|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Template "Sicherheitskonzept inkl. BSI Kompendium 2023"

3. Februar 2023

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | TMP400009 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments | Template "Sicherheitskonzept inkl. BSI Kompendium 2023" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 5 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc126339537)

[Dokumentenhistorie 3](#_Toc126339538)

[Inhaltsverzeichnis 4](#_Toc126339539)

[1 Überblick 10](#_Toc126339540)

[1.1 Abgrenzung des Informationsverbundes 10](#_Toc126339541)

[1.2 Verfahrensdaten 10](#_Toc126339542)

[2 IT-Strukturanalyse 10](#_Toc126339543)

[2.1 Geschäftsprozesse 10](#_Toc126339544)

[2.2 Anwendungen 10](#_Toc126339545)

[2.3 IT-System 10](#_Toc126339546)

[2.4 Industrielle IT 10](#_Toc126339547)

[2.5 Netze und Kommunikation 10](#_Toc126339548)

[2.6 Räume und Gebäude 11](#_Toc126339549)

[3 Schutzbedarf 11](#_Toc126339550)

[3.1 Schutzbedarfserhebung für die Prozesse 18](#_Toc126339551)

[3.1.1 Prozess <1> 18](#_Toc126339552)

[3.1.2 Prozess <n> 18](#_Toc126339553)

[3.1.3 Zusammenfassung der Schutzbedarfserhebung für die Prozesse 18](#_Toc126339554)

[3.2 Abgeleiteter Schutzbedarf für die Anwendungen 18](#_Toc126339555)

[3.2.1 Anwendung <1> 18](#_Toc126339556)

[3.2.2 Anwendung <n> 19](#_Toc126339557)

[3.2.3 Zusammenfassung der Schutzbedarfsvererbung für die Anwendungen 19](#_Toc126339558)

[3.3 Abgeleiteter Schutzbedarf für die IT-Systeme 19](#_Toc126339559)

[3.3.1 IT-System <1> 19](#_Toc126339560)

[3.3.2 IT-System <n> 20](#_Toc126339561)

[3.3.3 Zusammenfassung der Schutzbedarfsvererbung für die IT-System 20](#_Toc126339562)

[3.4 Abgeleiteter Schutzbedarf für die Netzkomponenten 20](#_Toc126339563)

[3.4.1 Netzkomponente <1> 20](#_Toc126339564)

[3.4.2 Netzkomponente <n> 21](#_Toc126339565)

[3.4.3 Zusammenfassung der Schutzbedarfsvererbung für die Netzkomponenten 21](#_Toc126339566)

[3.4.4 Abgeleiteter Schutzbedarf – Kommunikationsverbindungen 21](#_Toc126339567)

[3.5 Abgeleiteter Schutzbedarf für die Infrastruktur 22](#_Toc126339568)

[3.5.1 Gebäude/Raum <1> 22](#_Toc126339569)

[3.5.2 Gebäude/Raum <n> 22](#_Toc126339570)

[3.5.3 Zusammenfassung der Schutzbedarfsvererbung für die Gebäude/Räume 22](#_Toc126339571)

[4 Modellierung nach IT-Grundschutz 23](#_Toc126339572)

[4.1 Schicht ISMS 23](#_Toc126339573)

[4.2 Schicht ORP (Organisation und Personal) 23](#_Toc126339574)

[4.3 Schicht CON (Konzepte und Vorgehensweisen) 23](#_Toc126339575)

[4.4 Schicht OPS (Betrieb) 24](#_Toc126339576)

[4.5 Schicht DER (Detektiv und Reaktion) 25](#_Toc126339577)

[4.6 Schicht APP (Anwendungen) 25](#_Toc126339578)

[4.7 Schicht SYS (IT-Systeme) 26](#_Toc126339579)

[4.8 Schicht IND (Industrielle IT) 27](#_Toc126339580)

[4.9 Schicht NET (Netze und Kommunikation) 28](#_Toc126339581)

[4.10 Schicht INF (Infrastruktur) 28](#_Toc126339582)

[5 IT-Grundschutz-Check 29](#_Toc126339583)

[5.1 Durchführung 29](#_Toc126339584)

[5.2 Ergebnisse 29](#_Toc126339585)

[5.2.1 Schicht ISMS 30](#_Toc126339586)

[5.2.2 Schicht ORP (Organisation und Personal) 30](#_Toc126339587)

[5.2.3 Schicht CON (Konzepte und Vorgehensweisen) 30](#_Toc126339588)

[5.2.4 Schicht OPS (Betrieb) 30](#_Toc126339589)

[5.2.5 Schicht DER (Detektion und Reaktion) 30](#_Toc126339590)

[5.2.6 Schicht APP (Anwendungen) 30](#_Toc126339591)

[5.2.7 Schicht SYS (IT-Systeme) 31](#_Toc126339592)

[5.2.8 Schicht IND (Industrielle IT) 31](#_Toc126339593)

[5.2.9 Schicht NET (Netze und Kommunikation) 31](#_Toc126339594)

[5.2.10 Schicht INF (Infrastruktur) 31](#_Toc126339595)

[6 Risikoanalyse 31](#_Toc126339596)

[6.1 <Betrachtungsobjekt> 33](#_Toc126339597)

[G 0.1 Feuer 33](#_Toc126339598)

[G 0.2 Ungünstige klimatische Bedingungen 34](#_Toc126339599)

[G 0.3 Wasser 34](#_Toc126339600)

[G 0.4 Verschmutzung, Staub, Korrosion 34](#_Toc126339601)

[G 0.5 Naturkatastrophen 35](#_Toc126339602)

[G 0.6 Katastrophen im Umfeld 35](#_Toc126339603)

[G 0.7 Großereignisse im Umfeld 35](#_Toc126339604)

[G 0.8 Ausfall oder Störung der Stromversorgung 36](#_Toc126339605)

[G 0.9 Ausfall oder Störung von Kommunikationsnetzen 36](#_Toc126339606)

[G 0.10 Ausfall oder Störung von Versorgungsnetzen 36](#_Toc126339607)

[G 0.11 Ausfall oder Störung von Dienstleistern 37](#_Toc126339608)

[G 0.12 Elektromagnetische Störstrahlung 37](#_Toc126339609)

[G 0.13 Abfangen kompromittierender Strahlung 37](#_Toc126339610)

[G 0.14 Ausspähen von Informationen (Spionage) 38](#_Toc126339611)

[G 0.15 Abhören 38](#_Toc126339612)

[G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten 38](#_Toc126339613)

[G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten 39](#_Toc126339614)

[G 0.18 Fehlplanung oder fehlende Anpassung 39](#_Toc126339615)

