**Basis-Absicherung**

IT-Grundschutz Profil  
für die  
Bau Cool GmbH

**Version 0.1**

**Inhaltsverzeichnis**

[**1. Formalien** 3](#_Toc47889565)

[**2. Haftungsausschluss** 3](#_Toc47889566)

[**3. Management Summary** 3](#_Toc47889567)

[**4. Festlegung des Geltungsbereichs** 4](#_Toc47889568)

[**5. Abgrenzung des Informationsverbundes** 4](#_Toc47889569)

[**6. Relevante Zielobjekte - Referenzarchitektur** 5](#_Toc47889570)

[**6. Anforderungen** 6](#_Toc47889571)

[6.1 Prozess-Bausteine 6](#_Toc47889572)

[6.2 System-Bausteine 6](#_Toc47889573)

[**7. Anwendungshinweise** 7](#_Toc47889574)

# **1. Formalien**

|  |  |
| --- | --- |
| **Titel** | IT-Grundschutz-Profil der *Bau Cool GmbH* |
| **Autor** | Peter Hämmerle und ISB |
| **Stand / Datum** |  |
| **Revisionszyklus** | Die Aktualität des Dokuments soll spätestens alle zwei Jahre überprüft werden. |

# **2. Haftungsausschluss**

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Mitwirkenden an diesem Dokument haben keinen Einfluss auf dessen weitere Nutzung durch die einzelnen Anwender und können daher naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen.

# **3. Management Summary**

Das vorliegende IT-Grundschutz-Profil dient der grundlegenden Erstabsicherung, als Einstieg in die Informationssicherheit gemäß der IT-Grundschutz-Vorgehensweise „Basis-Absicherung“. Eine Überprüfung der Maßnahmen soll alle zwei Jahre erfolgen. Falls notwendig werden dann zeitnah notwendige Anpassungen vorgenommen oder das Grundschutzniveau erhöht.

Abzusichern sind die primären Geschäftsprozesse Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung und Abrechnung.

Bei der Zusammenarbeit mit externen Dienstleistern soll das vorliegende Sicherheitskonzept als Grundlage für die Zusammenarbeit verwendet werden. Die formulierten Anforderungen werden entsprechend in Vertragsbedingungen übernommen.

# **4. Festlegung des Geltungsbereichs**

|  |  |
| --- | --- |
| **Zielgruppe** | Dieses IT-Grundschutz-Profil richtet sich an den Handwerksbetrieb Bau Cool GmbH. |
| **Schutzbedarf** | Die in diesem IT-Grundschutz-Profil verwendete Vorgehensweise der Basis-Absicherung betrachtet den Schutzbedarf nicht, da es sich um eine grundlegende Absicherung in der Breite und nicht Tiefe handelt. Erst mit der darauf aufbauenden Vorgehensweise der Standard-Absicherung findet er Berücksichtigung. |
| **IT-Grundschutz Vorgehensweise** | Die in diesem Profil aufgeführten Anforderungen sind Empfehlungen, die mindestens die Anforderungen der Basis-Absicherung des BSI-Standards 200-2 [BSI-200-2] abdecken. |
| **ISO 27001 Kompatibilität** | Mit dieser Basis-Absicherung wird ein nicht zertifizierungsfähiger Basis-Schutz gemäß ISO27001:2015 erreicht. |
| **Rahmenbedingungen** | Dieses IT-Grundschutz-Profil basiert auf dem IT-Grundschutz-Kompendium des BSI in der Edition 2018. |

# **5. Abgrenzung des Informationsverbundes**

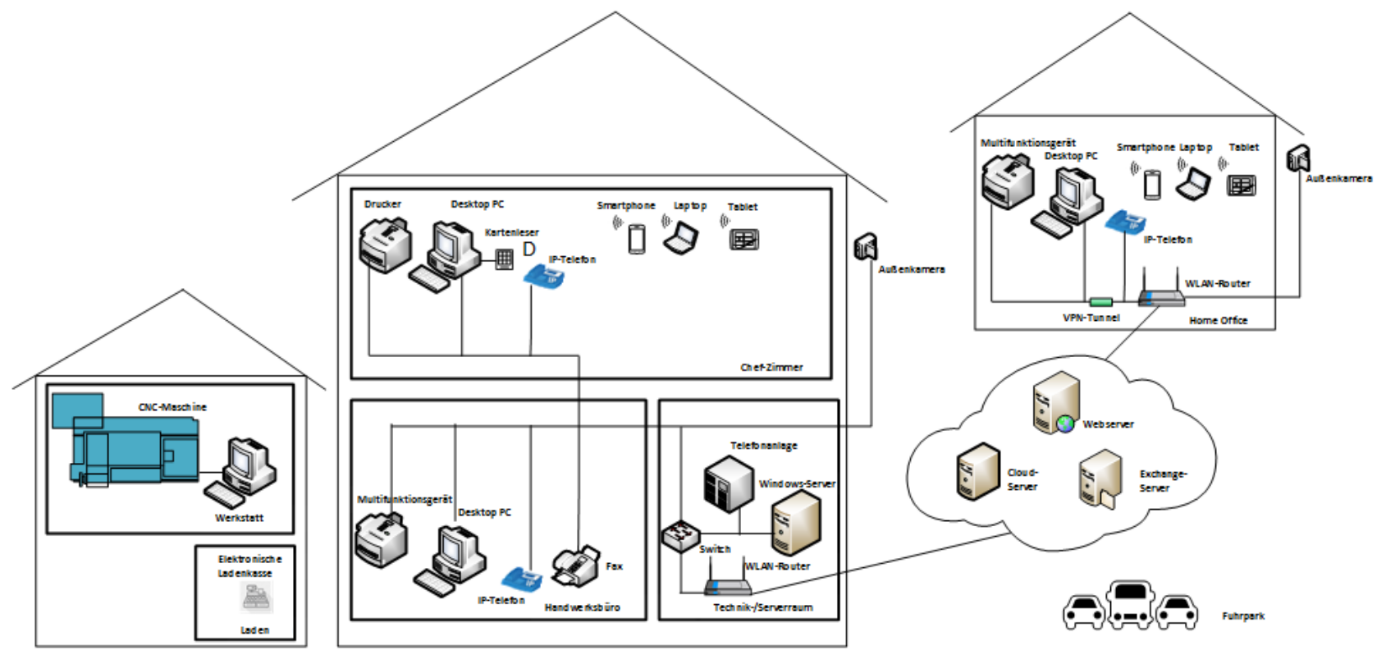
|  |  |
| --- | --- |
| **Bestandteile** | Zum Informationsverbund gehören alle Prozesse und Verfahren der *Bau Cool GmbH*, die zur Absicherung des Kerngeschäfts notwendig sind. Gegenstand für das vorliegenden IT-Grundschutz-Profil sind die Anwendungsgebiete:   * Auftragsgewinnung * Angebotserstellung * Auftragsdurchführung * Abrechnung |
| **Nicht berücksichtigte Objekte** | Dieses Dokument betrachtet ausschließlich wertschöpfende Kernprozesse der *Bau Cool GmbH*. Andere relevante Prozesse bleiben unberücksichtigt. |

# **6. Relevante Zielobjekte - Referenzarchitektur**

Das IT-Grundschutz-Profil soll möglichst alle relevanten Zielobjekte wie zum Beispiel PCs, Netzwerkkomponenten, Software-Programme beinhalten, auf die sich geeignete Schutzmaßnahmen zur Erhöhung der Informationssicherheit in einem Handwerksbetrieb beziehen.

|  |  |
| --- | --- |
| **Referenzarchitektur** | Im Rahmen der zur Identifizierung der Zielobjekte notwendigen Strukturanalyse wurden ausgehend von den vier Geschäftsprozessen Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung und Abrechnung der sogenannte Untersuchungsgegenstand (Referenzarchitektur) entwickelt. Dieser legt fest, auf welche konkreten Zielobjekte die Anforderungen des IT-Grundschutzes angewendet werden müssen. Hierzu zählen im Einzelnen:   * Anwendungen * IT-Systeme (Server, Desktop-Systeme, Mobile Devices etc.) sowie Netze, Netzkomponenten und Kommunikationsverbindungen * Infrastruktur (z. B. Gebäude und Räume) |

**Netzplan der Bau Cool GmbH**



|  |  |
| --- | --- |
| **IT-Systeme** | * Windows Server * Desktop-Server * Laptop * Smartphone & Tablet * Drucker & Multifunktionsgerät |
| **Netze und Kommunikation** | * Router & Switch * Telefonanlage * IP-Telefon * Fax |
| **Anwendungen** | * Office-Produkte * Web-Browser * Mobile-Anwendungen * E-Mail- und Termin-Programme * Branchensoftware * Warenwirtschaft * Produktionssoftware * Webserver * Cloud Server * Exchange Server |
| **Infrastruktur** | * Gebäude * Fuhrpark * Home-Office * Mobiles Arbeiten * CNC Maschiene |

