MUSTER-IT-SICHERHEITSKONZEPT FÜR MITTLERE UND GROSSE EINRICHTUNGEN

MANAGEMENT SUMMARY

Das Muster-IT-Sicherheitskonzept gibt eine Empfehlung zur Umsetzung der Vorgaben zur IT-Sicherheit gemäß der Anforderungen des Datenschutzgesetzes der EKD (DSG-EKD) sowie der Ratsverordnung zur IT-Sicherheit.

Das Ziel ist die Ermittlung von Sicherheitsanforderungen, die Beurteilung des erreichten Sicherheitsniveaus sowie die Festlegung angemessener Sicherheitsmaßnahmen. Den IT-Sicherheitsbeauftragten, den Fachverantwortlichen und den Administratoren wird ein Werkzeug zur Erstellung von IT-Sicherheitskonzepten an die Hand gegeben. Für kleine Einrichtungen existiert ein separates Muster-IT-Sicherheitskonzept. Grundsätzlich ist eine Sensibilisierung aller Mitarbeitenden für das Thema IT-Sicherheit notwendig. Hierfür liegt ein entsprechendes Schulungskonzept vor [Anlage C1 Schulungskonzept IT-Sicherheit]. Darüber hinaus ist die Erstellung von Vereinbarungen notwendig, die den Umgang der Mitarbeitenden mit IT regeln [Anlage C2 BFDI Musterformular].

Das Muster-IT-Sicherheitskonzept wurde konform zu den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI), welche in den BSI-Standards 100-1 bis 100-4 beschrieben sind, sowie den IT-Grundschutz-Katalogen (Stand 13. Ergänzungslieferung) erstellt.

Die IT-Grundschutz-Vorgehensweise besteht aus den folgenden Einzelschritten:

- **Definition des Informationsverbundes:** Zu Beginn dieses IT-Sicherheitskonzepts wird fest-gelegt, welcher Bereich der Einrichtung abgedeckt wird (Geltungsbereich).
- **Strukturanalyse:** Grundlage eines jeden IT-Sicherheitskonzepts ist die genaue Kenntnis der Informationen, Prozesse und unterstützenden technischen Systeme des betrachteten Informationsverbundes. Ziel der Strukturanalyse ist es, die hierfür erforderlichen Kenntnisse zusammenzustellen und aufzubereiten.
- **Schutzbedarfsfeststellung:** Bei der Schutzbedarfsfeststellung wird ermittelt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.
- **Modellierung:** Für den betrachteten Informationsverbund werden die relevanten Bausteine (Maßnahmensammlung) der IT-Grundschutz-Kataloge ausgewählt, auf deren Basis im weiteren Verlauf mögliche Sicherheitsmaßnahmen definiert werden.
- **Basis-Sicherheitscheck:** Ein Überblick über das vorhandene Sicherheitsniveau wird erarbeitet. Mit Hilfe von Interviews wird der Status quo des bestehenden Informationsverbunds in Bezug auf den Umsetzungsstatus für jede relevante Maßnahme bewertet.
- **Ergänzende Sicherheitsanalyse:** Die ergänzende Sicherheitsanalyse stellt sicher, dass die nicht vollständig abgedeckten Risiken (z. B. bei höherem Schutzbedarf) ermittelt werden.
- **Risikoanalyse:** Ziel der Risikoanalyse ist, die vorhandenen Risiken durch eine Risikobehandlung auf ein verträgliches bzw. akzeptables Maß (Restrisiko) zu reduzieren.

Die Beispiele am Ende jedes Kapitels geben einen Einblick, wie ein Sicherheitskonzept zu erstellen ist. Das Sicherheitskonzept muss regelmäßig fortgeschrieben und mit dem zuständigen IT-Sicherheitsbeauftragten abgestimmt werden.

1 ZIELSETZUNG DES IT-SICHERHEITSKONZEPTS

1.1 Rahmenbedingungen / Ausgangslage

Mit der Novellierung des EKD-Datenschutzgesetzes (DSG-EKD) sowie dem Erlass einer Ratsverordnung zur IT-Sicherheit sind alle Einrichtungen der Evangelischen Kirche Deutschland (EKD), ihrer Gliedkirchen, gliedkirchlichen Zusammenschüsse, Diakonischen Werke und Einrichtungen zur Einhaltung der IT-Sicherheit und zur Erstellung, Umsetzung und Fortschreibung von IT-Sicherheitskonzepten verpflichtet. Das vorliegende Muster IT-Sicherheitskonzept soll Hinweise und Hilfen zur Umsetzung geben.