[G 0.19 Offenlegung schützenswerter Informationen 39](#_Toc126339616)

[G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle 40](#_Toc126339617)

[G 0.21 Manipulation von Hard- oder Software 40](#_Toc126339618)

[G 0.22 Manipulation von Informationen 40](#_Toc126339619)

[G 0.23 Unbefugtes Eindringen in IT-Systeme 41](#_Toc126339620)

[G 0.24 Zerstörung von Geräten oder Datenträgern 41](#_Toc126339621)

[G 0.25 Ausfall von Geräten oder Systemen 41](#_Toc126339622)

[G 0.26 Fehlfunktion von Geräten oder Systemen 42](#_Toc126339623)

[G 0.27 Ressourcenmangel 42](#_Toc126339624)

[G 0.28 Software-Schwachstellen oder -Fehler 42](#_Toc126339625)

[G 0.29 Verstoß gegen Gesetze oder Regelungen 43](#_Toc126339626)

[G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen 43](#_Toc126339627)

[G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen 43](#_Toc126339628)

[G 0.32 Missbrauch von Berechtigungen 44](#_Toc126339629)

[G 0.33 Personalausfall 44](#_Toc126339630)

[G 0.34 Anschlag 44](#_Toc126339631)

[G 0.35 Nötigung, Erpressung oder Korruption 45](#_Toc126339632)

[G 0.36 Identitätsdiebstahl 45](#_Toc126339633)

[G 0.37 Abstreiten von Handlungen 45](#_Toc126339634)

[G 0.38 Missbrauch personenbezogener Daten 46](#_Toc126339635)

[G 0.39 Schadprogramme 46](#_Toc126339636)

[G 0.40 Verhinderung von Diensten (Denial of Service) 46](#_Toc126339637)

[G 0.41 Sabotage 47](#_Toc126339638)

[G 0.42 Social Engineering 47](#_Toc126339639)

[G 0.43 Einspielen von Nachrichten 47](#_Toc126339640)

[G 0.44 Unbefugtes Eindringen in Räumlichkeiten 48](#_Toc126339641)

[G 0.45 Datenverlust 48](#_Toc126339642)

[G 0.46 Integritätsverlust schützenswerter Informationen 48](#_Toc126339643)

[G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe 49](#_Toc126339644)

[6.2 Auflistung aller Zusatzmaßnahmen zur Reduzierung des Risikos 49](#_Toc126339645)

[6.2.1 Schicht ISMS 49](#_Toc126339646)

[6.2.2 Schicht ORP (Organisation und Personal) 49](#_Toc126339647)

[6.2.3 Schicht CON (Konzepte und Vorgehensweisen) 49](#_Toc126339648)

[6.2.4 Schicht OPS (Betrieb) 50](#_Toc126339649)

[6.2.5 Schicht DER (Detektion und Reaktion) 50](#_Toc126339650)

[6.2.6 Schicht APP (Anwendungen) 50](#_Toc126339651)

[6.2.7 Schicht SYS (IT-Systeme) 50](#_Toc126339652)

[6.2.8 Schicht IND (Industrielle IT) 50](#_Toc126339653)

[6.2.9 Schicht NET (Netze und Kommunikation) 51](#_Toc126339654)

[6.2.10 Schicht INF (Infrastruktur) 51](#_Toc126339655)

[6.3 Auflistung aller besonderen Restrisiken 51](#_Toc126339656)

Abkürzungsverzeichnis

Siehe Anlage zentrales Abkürzungsverzeichnis Informationssicherheit.

Abbildungsverzeichnis

**Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.**

Tabellenverzeichnis

[Tabelle 1: Sicherheitsziel Verfügbarkeit - Informationsklassifizierung und Kritikalitätsmatrix 13](#_Toc126339657)

[Tabelle 2: Sicherheitsziel Vertraulichkeit - Informationsklassifizierung und Kritikalitätsmatrix 15](#_Toc126339658)

[Tabelle 3: Sicherheitsziel Integrität - Informationsklassifizierung und Kritikalitätsmatrix 17](#_Toc126339659)

[Tabelle 4: Abgeleiteter Schutzbedarf - Anwendung <n> 19](#_Toc126339660)

[Tabelle 5: Übersicht der durchgeführten IT-Grundschutz-Checks 29](#_Toc126339661)

[Tabelle 6: noch offenen Grundschutz-Maßnahmen - Schicht ISMS 30](#_Toc126339662)

[Tabelle 7: noch offenen Grundschutz-Maßnahmen - Schicht ORP 30](#_Toc126339663)

[Tabelle 8: noch offenen Grundschutz-Maßnahmen - Schicht CON 30](#_Toc126339664)

[Tabelle 9: noch offenen Grundschutz-Maßnahmen - Schicht OPS 30](#_Toc126339665)

[Tabelle 10: noch offenen Grundschutz-Maßnahmen - Schicht DER 30](#_Toc126339666)

[Tabelle 11: noch offenen Grundschutz-Maßnahmen - Schicht APP 30](#_Toc126339667)

[Tabelle 12: noch offenen Grundschutz-Maßnahmen - Schicht SYS 31](#_Toc126339668)

[Tabelle 13: noch offenen Grundschutz-Maßnahmen - Schicht IND 31](#_Toc126339669)

[Tabelle 14: noch offenen Grundschutz-Maßnahmen - Schicht NET 31](#_Toc126339670)

[Tabelle 15: noch offenen Grundschutz-Maßnahmen - Schicht INF 31](#_Toc126339671)

[Tabelle 16: Risikoanalyse - Bewertung von Eintrittswahrscheinlichkeiten 32](#_Toc126339672)

[Tabelle 17: Risikoanalyse - Bewertung von Auswirkungen 32](#_Toc126339673)

[Tabelle 18: Risikoanalyse - Bewertung von Risiken 33](#_Toc126339674)

[Tabelle 19: Zusatzmaßnahmen aus der Risikoanalyse - Schicht ISMS 49](#_Toc126339675)

[Tabelle 20: Zusatzmaßnahmen aus der Risikoanalyse - Schicht ORP 49](#_Toc126339676)

[Tabelle 21: Zusatzmaßnahmen aus der Risikoanalyse - Schicht CON 50](#_Toc126339677)

[Tabelle 22: Zusatzmaßnahmen aus der Risikoanalyse - Schicht OPS 50](#_Toc126339678)

[Tabelle 23: Zusatzmaßnahmen aus der Risikoanalyse - Schicht DER 50](#_Toc126339679)

[Tabelle 24: Zusatzmaßnahmen aus der Risikoanalyse - Schicht APP 50](#_Toc126339680)

[Tabelle 25: Zusatzmaßnahmen aus der Risikoanalyse - Schicht SYS 50](#_Toc126339681)

[Tabelle 26: Zusatzmaßnahmen aus der Risikoanalyse - Schicht IND 50](#_Toc126339682)

[Tabelle 27: Zusatzmaßnahmen aus der Risikoanalyse - Schicht NET 51](#_Toc126339683)

[Tabelle 28: Zusatzmaßnahmen aus der Risikoanalyse - Schicht INF 51](#_Toc126339684)

[Tabelle 29: Von der geschäftsführung übernommene Restrisiken 51](#_Toc126339685)

# Überblick

## Abgrenzung des Informationsverbundes

Die folgende Abbildung zeigt eine abstrahierte Sicht auf den Informationsverbund im Sinne eines bereinigten Netzplans nach dem BSI-Standard 200-2 und weist dabei die Grenzen und Schnittstellen des in diesem Sicherheitskonzept betrachteten Informationsverbunds aus.