# **6. Anforderungen**

## 6.1 Prozess-Bausteine

|  |  |
| --- | --- |
| **Anforderungen**  **Router & Switch**  **NET. 3.1** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen für den Baustein NET.3.1 Router und Switches aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauf- tragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Informationssicherheitsbeauftragter (ISB)  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein NET.3.1 Router und Switches vorrangig erfüllt werden: NET.3.1.A1 Sichere Grundkonfiguration eines Routers oder Switches (B)  Bevor ein Router oder Switch eingesetzt wird, MUSS er sicher konfiguriert werden. Die Geräte DÜRFEN NUR von dafür autorisierten Personen installiert und konfiguriert werden. Alle Konfigurationsänderungen SOLLTEN nachvoll- ziehbar dokumentiert sein (siehe NET.3.1.A9 Betriebsdokumentationen). Die Integrität der Konfigurationsdateien MUSS in geeigneter Weise geschützt werden. Zugangspasswörter MÜSSEN verschlüsselt gespeichert werden.  Router und Switches MÜSSEN so konfiguriert sein, dass nur zwingend erforderliche Dienste, Protokolle und funkti- onale Erweiterungen genutzt werden. Nicht benötigte Dienste, Protokolle und funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden. Ebenfalls MÜSSEN nicht benutzte Schnittstellen auf Routern und Swit- ches deaktiviert werden. Unbenutzte Netzports MÜSSEN nach Möglichkeit deaktiviert oder zumindest einem dafür eingerichteten Unassigned-VLAN zugeordnet werden.  Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin er- füllt sein. Auch SOLLTE begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden.  Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen verborgen werden. Unnötige Auskunftsdienste MÜSSEN deaktiviert werden.  Bevor Router und Switches in Betrieb genommen werden, MÜSSEN die Standard-Benutzerkonten geändert wer- den. Passwörter dieser Konten MÜSSEN geändert werden. Nicht benutzte Benutzerkonten MÜSSEN deaktiviert werden. Entsprechend dem Rechte- und Rollenkonzept MÜSSEN anschließend die vorgesehenen Benutzerkonten und -rollen eingerichtet werden.  N ET.3.1.A2 Einspielen von Updates und Patches (B)  Die Verantwortlichen MÜSSEN sich regelmäßig über bekannt gewordene Schwachstellen informieren. Updates und Patches MÜSSEN so schnell wie möglich eingespielt werden. Vorab SOLLTE auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Solange keine Patches für be- kannte Schwachstellen verfügbar sind, MÜSSEN andere geeignete Maßnahmen getroffen werden, um Router und Switches zu schützen.  IT-Grundschutz-Kompendium: Stand Februar 2020 3  NET.3: Netzkomponenten NET.3.1  Es MUSS darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen wer- den. Sofern vom Hersteller angeboten, SOLLTEN die Update-Prüfsummen verglichen bzw. die digitalen Signaturen überprüft werden.  NET.3.1.A3 Restriktive Rechtevergabe (B)  Es MUSS geregelt werden, wer auf einen Router oder Switch zugreifen darf. Dabei DÜRFEN immer NUR so viele Zugriffsrechte vergeben werden, wie für die jeweiligen Aufgaben erforderlich sind (Prinzip der geringsten Berechti- gungen, engl. Least Privileges). Nicht mehr benötigte Benutzerkonten MÜSSEN entfernt werden. Es MUSS sicher- gestellt werden, dass nur mit Administrator-Rechten gearbeitet wird, wenn es notwendig ist.  NET.3.1.A4 Schutz der Administrationsschnittstellen (B)  Alle Administrations- und Managementzugänge der Router und Switches MÜSSEN auf einzelne Quell-IP-Adressen bzw. -Adressbereiche eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht vertrauenswürdigen Net- zen heraus nicht direkt auf die Administrationsschnittstellen zugegriffen werden kann.  Um Router und Switches zu administrieren bzw. zu überwachen, SOLLTEN ausreichend verschlüsselte Protokolle eingesetzt werden. Sollte dennoch auf unverschlüsselte und damit unsichere Protokolle zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz (Out-of-Band-Management) genutzt werden. Die Managementschnittstellen und die Administrationsverbindungen MÜSSEN durch eine separate Firewall geschützt werden. Für die Schnittstellen MÜSSEN geeignete Zeitbeschränkungen vorgegeben werden.  Alle für das Management-Interface nicht benötigten Dienste MÜSSEN deaktiviert werden. Verfügt eine Netzkom- ponente über eine dedizierte Hardwareschnittstelle, MUSS der unberechtigte Zugriff darauf in geeigneter Weise unterbunden werden.  NET.3.1.A5 Schutz vor Fragmentierungsangriffen (B)  Am Router und Layer-3-Switch MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6-Fragmentierungs- angriffe abzuwehren.  NET.3.1.A6 Notfallzugriff auf Router und Switches (B)  Es MUSS für die Administratoren immer möglich sein, direkt auf Router und Switches zuzugreifen, sodass diese weiterhin lokal administriert werden können, auch wenn das gesamte Netz ausfällt.  NET.3.1.A7 Protokollierung bei Routern und Switches (B)  Ein Router oder Switch MUSS so konfiguriert werden, dass er unter anderem folgende Ereignisse protokolliert:  • Konfigurationsänderungen (möglichst automatisch),  • Reboot,  • Systemfehler,  • Statusänderungen pro Interface, System und Netzsegment sowie  • Login-Fehler (zumindest dann, wenn sie wiederholt auftreten).  Die Verantwortlichen MÜSSEN darauf achten, dass bei der Protokollierung alle rechtlichen Rahmenbedingungen eingehalten werden. Änderungen an der Konfiguration SOLLTEN zudem automatisch protokolliert werden.  NET.3.1.A8 Regelmäßige Datensicherung (B)  Die Konfigurationsdateien von Routern und Switches MÜSSEN regelmäßig gesichert werden. Die Sicherungsko- pien MÜSSEN so abgelegt werden, dass im Notfall darauf zugegriffen werden kann.  NET.3.1.A9 Betriebsdokumentationen (B)  Die wichtigsten betrieblichen Aufgaben eines Routers oder Switches MÜSSEN geeignet dokumentiert werden. Es SOLLTEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden. Die Doku- mentation SOLLTEN vor unbefugten Zugriffen geschützt werden. |
| **Anforderungen**  **Telefonanlage**  **NET. 4.1** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.4.1 TK-Anlagen aufgeführt. Grundsätzlich ist der TK-Anlagen-Verantwortliche für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbe- auftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und regelmäßig überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen auf- geführt.  Grundsätzlich zuständig Weitere Zuständigkeiten  TK-Anlagen-Verantwortlicher IT-Betrieb, Leiter IT  NET.4.1 NET.4: Telekommunikation 3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein NET.4.1 TK-Anlagen vorrangig erfüllt werden: NET.4.1.A1 Anforderungsanalyse und Planung für TK-Anlagen [Leiter IT, IT-Betrieb] (B)  Vor der Beschaffung oder Erweiterung einer TK-Anlage MUSS eine Anforderungsanalyse durchgeführt werden. Im Rahmen dieser Analyse MUSS festgelegt werden, welche Funktionen die TK-Anlage bieten soll. Hierbei MÜSSEN neben der Ausprägung der TK-Anlage auch die Anzahl der Verbindungen und Anschlüsse, eine mögliche Erweiter- barkeit, die grundlegenden Sicherheitsfunktionen und die Anforderungen an die Grundwerte der Informationssi- cherheit berücksichtigt werden. Darüber hinaus MÜSSEN je nach Bedarf Support- und Wartungsverträge für die TK-Anlage berücksichtigt werden. Basierend auf den ermittelten Anforderungen MUSS anschließend der Einsatz der TK-Anlage geplant und dokumentiert werden. Die Anforderungen und die Planung MÜSSEN mit den entspre- chenden IT-Verantwortlichen abgestimmt werden.  NET.4.1.A2 Auswahl von TK-Diensteanbietern [Leiter IT] (B)  Um mit Personen telefonieren zu können, deren Telefone nicht an die institutionseigene TK-Anlage angeschlossen sind, MUSS ein TK-Diensteanbieter beauftragt werden. Dabei MÜSSEN die Anforderungen an die TK-Anlage, die Sicherheitsrichtlinie sowie vertragliche und finanzielle Aspekte berücksichtigt werden. Alle vereinbarten Leistungen MÜSSEN eindeutig schriftlich festgehalten werden.  NET.4.1.A3 Änderung voreingestellter Passwörter (B)  Standardpasswörter MÜSSEN durch ausreichend starke Passwörter ersetzt werden. Vordefinierte Logins MÜSSEN geändert werden. Die Änderungen MÜSSEN durchgeführt werden, bevor die TK-Anlage in Betrieb genommen wird.  NET.4.1.A4 Absicherung von Remote-Zugängen (B)  ES MUSS geprüft werden, ob interne oder externe Remote-Zugänge zur TK-Anlage benötigt werden. Die externe Fernwartung SOLLTE dabei nach Möglichkeit unterbunden werden. Alle nicht benötigten Remote-Zugänge MÜS- SEN deaktiviert werden. Alle anderen Remote-Zugänge MÜSSEN vor unberechtigtem Zugriff geschützt und auf die notwendigen Personen beschränkt werden.  NET.4.1.A5 Protokollierung bei TK-Anlagen (B)  Bei TK-Anlagen MÜSSEN geeignete Daten erfasst und bei Bedarf intern ausgewertet werden. Protokolliert werden MÜSSEN zusätzlich alle systemtechnischen Eingriffe, die Programmveränderungen beinhalten, sowie Auswer- tungsläufe, Datenübermittlungen und Datenzugriffe. Alle Administrationsarbeiten an der TK-Anlage MÜSSEN ebenfalls protokolliert werden. Die protokollierten Informationen SOLLTEN regelmäßig kontrolliert werden. |

