Verarbeitung und Übermittlung, so dass eine Kontrolle ihrer Verwendung für einen anderen Zweck ermöglicht werden kann.

Zusätzlich sollen Prozesse laufend vom Prozessverantwortlichen überprüft werden, ob wirklich nur die Mitarbeiter mit den personenbezogenen Daten in Berührung kommen, die auch wirklich für die Abarbeitung des Prozesses notwendig sind. Dies wird durch die Verwendung möglichst kurzer Kommunikations- oder Transportwege erreicht. Konkret sollen personenbezogene Daten daher keinesfalls durch Kettenübertragung übertragen werden. Es

[4]M 2.37 - Der aufgeräumte Arbeitsplatz
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02037.html
[5]M 4.2 - Bildschirmsperre
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04002.html
[6]Art 5 DSGVO

ist somit unzulässig, personenbezogene Daten an eine Stelle zu übertragen die lediglich als weiterer Überträger der Nachricht dient (Kettenübertragung).

3.2.3. Bring Your Own Device / Cloud Dienste / Einsatz von Messengern.

Bei **Bring Your Own Device** (BYOD) nutzt das Personal private Geräte (wie beispielsweise Mobiltelefone oder Laptops) für dienstliche Zwecke. BYOD ist aufgrund der damit verbundenen Sicherheitsrisiken generell zu untersagen und dies den Mitarbeitern auch nachweislich als Richtlinie mitzuteilen.
Zu beachten ist, dass bereits das Einrichten der dienstlichen E-Mail-Box auf einem privaten Gerät (Laptop, Heim-PC, Smartphone) als BYOD zählt und daher nicht zulässig ist.
Lässt es sich nicht vermeiden, BYOD im Unternehmen zu erlauben, so sind weiterführende Maßnahmen umzusetzen. Das BSI bietet hierfür ein Überblickspapier zum Thema BYOD.[7]

Sollten personenbezogene Daten bei einem **Cloud-Anbieter**. gespeichert und/oder verarbeitet werden, so wird der Cloud-Anbieter gemäß DSGVO zum Auftragsverarbeiter, das Unternehmen bleibt Verantwortlicher iSd DSGVO.
Laut DSGVO Art 28 Abs 1 ist der Zuständige verpflichtet, nur solche Anbieter zu beauftragen, welche hinreichende Garantien (möglich ist zB der Nachweis durch eine Zertifizierung nach DSGVO Art 42) dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Messenger wie beispielsweise WhatsApp oder der Facebook Messenger sind für die Firmenkommunikation verboten. Es kann nicht sichergestellt werden, wie und wo die übertragenen Daten gespeichert werden; zudem ist WhatsApp nur zum privaten Gebrauch erlaubt. Des Weiteren greift WhatsApp beispielsweise auf das gesamte Adressbuch des Benutzers zu und lädt dieses auf US-amerikanische Server. Somit ist selbst die Installation von WhatsApp bereits nicht mehr mit der DSGVO vereinbar. Die Mitarbeiter müssen darüber informiert werden, dass jegliche Kommunikation über nicht explizit erlaubte Nachrichtendienste zu unterlassen ist.
Eine zusätzliche Möglichkeit unerlaubte Apps zu unterbinden ist, die Installation von solchen Messenger-Apps mittels Mobile-Device-Management-Software zu verhindern.

[7] Zunehmend löst sich die Grenze zwischen beruflicher und privater Nutzung auf, viele IT-Systeme, Programme und Dienste werden mittlerweile sowohl im beruflichen wie auch im privaten Umfeld benutzt. Diese Entwicklung wird als Consumerisation bezeichnet (Überblickspapier IT-Consumerisation und BYOD https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf

4. Übertragungs- und Eingabekontrolle

Die Übertragungs- und Eingabekontrolle beschäftigt sich mit der Übertragung und Speicherung von personenbezogenen Daten. Es werden Maßnahmen beschrieben, welche verhindern, dass personenbezogene Daten bei der Übertragung unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Des Weiteren wird in diesem Kapitel die Nachvollziehbarkeit bei der Eingabe von personenbezogenen Daten behandelt.