[Abbildung vom Informationsverbund]

## Verfahrensdaten

[Beschreibung der im Verfahren erhobenen und verarbeiteten Daten und der grundsätzlichen Datenflüsse]

# IT-Strukturanalyse

## Geschäftsprozesse

| ID | Geschäftsprozess | Typ des Prozesses | Erläuterung |
| --- | --- | --- | --- |
| P-0001 |  | <Hauptprozess>  <Unterstützungsprozess> |  |

## Anwendungen

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Anwendung | Typ der Anwendung | Erläuterung |
| APP-0001 |  |  |  |

## IT-System

| ID | IT-System | Plattform | Erläuterung |
| --- | --- | --- | --- |
| SYS-0001 |  |  |  |

## Industrielle IT

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Industrielle IT | Plattform | Erläuterung |
| IND-0001 |  |  |  |

## Netze und Kommunikation

| ID | Netzkomponente | Plattform | Erläuterung |
| --- | --- | --- | --- |
| NET-0001 |  |  |  |

In der nachfolgenden Tabelle werden die Kommunikationsverbindungen, eingesetzten Protokolle sowie etwaige Authentisierungsverfahren benannt.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Verbindungsaufbau von --> zu | Protokoll | Port | Verschlüsselung | Zweck / Kommunikationsinhalte |
| V-0001 |  |  |  |  |  |

## Räume und Gebäude

| ID | Räume und Gebäude | Erläuterung |
| --- | --- | --- |
| INF-0001 |  |  |

# Schutzbedarf

Alle Daten (und damit auch die sie verarbeitenden Systeme) müssen gemäß den Sicherheitszielen Vertraulichkeit, Verfügbarkeit und Integrität durch den Informationseigentümer klassifiziert und dementsprechend gekennzeichnet sein, um jederzeit eine angemessene Verarbeitung der Informationen zu gewährleisten.

Die Informationsklassifizierungen erfolgen nach der im BSI-Standard 200-2 dargestellten Vorgehensweise und bezieht sich dementsprechend auf die Sicherheitsziele **Vertraulichkeit**, **Integrität**, **Verfügbarkeit**. Die Zuordnung des Schutzbedarfs erfolgt jeweils in den Stufen „**normal**“, „**hoch**“ und „**sehr hoch**“.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Szenario | Normal | Hoch | Sehr hoch |
| Verfügbarkeit | Beeinträchtigung der Aufgabenerfüllung | Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden.  Ein Ausfall der Plattform bzw. des Verfahrens ab 18 Stunden und 15 Minuten (SLA 97,50% per Monat) führt zu Beeinträchtigungen der verarbeitenden Prozesse. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer und 18 Stunden. | Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt.  Ein Ausfall der Plattform bzw. des Verfahrens ab 7 Stunden (SLA 99,00% per Monat) führt zu Beeinträchtigungen der verarbeitenden Prozesse. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer und 7 Stunden. | Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.  Ein Ausfall der Plattform bzw. des Verfahrens ab 44 Minuten (SLA 99,90% per Monat) führt zu Beeinträchtigungen der verarbeitenden Prozesse. Die maximal tolerierbare Ausfallzeit (MTA) liegt unter 44 Minuten. |
| Verstöße gegen Gesetze, Vorschriften und Verträge | Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen.  Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen. | Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen.  Vertragsverletzungen mit hohen Konventionalstrafen. | Fundamentaler Verstoß gegen Vorschriften und Gesetze.  Vertragsverletzungen, deren Haftungsschäden sehr hoch für die <Institution> sind. |
| Beeinträchtigung der informationellen Selbstbestimmung | Verstöße gegen Art. 15, 12 III DSGVO können zu einer Beeinträchtigung der informationellen Selbstbestimmung führen. | Verstöße gegen Art. 15, 12 III DSGVO können zu einer Beeinträchtigung der informationellen Selbstbestimmung führen. | Verstöße gegen Art. 15, 12 III DSGVO können zu einer Beeinträchtigung der informationellen Selbstbestimmung führen. |
| Beeinträchtigung der persönlichen Unversehrtheit | Eine Beeinträchtigung erscheint nicht möglich. | Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden. | Es besteht unmittelbare Gefahr für Leib und Leben.  Durch fehlende Zugriffsmöglichkeit auf die Informationen/Daten besteht unmittelbar Gefahr einer gravierenden Beeinträchtigung für Betroffene. |
| Negative Außenwirkung | Es ist eine nur geringe negative Außenwirkung bzw. ein interner Vertrauensverlust anzunehmen.  Beeinträchtigungen werden von Kunden/Mitarbeitenden als bedeutungslos eingeschätzt bzw. gar nicht wahrgenommen.  Das Vertrauen ist punktuell beeinträchtigt (einzelne Mitarbeitende, einzelner Bereich / Service) und nicht flächendeckend auf die gesamte <Institution> bezogen. | Ein erheblicher öffentlicher sowohl temporärer als auch dauerhafter Vertrauensverlust für die <Institution> ist anzunehmen.  Der fehlende Zugriff auf Informationen/Daten bzw. der Ausfall des Verfahrens wird von Kunden/Mitarbeitenden bemerkt und wahrgenommen.  Das Vertrauen in die <Institution> ist bei einzelnen Kunden/Mitarbeitende beeinträchtigt.  Der Vertrauensverlust ist nur mit hohem Aufwand auszugleichen.  Es entsteht ein Imageverlust, der sich auf weitere Teile der <Institution> auswirkt.  Einzelne Kunden/Mitarbeitende beenden oder weigern die Nutzung des Verfahrens. | Ein enormer öffentlicher Vertrauensverlust ist für die <Institution> anzunehmen.  Es drohen politische Konsequenzen.  Ein Großteil der Kunden/Mitarbeitenden beenden oder weigern die Nutzung des Verfahrens.  Es entsteht ein Vertrauensverlust gegenüber einem Großteil der Kunden/Mitarbeitende mit erheblichen Zweifeln an die Zuverlässigkeit der <Institution>.  Das Image wird erheblich beschädigt und wirkt sich auf die gesamte <Institution> aus.  Der Imageverlust kann auf unbestimmte Zeit nicht ausgeglichen werden. |
| Finanzielle Auswirkungen | Der finanzielle Schaden beläuft sich auf ≤ €€. | Der finanzielle Schaden beläuft sich auf ≤ €€€€. | Der finanzielle Schaden beläuft sich auf ≥ €€€€. |