Für kleine Einrichtungen existiert ein separates Muster-IT-Sicherheitskonzept.

1.2 Zielsetzung und Vorgehensweise

Alle kirchlichen Einrichtungen sind für IT-Sicherheit verantwortlich. Die IT-Sicherheit ist Teil der Informationssicherheit. Diese Vorgabe wird durch das Datenschutzgesetz der EKD in der Novellierung aus dem Jahre 2013 aufgestellt.

Die Vorgaben des Datenschutzes sind im DSG-EKD formuliert. Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung und den Umgang seiner personenbezogenen Daten in dem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").

Mit diesem Muster-IT-Sicherheitskonzept wird den IT-Sicherheitsbeauftragten, den Fachverantwortlichen und Administratoren ein Werkzeug zur Erstellung von Sicherheitskonzepten an die Hand gegeben. Die Beispiele am Ende jedes Kapitels geben einen Einblick, wie dieses Dokument zu erstellen ist. Die im Dokument vorkommenden Platzhalter (gelber Text in eckigen Klammern) sind für spezifische Einträge der jeweiligen Einrichtung. Dieses Dokument muss regelmäßig fortgeschrieben werden und mit dem zuständigen IT-Sicherheitsbeauftragten abgestimmt werden.

Kleine Organisationen werden wie folgt definiert: kleinste und kleine Einrichtungen verfügen über kein geschultes IT-Personal, nur eine minimale Infrastruktur und eine überwiegend dezentrale Datenhaltung, z. T. zentrale Anwendungen (Melde-, Finanz- und Personalwesen). Zudem existiert z. T. keine ausreichende Abgrenzung zu privaten Bereichen (Räume und Geräte). In der Regel gibt es keine IT-Standards (Datensicherung, Kennwortregelungen) und auch keine Server.

Mittlere und große Einrichtungen hingegen verfügen über eigenes geschultes IT-Personal oder externe Mitarbeitende sowie über eine professionelle IT-Infrastruktur mit eigenen Servern. Zudem existieren in der Regel bereits unterschiedlich ausgeprägte IT-Standards (z. B. Datensicherung, Kennwortregelungen, Protokollierung). Es gibt z. T. Dienstleistungen, die durch Outsourcing betrieben werden.

Informationssicherheit sorgt dafür, dass die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit gewahrt werden. Vertraulichkeit schützen bedeutet, die IT-Systeme und Anwendungen so zu sichern, dass nur autorisierte Personen auf die verarbeiteten Daten Zugriff haben. Integrität schützt die Daten vor Manipulationen. Verfügbarkeit hingegen sorgt dafür, dass Daten im gewünschten Zeitraum zur Verfügung stehen und darauf zugegriffen werden kann.

Ziel dieses IT-Sicherheitskonzepts ist die Ermittlung von Sicherheitsanforderungen, die Beurteilung des erreichten Sicherheitsniveaus sowie die Festlegung angemessener zu ergreifender Sicherheitsmaßnahmen. Die Grafik (Abbildung 2) veranschaulicht die grundsätzliche Vorgehensweise, die sich in der Struktur dieses Muster-IT-Sicherheitskonzeptes wiederfindet.

Abbildung 1: Vorgehensweise IT-Sicherheitsmanagement nach BSI-Standard 100-2

(Die Nummerierung bezieht sich auf die Kapitel dieses Dokuments)

1.3 Methodik und Werkzeuge

Das Muster-IT-Sicherheitskonzept wurde basierend auf den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) erstellt, welche in den BSI-Standards 100-1 bis 100-4 beschrieben sind. Wesentlich ist hierbei die methodische Umsetzung der Anforderungen des

- BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise* sowie die Anwendung der
- IT-Grundschutz-Kataloge (Stand 13. Ergänzungslieferung) und des
- BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz inklusive der Ergänzung zum BSI-Standard 100-3, Version 2.5.