4.1. Nachvollziehbarkeit

Aufgrund Art 5DSGVO ist es notwendig, nachvollziehen zu können, von welchem Mitarbeiter, zu welcher Zeit personenbezogene Daten eingefügt, geändert oder gelöscht wurden. Es ist somit erforderlich (insbesondere bei der Verarbeitung von besonderen Datenkategorien zB Gesundheits-, Biometrie-, Strafdaten oder Religionsbekenntnis), ein Dokumentenmanagementsystem (zB Dokumentenversionierung) zu implementieren.

4.2. Einsatz von Software

Es darf auf betrieblichen Arbeitsplätzen nur Software eingesetzt werden, welche auch vom Zuständigen genehmigt wurde.
Die Verwendung von nicht genehmigter Software birgt unabschätzbare Risiken. So könnte beispielsweise eine unzulässige Software versteckte Schadsoftware (Trojaner, Ransomware, AdWare, Spyware) enthalten oder auf Ressourcen wie Fotos, Mails, Kontakte, Netzwerk, etc. zugreifen und somit die Vertraulichkeit der Systeme und in der Folge auch die Privatsphäre der gespeicherten Personen gefährden.
Um sicherzustellen, dass auf betrieblichen Arbeitsgeräten keine unerwünschten Programme (bzw. APPs) installiert werden und das System nicht über den vorgesehenen Funktionsumfang hinaus unkontrolliert genutzt wird, muss das Installieren nicht genehmigter Software verboten und soweit technisch möglich, verhindert werden („normale Benutzer“ dürfen keine Administratorrechte auf den betrieblichen IT-Geräten besitzen, damit kann auch die Installation von unzulässiger Software verhindert werden).
Wird ein Mobile-Device-Managementsystem bzw. ein vergleichbares Managementsystem für Arbeitsplatzgeräte verwendet, so kann das unautorisierte Installieren technisch unterbunden werden.
Es muss sichergestellt werden, dass Mitarbeiter über das Nutzungsverbot informiert werden und dieses von den Mitarbeitern unterzeichnet wird.
Es ist vom Zuständigen ein Verzeichnis der erlaubten Software zu führen und Mitarbeitern zugänglich zu machen. Sollte der Einsatz einer noch nicht genehmigten Software für den Betrieb notwendig sein, so ist diese vorher durch den Zuständigen genehmigen zu lassen.

4.3. Firewall

Eine Firewall kontrolliert den Datenverkehr zwischen dem internen Netzwerk und dem Internet. Unerwünschte Verbindungsanfragen von außerhalb können durch den Einsatz einer Firewall blockiert werden. Eine direkte Verbindung zwischen dem LAN-Netzwerk und dem

Internet ist verboten. Zur Trennung ist eine Firewall zu installieren, wobei für den Betrieb der Firewall nachfolgende Vorgaben umzusetzen sind:

- Jede Kommunikation zwischen dem internen Netzwerk und dem Internet muss ausnahmslos über die Firewall laufen.
- Es dürfen nur jene Ports ein- und ausgehend geöffnet werden, welche für den Betrieb notwendig sind.
- Es ist ein regelmäßiges Überprüfen der Firewall-Logs zur Erkennung von Angriffen umzusetzen
- Die Software der Firewall muss regelmäßig aktualisiert werden (Wartungsvertrag)

4.4. Virtual Private Networks (VPN)

Oft ist es notwendig, Mitarbeiter, die außer Haus tätig sind, an das interne Netzwerk anzubinden. Interne IT-Systeme dürfen jedoch nicht ungesichert von Außerhalb erreichbar sein. Eine Lösung, Mitarbeiter von außerhalb auf die interne IT-Infrastruktur zugreifen zu lassen, bietet VPN.
Da es sich bei VPN um einen kritischen Bestand der IT-Infrastruktur handelt, ist bei der Beschaffung der VPN-Komponenten darauf zu achten, diese nur von autorisierten und kompetenten Lieferanten mit nachgewiesenen Fachkenntnissen zu beziehen.