Tabelle 1: Sicherheitsziel Verfügbarkeit - Informationsklassifizierung und Kritikalitätsmatrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vertraulichkeit | Szenario | Normal | Hoch | Sehr hoch |
| Beeinträchtigung der Aufgabenerfüllung | Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. | Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. | Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. |
| Verstöße gegen Gesetze, Vorschriften und Verträge | Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen.  Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.  z.B. keine juristischen Konsequenzen | Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen.  Vertragsverletzungen mit hohen Konventionalstrafen.  z.B. Ahndung als Ordnungswidrigkeit | Fundamentaler Verstoß gegen Vorschriften und Gesetze.  Daten, die besonderen rechtlichen Verschwiegenheitsbeschränkungen unterliegen und deren Preisgabe einen Straftatbestand darstellen.  Vertragsverletzungen, deren Haftungsschäden sehr hoch sind. |
| Beeinträchtigung der informationellen Selbstbestimmung | Eine Veröffentlichung personenbezogener Daten hätte für die Betroffenen hinsichtlich ihrer gesellschaftlichen Stellung oder ihrer wirtschaftlichen Verhältnisse nur geringfügige Konsequenzen.  Es handelt sich nicht um sensible Daten. | Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren.  Im Falle der erheblichen Beeinträchtigung handelt es sich um sensible Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln. | Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren.  Im Falle der erheblichen Beeinträchtigung handelt es sich um sensible Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln. |
| Beeinträchtigung der persönlichen Unversehrtheit | Eine Beeinträchtigung erscheint nicht möglich. | Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden. | Es besteht Gefahr für Leib und Leben. |
| Negative Außenwirkung | Es ist eine nur geringe negative Außenwirkung bzw. ein interner Vertrauensverlust anzunehmen.  Beeinträchtigungen werden von Kunden/Mitarbeitende als bedeutungslos eingeschätzt bzw. gar nicht wahrgenommen.  Das Vertrauen ist punktuell beeinträchtigt (einzelne Mitarbeitende /Service) und nicht flächendeckend auf die gesamte <Institution> bezogen. | Ein erheblicher öffentlicher sowohl temporärer als auch dauerhafter Vertrauensverlust für die <Institution> ist anzunehmen.  Der fehlende Zugriff auf Daten bzw. der Ausfall des Verfahrens wird von Kunden/Mitarbeitende bemerkt und wahrgenommen.  Das Vertrauen in die <Institution> ist bei einzelnen Kunden/Mitarbeitende beeinträchtigt.  Es entsteht ein Imageverlust, der sich auf weitere Teile der <Institution> auswirkt. | Ein enormer öffentlicher Vertrauensverlust ist anzunehmen.  Es drohen politische Konsequenzen.  Es entsteht ein Vertrauensverlust gegenüber einem Großteil der Kunden/Mitarbeitende mit erheblichen Zweifeln an die Verschwiegenheit beim Umgang mit vertraulichen Daten.  Das Image wird erheblich beschädigt und wirkt sich auf die gesamte <Institution> aus.  Der Imageverlust kann auf unbestimmte Zeit nicht ausgeglichen werden. |
| Finanzielle Auswirkungen | Der finanzielle Schaden beläuft sich auf ≤ €€. | Der finanzielle Schaden beläuft sich auf ≤ €€€€. | Der finanzielle Schaden beläuft sich auf ≥ €€€€. |

Tabelle 2: Sicherheitsziel Vertraulichkeit - Informationsklassifizierung und Kritikalitätsmatrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Integrität | Szenario | Normal | Hoch | Sehr hoch |
| Beeinträchtigung der Aufgabenerfüllung | Bei Eintritt einer Verfälschung und/oder Löschung Daten sind die Schäden begrenzt.  Es entstehen Beeinträchtigungen in der Bearbeitung von Aufgaben (z.B. längere Bearbeitungszeit, umständlicherer Bearbeitung, höherer Aufwand bei der Beschaffung von Informationen).  Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden.  Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer und 18 Stunden. | Bei Eintritt einer Verfälschung und/oder Löschung Daten sind die Schäden begrenzt.  Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt.  Die Verfälschung und/oder Löschung führt zu erheblichen Arbeitseinschränkungen.  Eine schnelle Erkennung und Behebung der Verfälschung / Schäden ist erforderlich.  Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer und 7 Stunden. | Vorsätzliche oder durch Fehlfunktion verursachte Verfälschungen von Daten führen zu Schäden in sehr großem Ausmaß.  Bei Eintritt einer Verfälschung und/oder Löschung entsteht eine Arbeitsunfähigkeit und/oder Unmöglichkeit der Leistungserbringung.  Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.  Eine Verfälschung der Daten ist zu verhindern.  Die maximal tolerierbare Ausfallzeit (MTA) liegt unter 44 Minuten. |
| Verstöße gegen Gesetze, Vorschriften und Verträge | Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen.  Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen. | Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen.  Vertragsverletzungen mit hohen Konventionalstrafen. | Fundamentaler Verstoß gegen Vorschriften und Gesetze.  Daten, die besonderen rechtlichen Verschwiegenheitsbeschränkungen unterliegen und deren Preisgabe einen Straftatbestand darstellen.  Vertragsverletzungen, deren Haftungsschäden sehr hoch sind. |
| Beeinträchtigung der informationellen Selbstbestimmung | Eine Veränderung, Verfälschung und/oder Löschung  personenbezogener Daten hätte für die Betroffenen hinsichtlich ihrer gesellschaftlichen Stellung oder ihrer wirtschaftlichen Verhältnisse nur geringfügige Konsequenzen.  Es handelt sich nicht um sensible Daten. | Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren.  Im Falle der erheblichen Beeinträchtigung handelt es sich um sensible Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln. | Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren.  Im Falle der erheblichen Beeinträchtigung handelt es sich um sensible Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln. |
| Beeinträchtigung der persönlichen Unversehrtheit | Eine Beeinträchtigung erscheint nicht möglich. | Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden. | Es besteht Gefahr für Leib und Leben. |
| Negative Außenwirkung | Es ist eine nur geringe negative Außenwirkung bzw. ein interner Vertrauensverlust anzunehmen.  Beeinträchtigungen werden von Kunden/Mitarbeitende als bedeutungslos eingeschätzt bzw. gar nicht wahrgenommen.  Das Vertrauen ist punktuell beeinträchtigt (einzelne Mitarbeitende, einzelner Bereich/Service) und nicht flächendeckend auf die gesamte <Institution> bezogen. | Ein erheblicher öffentlicher sowohl temporärer als auch dauerhafter Vertrauensverlust für die <Institution> ist anzunehmen.  Der fehlende Zugriff auf Daten bzw. der Ausfall des Verfahrens wird von Kunden/Mitarbeitenden bemerkt und wahrgenommen.  Das Vertrauen in die <Institution> ist bei einzelnen Kunden/Mitarbeitende beeinträchtigt.  Es entsteht ein Imageverlust, der sich auf weitere Teile der <Institution> auswirkt. | Ein enormer öffentlicher Vertrauensverlust ist anzunehmen.  Es drohen politische Konsequenzen.  Es entsteht ein Vertrauensverlust gegenüber einem Großteil der Kunden/Mitarbeitende mit erheblichen Zweifeln an die Verschwiegenheit beim Umgang mit vertraulichen Daten.  Das Image wird erheblich beschädigt und wirkt sich auf die gesamte <Institution> aus.  Der Imageverlust kann auf unbestimmte Zeit nicht ausgeglichen werden. |
| Finanzielle Auswirkungen | Der finanzielle Schaden beläuft sich auf ≤ €€. | Der finanzielle Schaden beläuft sich auf ≤ €€€€. | Der finanzielle Schaden beläuft sich auf ≥ €€€€. |