Das Muster-IT-Sicherheitskonzept sollte weitgehend unter Verwendung einer Software (siehe Anlage C3 Tool-Unterstützung IT-Grundschutz) erstellt werden. Um das Rahmendokument schlank und lesbar zu gestalten, sind die hier getroffenen Aussagen im Detail durch die Informationen, die in den im Anhang befindlichen Berichten enthalten sind, zu ergänzen. Alle Daten sind in einer Datenbank gespeichert, um eine leichte Wartbarkeit zu gewährleisten.

2 INFORMATIONSVERBUND

Zu Beginn dieses IT-Sicherheitskonzepts wird festgelegt, welcher Bereich der Organisation abgedeckt wird, bzw. der Geltungsbereich abgegrenzt. Dies können z. B. bestimmte Organisationseinheiten oder auch Bereiche sein, die Fachaufgaben oder -verfahren bearbeiten, inklusive der dafür notwendigen IT-Ressourcen und Infrastruktur.

Die folgenden Aspekte müssen in der Definition enthalten sein:

- Eindeutige Abgrenzung des Geltungsbereiches,
- Festlegung, welche kritischen Fachanwendungen/Fachaufgaben oder Teile der Organisation der Geltungsbereich beinhalten soll,
- Beschreibung der Schnittstellen mit externen Partnern/Dienstleistern.

2.1 Definition des Informationsverbund

Ein Informationsverbund wird durch IT-Komponenten, Informationen, organisatorische Regelungen, Aufgabenbereiche und Zuständigkeiten sowie die physische Infrastruktur definiert.

2.2 Kritische Fachaufgaben und -verfahren

Im betrachteten Informationsverbund sind alle IT-Anwendungen, -Systeme, Netzwerke, Räume und Gebäude enthalten, die für die Fachaufgaben und -verfahren eine Rolle spielen. Zudem müssen die Fachverfahren beschrieben werden. Diese stellen die zentrale Dienstleistung und damit auch das zentrale Verfahren dar.

2.3 Beispiel Informationsverbund

2.3.1 Definition des Informationsverbundes

Beispiel:

Der Informationsverbund unterstützt die Geschäftsprozesse zur Erbringung der seelsorgerischen Beratungsdienstleistungen durch die Mustereinrichtung. Zur Erbringung der Beratungsleistungen benötigt die Mustereinrichtung unterschiedlichste IT-Systeme.

Primär werden IT-Systeme mit einem Windows-Betriebssystem eingesetzt. Im Rahmen der Beratungstätigkeit werden Notebooks verwendet, mit denen, bei einem mobilen Einsatz vor Ort, die Einwahl über eine VPN-Verbindung in das interne Netzwerk der Organisation erfolgt. Für die Bürokommunikation am Standort Außendorf wurde eine E-Mail-Infrastruktur mit Smartphone-Integration implementiert. Im Rahmen der Projekttätigkeiten wird auf Serversysteme zugegriffen, welche sich in einem gesicherten Serverraum der Mustereinrichtung am Standort Außendorf befinden. Die bereitgestellten Serversysteme werden zum Teil in einer Virtualisierungsinfrastruktur abgebildet. Entsprechend der Funktionalität und des Schutzbedarfs erfolgt eine Aufteilung der IT-Systeme in unterschiedliche Netze.

2.3.2 Kritische Fachaufgaben und -verfahren

Beispiel:

Das Fachverfahren lässt sich grob unterteilen in

- Abhalten der Beratungsleistungen (Werbung, Kundeninformation),
- Abrechnung der Beratungsleistungen (Rechnungswesen) und
- Durchführung der Beratungsleistungen (Einsatzplanung, Beratungstermine etc.).

Die reine Beratung läuft unabhängig von den untersuchten IT-Systemen. Allerdings wird ein Ausfall von zentralen IT-Systemen relativ schnell Auswirkungen auf die Beratung zeigen, wenn z. B. keine Termine mehr vergeben, keine Einsätze mehr geplant und keine Betriebsmittel mehr gewartet werden können.