|  |  |
| --- | --- |
| **Anforderungen**  **IP-Telefon**  **NET. 4.2** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.4.2 VoIP aufgeführt. Grundsätzlich ist der IT- Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategi- schen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und regelmäßig überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig Weitere Zuständigkeiten  IT-Betrieb Benutzer, Leiter IT  2  IT-Grundschutz-Kompendium: Stand Februar 2020  NET.4.2 NET.4: Telekommunikation 3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein NET.4.2 VoIP vorrangig erfüllt werden: NET.4.2.A1 Planung des VoIP-Einsatzes [Leiter IT] (B)  Die Bedingungen, unter denen VoIP eingesetzt werden soll, MÜSSEN festgelegt werden. Es MUSS unter anderem entschieden werden, ob vollständig oder partiell auf VoIP umgestiegen werden soll. Besondere Anforderungen an die Verfügbarkeit von VoIP oder an die Vertraulichkeit und Integrität der Telefonate bzw. der Signalisierungsinfor- mationen SOLLTEN vorab ermittelt werden. Geeignete Signalisierungs- und Medientransportprotokolle MÜSSEN vor dem Einsatz ausgewählt werden.  Es SOLLTE entschieden werden, ob und wie die VoIP-Infrastruktur an öffentliche (Daten-)Netze angebunden wer- den soll. Die Kapazitäten und das Design von vorhandenen Datennetzen SOLLTEN bei der Planung berücksichtigt werden.  NET.4.2.A2 Sichere Administration der VoIP-Middleware [Leiter IT] (B)  Es MUSS ein Administrationskonzept erstellt werden, das ein Rollenkonzept mit verschiedenen Berechtigungsstu- fen beinhaltet. Die eingesetzten Software-Komponenten MÜSSEN regelmäßig mit Updates aus vertrauenswürdi- gen Quellen aktualisiert werden.  NET.4.2.A3 Sichere Administration und Konfiguration von VoIP-Endgeräten (B)  Nicht benötigte Funktionen der Endgeräte MÜSSEN deaktiviert werden. Die Konfigurationseinstellungen DÜRFEN NICHT unberechtigt geändert werden. Alle Sicherheitsfunktionen der Endgeräte SOLLTEN vor dem produktiven Ein- satz getestet werden. Die eingesetzten Software-Komponenten MÜSSEN regelmäßig mit Updates aus vertrauens- würdigen Quellen aktualisiert werden. Die eingesetzten Sicherheitsmechanismen und die verwendeten Parameter SOLLTEN dokumentiert werden.  NET.4.2.A4 Einschränkung der Erreichbarkeit über VoIP [Leiter IT] (B)  Es MUSS entschieden werden, wie externe Gesprächspartner auf die VoIP-Architektur zugreifen können. Es MUSS verhindert werden, dass IT-Systeme aus unsicheren Netzen direkte Datenverbindungen auf die VoIP-Komponenten der Institution aufbauen können. Wenn alle ein- und ausgehenden Verbindungen über ein zentrales IT-System ab- gewickelt werden sollen, SOLLTE sichergestellt werden, dass alle Signalisierungs- und Sprachinformationen zwi- schen dem öffentlichen und dem privaten Datennetz nur über dieses autorisierte System ausgetauscht werden.  NET.4.2.A5 Sichere Konfiguration der VoIP-Middleware (B)  Die VoIP-Komponenten MÜSSEN so konfiguriert sein, dass sie den Schutzbedarf angemessen erfüllen. Die Default- Konfigurationen der VoIP-Middleware MÜSSEN vor der produktiven Inbetriebnahme angepasst werden. Alle Instal- lations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass die Installation und Konfiguration durch einen sachkundigen Dritten anhand der Dokumentation nachvollzogen und wiederholt werden können. Es SOLLTE eine Regelung zur restriktiven Anmeldung von Geräten und Benutzern erstellt werden. Alle nicht benötig- ten Dienste der VoIP-Middleware MÜSSEN deaktiviert werden.  NET.4.2.A6 Protokollierung bei VoIP (B)  Es MUSS entschieden werden, welche Informationen protokolliert werden sollen, wie lange die Protokolldaten auf- bewahrt werden und wer unter welchen Voraussetzungen die Protokolldaten einsehen darf. Datenschutzrelevante Vorgaben MÜSSEN bei der Protokollierung berücksichtigt werden. Alle Protokolldaten MÜSSEN vor unbefugtem Zugriff geschützt werden.  Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden. Die Protokolldaten SOLLTEN zeitnah ausgewertet werden. |
| Anforderungen  Fax  NET.4.3 | Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.4.3 Faxgeräte und Faxserver aufgeführt.  Grundsätzlich ist der Fax-Verantwortliche für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und regelmäßig überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen  Anforderungen aufgeführt.  Grundsätzlich zuständig Fax-Verantwortlicher  Weitere Zuständigkeiten Benutzer, Beschaffungsstelle, Haustechnik, IT-Betrieb, Informationssicherheitsbeauftragter (ISB) |

## 6.2 System-Bausteine

|  |  |
| --- | --- |
| **Anforderungen**  **Desktop-System**  **SYS.2** | Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.1 Allgemeiner Client aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte  (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch  andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann  jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Benutzer, Haustechnik  IT-Grundschutz-Kompendium: Stand Februar 2020 3  SYS.2: Desktop-Systeme SYS.2.1  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein SYS.2.1 Allgemeiner Client vorrangig erfüllt werden:  SYS.2.1.A1 Sichere Benutzerauthentisierung (B)  Um den Client zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Sollen die Benutzer  hierfür Passwörter verwenden, MÜSSEN sichere Passwörter gewählt werden. Die Passwörter MÜSSEN der Passwort-Richtlinie der Institution entsprechen (siehe ORP.4 Identitäts- und Berechtigungsmanagement).  SYS.2.1.A2 Rollentrennung (B)  Der Client MUSS so eingerichtet werden, dass normale Tätigkeiten nicht mit Administratorrechten ausgeübt werden. NUR Administratoren DÜRFEN Administratorrechte erhalten. Es DÜRFEN NUR Administratoren die Systemkonfiguration ändern, Anwendungen installieren bzw. entfernen oder Systemdateien modifizieren bzw. löschen können. Benutzer DÜRFEN NUR ausschließlich lesenden Zugriff auf Systemdateien haben.  Ablauf, Rahmenbedingungen und Anforderungen an administrative Aufgaben sowie die Aufgabentrennungen  zwischen den verschiedenen Rollen der Benutzer des IT-Systems SOLLTEN in einem Benutzer- und Administrationskonzept festgeschrieben werden.  SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen (B)  Automatische Update-Mechanismen (Autoupdate) MÜSSEN aktiviert werden, sofern nicht andere Mechanismen  wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden.  Wenn für Autoupdate-Mechanismen ein Zeitintervall vorgegeben werden kann, SOLLTE mindestens täglich automatisch nach Updates gesucht und diese installiert werden.  SYS.2.1.A4 Regelmäßige Datensicherung (B)  Clients MÜSSEN in das Datensicherungskonzept der Institution einbezogen werden. Es MÜSSEN Regelungen getroffen werden, welche lokal abgespeicherten Daten wie, von wem, wann und wie regelmäßig gesichert werden.  Es MÜSSEN mindestens diejenigen Daten regelmäßig gesichert werden, die nicht aus anderen Informationen abgeleitet werden können. Bei vertraulichen und ausgelagerten Backups SOLLTEN die gesicherten Daten verschlüsselt  gespeichert werden. Für eingesetzte Software SOLLTE separat entschieden werden, ob sie von der regelmäßigen  Datensicherung erfasst werden muss. Die Benutzer SOLLTEN über die Regelungen zur Datensicherung informiert  werden. Es MUSS regelmäßig getestet werden, ob die Datensicherung wie gewünscht funktioniert, vor allem, ob  gesicherte Daten problemlos zurückgespielt werden können.  SYS.2.1.A5 Verwendung einer Bildschirmsperre [Benutzer] (B)  Damit Unbefugte nicht auf aktive Clients zugreifen können, MUSS eine Bildschirmsperre verwendet werden. Sie  SOLLTE sich sowohl manuell vom Benutzer aktivieren lassen als auch nach einer vorgegebenen Zeit der Inaktivität  automatisch gestartet werden. Es MUSS sichergestellt sein, dass die Bildschirmsperre erst nach einer erfolgreichen  Benutzerauthentisierung deaktiviert werden kann.  SYS.2.1.A6 Einsatz von Viren-Schutzprogrammen (B)  Abhängig vom installierten Betriebssystem und von anderen vorhandenen Schutzmechanismen des Clients MUSS  geprüft werden, ob Viren-Schutzprogramme eingesetzt werden sollen. Soweit vorhanden, MÜSSEN konkrete Aussagen, ob ein Virenschutz notwendig ist, aus den Betriebssystem-Bausteinen des IT-Grundschutz-Kompendiums  berücksichtigt werden. Die entsprechenden Signaturen eines Viren-Schutzprogrammes MÜSSEN regelmäßig aktualisiert werden. Neben Echtzeit- und On-Demand-Scans MUSS eine eingesetzte Lösung ermöglichen, auch komprimierte Daten nach Schadprogrammen zu durchsuchen.  Viren-Schutzprogramme auf den Clients MÜSSEN so konfiguriert sein, dass die Benutzer weder sicherheitsrelevante Änderungen an den Einstellungen vornehmen können noch die Viren-Schutzprogramme deaktivieren können.  4 IT-Grundschutz-Kompendium: Stand Februar 2020  SYS.2.1 SYS.2: Desktop-Systeme  SYS.2.1.A7 Protokollierung auf Clients (B)  Es MUSS entschieden werden, welche Informationen auf Clients mindestens protokolliert werden sollen, wie lange  die Protokolldaten aufbewahrt werden und wer unter welchen Voraussetzungen die Protokolldaten einsehen darf.  Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden. Es SOLLTE geprüft werden, ob  die Speicherung der Protokolldaten auf den jeweiligen Clients selbst ausreichend ist oder ob eine zentrale Speicherung erfolgen soll.  SYS.2.1.A8 Absicherung des Bootvorgangs (B)  Der Startvorgang des IT-Systems („Booten“) MUSS gegen Manipulation abgesichert werden. Es MUSS festgelegt  werden, von welchen Medien gebootet werden darf. Es SOLLTE entschieden werden, ob und wie der Bootvorgang  kryptografisch geschützt werden soll. Es MUSS sichergestellt werden, dass nur Administratoren die Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können. NUR Administratoren DÜRFEN von eingebauten optischen oder externen Speichermedien booten können. Die Konfigurationseinstellungen des Bootvorgangs DÜRFEN NUR durch Administratoren verändert werden können. Alle nicht benötigten  Funktionen in der Firmware MÜSSEN deaktiviert werden |
| **Anforderungen**  **Laptop**  **SYS.3.1** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.1 Laptops aufgeführt. Grundsätzlich ist der  IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen  geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit  in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  2 IT-Grundschutz-Kompendium: Stand Februar 2020  SYS.3.1 SYS.3: Mobile Devices  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Benutzer, Beschaffungsstelle  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein SYS.3.1 Laptops vorrangig erfüllt werden:  SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops (B)  Es MUSS klar geregelt werden, was Mitarbeiter bei der mobilen Nutzung von Laptops berücksichtigen müssen. Es  MUSS insbesondere festgelegt werden, welche Laptops mobil genutzt werden dürfen, wer sie mitnehmen darf und  welche grundlegenden Sicherheitsmaßnahmen dabei zu beachten sind. Die Benutzer MÜSSEN auf die Regelungen  hingewiesen werden.  SYS.3.1.A2 Zugriffsschutz am Laptop [Benutzer] (B)  Auf allen Laptops MUSS ein angemessener Zugriffsschutz vorhanden sein, der verhindert, dass das Gerät unberechtigt benutzt werden kann. Es MUSS geprüft werden, ob sich alle Benutzer an die Regeln für den korrekten Umgang  mit dem eingerichteten Zugriffsschutz halten.  SYS.3.1.A3 Einsatz von Personal Firewalls (B)  Auf Laptops MUSS eine Personal Firewall aktiv sein. Die Filterregeln der Firewall MÜSSEN so restriktiv wie möglich  sein. Sie MÜSSEN regelmäßig getestet werden. Die Personal Firewall MUSS so konfiguriert werden, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können.  SYS.3.1.A4 Einsatz von Antivirenprogrammen [Benutzer] (B)  Abhängig vom installierten Betriebssystem und anderen vorhandenen Schutzmechanismen MUSS auf allen Laptops der Institution ein Antivirenprogramm installiert und aktiviert sein. Es MUSS sichergestellt werden, dass sowohl  das Scan-Programm als auch die Signaturen stets auf dem aktuellen Stand sind. Die Benutzer MÜSSEN mit der Antivirensoftware vertraut gemacht werden, besonders auch mit On-Demand-Scans.  Der gesamte Datenbestand der Laptops MUSS regelmäßig auf Schadprogramme geprüft werden. Wenn der Laptop infiziert ist, MUSS im Offlinebetrieb untersucht werden, ob das gefundene Schadprogramm bereits vertrauliche  Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.  Das Antivirenprogramm MUSS zudem nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen  werden. Auch MÜSSEN alle auf dem Laptop benutzten Internet-Dienste (HTTP, FTP) sowie verschlüsselte Daten ausreichend vor Schadprogrammen geschützt werden.  Außerdem MUSS sichergestellt werden, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme vornehmen können.  SYS.3.1.A5 Datensicherung [Benutzer] (B)  Alle Daten, die auf Laptops nur lokal gespeichert werden, MÜSSEN regelmäßig gesichert werden. Hierfür MÜSSEN  abhängig vom Volumen des Datenbestands geeignete Verfahren zur Datensicherung ausgewählt werden. Die Datensicherung MUSS weitgehend automatisiert werden, sodass die Benutzer möglichst wenig Aktionen selbst  durchführen müssen |