Tabelle 3: Sicherheitsziel Integrität - Informationsklassifizierung und Kritikalitätsmatrix

## Schutzbedarfserhebung für die Prozesse

### Prozess <1>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### Prozess <n>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### Zusammenfassung der Schutzbedarfserhebung für die Prozesse

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Prozess | Verfügbarkeit | Integrität | Vertraulichkeit | Maximum |
|  |  |  |  |  |
|  |  |  |  |  |

## Abgeleiteter Schutzbedarf für die Anwendungen

### Anwendung <1>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### Anwendung <n>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

Tabelle 4: Abgeleiteter Schutzbedarf - Anwendung <n>

### Zusammenfassung der Schutzbedarfsvererbung für die Anwendungen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Anwendung | Verfügbarkeit | Integrität | Vertraulichkeit | Maximum |
|  |  |  |  |  |

## Abgeleiteter Schutzbedarf für die IT-Systeme

### IT-System <1>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### IT-System <n>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### Zusammenfassung der Schutzbedarfsvererbung für die IT-System

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IT-Systeme | Verfügbarkeit | Integrität | Vertraulichkeit | Maximum |
|  |  |  |  |  |

## Abgeleiteter Schutzbedarf für die Netzkomponenten

### Netzkomponente <1>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### Netzkomponente <n>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### Zusammenfassung der Schutzbedarfsvererbung für die Netzkomponenten

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Netzkomponente | Verfügbarkeit | Integrität | Vertraulichkeit | Maximum |
|  |  |  |  |  |

### Abgeleiteter Schutzbedarf – Kommunikationsverbindungen

Der Schutzbedarf für die Kommunikationsverbindungen ergibt sich aus dem Schutzbedarf der jeweils abhängigen Anwendungen bzw. der übertragenen Daten.

Verbindungsstart- und -endpunkte, die in Klammern gesetzt sind, sind nicht Gegenstand des betrachteten Informationsverbunds. Die entsprechenden Kommunikationsverbindungen stellen damit Außenverbindungen des Verbunds dar. Um eine bessere Lesbarkeit zu ermöglichen werden die folgenden Kürzel verwendet:

* N - Normal
* H - Hoch
* SH - Sehr hoch

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Startpunkt → Endpunkt | Außenverbindung | Verfügbarkeit | Integrität | Vertraulichkeit | Maximum | Begründung |
|  |  | <Ja>  <Nein> | <N>  <H>  <SH> | <N>  <H>  <SH> | <N>  <H>  <SH> | <N>  <H>  <SH> |  |

## Abgeleiteter Schutzbedarf für die Infrastruktur

### Gebäude/Raum <1>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### Gebäude/Raum <n>

|  |  |  |
| --- | --- | --- |
| Grundwert | Schutzbedarf | Begründung |
| Verfügbarkeit | <normal>  <hoch>  <sehr hoch> |  |
| Integrität | <normal>  <hoch>  <sehr hoch> |  |
| Vertraulichkeit | <normal>  <hoch>  <sehr hoch> |  |
| Maximum | <normal>  <hoch>  <sehr hoch> | Maximum Prinzip  Kumulationseffekt  Verteilungseffekt |

### Zusammenfassung der Schutzbedarfsvererbung für die Gebäude/Räume

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gebäude/Raum | Verfügbarkeit | Integrität | Vertraulichkeit | Maximum |
|  |  |  |  |  |

# Modellierung nach IT-Grundschutz

Die Modellierung nach IT-Grundschutz umfasst die Abbildung der in Kapitel 1 identifizierten Objekte auf Bausteine des BSI IT-Grundschutzkompendium in der Version 02/2021.

## Schicht ISMS

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| ISMS.1 Sicherheitsmanagement |  |  |  |

## Schicht ORP (Organisation und Personal)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| ORP.1 Organisation |  |  |  |
| ORP.2 Personal |  |  |  |
| ORP.3 Sensibilisierung und Schulung zur Informationssicherheit |  |  |  |
| ORP.4 Identitäts- und Berechtigungsmanagement |  |  |  |
| ORP.5 Compliance Management (Anforderungsmanagement) |  |  |  |

## Schicht CON (Konzepte und Vorgehensweisen)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| CON.1 Kryptokonzept |  |  |  |
| CON.2 Datenschutz |  |  |  |
| CON.3 Datensicherungskonzept |  |  |  |
| CON.6 Löschen und Vernichten |  |  |  |
| CON.7 Informationssicherheit auf Auslandsreisen |  |  |  |
| CON.8 Software-Entwicklung |  |  |  |
| CON.9 Informationsaustausch |  |  |  |
| CON.10 Entwicklung von Webanwendungen |  |  |  |
| CON.11.1GeheimschutzVS-NURFÜRDENDIENSTGEBRAUCH (VS-NfD) |  |  |  |