Die Verarbeitung kritischer Daten bezieht sich in erster Linie auf personenbezogene Daten von Mitarbeitern (Dienstpläne, Gehaltsabrechnung, Personalakte etc.) und Kunden (Beratungsprotokolle, Kundenakten). Weiterhin sind kritische Geschäftsdaten in Form der finanziellen und kirchlichen Planung im Rahmen des Üblichen vorhanden.

Zusätzlich zum zentralen Kernprozess werden die üblichen Verwaltungsprozesse (Finanz- und Rechnungswesen, Controlling, Personal, Gebäudemanagement) betrachtet.

2.3.3 Beschreibung der Schnittstellen mit externen Partnern/Dienstleistern

Beispiel:

Ein externer Dienstleister ist für das Hosting der Website zuständig. Sämtliche Inhalte werden von der Internet AG bereitgestellt. Der Dienstleister formatiert die Inhalte in das Webseitenformat und veröffentlicht diese nach einem Freigabeprozess auf der Website.

3 IT-STRUKTURANALYSE

Grundlage eines jeden Sicherheitskonzepts ist die genaue Kenntnis der Informationen, Prozesse und unterstützenden technischen Systeme des betrachteten Informationsverbundes. Ziel der Strukturanalyse ist es, die hierfür erforderlichen Kenntnisse zusammenzustellen und aufzubereiten.

Die Strukturanalyse gliedert sich in folgende Teilaufgaben:

- Erhebung des bereinigten Netzplans
- Erfassung der zum Geltungsbereich zugehörigen Fachverfahren, Anwendungen und IT-Systeme
- Erfassung der Netzwerkstruktur und der räumlichen Gegebenheiten

3.1 Bereinigter Netzplan

Einen Überblick über den betrachteten Informationsverbund gibt der bereinigte Netzplan. Dieser bereinigte Netzplan beinhaltet die wesentlichen Informationen über Clients, Server, Netzkomponenten, Kommunikationsverbindungen (Netze) und teilweise auch geografische Verteilungen von Gebäuden und Räumen. Besonders wichtig ist die Darstellung und Auszeichnung aller vorhandenen Kommunikationsstrecken bzw. Netzwerke wie z. B. DMZ, RZ-LAN oder auch VPN.

3.2 Wesentliche IT-Anwendungen und IT-Systeme

Zur Unterstützung der Fachaufgaben und -verfahren ist eine Vielzahl von verschiedenen IT-Anwendungen im Gebrauch.

Eine Liste aller vorhandenen IT-Anwendungen findet sich in Tabelle 2. Eine IT-Anwendung kann dabei ein bestimmtes Software-Produkt (z. B. ein Programm zur Ressourcenplanung), eine sinnvoll abgegrenzte Einzelaufgabe (z. B. Bürokommunikation) oder eine Fachaufgabe (z. B. Abrechnung von Reisekosten) sein.

Eine Liste aller im Informationsverbund vorhandenen IT-Systeme (Server, Clients, aktive Netzkomponenten etc.) findet sich in Tabelle 3.

3.3 Netzwerkstruktur und räumliche Gegebenheiten

Die Netzwerkstruktur kann im Wesentlichen aus der Darstellung des Informationsverbundes (siehe Unterkapitel 3.1 oben) entnommen werden. Netzwerkverbindungen terminieren normalerweise immer an zwei oder mehreren der unter den IT-Systemen dokumentierten Netzwerkkomponenten (Router, Switches etc.). Der bereinigte Netzplan stellt die Komponenten im Informationsverbund und deren Vernetzung dar. Dabei sind gleichartige Komponenten (z. B. Client-Systeme) zu Gruppen zusammengefasst.

Eine Liste aller vorhandenen Kommunikationsverbindungen findet sich in Tabelle 4.

Eine Liste aller Räume und Gebäude findet sich in Tabelle 5.