|  |  |
| --- | --- |
| **Anforderungen**  **Smartphone & Tablet**  **SYS.3.2** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.1 Allgemeine Smartphones und Tablets aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicher- heitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zustän- dig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Benutzer, Fachverantwortliche  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein SYS.3.2.1 Allgemeine Smartphones und Tablets vorrangig erfüllt werden:  SYS.3.2.1.A1 Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets (B)  Bevor eine Institution Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, MUSS eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden. Hierbei MUSS unter anderem festgelegt werden, wer auf welche Informationen der Institution zugreifen darf.  SYS.3.2.1.A2 Festlegung einer Strategie für die Cloud-Nutzung (B)  Die Institution MUSS im Zusammenhang mit Smartphones und Tablets eine generelle Strategie für die damit ver- bundene Cloud-Nutzung sowie für den Schutz und die Kontrolle der Informationen festlegen. Die erlaubte Nut- zung von Cloud-Diensten für Informationen der Institution MUSS geklärt und festgelegt werden. Die Benutzer MÜSSEN regelmäßig bezüglich der Nutzung solcher Cloud-Dienste geschult werden.  SYS.3.2.1.A3 Sichere Grundkonfiguration für mobile Geräte (B)  Alle mobilen Endgeräte MÜSSEN so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen. Dafür MUSS eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammenge-  IT-Grundschutz-Kompendium: Stand Februar 2020 3  SYS.3.2: Tablet und Smartphone SYS.3.2.1  stellt und dokumentiert werden. Nicht benötigte Funktionen SOLLTEN deaktiviert werden. Die Freischaltung von Kommunikationsschnittstellen MUSS geregelt und auf das dienstlich notwendige Maß reduziert werden. Nicht be- nutzte Schnittstellen SOLLTEN deaktiviert werden. Wenn eine Institution ein MDM einsetzt, MUSS bei der Übergabe des mobilen Endgerätes bereits der MDM-Client installiert sein.  SYS.3.2.1.A4 Verwendung eines Zugriffschutzes [Benutzer] (B)  Smartphones und Tablets MÜSSEN mit einem angemessen komplexen Gerätesperrcode geschützt werden. Die Nutzung der Bildschirmsperre MUSS vorgeschrieben werden. Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm MUSS deaktiviert sein. Alle mobilen Geräte MÜSSEN nach einer angemessen kurzen Zeit- spanne selbsttätig die Bildschirmsperre aktivieren. Diese Zeitspanne MUSS in Abhängigkeit zum angestrebten Schutzniveau stehen.  Nach mehreren fehlgeschlagenen Versuchen, den Bildschirm zu entsperren, SOLLTE sich das mobile Gerät in den Werkszustand zurücksetzen. Es SOLLTEN dabei die Daten oder die Verschlüsselungsschlüssel sicher vernichtet wer- den. Es SOLLTE vermieden werden, dass die Benutzer bei einem Passwortwechsel Kennworte nutzen, die erst vor Kurzem verwendet wurden. Die Anzahl der Kennworte, nach der sich ein Passwort wiederholen darf, SOLLTE fest- gelegt werden.  SYS.3.2.1.A5 Updates von Betriebssystem und Apps (B)  Es MUSS ein Prozess für Updates des Betriebssystems und der eingesetzten Apps etabliert werden. Die Aktualisie- rungen MÜSSEN getestet werden. Dabei SOLLTEN insbesondere bisher benötigte Funktionen, Sicherheitsmechanis- men und die Durchsetzung von Compliance-Anforderungen geprüft werden. Nach der Freigabe MÜSSEN die Aktu- alisierungen zeitnah ausgerollt werden. Bereits bei der Auswahl von zu beschaffenden mobilen Geräten MUSS die Institution darauf achten, dass der Hersteller über den geplanten Nutzungszeitraum Sicherheitsaktualisierungen für die Geräte bereitstellt. Ältere Geräte, für die keine Aktualisierungen mehr bereitgestellt werden, MÜSSEN aus- gesondert und durch vom Hersteller unterstützte Geräte ersetzt werden. Apps SOLLTEN unter Berücksichtigung von Sicherheitsaspekten ebenfalls NICHT mehr eingesetzt werden, wenn sie nicht mehr durch den Hersteller unter- stützt werden.  SYS.3.2.1.A6 Datenschutzeinstellungen (B)  Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen MUSS angemessen eingeschränkt werden. Die Datenschutzeinstellungen MÜSSEN so restriktiv wie möglich konfiguriert werden. Insbesondere der Zugriff auf Kamera, Mikrofon sowie Ortungs- und Gesundheits- bzw. Fitnessdaten MUSS auf Konformität mit den organisati- onsinternen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. deaktiviert werden.  SYS.3.2.1.A7 Verhaltensregeln bei Sicherheitsvorfällen [Fachverantwortliche, Benutzer] (B)  Generell MÜSSEN alle Sicherheitsvorfälle gemeldet und behandelt werden. Gehen Geräte verloren oder werden unberechtigte Änderungen an Gerät und Software festgestellt, MÜSSEN die Verantwortlichen sofort geeignete Ge- genmaßnahmen einleiten.  Die möglichen Konsequenzen sicherheitskritischer Ereignisse MÜSSEN untersucht werden. Letztlich MÜSSEN alle erforderlichen Maßnahmen ergriffen werden, um auszuschließen, dass auf vertrauliche und geschäftskritische In- formationen der Institution zugegriffen werden kann.  SYS.3.2.1.A8 Keine Installation von Apps aus unsicheren Quellen (B)  Es MUSS unterbunden werden, dass sich Apps aus alternativen Märkten oder aus dem Dateisystem installieren las- sen. |
| **Anforderungen**  **Drucker&Multifunktionsgerät**  **SYS.4.1** | 3 Anforderungen  Im Folgenden sind spezifische Anforderungen des Bausteins SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) und der Datenschutzbeauftragte sind bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen auf- geführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Informationssicherheitsbeauftragter (ISB)  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte vor- rangig erfüllt werden:  SYS.4.1.A1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (B)  Die Institution MUSS den sicheren Einsatz von Druckern, Kopierern und Multifunktionsgeräten planen. Es MUSS geplant werden, wo die Geräte aufgestellt werden dürfen. Außerdem MUSS festgelegt sein, wer auf die Drucker, Kopierer und Multifunktionsgeräte zugreifen darf. Die Ergebnisse SOLLTEN in einem Basiskonzept dokumentiert werden.  SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte (B)  Der IT-Betrieb MUSS Drucker, Kopierer und Multifunktionsgeräte so aufstellen und absichern, dass nur befugte Be- nutzer die Geräte verwenden und auf verarbeitete Informationen zugreifen können. Außerdem MUSS sicherge- stellt sein, dass nur berechtigte Personen die Geräte administrieren, warten und reparieren können. Mit Dienstleis- tern (z. B. für die Wartung) MÜSSEN schriftliche Vertraulichkeitsvereinbarungen getroffen werden.  Drucker, Kopierer und Multifunktionsgeräte MÜSSEN mit Gerätepassworten versehen sein, um so den Zugriff per Webserver und Bedienfeld zu sperren. Diese MÜSSEN die Vorgaben des Identitäts- und Berechtigungsmanagement der Institution erfüllen. Das Passwort DARF NUR berechtigten Benutzern bekannt sein.  SYS.4.1.A3 ENTFALLEN (B)  Diese Anforderung ist entfallen.  SYS.4.1.A12 Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln (B)  Bevor die Institution Altgeräte entsorgt oder zurückgibt, MÜSSEN alle vertraulichen Daten auf den Geräten sicher gelöscht werden. Ist das nicht möglich, MÜSSEN die Massenspeicher ausgebaut und durch geeignete Prozesse ver- nichtet werden. Mit der Entsorgung beauftragte Dienstleister MÜSSEN verpflichtet werden, die erforderlichen Si- cherheitsmaßnahmen einzuhalten.  SYS.4.1.A13 ENTFALLEN (B)  Diese Anforderung ist entfallen.  SYS.4.1.A22 Ordnungsgemäße Entsorgung ausgedruckter Dokumente (B)  Nicht benötigte, aber ausgedruckte Dokumente mit institutionskritischen Informationen MÜSSEN in geeigneter Weise vernichtet werden, z. B. in geeigneten Papiercontainern. Sind Heimarbeitsplätze mit Druckern, Kopierern oder Multifunktionsgeräten ausgestattet, SOLLTE gewährleistet werden, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können. |