## Schicht OPS (Betrieb)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| OPS.1.1.1AllgemeinerIT-Betrieb |  |  |  |
| OPS.1.1.2 Ordnungsgemäße IT-Administration |  |  |  |
| OPS.1.1.3 Patch- und Änderungsmanagement |  |  |  |
| OPS.1.1.4 Schutz vor Schadprogrammen |  |  |  |
| OPS.1.1.5 Protokollierung |  |  |  |
| OPS.1.1.6 Software-Tests und –Freigaben |  |  |  |
| OPS.1.1.7 Systemmanagement |  |  |  |
| OPS.1.2.2 Archivierung |  |  |  |
| OPS.1.2.4 Telearbeit |  |  |  |
| OPS.1.2.5 Fernwartung |  |  |  |
| OPS.1.2.6 NTP -Zeitsynchronisation |  |  |  |
| OPS.2.1 Outsourcing für Kunden |  |  |  |
| OPS.2.2 Cloud-Nutzung |  |  |  |
| OPS.2.3NutzungvonOutsourcing |  |  |  |
| OPS.3.2AnbietenvonOutsourcing |  |  |  |

## Schicht DER (Detektiv und Reaktion)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| DER.1 Detektion von sicherheitsrelevanten Ereignissen |  |  |  |
| DER.2.1 Behandlung von Sicherheitsvorfällen |  |  |  |
| DER.2.2 Vorsorge für die IT-Forensik |  |  |  |
| DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle |  |  |  |
| DER.3.1 Audits und Revisionen |  |  |  |
| DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision |  |  |  |
| DER.4 Notfallmanagement |  |  |  |

## Schicht APP (Anwendungen)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| APP.1.1 Office-Produkte |  |  |  |
| APP.1.2 Web-Browser |  |  |  |
| APP.1.4 Mobile Anwendungen (Apps) |  |  |  |
| APP.2.1 Allgemeiner Verzeichnisdienst |  |  |  |
| APP.2.2 Active Directory |  |  |  |
| APP.2.3 OpenLDAP |  |  |  |
| APP.3.1 Webanwendungen |  |  |  |
| APP.3.2 Webserver |  |  |  |
| APP.3.3 Fileserver |  |  |  |
| APP.3.4 Samba |  |  |  |
| APP 3.6 DNS-Server |  |  |  |
| APP.4.2 SAP-ERP-System |  |  |  |
| APP.4.3 Relationale Datenbanksysteme |  |  |  |
| APP.4.4 Kubernetes |  |  |  |
| APP.4.6 SAP ABAP-Programmierung |  |  |  |
| APP.5.2 Microsoft Exchange und Outlook |  |  |  |
| APP.5.3 Allgemeiner E-Mail-Client und -Server |  |  |  |
| APP.5.4UnifiedCommunicationsundCollaboration(UCC) |  |  |  |
| APP.6 Allgemeine Software |  |  |  |
| APP.7 Entwicklung von Individualsoftware |  |  |  |

## Schicht SYS (IT-Systeme)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| SYS.1.1 Allgemeiner Server |  |  |  |
| SYS.1.2.2 Windows Server 2012 |  |  |  |
| SYS.1.2.3 Windows Server |  |  |  |
| SYS.1.3 Server unter Linux und Unix |  |  |  |
| SYS.1.5 Virtualisierung |  |  |  |
| SYS.1.6 Containerisierung |  |  |  |
| SYS.1.7 IBM Z-System |  |  |  |
| SYS.1.8 Speicherlösungen |  |  |  |
| SYS.1.9Terminalserver |  |  |  |
| SYS.2.1 Allgemeiner Client |  |  |  |
| SYS.2.2.3 Clients unter Windows |  |  |  |
| SYS.2.3 Clients unter Linux und Unix |  |  |  |
| SYS.2.4 Clients unter macOS |  |  |  |
| SYS.2.5Client-Virtualisierung |  |  |  |
| SYS.2.6VirtualDesktopInfrastructure |  |  |  |
| SYS.3.1 Laptops |  |  |  |
| SYS.3.2.1 Allgemeine Smartphones und Tablets |  |  |  |
| SYS.3.2.2 Mobile Device Management (MDM) |  |  |  |
| SYS.3.2.3 iOS (for Enterprise) |  |  |  |
| SYS.3.2.4 Android |  |  |  |
| SYS.3.3 Mobiltelefon |  |  |  |
| SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte |  |  |  |
| SYS.4.3 Eingebettete Systeme |  |  |  |
| SYS.4.4 Allgemeines IoT-Gerät |  |  |  |
| SYS.4.5 Wechseldatenträger |  |  |  |

## Schicht IND (Industrielle IT)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| IND.1 Prozessleit- und Automatisierungstechnik |  |  |  |
| IND.2.1 Allgemeine ICS-Komponente |  |  |  |
| IND.2.2 Speicherprogrammierbare Steuerung (SPS) |  |  |  |
| IND.2.3 Sensoren und Aktoren |  |  |  |
| IND.2.4 Maschine |  |  |  |
| IND.2.7 Safety Instrumented Systems |  |  |  |
| IND.3.2FernwartungimindustriellenUmfeld |  |  |  |

## Schicht NET (Netze und Kommunikation)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| NET.1.1 Netzarchitektur und -design |  |  |  |
| NET.1.2 Netzmanagement |  |  |  |
| NET.2.1 WLAN-Betrieb |  |  |  |
| NET.2.2 WLAN-Nutzung |  |  |  |
| NET.3.1 Router und Switches |  |  |  |
| NET.3.2 Firewall |  |  |  |
| NET.3.3 VPN |  |  |  |
| NET.3.4NetworkAccessControl |  |  |  |
| NET.4.1 TK-Anlagen |  |  |  |
| NET.4.2 VoIP |  |  |  |
| NET.4.3 Faxgeräte und Faxserver |  |  |  |

## Schicht INF (Infrastruktur)

| Baustein | Wird in diesem Sicherheitskonzept betrachtet | | |
| --- | --- | --- | --- |
| Ja | Nein | Begründung |
| INF.1 Allgemeines Gebäude |  |  |  |
| INF.2 Rechenzentrum sowie Serverraum |  |  |  |
| INF.5 Raum sowie Schrank für technische Infrastruktur |  |  |  |
| INF.6 Datenträgerarchiv |  |  |  |
| INF.7 Büroarbeitsplatz |  |  |  |
| INF.8 Häuslicher Arbeitsplatz |  |  |  |
| INF.9 Mobiler Arbeitsplatz |  |  |  |
| INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume |  |  |  |
| INF.11 Allgemeines Fahrzeug |  |  |  |
| INF.12 Verkabelung |  |  |  |
| INF.13 Technisches Gebäudemanagement |  |  |  |
| INF.14 Gebäudeautomation |  |  |  |

# IT-Grundschutz-Check

## Durchführung

Im IT-Grundschutz-Check wurde zu allen modellierten Bausteinen ermittelt, wie die dort enthaltenen Sicherheitsanforderungen unter Berücksichtigung des Schutzbedarfes erfüllt werden.