3.4 Beispiel Strukturanalyse

3.4.1 Bereinigter Netzplan

Beispiel:

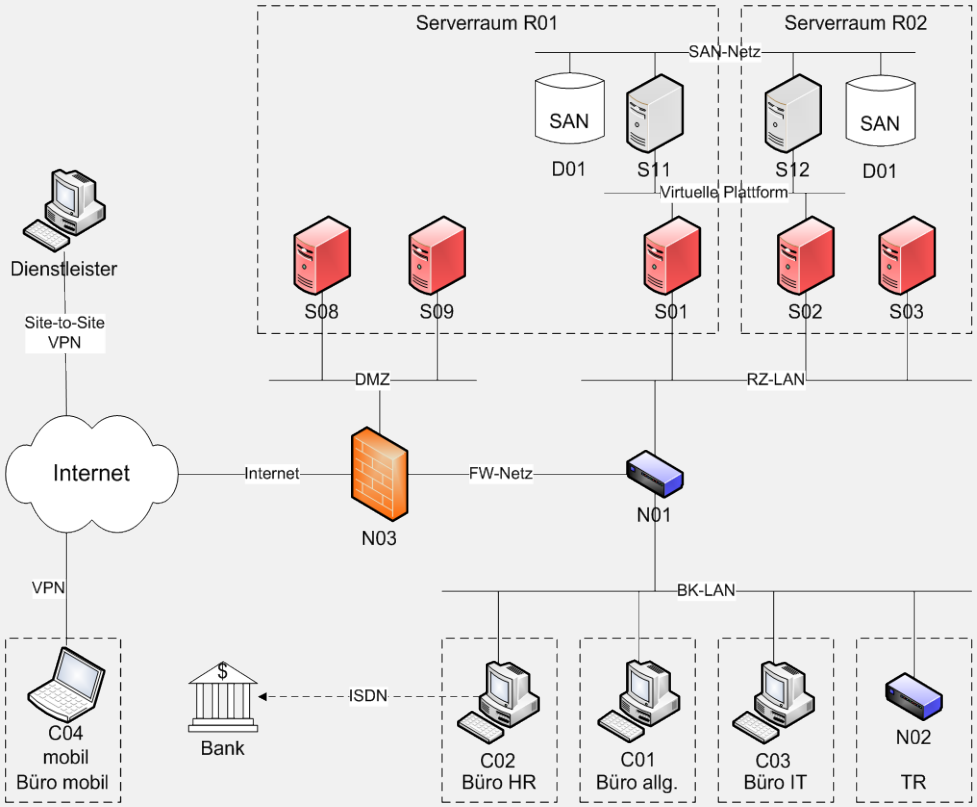

Abbildung 2: Betrachteter IT-Verbund

3.4.2 Wesentliche IT-Anwendungen und IT-Systeme

Beispiel:

Zu den zentralen Fachverfahren gehören:

- Personalwesen
- Finanzwesen
- Bürokommunikation

Beispiel:

Tabelle 1: Anwendungen

Nr.	*Bezeichnung*	*Art*	*Anwender*
A100	*Bürokommunikation*	*Softwarepaket MS-Office*	*Alle*
A101	*Personaldatenverarbeitung mit MS Office*	*Softwarepaket MS-Office*	*Personalsachbearbeiter / Abteilung HR*
A110	*Dateiablage*	*Anwendung allgemein*	*Alle*
A120	*Drucken*	*Druckdienste*	*Alle*
A130	*E-Mail*	*E-Mail unter Outlook 2000 / Exchange 2000*	*Alle*
A150	*Intranet*	*Apache Webserver auf Unix / Linux*	*Alle*
A160	*Internet-Zugang*	*Anwendung allgemein*	*Alle*
A200	*IT-Betrieb Verzeichnisdienst*	*Verzeichnisdienst auf der Basis Active Directory*	*Alle*
A210	*IT-Betrieb Backup*	*Datensicherung und Archivierung*	*Alle*
A220	*IT-Betrieb allgemein (Virenschutz, Netzwerk, Firewall etc.)*	*Anwendung allgemein*	*IT-Abteilung*
A230	*IT-Service / Helpdesk Tool*	*Anwendung allgemein*	*IT-Abteilung*
A300	*SAP (Modul FI)*	*SAP R/3 / mySAP*	*Rechnungswesen*

Beispiel:

Tabelle 2: IT-Systeme

Nr.	*Bezeichnung*	*Art*	*Anzahl*	*Ort*
S001	*Domänencontroller*	*Windows 2003-Server*	*2*	*RZ*
…	*…*	*…*	*…*	*…*
N001	*Core Switch*	*3Com-Switch*	*10*	*TRs*
C001	*Standard-Clients*	*Windows XP*	*3000*	*Büros*

Beispiel:

Tabelle 3: Kommunikationsverbindungen

Nr.	***Bezeichnung***	***Art***
K001	*Client-LAN*	*Heterogenes Netzwerk*
K002	*Server-LAN*	*Heterogenes Netzwerk*

Beispiel:

Räumlich erstreckt sich der Betrachtungsbereich neben dem Hauptstandort (Außendorf, Über den Linden 1) und dem gegenüberliegenden Serverraum im Gebäude (Außendorf, Königsdamm 1) auf verschiedene über das Stadtgebiet verteilte Außenstellen.