Die eingesetzte VPN-Lösung muss hinsichtlich Security dem aktuellen Stand der Technik entsprechen, was zB für die eingesetzten Verschlüsselungsverfahren bedeutet:

- Symmetrische Verschlüsselung - mindestens AES-128, besser AES-256
- Asymmetrische Verschlüsselung - mindestens RSA-3000 oder ECDH-256
- Authentifizierung der Client-Geräte mittels Zertifikat oder Zwei-Faktor-Authentifizierung

4.5. Wireless LAN

4.5.1. Internes WLAN

Angriffe auf die IT-Infrastruktur über Wireless LAN dürfen nicht unterschätzt werden. So wäre es einem Angreifer bei einem ungesicherten WLAN möglich, Firmendaten auszuspionieren und somit den Datenschutz zu gefährden.
Bei der Planung und Installation eines WLANs ist darauf zu achten, dass dieses dem aktuellen Stand der Technik hinsichtlich der Security Implementierung (WPA2-PSK oder WPA2-Enterprise) entspricht. Bei der Positionierung der WLAN-Komponenten sollte darauf geachtet werden, dass diese vor unautorisiertem physischem Zugriff geschützt sind (manipulationssichere Montage, Schutzgehäuse).
Die Zugangsdaten zum Webinterface bzw. zu dem Konfigurationsmenü sind bei der Ersteinrichtung zu ändern (der Zugang zum Access-Point darf nicht über Standardpasswörter möglich sein).

Wenn ein Pre-Shared-Key (WPA2-PSK) verwendet wird, so muss das Passwort für den Pre-Shared-Key folgende Anforderungen erfüllen:

- Mindestens 20 Zeichen lang.

- Muss jeweils mindestens einen Großbuchstaben, einen Kleinbuchstaben, sowie aus einem Sonderzeichen oder einer Zahl bestehen.
- Wird das Passwort geändert, so darf das bereits verwendete Passwort niemals erneut verwendet werden.

Sollte der Access-Point die Möglichkeit bieten, über WPS eine Verbindung aufzubauen, so ist das Verwenden von WPS untersagt und diese Funktion zu deaktivieren.
Da sich auch im WLAN-Bereich ständig neue Sicherheitslücken ergeben, ist dafür Sorge zu tragen, dass die WLAN-Komponenten regelmäßige Firmware-/Software-Updates erhalten (Wartungsvertrag).

4.5.2. Gäste-WLAN

Das interne Firmennetzwerk darf für Besucher nicht zugänglich sein. Sollten Besucher Zugriff auf das Internet benötigen, so ist ein separates Gäste-WLAN einzurichten. Ein Zugriff auf das interne Firmennetzwerk darf über das Gäste-WLAN nicht möglich sein.
Der Zugang zum Gäste-WLAN ist entsprechend dem Stand der Technik (WPA2-PSK) mittels Kennwort zu sichern, um zu verhindern, dass nicht autorisierte Personen den Access-Point als kostenlosen Internetzugang missbrauchen.
Das Gäste-WLAN-Kennwort ist regelmäßig zu ändern (zB monatlich), um eine dauerhafte unautorisierte Nutzung (kostenloser „Internetersatz“ für Nachbarschaft) durch Dritte zu verhindern.

Ist die Einrichtung eines Gäste-WLANs im bereits vorhandenen Verwaltungs-WLAN nicht möglich, so wird empfohlen, ein neues WLAN-Netzwerk über einen vom Verwaltungsnetzwerk getrennten Access-Point zB mittels mobilem Hotspot (beispielsweise einen WebCube) oder sogar extra Internetzugang mit WLAN-Router bereitzustellen.