Zu jeder Anforderung wurde dabei erhoben, ob diese durch die vorhandene Realisierung vollständig („ja“), in Teilen („teilweise“) oder nicht („nein“) erfüllt wird, oder ob die Anforderung auf den betrachteten Informationsverbund aus bestimmten Gründen nicht anwendbar ist („entbehrlich“). Durch die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen werden Verbesserungsmöglichkeiten aufgezeigt. Folgende IT-Grundschutz-Checks wurden durchgeführt.

| Baustein/Zielobjekt | Datum | Ansprechpartner |
| --- | --- | --- |
|  |  |  |

Tabelle 5: Übersicht der durchgeführten IT-Grundschutz-Checks

## Ergebnisse

Aus der Prüfung der Anforderungen im IT-Grundschutz-Check resultierenden die folgenden offenen Grundschutz-Maßnahmen (oGM):

### Schicht ISMS

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 1.1 |  |  |

Tabelle 6: noch offenen Grundschutz-Maßnahmen - Schicht ISMS

### Schicht ORP (Organisation und Personal)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 2.1 |  |  |

Tabelle 7: noch offenen Grundschutz-Maßnahmen - Schicht ORP

### Schicht CON (Konzepte und Vorgehensweisen)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 3.1 |  |  |

Tabelle 8: noch offenen Grundschutz-Maßnahmen - Schicht CON

### Schicht OPS (Betrieb)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 4.1 |  |  |

Tabelle 9: noch offenen Grundschutz-Maßnahmen - Schicht OPS

### Schicht DER (Detektion und Reaktion)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 5.1 |  |  |

Tabelle 10: noch offenen Grundschutz-Maßnahmen - Schicht DER

### Schicht APP (Anwendungen)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 6.1 |  |  |

Tabelle 11: noch offenen Grundschutz-Maßnahmen - Schicht APP

### Schicht SYS (IT-Systeme)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 7.1 |  |  |

Tabelle 12: noch offenen Grundschutz-Maßnahmen - Schicht SYS

### Schicht IND (Industrielle IT)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 8.1 |  |  |

Tabelle 13: noch offenen Grundschutz-Maßnahmen - Schicht IND

### Schicht NET (Netze und Kommunikation)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 9.1 |  |  |

Tabelle 14: noch offenen Grundschutz-Maßnahmen - Schicht NET

### Schicht INF (Infrastruktur)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
| oGM 10.1 |  |  |

Tabelle 15: noch offenen Grundschutz-Maßnahmen - Schicht INF

# Risikoanalyse

Die Risikoanalyse in diesem IT-Sicherheitskonzept erfolgt für den Informationsverbund nach dem BSI-Standard 200-3 und beachtet zusätzlich die Anforderungen der KritisV hinsichtlich der zur Verfügung stehendene Risikobehandlungsoptionen.

Aufgrund der Erfahrungen bei der Durchführung von Risikoanalysen hat es sich nicht bewährt, für die Risikoanalyse einzelne Serverobjekte als Betrachtungsgegenstand anzuführen, da gerade die modellierbaren Komponenten i. d. R. über die Maßnahmen zu den IT-Grundschutzanforderungen bereits gut abgesichert sind. In der Risikoanalyse müssen vielmehr die anwendungsspezifischen bzw. prozessspezifischen Besonderheiten betrachtet werden, die entweder nicht modellierbar sind oder durch die Anforderungen der Bausteine alleine nicht ausreichend abgesichert sind, um den hohen und sehr hohen Schutzbedarf zu erfüllen.

Daher wird als Betrachtungsgegenstand für die Risikoanalyse *<Betrachtungsobjekt>* insgesamt als betrachtetes Objekt zugrunde gelegt. Wo eine differenzierte Betrachtung sinnvoll ist, erfolgt dies durch Aufteilung der betrachteten Gefährdungen auf einzelne Teilprozesse, Teilanwendungen oder Objekte.

Dieses Vorgehen wird durch den BSI-Standard 200-3 explizit zugelassen (Kap. 2, S. 10):

*Bei den betrachteten Zielobjekten muss es sich nicht zwangsläufig um systemorientierte Zielobjekte (z. B. Anwendungen, IT-Systeme oder Räume) handeln. Vielmehr kann die Risikoanalyse auch auf Geschäftsprozessebene durchgeführt werden.*

Grundlage für die Risikoanalyse ist der Katalog „Elementare Gefährdungen“ aus dem IT-Grundschutzkompendium. Dazu wurden die für die betrachtete Anwendung relevanten Gefährdungen aus dem Katalog ausgewählt und für den Anwendungsfall konkretisiert. In der Konkretisierung können aus einer elementaren Gefährdung auch mehrere konkrete Gefährdungen abgeleitet werden.

Die Betrachtung zu jeder einzelnen Gefährdung erfolgt in tabellarischer Form. Die Darstellung umfasst dabei:

1. eine Beschreibung der konkreten Gefährdung
2. eine Beschreibung der gegen die Gefährdung wirkenden Maßnahmen
3. eine Beschreibung des verbleibenden Risikos
4. eine Bewertung der Eintrittswahrscheinlichkeit
5. eine Bewertung der Auswirkungen
6. eine Bewertung des Risikos
7. sofern erforderlich Benennung/Beschreibung von mitigierenden Maßnahmen

Die Kategorien für die Bewertung wurden bewusst einfach gehalten, um die Risikoanalyse überschaubar zu halten. Für die meisten IT-bezogenen Risiken ist eine genauere Bewertung in der Praxis ohnehin mit sehr großen Unsicherheiten verbunden. Die Bewertungsskalen sind:

| Bewertung von Eintrittswahrscheinlichkeiten | Bedeutung |
| --- | --- |
| auszuschließen/unwahrscheinlich | Ein Eintritt des Risikos ist entweder auszuschließen oder so unwahrscheinlich, dass damit im Betrieb der Anwendung nicht gerechnet werden muss. |
| nicht auszuschließen/wahrscheinlich | Mit dem Eintreten des Risikos muss realistisch gerechnet werden. |