## 6.3 Anwendungs-Bausteine

|  |  |
| --- | --- |
| **Anforderungen**  **Office-Produkt**  **APP.1.1** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.1 Office-Produkte aufgeführt. Grundsätz- lich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforde- rungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb Weitere Zuständigkeiten Benutzer  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein APP.1.1 Office-Produkte vorrangig erfüllt werden: APP.1.1.A1 Sicherstellen der Integrität von Office-Produkten (B)  Bei der Installation von Office-Produkten MUSS sichergestellt werden, dass ausschließlich unveränderte Kopien der freigegebenen Originalsoftware verwendet werden. Updates MÜSSEN ausschließlich aus sicheren Quellen bezogen werden. Falls zu einem Office-Produkt Prüfsummen angeboten werden, SOLLTEN diese vor der Installation über- prüft werden. Falls zu einem Office-Produkt digitale Signaturen verfügbar sind, SOLLTEN diese vor der Installation des Pakets überprüft werden. Die Administratoren SOLLTEN über die Bedeutung und Aussagekraft von Prüfsum- men und digitalen Signaturen informiert werden. Ebenso wie bei einer Neuinstallation MUSS bei der Installation von Updates sichergestellt werden, dass die Update-Pakete unverändert sind.  IT-Grundschutz-Kompendium: Stand Februar 2020 3  APP.1: Client-Anwendungen APP.1.1 APP.1.1.A2 Einschränken von Aktiven Inhalten (B)  Das automatische Ausführen von eingebetteten Aktiven Inhalten, wie beispielsweise Makros oder ActiveX-Elemen- ten, MUSS in den Einstellungen aller verwendeten Office-Produkte deaktiviert werden. Ist die Ausführung Aktiver Inhalte für einen Geschäftsprozess notwendig, MUSS darauf geachtet werden, dass Aktive Inhalte nur von vertrau- enswürdigen Quellen ausgeführt werden. Alle Benutzer MÜSSEN in Schulungen bezüglich der Gefährdungen durch Aktive Inhalte sensibilisiert werden. Sie MÜSSEN hinsichtlich der Funktionen, die Aktive Inhalte einschränken, eingewiesen werden.  APP.1.1.A3 Sicheres Öffnen von Dokumenten aus externen Quellen [Benutzer] (B)  Alle aus externen Quellen bezogenen Dokumente MÜSSEN vor dem Öffnen auf Schadsoftware überprüft werden. Alle als problematisch eingestuften und alle innerhalb der Institution nicht benötigten Dateiformate MÜSSEN ver- boten werden. Die Benutzer MÜSSEN zum Umgang mit Dokumenten aus externen Quellen geschult und sensibili- siert werden. Die Prüfung von Dokumenten aus externen Quellen SOLLTE durch technische Maßnahmen erzwun- gen werden.  APP.1.1.A4 Absichern des laufenden Betriebs von Office-Produkten (B)  Der IT-Betrieb und die Informationssicherheitsbeauftragten (ISB) MÜSSEN sich regelmäßig über bekannt gewor- dene Sicherheitslücken der Office-Produkte informieren. Vorhandene Patches MÜSSEN zeitnah eingespielt werden.  Die Benutzer SOLLTEN über die Möglichkeiten und Grenzen von Sicherheitsfunktionen der eingesetzten Software und der genutzten Speicherformate informiert werden. Die Vorgaben für die sichere Nutzung von Office-Produk- ten SOLLTEN in der Sicherheitsrichtlinie integriert werden. |
| **Anforderungen**  **Web-Browser**  **APP.1.1** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.2 Webbrowser aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb Weitere Zuständigkeiten Benutzer  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein APP.1.2 Webbrowser vorrangig erfüllt werden: APP.1.2.A1 Verwendung von Sandboxing (B)  Der eingesetzte Webbrowser MUSS sicherstellen, dass jede Instanz und jeder Verarbeitungsprozess nur auf die ei- genen Ressourcen zugreifen kann (Sandboxing). Webseiten MÜSSEN als eigenständige Prozesse oder mindestens als eigene Threads voneinander isolierten werden. Plug-ins und Erweiterungen MÜSSEN ebenfalls in isolierten Be- reichen ausgeführt werden. Der verwendete Webbrowser SOLLTE die aktuelle Version der Content Security Policy (CSP) gemäß den Spezifikationen des World Wide Web Consortium (W3C) umsetzen.  APP.1.2.A2 Unterstützung sicherer Verschlüsselung der Kommunikation (B)  Der Webbrowser MUSS Transport Layer Security (TLS) in einer sicheren Version unterstützen. Unsichere Versionen von TLS SOLLTEN deaktiviert werden. Der Webbrowser MUSS den Sicherheitsmechanismus HTTP Strict Transport Security (HSTS) gemäß RFC 6797 unterstützen. Für alle wichtigen öffentlichen TLS-verschlüsselten Web-Dienste SOLLTEN die Domains in die HSTS-Preload-Liste des Browsers eingefügt werden.  APP.1.2.A3 Verwendung von vertrauenswürdigen Zertifikaten [Benutzer] (B)  Der Webbrowser MUSS eine Liste vertrauenswürdiger Wurzelzertifikats-Aussteller bereitstellen. Er MUSS die von der Institution selbst bereitgestellten Zertifikate akzeptieren. Der Webbrowser MUSS Extended-Validation-Zertifi- kate unterstützen. Wurzelzertifikate DÜRFEN NUR mit Administrationsrechten hinzugefügt, geändert oder ge- löscht werden. Zertifikate MÜSSEN durch den Webbrowser lokal widerrufen werden können.  Der Webbrowser MUSS die Gültigkeit der Server-Zertifikate mithilfe des öffentlichen Schlüssels und unter Berück- sichtigung des Gültigkeitszeitraums vollständig prüfen. Auch der Sperrstatus der Server-Zertifikate MUSS vom Webbrowser geprüft werden. Die Zertifikatskette einschließlich des Wurzelzertifikats MUSS verifiziert werden.  Der Webbrowser MUSS dem Benutzer eindeutig und gut sichtbar darstellen, ob die Kommunikation im Klartext oder verschlüsselt erfolgt. Der Webbrowser SOLLTE dem Benutzer auf Anforderung das verwendete Serverzertifikat anzeigen können. Der Webbrowser MUSS dem Benutzer signalisieren, wenn Zertifikate fehlen, ungültig sind oder widerrufen wurden. Die verschlüsselte Verbindung DARF in einem solchen Fall NUR nach ausdrücklicher Bestäti- gung durch den Benutzer hergestellt werden.  APP.1.2.A4 Versionsprüfung und Aktualisierung des Webbrowsers (B)  Der Webbrowser MUSS über einen Mechanismus verfügen, der den eigenen Versionsstand sowie den Versions- stand aller geladenen oder aktivierten Erweiterungen und Plug-ins zuverlässig erkennen und anzeigen kann.  Sicherheitsaktualisierungen, Plug-ins und Erweiterungen MÜSSEN unverzüglich eingespielt werden. Der Webbrow- ser SOLLTE Updates automatisch einspielen können. Ist kein Update für eine bekannt gewordene kritische Schwachstelle verfügbar, MÜSSEN zeitnah Maßnahmen zur Risikominderung ergriffen werden. |