Tabelle 4: Räume und Gebäude

Nr.	***Bezeichnung***	***Art***	***Anzahl***	***Gebäude***
G001	*Gebäude Außendorf*	*Allgemeines Gebäude*	*1*	*-*
…	…	…	…	…
R001	*Serverraum 1*	*Serverraum*	*1*	*G001*
R003	*Etagenverteiler*	*Technikraum*	*10*	*G001*

4 SCHUTZBEDARFSFESTSTELLUNG

Zweck der Schutzbedarfsfeststellung ist es zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Die Bewertung des notwendigen Schutzes orientiert sich dabei an den Schutzzielen Vertraulichkeit (VT), Integrität (IN) und Verfügbarkeit (VF).

Die Schutzbedarfsfeststellung gliedert sich in die folgenden Teilaufgaben:

- Erhebung des Schutzbedarfs für jede IT-Anwendung
- Vererbung des Schutzbedarfs für IT-Systeme
- Vererbung des Schutzbedarfs für Netze/Kommunikationsverbindungen
- Vererbung des Schutzbedarfs für Räume und Gebäude

4.1 Erhebung des Schutzbedarfs für IT-Anwendungen

Ausgehend von den Fachaufgaben und -verfahren ist für jede in der Liste der IT-Anwendungen[1] aufgeführte Anwendung der Schutzbedarf in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit zu dokumentieren und zu begründen (siehe Abbildung 4). Dies geschieht dadurch, dass man für jedes dieser Schutzziele abschätzt, welche Schäden durch seine Verletzung eintreten könnten.

[1] Im IT-Grundschutz wird zwischen Geschäftsprozessen und Anwendungen nicht unterschieden. Aus diesem Grund werden diese Begriffe im Weiteren nahezu synonym verwendet. Bei der Erfassung der Anwendungen wird die Verbindung zum jeweiligen Geschäftsprozess hergestellt – im Zweifelsfall werden Anwendungen für jeden nutzenden Geschäftsprozess einzeln erfasst.

Gesamtschutzbedarf der Anwendung	
Allgemeine Daten:	
Anwendungsname:	Webshop
Unterstützter Prozess:	Einkauf
Auf folgenden System(en) installiert:	Webserver, DB-Server
Organisationseinheit (OE):	Einkauf IT
Informationseigentümer (Name):	IT-Leitung

Definierte Schutzbedarfsklasse			
Schadenszenario	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
Verstoß gegen Gesetze / Vorschriften / Verträge	*hoch*	*hoch*	*normal*
Beeinträchtigung des informationellen Selbstbestimmungsrechts	*normal*	*normal*	*normal*
Beeinträchtigung der persönlichen Unversehrtheit	*normal*	*normal*	*normal*
Beeinträchtigung der Aufgabenerfüllung	*hoch*	*normal*	*normal*
Negative Außenwirkung	*hoch*	*normal*	*normal*
Finanzielle Auswirkungen	*hoch*	*normal*	*normal*
Gesamtbewertung	**hoch**	**hoch**	**normal**

Abbildung 3: Erhebung des Schutzbedarfs für eine Anwendung

Schäden, die bei einem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für eine IT-Anwendung einschließlich ihrer Daten, den zugrunde liegenden IT-Systemen und den Räumen, in denen diese betrieben werden, entstehen können, lassen sich typischerweise folgenden Schadensszenarien zuordnen:

- Verstoß gegen Gesetze/Vorschriften/Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Außenwirkung und
- finanzielle Auswirkungen.