4.5.3. Öffentliche Hot-Spots

Sollte ein WLAN betreiben werden, welches der Öffentlichkeit einen Internetzugang bietet (öffentlicher Hot-Spot), so sind aufgrund der aktuellen Rechtslage[8] Zugriffskontroll-Maßnahmen für die Nutzung des Hot-Spots zu treffen, um Haftungsansprüche auszuschließen.
Dazu geeignete Maßnahmen sind:

- One-Time-Zugangspasswörter/Token, die persönlich ausgehändigt werden
- Registrierung von individuellen WLAN-Gästeaccounts
- Dauerhaft registrierte WLAN-Nutzeraccounts

4.6. Sicheres Drucken

Beim Ausdrucken von Dokumenten mit personenbezogenen Daten ist darauf zu achten, dass die Ausdrucke nicht für andere unberechtigte Personen zugänglich gemacht werden. Dies wäre insbesondere dann der Fall, wenn die Dokumente auf einem Drucker außerhalb des eigenen Büros (zB am Gang, wo sich Fremdpersonen aufhalten können) ausgedruckt werden.
Sollten die Daten auf einem Drucker außerhalb des eigenen Büros ausgedruckt werden, so ist sicherzustellen, dass nur der Benutzer, welcher den Druck veranlasst hat, Zugriff auf den Ausdruck hat. Dies lässt sich beispielsweise dadurch sicherstellen, dass der Druck mittels PIN

[8]EUGH, Urteil 15.09.2016, C-484/14.

(lässt sich in der Regel bei größeren Druckern in den Druckeinstellungen auswählen) geschützt wird.
Der Drucker wartet dann so lange mit dem Ausdruck, bis der Benutzer direkt am Drucker den gesendeten Auftrag auswählt und sich mittels PIN authentifiziert.

4.7. Datenübertragung

Jegliche Übertragung von personenbezogenen Daten hat nur über genehmigte, dem Schutzbedarf der Daten entsprechend abgesicherte Wege/Methoden zu erfolgen. Eine Übertragung von personenbezogenen Daten ist nur über vom Zuständigen genehmigte Übertragungswege/-medien und -verfahren zulässig.

Wird E-Mail verwendet, um personenbezogene Daten an andere zu übermitteln, so sind die personenbezogenen Inhalte vor dem Versand zu verschlüsseln. Die E-Mail selbst muss verschlüsselt werden, wenn der E-Mail-Text selbst personenbezogene Daten enthält. Befinden sich die personenbezogenen Daten jedoch ausschließlich im Anhang, so reicht es, nur den Anhang zu verschlüsseln.
Der Anhang lässt sich verschlüsseln, indem zum Beispiel die personenbezogenen Daten/Dokumente **in einem verschlüsselten Zip-Archiv als E-Mail-Anhang** übermittelt werden. Tools wie beispielsweise 7-Zip oder WinRAR unterstützen die Verschlüsselung von Zip-Archiven. Es ist jedoch bei der Verschlüsselung darauf zu achten, dass ein Tool mit dem Stand der Technik entsprechender Verschlüsselungsstärkte (mindestens mit AES-128) und einem sicheren Passwort (Maßnahme - Passwortrichtlinie) verwendet wird.
Das Passwort, welches zum Entschlüsseln benötigt wird, darf dabei nicht in der E-Mail mitübertragen werden, sondern ist dem Empfänger über einen getrennten Weg, beispielsweise persönlich, per Anruf oder per SMS mitzuteilen.

Eine Übersendung von (personenbezogenen) Daten via E-Mail an Externe ist nur dann zulässig, wenn die Vertraulichkeit sichergestellt werden kann und wenn zuvor überprüft wurde, dass die Empfänger-E-Mail-Adresse auch tatsächlich dem beabsichtigten Empfänger gehört und sich dieser auch als berechtigter Empfänger eindeutig ausgewiesen hat. Möglich ist dazu zB die Verwendung von Services wie „E-Brief“ der österreichischen Post oder andere für die elektronische Zustellung von Behördenschriftstücken geeignete Systeme oder auch zB das „Bürgerpostfach“.