Tabelle 16: Risikoanalyse - Bewertung von Eintrittswahrscheinlichkeiten

| Bewertung von Auswirkungen | Bedeutung |
| --- | --- |
| vernachlässigbar/gering | Aus dem Eintritt des Risikos entsteht kein Schaden, oder der resultierende Schaden ist so gering, dass er zusätzliche Aufwände für die Risikobehandlung nicht rechtfertigt. |
| erheblich | Der Eintritt des Risikos hat beträchtliche Auswirkungen. Ein Eintritt des Risikos ist durch eine geeignete Risikobehandlung zu verhindern. |

Tabelle 17: Risikoanalyse - Bewertung von Auswirkungen

| Bewertung von Risiken | Bedeutung |
| --- | --- |
| tragbar | Das Risiko liegt im Rahmen der für einen IT-Betrieb unvermeidlichen Basisrisiken. Es erfordert keine Maßnahmen zur Risikobehandlung. |
| untragbar | Das Risiko geht über die für einen IT-Betrieb unvermeidlichen Basisrisiken hinaus und erfordert eine geeignete Risikobehandlung.  Risiken werden als untragbar bewertet, wenn ihre Eintrittswahrscheinlichkeit „nicht auszuschließen/wahrscheinlich“ und ihre Auswirkungen „erheblich“ sind. |

Tabelle 18: Risikoanalyse - Bewertung von Risiken

Für die Behandlung offener Risiken wird einerseits auf die noch **offenen Grundschutzmaßnahmen** aus Abschnitt 5.2 verwiesen („**oGM S.N**“), sofern diese ausreichen, um das Risiko geeignet zu behandeln.

**ZM [Schicht].[Nr.]**

Dabei bezeichnet [Schicht] die entsprechende Themengruppe und [Nr.] eine fortlaufende Nummer pro Schicht. Die Schichten sind:

* 01 -ISMS
* 02 – ORP
* 03 – CON
* 04 – OPS
* 05 – DER
* 06 – APP
* 07 – SYS
* 08 – IND
* 09 – NET
* 10 – INF

## <Betrachtungsobjekt>

G 0.1 Feuer

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.2 Ungünstige klimatische Bedingungen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.3 Wasser

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.4 Verschmutzung, Staub, Korrosion

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.5 Naturkatastrophen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.6 Katastrophen im Umfeld

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.7 Großereignisse im Umfeld

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.8 Ausfall oder Störung der Stromversorgung

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.10 Ausfall oder Störung von Versorgungsnetzen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.11 Ausfall oder Störung von Dienstleistern

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.12 Elektromagnetische Störstrahlung

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.13 Abfangen kompromittierender Strahlung

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.14 Ausspähen von Informationen (Spionage)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.15 Abhören

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.18 Fehlplanung oder fehlende Anpassung

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.19 Offenlegung schützenswerter Informationen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.21 Manipulation von Hard- oder Software

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.22 Manipulation von Informationen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.23 Unbefugtes Eindringen in IT-Systeme

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.24 Zerstörung von Geräten oder Datenträgern

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.25 Ausfall von Geräten oder Systemen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.26 Fehlfunktion von Geräten oder Systemen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.27 Ressourcenmangel

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.28 Software-Schwachstellen oder -Fehler

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.29 Verstoß gegen Gesetze oder Regelungen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.32 Missbrauch von Berechtigungen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.33 Personalausfall

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.34 Anschlag

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.35 Nötigung, Erpressung oder Korruption

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.36 Identitätsdiebstahl

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.37 Abstreiten von Handlungen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.38 Missbrauch personenbezogener Daten

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.39 Schadprogramme

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.40 Verhinderung von Diensten (Denial of Service)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.41 Sabotage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.42 Social Engineering

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.43 Einspielen von Nachrichten

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.45 Datenverlust

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.46 Integritätsverlust schützenswerter Informationen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beschreibung | <kurze präzise Beschreibung der Gefährdung unter Berücksichtigung des Betrachtungsobjektes> | | | |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | | |
| Verbleibendes Risiko | Risikobewertung | | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | | |
| Risiko­behandlung | ZM X.X | <Titel>  <Beschreibung der Zusatzmaßnahme> | | |

## Auflistung aller Zusatzmaßnahmen zur Reduzierung des Risikos

Dieses Kapitel fasst die in der Risikoanalyse beschriebenen Zusatzmaßnahmen nach den Schichten des BSI-IT-Grundschutz Kompendiums zusammen und benennt jeweils den aktuellen Umsetzungsstatus.

|  |  |
| --- | --- |
| ■ Ja | Die Maßnahme ist gemäß Aussage der Verantwortlichen <beim Dienstleister/vom Bereich> umgesetzt. |
| ■ Nein | Die Maßnahme ist bisher nicht umgesetzt. |

### Schicht ISMS

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 1.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 19: Zusatzmaßnahmen aus der Risikoanalyse - Schicht ISMS

### Schicht ORP (Organisation und Personal)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 2.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 20: Zusatzmaßnahmen aus der Risikoanalyse - Schicht ORP

### Schicht CON (Konzepte und Vorgehensweisen)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 3.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 21: Zusatzmaßnahmen aus der Risikoanalyse - Schicht CON

### Schicht OPS (Betrieb)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 4.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 22: Zusatzmaßnahmen aus der Risikoanalyse - Schicht OPS

### Schicht DER (Detektion und Reaktion)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 5.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 23: Zusatzmaßnahmen aus der Risikoanalyse - Schicht DER

### Schicht APP (Anwendungen)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 6.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 24: Zusatzmaßnahmen aus der Risikoanalyse - Schicht APP

### Schicht SYS (IT-Systeme)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 7.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 25: Zusatzmaßnahmen aus der Risikoanalyse - Schicht SYS

### Schicht IND (Industrielle IT)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 8.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 26: Zusatzmaßnahmen aus der Risikoanalyse - Schicht IND

### Schicht NET (Netze und Kommunikation)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 9.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 27: Zusatzmaßnahmen aus der Risikoanalyse - Schicht NET

### Schicht INF (Infrastruktur)

| Nr. | Beschreibung der zusätzlichen Maßnahme | Status |
| --- | --- | --- |
| ZM 10.1 | <Titel>  <Beschreibung der Zusatzmaßnahme> | ■ Ja  ■ Nein |

Tabelle 28: Zusatzmaßnahmen aus der Risikoanalyse - Schicht INF

## Auflistung aller besonderen Restrisiken

In der Risikoanalyse wurden die folgenden verbleibenden Restrisiken (RR) identifiziert, die von der Geschäftsführung bewusst übernommen werden.

| Nr. | Beschreibung |
| --- | --- |
| RR 1 | <Titel>  <Beschreibung des Restrisiko> |

Tabelle 29: Von der geschäftsführung übernommene Restrisiken