|  |  |
| --- | --- |
| **Anforderungen**  **Mobile-Anwendungen**  **APP.1.4** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.4 Mobile Anwendungen (Apps) aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauf- tragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Benutzer, Datenschutzbeauftragter, Fachverantwortliche  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein APP.1.4 Mobile Anwendungen (Apps) vorrangig erfüllt werden:  APP.1.4.A1 Anforderungsanalyse für die Nutzung von Apps [Fachverantwortliche] (B)  Bevor eine App installiert und genutzt wird, MUSS unter Einbeziehung der jeweiligen Fachverantwortlichen klar definiert werden, welche Geschäftsprozesse die App unterstützen und an welche IT-Komponenten der Institution sie angebunden werden soll. Ferner MÜSSEN Sicherheitsanforderungen für die App festgelegt werden. Außerdem MÜSSEN Schutzbedarf und die rechtlichen Rahmenbedingungen der zu verarbeitenden Daten betrachtet werden.  In der Anforderungsanalyse MÜSSEN insbesondere Risiken betrachtet werden, die sich aus der mobilen Nutzung ergeben. Die Institution MUSS prüfen, ob ihre Kontroll- und Einflussmöglichkeiten auf die Betriebssystemumge- bung mobiler Endgeräte ausreichend sind, um sie sicher nutzen zu können.  APP.1.4.A2 Regelungen für die Verwendung von mobilen Endgeräten und Apps [Benutzer] (B)  Da für mobile Endgeräte oft nicht alle sicherheitsrelevanten Aspekte technisch gelöst werden können, MUSS für die Mitarbeiter eine Richtlinie für die Nutzung von Apps erstellt werden. Diese MUSS mindestens regeln,  • welche Daten auf den Geräten verarbeitet werden dürfen (auch: inwieweit eine private Nutzung gestattet ist),  • durch wen welche Apps auf den Geräten installiert werden dürfen,  • wie sich Benutzer in öffentlichen Datennetzen verhalten sollen und  • was zu tun ist, wenn ein Gerät verloren geht.  Diese Vorgaben MÜSSEN mit den etablierten Regelungen der Institution abgestimmt werden.  APP.1.4.A3 Verwendung sicherer Quellen für Apps [Benutzer] (B)  Es MUSS sichergestellt werden, dass Apps nur aus sicheren und vertrauenswürdigen Quellen bezogen werden kön- nen. Es DÜRFEN NUR vertrauenswürdige App Stores verwendet werden. Interne Apps der Institution und Apps, die schutzbedürftige Informationen verarbeiten, SOLLTEN über einen institutionseigenen App Store oder via MDM ver- teilt werden.  APP.1.4.A4 Test und Freigabe von Apps [Datenschutzbeauftragter, Fachverantwortliche] (B)  Es MUSS sichergestellt werden, dass sich die App in den vorhandenen Betrieb integrieren lässt und alle Anforderun- gen der fachlichen Bereiche, der Informationssicherheit und des Datenschutzes eingehalten werden. Bevor eine  4 IT-Grundschutz-Kompendium: Stand Februar 2020  APP.1.4 APP.1: Client-Anwendungen  neue App bzw. eine neue Version einer App eingesetzt wird, SOLLTE diese getestet und danach ausdrücklich freige- geben werden. Für alle Bereiche SOLLTEN entsprechende Tests entwickelt sowie Freigabekriterien definiert werden. Die Ergebnisse der Tests SOLLTEN dokumentiert werden und als Basis für die Freigabe der App dienen. Es SOLLTE insbesondere darauf geachtet werden, dass die Tests auf allen in der Institution verwendeten Gerätemodellen und Betriebssystemumgebungen durchgeführt werden. Die Freigabekriterien SOLLTEN bei allen erfüllt sein.  APP.1.4.A5 Minimierung und Kontrolle von App-Berechtigungen [Fachverantwortliche] (B)  Bevor eine App in einer Institution eingeführt wird, MUSS sichergestellt werden, dass sie nur die minimal benötig- ten App-Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen MÜSSEN hinter- fragt und gegebenenfalls unterbunden werden.  Sicherheitsrelevante Berechtigungseinstellungen MÜSSEN so fixiert werden, dass sie nicht durch Benutzer oder Apps geändert werden können. Wo dies technisch nicht möglich ist, MÜSSEN die Berechtigungseinstellungen re- gelmäßig geprüft und erneut gesetzt werden.  APP.1.4.A6 Patchmanagement für Apps (B)  Updates für Apps MÜSSEN zeitnah eingespielt werden. Falls die Institution ein System für MDM einsetzt, MÜSSEN verfügbare Updates damit gesteuert werden. Für jeden Patch MUSS bewertet werden, wie er sich auf die Sicherheit auswirkt. Danach SOLLTE er entsprechend priorisiert werden.  Wenn keine Patches zur Verfügung stehen, MÜSSEN geeignete Gegenmaßnahmen ergriffen werden, wenn bei Apps Schwachstellen bekannt sind. Ist dies nicht möglich, DÜRFEN Apps mit bekannten offenen Schwachstellen NICHT verwendet werden.  APP.1.4.A7 Sichere Speicherung lokaler App-Daten (B)  Wenn Apps auf interne Dokumente der Institution zugreifen können, MUSS sichergestellt sein, dass die lokale Da- tenhaltung der App angemessen abgesichert ist. Insbesondere MÜSSEN Zugriffsschlüssel verschlüsselt abgelegt werden. Außerdem DÜRFEN vertrauliche Daten NICHT vom Betriebssystem an anderen Ablageorten zwischenge- speichert werden.  APP.1.4.A8 Verhinderung von Datenabfluss (B)  Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Benutzer- profile erstellt werden, MUSS die App-Kommunikation geeignet eingeschränkt werden. Dazu SOLLTE die Kommu- nikation im Rahmen des Test- und Freigabeverfahrens analysiert werden. Weiterhin SOLLTE überprüft werden, ob eine App ungewollte Protokollierungs- oder Hilfsdateien schreibt, die möglicherweise vertrauliche Informationen enthalten. |
| **Anforderungen**  **Business-Anwendung**  **APP.4** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.4.2 SAP-ERP-System aufgeführt. Grundsätz- lich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforde- rungen gemäß dem festgelegten Sicherheitskonzept erfüllt und regelmäßig überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Entwickler, Fachabteilung, Leiter IT, Notfallbeauftragter  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein APP.4.2 SAP-ERP-System vorrangig erfüllt werden: APP.4.2.A1 Sichere Konfiguration des SAP-ABAP-Stacks (B)  Der SAP-ABAP-Stack MUSS sicher konfiguriert werden. Dazu MÜSSEN die jeweiligen Profilparameter gesetzt wer- den, z. B. für die Passwortsicherheit, Authentisierung und Verschlüsselung. Auch MÜSSEN die Systemänderbarkeit und die Mandanten konfiguriert, das IMG-Customizing durchgeführt und die Betriebssystemkommandos abgesi- chert werden.  2 IT-Grundschutz-Kompendium: Stand Februar 2020  APP.4.2 APP.4: Business-Anwendungen APP.4.2.A2 Sichere Konfiguration des SAP-JAVA-Stacks (B)  Der SAP-JAVA-Stack MUSS sicher konfiguriert werden, falls dieser eingesetzt wird. Dafür MÜSSEN andere Sicher- heitsmechanismen und -konzepte erstellt werden als für den SAP-ABAP-Stack. Deshalb MÜSSEN Administratoren die Architektur des JAVA-Stacks kennen und wissen, wie er administriert wird. Zudem MÜSSEN nicht benötigte Dienste abgeschaltet, Standardinhalte entfernt, HTTP-Dienste geschützt und Zugriffe auf Administrationsschnitt- stellen eingeschränkt werden.  APP.4.2.A3 Netzsicherheit (B)  Um die Netzsicherheit zu gewährleisten, MÜSSEN entsprechende Konzepte unter Berücksichtigung des SAP-ERP- Systems erstellt und Einstellungen am System durchgeführt werden.  Weiterhin SOLLTEN der SAP-Router und SAP Web Dispatcher eingesetzt werden, um ein sicheres SAP-Netz zu im- plementieren und aufrechtzuerhalten.  Um Sicherheitslücken aufgrund von Fehlinterpretationen oder Missverständnissen zu vermeiden, MÜSSEN sich die Bereiche IT-Betrieb, Firewall-Betrieb, Portalbetrieb und SAP-Betrieb miteinander abstimmen.  APP.4.2.A4 Absicherung der ausgelieferten SAP-Standardbenutzer-Kennungen (B)  Direkt nach der Installation eines SAP-ERP-Systems MÜSSEN die voreingestellten Passwörter der Standardbenutzer- Kennungen geändert werden. Auch MÜSSEN die eingerichteten SAP-Standardbenutzer-Kennungen mithilfe ge- eigneter Maßnahmen abgesichert werden. Bestimmte Standardbenutzer-Kennungen DÜRFEN NICHT benutzt wer- den, z. B. für RFC-Verbindungen und Background-Jobs.  APP.4.2.A5 Konfiguration und Absicherung der SAP-Benutzerverwaltung (B)  Die SAP-Benutzerverwaltung für ABAP-Systeme MUSS sorgfältig und sicher administriert werden. Aktivitäten, wie Benutzer anlegen, ändern und löschen, Passwörter zurücksetzen und entsperren sowie Rollen und Profile zuord- nen, MÜSSEN zu den Aufgaben der Benutzeradministration gehören. Der Benutzeradministrator MUSS im Um- gang mit der SAP-Benutzerverwaltung ausreichend geschult sein. Er SOLLTE sein Wissen regelmäßig vertiefen und aktualisieren.  APP.4.2.A6 Erstellung und Umsetzung eines Benutzer- und Berechtigungskonzeptes [Fachabteilung, Entwickler, Leiter IT] (B)  Für SAP-ERP-Systeme MUSS ein Benutzer- und Berechtigungskonzept ausgearbeitet und umgesetzt werden. Dabei MÜSSEN folgende Punkte berücksichtigt werden:  • Identitätsprinzip, Minimalprinzip, Stellenprinzip, Belegprinzip der Buchhaltung, Belegprinzip der Berechtigungs- verwaltung, Funktionstrennungsprinzip (Segregation of Duties, SoD), Genehmigungsprinzip, Standardprinzip, Schriftformprinzip und Kontrollprinzip MÜSSEN berücksichtigt werden.  • Benutzer-, Berechtigungs- und ggf. Profiladministrator MÜSSEN getrennte Verantwortlichkeiten und damit Be- rechtigungen haben.  • Vorgehensweisen im Rahmen der Berechtigungsadministration für Rollen anlegen, ändern, löschen, transportie- ren und SU24 Vorschlagswerte transportieren MÜSSEN definiert werden. Dabei SOLLTEN Berechtigungsrollen nur im Entwicklungssystem angelegt und gepflegt werden. Sie SOLLTEN mit Hilfe des Transport-Management- Systems (TMS) transportiert werden. Berechtigungen SOLLTEN in Berechtigungsrollen (PFCG-Rollen) angelegt, gespeichert und dem Benutzer zugeordnet werden (rollenbasiertes Berechtigungskonzept). Da sich einzelne kri- tische Aktionen in den Rollen nicht immer vermeiden lassen, SOLLTEN sie von kompensierenden Kontrollen (mi- tigation controls) abgedeckt werden.  • Vorgehensweisen im Rahmen der Berechtigungsvergabe für Benutzer und Berechtigungen beantragen, geneh- migen, ändern und löschen MÜSSEN definiert werden. Alle Berechtigungen SOLLTEN nach dem Prinzip der mini- malen Berechtigungsvergabe zugeteilt werden.  • Namenskonventionen für Benutzerkennungen und technische Rollennamen MÜSSEN definiert werden.  • Vorschlagswerte und Prüfkennzeichen SOLLTEN in der Transaktion SU24 gepflegt werden. Die Vorgehensweise dazu SOLLTE im Benutzer- und Berechtigungskonzept beschrieben sein.  • Gesetzliche und interne Rahmenbedingungen wie die Grundsätze ordnungsgemäßer Buchführung (GoB), das Handelsgesetzbuch (HGB) oder interne Vorgaben der Institution MÜSSEN berücksichtigt werden.  IT-Grundschutz-Kompendium: Stand Februar 2020 3  APP.4: Business-Anwendungen APP.4.2 Das Benutzer- und Berechtigungskonzept SOLLTE auch den Betrieb technischer Konten abdecken, also auch die  Berechtigung von Hintergrund- und Schnittstellenbenutzern.  Es SOLLTEN geeignete Kontrollmechanismen angewandt werden, um SoD-Konfliktfreiheit von Rollen und die Ver- gabe von kritischen Berechtigungen an Benutzer zu überwachen.  Werden neben dem ABAP-Backend weitere Komponenten wie SAP HANA und SAP NetWeaver Gateway (für Fiori- Anwendungen) verwendet, MUSS das Design der Berechtigungen zwischen den Komponenten abgestimmt und synchronisiert werden.  APP.4.2.A7 Absicherung der SAP-Datenbanken (B)  Der Zugriff auf SAP-Datenbanken MUSS abgesichert werden. Administratoren SOLLTEN möglichst nur mit SAP- Tools auf die Datenbanken zugreifen können. Wird dazu Software von Drittherstellern benutzt, MÜSSEN zusätzli- che Sicherheitsmaßnahmen umgesetzt werden. Es DÜRFEN dann die Benutzer SAPR3 oder SAP<SID> NICHT für die Verbindung zur Datenbank benutzt werden. Außerdem MÜSSEN Standardpasswörter (SAPR3 oder SAP<SID>) geändert und bestimmte Datenbanktabellen (z. B. USR\* Tabellen) besonders geschützt werden.  APP.4.2.A8 Absicherung der SAP-RFC-Schnittstelle (B)  Zum Schutz der Remote-Function-Call (RFC)-Schnittstelle MÜSSEN RFC-Verbindungen, RFC-Berechtigungen und die RFC-Gateways sicher konfiguriert werden.  Es MÜSSEN für alle RFC-Verbindungen einheitliche Verwaltungsrichtlinien erstellt und umgesetzt werden. Dazu SOLLTEN die benötigten RFC-Verbindungen definiert und dokumentiert werden. Verbindungen mit hinterlegtem Passwort SOLLTEN nicht von niedriger privilegierten auf höher privilegierte Systeme (z. B. von Dev nach Prod) konfi- guriert sein. Nicht mehr benutzte RFC-Verbindungen MÜSSEN gelöscht werden.  Alle RFC-Gateways MÜSSEN sicher administriert werden. Dazu MÜSSEN geeignete Profilparameter gesetzt wer- den, z. B. gw/monitor, gw/reg\_no\_conn\_info und snc/permit\_insecure\_start. Alle Verbindungen über ein Gateway MÜSSEN unter dem Sicherheitsaspekt analysiert und bewertet werden. Außerdem MUSS die Protokollierung aktiv sein. Es MÜSSEN Zugriffssteuerungslisten (ACLs) definiert werden.  APP.4.2.A9 Absicherung und Überwachung des Message-Servers (B)  Der Message-Server MUSS durch geeignete Einstellungen in den Profilparametern abgesichert werden. Es MUSS unter anderem entschieden werden, ob für den internen Message-Server noch ACLs aufgebaut werden. Der Mes- sage-Server MUSS mithilfe von geeigneten Mechanismen überwacht werden, damit z. B. Systemausfälle des Mes- sage-Servers schnell erkannt werden.  APP.4.2.A10 Regelmäßige Implementierung von Sicherheitskorrekturen [Fachabteilung] (B)  Support-Packages und Patches für das SAP-ERP-System MÜSSEN zeitnah nach Veröffentlichung bewertet werden. Es MUSS entschieden werden, ob das Support-Package beziehungsweise der Patch eingespielt werden soll. Wenn ein Support-Package oder der Patch nicht eingespielt wird oder werden kann, MÜSSEN die Entscheidung und die Gründe dafür dokumentiert werden. Das SAP-ERP-System SOLLTE regelmäßig aktualisiert werden. |