5. Verfügbarkeit/Belastbarkeit und Integrität

Es muss gewährleistet werden, dass die gespeicherten personenbezogenen Daten im Falle eines Ausfalls der IT-Systeme wiederhergestellt werden können (Verfügbarkeit) und die verarbeiteten personenbezogenen Daten nicht durch eine Fehlfunktion des Systems beschädigt werden (Integrität).

5.1. Datensicherung

5.1.1. Datensicherungskonzept

Um im Falle eines Datenverlustes (zB technische Störung, Harddiskdefekt, unbeabsichtigtes Ändern/Löschen, Brandschaden, ...) verlorene Daten wiederherstellen zu können, muss vom dafür Verantwortlichen allenfalls in Zusammenarbeit mit dem IT-Leiter ein Datensicherungskonzept erstellt werden. Das Datensicherungskonzept regelt dabei den konkreten Umfang der Datensicherung.

Folgende Punkte müssen in diesem Dokument auf jeden Fall behandelt werden:

- Zuständigkeiten für die Datensicherung
- Art der Datensicherung (Vollständig/Inkrementell)
- Umfang der Datensicherung (welche Netzlaufwerke/Ordner werden gesichert)
- Verwendetes Sicherungsmedium (Maßnahme 5.1.2 – Auswahl des Sicherungsmediums)
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der aufzubewahrenden Sicherungen
- Aufbewahrungsort der Backup-Datenträger (Maßnahme 5.1.4 – Aufbewahrung der Backup-Datenträger)
- Wiederherstellung der Daten (Maßnahme 5.1.3 – Regelmäßige Überprüfung und Test der Datenträger)

Außerdem müssen die Mitarbeiter verpflichtet werden, alle dienstlichen Daten ausschließlich auf den vom Datensicherungskonzept umfassten, gesicherten Laufwerken/ Servern zu speichern, da ansonsten im Falle einer Störung des Arbeitsplatzrechners eine Wiederherstellung der lokal gespeicherten Daten in der Regel nicht mehr möglich ist.
Die Mitarbeiter sind außerdem zu verpflichten, dass temporär auf tragbaren Geräten (zB Laptop für Außendienst) gespeicherte Daten nach Rückkehr an den Büroarbeitsplatz auf stationäre Datenspeicher rückgeführt werden (oder es wird eine automatische Synchronisation von mobilen Geräten auf Server eingerichtet, wie dies zB bei Microsoft Betriebssystemen mit „Offline Foldern“ möglich ist).

5.1.2. Auswahl des Sicherungsmediums

Grundsätzlich sind alle Arten von Wechseldatenträgern als Sicherungsmedien geeignet. Es ist bei der Auswahl des Sicherungsmediums darauf zu achten, dass die verwendete Technologie für eine längere (gesetzlich vorgeschriebene) Aufbewahrungsdauer geeignet ist. Dies gilt besonders für Daten, welche durch eine gesetzliche Verpflichtung aufbewahrt werden müssen. Für eine dauerhafte Langzeitsicherung/-archivierung sind einmalbeschreibbare optische Speichermedien (DVD, Blu-ray) für Zeiträume von ca. 10 Jahren geeignet. Für

längere Archivierungszeiträume sind Spezialmedien (WORM) mit speziellen Archivierungseigenschaften zu verwenden.

5.1.3. Regelmäßige Überprüfung und Test der Datensicherung

Um eine Wiederherstellung der Daten nach einer Störung zu garantieren, muss die Wiederherstellbarkeit in regelmäßigen Zeitabständen getestet werden. Damit wird verhindert, dass bei einem Ausfall nicht mehr auf die Backups zugegriffen werden kann.
Die notwendigen Schritte zur Wiederherstellung der Daten sind vom Zuständigen im Datensicherungskonzept zu dokumentieren, damit die Daten im Bedarfsfall auch durch fachkundige Dritte wiederhergestellt werden können.[9]

5.1.4. Aufbewahrung der Backup-Datenträger

Backup-Datenträger sind von den zu sichernden Systemen räumlich getrennt aufzubewahren. Falls möglich, sollte eine Kopie einer vollständigen Datensicherung wöchentlich in ein anderes Gebäude ausgelagert werden. Dadurch lässt sich vermeiden, dass im Falle eines Brandes, Wasserschadens, etc. die Systeme und Backups gleichzeitig zerstört werden.
Es muss sichergestellt werden, dass die Backup-Datenträger vor unbefugtem Zugriff geschützt gelagert werden. Dies sollte durch Wegsperren der Datenträger in einem Datenträger-Safe geschehen.
Zusätzlich ist die Verschlüsselung der Backup-Datenträger zu empfehlen (bei Neubeschaffung von Sicherungsbandlaufwerken sollte dies Standard sein). Bei der Verschlüsselung ist darauf zu achten, dass die Backup-Datenträger mindestens mit AES-128 verschlüsselt werden (ab Ultrium/LTO 4).
Backup-Datenträger sind unveränderbar und unverwechselbar zu beschriften und mit einem Klassifizierungsvermerk (abhängig von den darauf enthaltenen Daten) zu versehen.

5.1.5. Aufbewahrungsdauer - gesetzliche Verpflichtungen

Besondere Vorschriften betreffend Aufbewahrung von Dokumenten finden sich insbesondere in den Bereichen Arbeitsrecht, Abgabenrecht, Vertragsrecht, Rechnungswesen, sowie in weiteren branchenspezifischen Normen.
Die Homepage der WKO bietet einen Auszug an konkreten Aufbewahrungsfristen.[10]

5.2. Regelmäßige Software Updates

Durch Updates werden meist Sicherheitslücken im Betriebssystem, beziehungsweise in einer Anwendung geschlossen. Es ist somit zwingend erforderlich, alle eingesetzten Anwendungen immer auf dem neusten Softwarestand zu halten. Updates für Windowssysteme lassen sich über „Windows Server Update Services“ (WSUS) zentral verwalten und verteilen. Zu beachten ist, dass die WSUS nur Updates für Windows und andere Microsoft Produkte bereitstellt. Updates für Drittprogramme wie beispielsweise Virenscanner, Adobe Reader oder Java müssen lokal auf den Geräten durchgeführt werden. Alle Geräte sind regelmäßig (mindestens

[9]B 1.4 – Datensicherungskonzept:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01004.html
[10]WKO, EU-Datenschutz-Grundverordnung (DSGVO): Speicher- und Aufbewahrungsfristen:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html

einmal im Monat) durch den Zuständigen auf notwendige Updates zu überprüfen, um sicherzustellen, dass alle Geräte auf dem neuesten Softwarestand sind.
Beim Beziehen der Updates ist darauf zu achten, diese nur direkt vom Softwarehersteller zu beziehen. Weitere Informationen zur Beschaffung von Updates finden sich im BSI IT-Grundschutz M 4.177 - Sicherstellung der Integrität und Authentizität von Softwarepaketen.[11]
Es wird empfohlen, dass sich der Zuständige in Mailinglisten für aktuelle Sicherheitslücken (zB bei https://cert-bund.de/) einträgt, um immer über aktuelle Sicherheitslücken und deren Behebung durch Updates informiert zu sein.[12]
Bei Updates für betriebskritische Programme empfiehlt es sich, das Update zuerst auf einem Testsystem zu installieren und zu testen, bevor es auf allen betroffenen Systemen installiert wird.

5.3. Virenschutz

Zur Abwehr von Schadsoftware müssen alle Computer mit einem Virenschutzprogramm ausgestattet werden. Bei der Auswahl und Konfiguration des Virenschutzprogramms sind folgende grundlegende Anforderungen zu beachten:

- Die Virensignaturdateien müssen laufend automatisch aktualisiert werden.
- Automatische Virensuchläufe über alle Datenträger des Computers müssen konfiguriert werden, um eine regelmäßige Prüfung des gesamten Datenbestandes zu gewährleisten.
- Der Virenscanner muss über einen aktiven Echtzeitschutz verfügen, um beim Zugriff auf eine Datei eine geeignete Warnung für den Benutzer ausgeben zu können.