|  |  |
| --- | --- |
| **Anforderungen**  **Webserver**  **APP.3.2** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.2 Webserver aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Fachverantwortliche, Leiter IT  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein APP.3.2 Webserver vorrangig erfüllt werden: APP.3.2.A1 Sichere Konfiguration eines Webservers (B)  Nachdem der IT-Betrieb einen Webserver installiert hat, MUSS er eine sichere Grundkonfiguration vornehmen. Dazu MUSS er insbesondere den Webserver-Prozess einem Benutzerkonto mit minimalen Rechten zuweisen. Der Webserver MUSS in einer gekapselten Umgebung ausgeführt werden, sofern dies vom Betriebssystem unterstützt wird. Dem Webserver-Dienst MÜSSEN alle nicht notwendige Schreibberechtigungen entzogen werden. Nicht be- nötigte Module und Funktionen des Webservers MÜSSEN deaktiviert werden.  APP.3.2.A2 Schutz der Webserver-Dateien (B)  Der IT-Betrieb MUSS alle Dateien auf dem Webserver, insbesondere Skripte und Konfigurationsdateien, so schüt- zen, dass sie nicht unbefugt gelesen und geändert werden können.  Es MUSS sichergestellt werden, dass Webanwendungen nur auf einen definierten Verzeichnisbaum zugreifen kön- nen (WWW-Wurzelverzeichnis). Der Webserver MUSS so konfiguriert sein, dass er nur Dateien ausliefert, die sich innerhalb des WWW-Wurzelverzeichnisses befinden.  Der IT-Betrieb MUSS alle nicht benötigten Funktionen, die Verzeichnisse auflisten, deaktivieren. Er MUSS Dateien, die nicht verändert werden sollen, vor Schreibzugriffen schützen. Vertrauliche Daten MÜSSEN vor unberechtigtem Zugriff geschützt werden. Insbesondere MUSS der IT-Betrieb sicherstellen, dass vertrauliche Dateien nicht in öffent- lichen Verzeichnissen des Webservers liegen.  APP.3.2.A3 Absicherung von Datei-Uploads und -Downloads (B)  Alle mithilfe des Webservers veröffentlichten Dateien MÜSSEN vorher auf Schadprogramme geprüft werden.  Es MUSS eine Maximalgröße für Datei-Uploads spezifiziert sein. Für Uploads MUSS genügend Speicherplatz reser- viert werden.  APP.3.2.A4 Protokollierung von Ereignissen (B)  Der Webserver MUSS mindestens folgende Ereignisse protokollieren:  • erfolgreiche Zugriffe auf Ressourcen,  • fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressour- cen und Server-Fehlern sowie  • allgemeine Fehlermeldungen.  Die Protokollierungsdaten SOLLTEN regelmäßig ausgewertet werden.  IT-Grundschutz-Kompendium: Stand Februar 2020 3  APP.3: Netzbasierte Dienste APP.3.2 APP.3.2.A5 Authentisierung (B)  Wenn sich Clients mit Hilfe von Passwörtern am Webserver authentisieren, MÜSSEN diese kryptografisch gesichert und vor unbefugtem Zugriff geschützt gespeichert werden.  APP.3.2.A6 ENTFALLEN (B)  Diese Anforderung ist entfallen.  APP.3.2.A7 Rechtliche Rahmenbedingungen für Webangebote [Fachverantwortliche] (B)  Werden über den Webserver Inhalte für Dritte publiziert oder Dienste angeboten, MÜSSEN dabei die relevanten rechtlichen Rahmenbedingungen beachtet werden. So MÜSSEN die jeweiligen Telemedien- und Datenschutzge- setze sowie das Urheberrecht eingehalten werden. Auch SOLLTEN die Anforderungen an die Barrierefreiheit gemäß Behindertengleichstellungsgesetz beachtet werden.  APP.3.2.A11 Verschlüsselung über TLS (B)  Der Webserver MUSS für alle Verbindungen durch nicht vertrauenswürdige Netze eine sichere Verschlüsselung über TLS anbieten (HTTPS). Falls es aus Kompatibilitätsgründen erforderlich ist, veraltete Verfahren zu verwenden, SOLLTEN diese auf so wenige Fälle wie möglich beschränkt werden.  Wenn eine HTTPS-Verbindung genutzt wird, DÜRFEN alle Inhalte NUR über HTTPS verfügbar sein. Sogenannter Mixed Content DARF NICHT verwendet werden. |
| **Anforderungen**  **Cloud Server**  **APP.3.3** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.3 Fileserver aufgeführt. Grundsätzlich ist  der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei  strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen  gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen  geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit  in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Benutzer  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein APP.3.3 Fileserver vorrangig erfüllt werden:  APP.3.3.A1 ENTFALLEN (B)  Diese Anforderung ist entfallen.  APP.3.3.A2 Einsatz von RAID-Systemen (B)  Die Institution MUSS festlegen, ob im Fileserver ein RAID-System eingesetzt werden soll. Eine Entscheidung gegen  ein solches System MUSS nachvollziehbar dokumentiert werden. Wenn ein RAID-System eingesetzt werden soll,  MUSS die Institution entscheiden:  • welches RAID-Level benutzt werden soll,  • wie lang die Zeitspanne für einen RAID-Rebuild-Prozess sein darf und  • ob ein Software- oder ein Hardware-RAID eingesetzt werden soll.  Bei einem Hardware-RAID SOLLTE der RAID-Controller redundant ausgelegt sein. In einem RAID SOLLTEN HotspareFestplatten vorgehalten werden.  APP.3.3.A3 Einsatz von Viren-Schutzprogrammen (B)  Alle Daten MÜSSEN durch ein Viren-Schutzprogramm auf Schadsoftware untersucht werden, bevor sie auf dem  Fileserver abgelegt werden.  APP.3.3.A4 ENTFALLEN (B)  Diese Anforderung ist entfallen.  APP.3.3.A5 Restriktive Rechtevergabe (B)  Der IT-Betrieb MUSS Zugriffsrechte auf die vom Fileserver verwalteten Dateien restriktiv vergeben. Es MUSS sichergestellt sein, dass jeder Benutzer nur auf die Daten zugreifen kann, die er benötigt, um seine Aufgaben zu erfüllen.  Systemverzeichnisse und -dateien DÜRFEN NICHT für unbefugte Benutzer freigegeben werden.  Der IT-Betrieb MUSS regelmäßig überprüfen, ob die Zugriffsberechtigungen noch aktuell sind und der Sicherheitsrichtlinie entsprechen. Zudem MUSS es einen definierten Prozess geben, um Berechtigungen neu einzurichten, zu  ändern oder zu entziehen. Alle Zugriffsrechte MÜSSEN nachvollziehbar dokumentiert werden.  IT-Grundschutz-Kompendium: Stand Februar 2020 3  APP.3: Netzbasierte Dienste APP.3.3  APP.3.3.A15 Planung von Fileservern (B)  Bevor eine Institution einen Fileserver einführt, SOLLTE sie entscheiden, wofür die Fileserver genutzt und welche  Informationen darauf verarbeitet werden. Die Institution SOLLTE jede benutzte Funktion eines Fileservers einschließlich deren Sicherheitsaspekte planen. Arbeitsplatzrechner DÜRFEN NICHT als Fileserver eingesetzt werden.  Der Speicherplatz des Fileservers MUSS ausreichend dimensioniert sein. Auch ausreichende Speicherreserven SOLLTEN vorgehalten werden. Es SOLLTE ausschließlich Speicher verwendet werden, der für einen Dauerbetrieb ausgelegt ist. Die Geschwindigkeit und die Anbindung der Speicher MUSS für den Einsatzzweck angemessen sein. |

|  |  |
| --- | --- |
| **Anforderungen**  **Exchange Server**  **APP.5.2** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.5.2 Microsoft Exchange und Outlook aufge- führt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheits- beauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig IT-Betrieb  Weitere Zuständigkeiten Informationssicherheitsbeauftragter (ISB)  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein APP.5.2 Microsoft Exchange und Outlook vorrangig erfüllt werden:  APP.5.2.A1 Planung des Einsatzes von Microsoft Exchange und Outlook (B)  Bevor Microsoft Exchange und Outlook eingesetzt werden, MUSS die Institution deren Einsatz sorgfältig planen. Dabei MUSS sie mindestens folgende Punkte beachten:  • Aufbau der E-Mail-Infrastruktur,  • anzubindende Clients beziehungsweise Server,  • Nutzung von funktionalen Erweiterungen sowie  • die zu verwendenden Protokolle.  APP.5.2.A2 Auswahl einer geeigneten Microsoft Exchange-Infrastruktur (B)  Der IT-Betrieb MUSS auf Basis der Planung des Einsatzes von Microsoft Exchange entscheiden, mit welchen Syste- men und Anwendungskomponenten sowie in welcher hierarchischen Abstufung die Microsoft Exchange-Infra- struktur realisiert wird. Im Rahmen der Auswahl MUSS auch entschieden werden, ob die Systeme als Cloud- oder lokaler Dienst betrieben werden sollen.  IT-Grundschutz-Kompendium: Stand Februar 2020 3  APP.5: E-Mail/Groupware/Kommunikation APP.5.2 APP.5.2.A3 Berechtigungsmanagement und Zugriffsrechte (B)  Zusätzlich zum allgemeinen Berechtigungskonzept MUSS die Institution ein Berichtigungskonzept für die Systeme der Microsoft Exchange-Infrastruktur erstellen, geeignet dokumentieren und anwenden.  Der IT-Betrieb MUSS serverseitige Benutzerprofile für einen rechnerunabhängigen Zugriff der Benutzer auf Micro- soft Exchange-Daten verwenden. Er MUSS die Standard-NTFS-Berechtigungen für das Microsoft Exchange-Ver- zeichnis so anpassen, dass nur autorisierte Administratoren und Systemkonten auf die Daten in diesem Verzeichnis zugreifen können.  APP.5.2.A4 ENTFALLEN (B)  Diese Anforderung ist entfallen.  APP.5.2.A5 Datensicherung von Microsoft Exchange (B)  Microsoft Exchange-Server MÜSSEN vor Installationen und Konfigurationsänderungen sowie in zyklischen Abstän- den gesichert werden. Dabei MÜSSEN insbesondere die Exchange-Server-Datenbanken gesichert werden.  Gelöschte Exchange-Objekte SOLLTEN erst nach einiger Zeit aus der Datenbank entfernt werden. |