Ergänzend sollten noch folgende Einstellungen im Betriebssystem beziehungsweise in Anwendungen gesetzt werden:

- Die Anzeige der Dateiendungen (.docx, .exe, .pdf, ...) sollte aktiviert werden, um Schadsoftware, die als E-Mail-Anhang oder Download heruntergeladen wird, leichter erkennen zu können.
- In Microsoft Word, Excel, PowerPoint sollten die Ausführung von Makros unterbunden werden. Die Mitarbeiter sind vom Zuständigen auf die Gefahren bei der Ausführung von Makros hinzuweisen.
- E-Mails mit Anhängen vom Dateityp .exe oder .msi sind zu blockieren.
- Anhänge bei E-Mails dürfen nicht automatisch geöffnet werden. Auch automatische Voransichten zB in E-Mail-Programmen sind zu deaktivieren.

Weiterführende Informationen zum Schutz vor Viren finden sich im österreichischen Informationssicherheitshandbuch in Kapitel 12.3 – Schutz vor Schadprogrammen und Schadfunktionen.

[11] M 4.177 Sicherstellung der Integrität und Authentizität von Softwarepaketen: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04177.html
[12] M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02035.html

6. IT-Security für Sondersysteme (ICS/SCADA)

Zur automatisierten Steuerung von Infrastruktur werden vermehrt **Industrielle Steuerungssysteme** (**Industrial Control Systems, ICS**) bzw Steuerungs- und Überwachungssysteme (**Supervisory Control And Data Acquisition, SCADA**) in unterschiedlichsten Bereichen eingesetzt. Beispiele dafür sind im Bereich der Ver-/Entsorgungsinfrastruktur die Bereiche Trinkwasserversorgung, Abwasserentsorgung (Steuerung von Pumpwerken, Kläranlagen), Photovoltaik-Systeme, Ortsnah- und Fernwärmesysteme, Heizungs- und Solaranlagensteuerungen.
Durch die vermehrte Verbindung der Steuerungssysteme mit dem Internet für eine Fernsteuerung, Fernüberwachung, Handy-App-Zugriff und auch Fernwartung, sind diese Systeme den gleichen Gefahren, wie auch „normale“ Office-IT-Anwendungen ausgesetzt.
Bei Angriffen auf die Steuerungssysteme (aus dem Internet, durch Schadsoftware im lokalen Netz von Fremdgräten, …) kann es zu empfindlichen Störungen für die Anlagen (Ausfall, Beschädigung, möglicher Datenabfluss, …) und/oder Beeinträchtigungen der Bevölkerung bis hin zu Personengefährdungen kommen.

Da ICS/SCADA Systeme im Regelfall nicht regelmäßig Softwareupdates erhalten (können) und darüber hinaus oft über lange Zeiträume (20+ Jahre) betrieben werden, ist eine laufende Aktualisierung der Systeme mit Sicherheitsupdates schwierig möglich. Zusätzlich ist bei vielen ICS/SCADA-Lösungen der Einsatz von Virenscannern nicht zulässig oder technisch nicht möglich. Als Konsequenz daraus sind ICS/SCADA Systeme häufig durch „alte“ Schadsoftware angreifbar oder stellen selbst eine Gefahr für andere Netzwerkbereiche (zB Office LAN) dar. **Eine Trennung von ICS/SCADA-Netzwerken von den restlichen Netzwerken (zB Office LAN, Server LAN) sowie ein striktes Unterbinden des Einbringens von Fremd-IT-Geräten in das ICS/SCADA Netz ist als Mindestmaßnahme umzusetzen**.
Weitere mit höchster Priorität zu setzende Maßnahmen sind die Abänderung von Standard-Passwörtern („admin/admin“) auf sichere Passwörter sowie die Abschottung von Fernzugriffen (Fernwartung, Web-Frontends) durch zB Firewallsysteme.