## 6.4 Industrielle IT-Bausteine

|  |  |
| --- | --- |
| **Anforderungen**  **CNC Maschiene**  **IND.2.4** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.4 Maschine aufgeführt. Grundsätzlich ist  der ICS-Informationssicherheitsbeauftragte (ICS-ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden.  Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen  haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig ICS-Informationssicherheitsbeauftragter  Weitere Zuständigkeiten ICS-Administrator  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein IND.2.4 Maschine vorrangig erfüllt werden:  IND.2.4.A1 Fernwartung durch Maschinen- und Anlagenbauer [ICS-Administrator] (B)  Für die Fernwartung einer Maschine SOLLTE es eine zentrale Richtlinie geben. Darin SOLLTE geregelt werden, wie  die jeweiligen Fernwartungslösungen einzusetzen sind und wie Kommunikationsverbindungen geschützt werden.  Sie SOLLTE auch beschreiben, welche Aktivitäten während der Fernwartung überwacht werden sollen.  Außerdem SOLLTE NICHT möglich sein, dass über die Fernwartung einer Maschine auf andere Systeme oder Maschinen der Institution zugegriffen werden kann.  Mit einem Dienstleister SOLLTE vereinbart werden, wie er die in der Maschine gespeicherten Informationen verwerten darf.  IND.2.4.A2 Betrieb nach Ende der Gewährleistung [ICS-Administrator] (B)  Es SOLLTE ein Prozess etabliert werden, der sicherstellt, dass die Maschine auch über den Gewährleistungszeitraum  hinaus sicher weiterbetrieben werden kann. Hierzu SOLLTEN mit dem Lieferanten weitere Unterstützungsleistungen vertraglich vereinbart werden. |

|  |  |
| --- | --- |
| **Anforderungen**  **Allgemeines Gebäude**  **INF.1** | 3 Anforderungen  Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.1 Allgemeines Gebäude aufgeführt. Grund- sätzlich ist die Haustechnik für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle An- forderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.  Grundsätzlich zuständig Haustechnik  Weitere Zuständigkeiten Bauleiter, Errichterfirma, Informationssicherheitsbeauftragter (ISB), Innerer Dienst, Institutionsleitung, Leiter Organisation, Mitarbeiter, Planer  3.1 Basis-Anforderungen  Die folgenden Anforderungen MÜSSEN für den Baustein INF.1 Allgemeines Gebäude vorrangig erfüllt werden: INF.1.A1 Planung der Gebäudeabsicherung [Planer] (B)  Je nach der (geplanten) Nutzung eines Gebäudes und dem Schutzbedarf der dort betriebenen Geschäftsprozesse MUSS festgelegt werden, wie das Gebäude abzusichern ist. Bei einem Gebäude MÜSSEN viele verschiedene Sicher- heitsaspekte zum Schutz von Personen im Gebäude, dem Schutz der Wirtschaftsgüter und der IT beachtet werden, von Brandschutz über Elektrik bis hin zur Zutrittskontrolle. Die Sicherheitsanforderungen aus den verschiedenen Bereichen MÜSSEN miteinander abgestimmt werden.  INF.1.A2 Angepasste Aufteilung der Stromkreise (B)  Es MUSS regelmäßig überprüft werden, ob die Absicherung und Auslegung der Stromkreise noch den tatsächli- chen Bedürfnissen genügen.  INF.1.A3 Einhaltung von Brandschutzvorschriften (B)  Die bestehenden Brandschutzvorschriften sowie die Auflagen der Bauaufsicht MÜSSEN eingehalten werden. Die Fluchtwege MÜSSEN vorschriftsmäßig ausgeschildert und freigehalten werden. Bei der Brandschutzplanung SOLLTE die örtliche Feuerwehr hinzugezogen werden. Es MUSS ein IT-bezogenes Brandschutzkonzept erstellt und umgesetzt werden, das die fehlenden IT bezogenen Anforderungen aus der Bauordnung zum Brandschutz enthält.  IT-Grundschutz-Kompendium: Stand Februar 2020 3  INF: Infrastruktur INF.1 Unnötige Brandlasten MÜSSEN vermieden werden.  Es MUSS einen Brandschutzbeauftragten oder eine mit dem Aufgabengebiet betraute Person geben, die auch ent- sprechend geschult ist.  INF.1.A4 Branderkennung in Gebäuden [Planer] (B)  Gebäude MÜSSEN mit einer ausreichenden Anzahl von Rauchmeldern ausgestattet sein. Bei größeren Gebäuden SOLLTE eine Brandmeldezentrale (BMZ) eingesetzt werden, auf die alle Melder aufgeschaltet sind. Bei Rauchdetek- tion MUSS eine Alarmierung im Gebäude ausgelöst werden. Diese MUSS sicherstellen, dass alle im Gebäude anwe- senden Personen diese wahrnehmen können. Die Funktionsfähigkeit aller Rauchmelder bzw. aller Komponenten einer Brandmeldeanlage MUSS regelmäßig überprüft werden. Es MUSS regelmäßig kontrolliert werden, dass die Fluchtwege benutzbar und frei von Hindernissen sind, damit das Gebäude in einer Gefahrensituation schnell ge- räumt werden kann.  INF.1.A5 Handfeuerlöscher (B)  Zur Sofortbekämpfung von Bränden MÜSSEN Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3 Tragbare Feuerlöscher) in ausreichender Zahl und Größe im Gebäude zur Verfügung stehen. Die Handfeuerlöscher MÜSSEN regelmäßig geprüft und gewartet werden. Die Mitarbeiter SOLLTEN in die Benutzung der Handfeuerlö- scher eingewiesen werden.  INF.1.A6 Geschlossene Fenster und Türen [Mitarbeiter] (B)  Fenster und nach außen öffnende Türen, etwa von Balkonen oder Terrassen, MÜSSEN zu Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Dafür MUSS es eine entsprechende Anweisung geben. Es MUSS regelmäßig überprüft werden, ob die Fenster und Türen nach Verlassen des Gebäudes verschlossen sind. Brand- und Rauch- schutztüren DÜRFEN NICHT dauerhaft offen gehalten werden.  INF.1.A7 Zutrittsregelung und -kontrolle [Leiter Organisation] (B)  Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen MUSS geregelt und kontrolliert werden. Es SOLLTE ein Konzept für die Zutrittskontrolle existieren. Die Zahl der zutrittsberechtigten Personen SOLLTE für jeden Bereich auf ein Mindestmaß reduziert werden. Weitere Personen DÜRFEN erst Zutritt erhalten, nachdem geprüft wurde, ob dies notwendig ist. Alle erteilten Zutrittsberechtigungen SOLLTEN dokumentiert werden. Die Zutrittskontroll- maßnahmen MÜSSEN regelmäßig auf ihre Wirksamkeit überprüft werden.  INF.1.A8 Rauchverbot (B)  Für Räume mit IT oder Datenträgern, in denen Brände oder Verschmutzungen zu hohen Schäden führen können, wie Serverräume, Datenträger- oder Belegarchive, MUSS ein Rauchverbot erlassen werden. Es MUSS regelmäßig kontrolliert werden, dass bei der Einrichtung oder Duldung von Raucherzonen der Zutrittsschutz nicht ausgehebelt wird. |
|  |  |

# **7. Anwendungshinweise**

Die in Kapitel 6 definierten Anforderungen sind im Zuge der Realisierungsplanung möglichst schnell umzusetzen. Nachdem dies erfolgt ist, sollte zeitnah entschieden werden, wann mit dem notwendigen, sich anschließenden Verbesserungsprozess begonnen wird.

**8. Umsetzung der Relevantesten Bausteine**

* R1: Soll vorrangig umgesetzt werden
* R2: Sollten als nächstes Umgesetzt werden
* R3: Wird ebenfalls benötigt

|  |  |  |
| --- | --- | --- |
| **Gerät:** | **Kennzahl** | **Gewichtung** |
| Exchange Server | APP.5.2 | R1 |
| Router&Switch | NET.3.1 | R1 |
| Telefonanlage | NET.4.1 | R1 |
| Windows Server | SYS.1.2.2 | R1 |
| Desktop-System | SYS.2 | R1 |
| Allgemeine Gebäude | INF.1 | R1 |
| IP-Telefon | NET.4.2 | R2 |
| Laptop | SYS.3.1 | R2 |
| Business-Anwendung | APP.4 | R2 |
| Webserver | APP.3.2 | R3 |
| Cloud Server | APP.3.3 | R3 |
| CNC Maschiene | IND.2.4 | R3 |
| Fax | NET.4.3 | R3 |
| Smartphone & Tablet | SYS.3.2 | R3 |
| Drucker/Multifunktionsgerät | Sys.4.1 | R3 |
| Office-Produkte | APP.1.1 | R3 |
| Web-Browser | APP.1.2 | R3 |
| Mobile-Anwendungen | APP.1.4 | R3 |
| Elektronische Ladenkasse | na |  |
| Kartenleser | na |  |
| Außenkammera | na |  |
| Fuhrpark | na |  |
| Home-Office | na |  |
| Mobiles Arbeiten | na |  |
| Warenwirtschaft | na |  |
| Produktionssoftware | na |  |