Die Betreiber von ISC/SCADA Systemen sollten daher die nachfolgend angeführten unterschiedlichen Themengebiete für alle vorhandenen ICS/SCADA Systeme mit den Lieferanten/Betreibern/Wartungspartner mit fachkundiger Anleitung behandeln, sowie bei Neuplanungen und -ausschreibungen die Aufnahme von ICS/SCADA Security Maßnahmen verpflichtend vorsehen.[13]
Für die sichere Planung und den sicheren Betrieb von ICS/SCADA Systemen existieren diverse Standards und Empfehlungen, wobei neben der facheinschlägigen Normengruppe IEC 62443/ISA-99[14], insbesondere auf das ICS Security Kompendium des BSI zu verweisen ist. Dieses Kompendium besteht aus mehreren Teilen, sowohl für Betreiber von ICS/SCADA-

[13]Auf EU-Ebene wurde für die Betreiber wesentlicher Dienste („kritische Infrastrukturen“) die „NIS-Richtlinie“, (EU) 2016/1148, verabschiedet, die bis 09.05.2018 in nationales Recht umzusetzen ist („NIS-G“).
[14]https://www.isa.org/isa99/

Systemen als auch für Hersteller und Integratoren.[15] Mit Priorität sollten nachfolgende Themenbereiche beachtet werden:

Bei der Planung von ICS-Systemen:

- Trennung von ICS-Netz und Office-Netz
- kein direkter Internetzugang, geregelter Fernwartungszugang
- kein direkter Datenaustausch von ICS-Netz ins Office-Netz (zB über USB-Sticks, E-Mail, FTP)

Bei der Beschaffung von ICS-Systemen Beachtung von:

- ICS-Kompendium für Lieferanten, ICS-Kompendium für Betreiber
- IEC 62443/ IAS-99

Bei der Installation und Abnahme:

- Sicherheitscheck
- Dokumentation insbesondere von Gesamtsystem, Netzwerkkonfiguration, Zugangsdaten, Wiederanlauf
- Sicherung der Konfiguration für Wiederherstellung

Zur Absicherung der Systeme gegen unautorisierten Zugriff:

- Änderung von Standardpasswörtern
- Absicherung von Fernwartungszugängen
- Eingeschränkter Zugang zu ICS-Netzwerk (keine Office Geräte oder Fremdgeräte im ICS-Netz erlaubt)

Bei der Betriebsführung:

- Sicherheitschecks
- Wartungsverpflichtung
- Updates (Security)
- Regelmäßige Backups
- Klare Zuständigkeiten

[15] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

7. Organisatorische Maßnahmen

Einige **Maßnahmen erfordern eine regelmäßige Überprüfung** durch den Zuständigen. Es wird empfohlen, die Überprüfung der Maßnahmen zu dokumentieren; insbesondere folgende Maßnahmen sollten in regelmäßigen Abständen überprüft werden:

Berechtigungskonzept (jährlich)

- Überprüfung aller vergebenen Berechtigungen auf Rechtmäßigkeit.

Regelmäßige Überprüfung und Test der Datensicherung (quartalsweise)

- Überprüfen der Datensicherung auf Fehler
- Überprüfen des Datensicherungskonzepts

Regelmäßige Software Updates (monatlich)

- Überprüfung, ob die eingesetzte Software noch auf den aktuellen Stand ist

Verschlüsselung von mobilen Geräten und externen Datenträgern (halbjährlich)

- Überprüfung, ob bei allen mobilen Geräten oder Datenträgern die Verschlüsselung aktiv ist

Passwortrichtlinie (halbjährlich)

- Regelmäßiges Ändern der Passwörter

Wiederkehrende Aufgaben sollten vom Verantwortlichen in einem Kalender vermerkt werden. Dadurch lässt sich sicherstellen, dass die Aufgaben auch tatsächlich zum geforderten Zeitpunkt durchgeführt werden und nicht auf deren Abarbeitung vergessen wird.