Wichtig ist es dabei, die möglichen Folgeschäden realistisch einzuschätzen. Der IT-Grundschutz definiert die folgenden drei Schutzbedarfskategorien:

- „normal“, d. h. die Schadensauswirkungen sind begrenzt und überschaubar,
- „hoch“, d. h. die Schadensauswirkungen können beträchtlich sein, bzw.
- „sehr hoch“, d. h. die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Die Definition der drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ geschieht anhand von möglichen Schäden (z. B. finanzielle Schäden oder Verstöße gegen Gesetze), die bei Beeinträchtigung von IT-Anwendungen in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit auftreten können.

Die im Rahmen des Projektes abgestimmten Schutzbedarfskategorien für die Mustereinrichtung befinden sich in der Anlage C4 Schutzbedarfskategorien und beispielhafte, detaillierte Schutzbedarfsfeststellung wichtiger kirchlicher Anwendungen finden sich in der Anlage C5 Schutzbedarfsfeststellung.

4.2 IT-Systeme

Der Schutzbedarf eines IT-Systems leitet sich aus dem Schutzbedarf der IT-Anwendungen ab, die auf dem IT-System ablaufen oder deren Daten das IT-System transportiert oder verarbeitet. Diese „Vererbung“ geschieht zunächst nach dem sogenannten „Maximum-Prinzip“, bei dem der maximale Schutzbedarf aller relevanten Ausgangsobjekte auf das Folgeobjekt weitergegeben wird. Für die IT-Systeme heißt das, dass sie den maximalen Schutzbedarf aller auf ihnen laufenden IT-Anwendungen erben.

Um den Schutzbedarf eines IT-Systems festzustellen, müssen die ermittelten Schäden für jedes IT-System in ihrer Gesamtheit betrachtet werden. Im Wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen nach dem Maximum-Prinzip den Schutzbedarf eines IT-Systems.

Bei der Betrachtung der möglichen Schäden und ihrer Folgen muss auch beachtet werden, dass Anwendungen Arbeitsergebnisse anderer Anwendungen als Eingangsgröße nutzen können. Diese Informationen können dabei auch auf anderen IT-Systemen erarbeitet worden sein. Eine – für sich betrachtet – weniger bedeutende Anwendung kann wesentlich an Wert gewinnen, wenn eine andere wichtige Anwendung auf ihre Ergebnisse angewiesen ist. In diesem Fall muss der ermittelte Schutzbedarf auch für die abhängigen Anwendungen und Informationen sichergestellt werden. Handelt es sich dabei um Anwendungen verschiedener IT-Systeme, dann müssen Schutzbedarfsanforderungen des einen IT-Systems auch auf das andere übertragen werden.

Werden mehrere Anwendungen/Informationen auf einem IT-System verarbeitet, so ist zu überlegen, ob durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann („Kumulationseffekt“). Zutreffendenfalls erhöht sich der Schutzbedarf des IT-Systems entsprechend.

Auch der umgekehrte Effekt kann eintreten. So ist es möglich, dass eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen. Hier ist der Schutzbedarf zu relativieren („Verteilungseffekt“).

Die Ableitung des Schutzbedarfs der IT-Systeme von den IT-Anwendungen findet sich in Tabelle 7.

4.3 Netze/Kommunikationsverbindungen

Im Gegensatz zu IT-Anwendungen und IT-Systemen fordert BSI IT-Grundschutz bei den Kommunikationsverbindungen die Unterscheidung zwischen kritischen und nichtkritischen Verbindungen. Kritisch ist eine Verbindung, wenn sie eine Außenverbindung darstellt, wenn sie hochschutzbedürftige Daten transportiert oder wenn über diese Verbindung bestimmte hochschutzbedürftige Daten nicht transportiert werden dürfen.

Die Kommunikationsverbindungen werden nach ihrer Kritikalität (K1 bis K5) klassifiziert. Neben der Kennzeichnung hohen Schutzbedarfs in den drei Grundwerten (K2, K3, K4) werden insbesondere die Außenverbindungen besonders gekennzeichnet (K1) - hier müssen wirksame Maßnahmen zum Schutz des Netzes getroffen werden.

Der Schutzbedarf der Kommunikationsverbindungen leitet sich zunächst von dem der darüber verbundenen IT-Systeme ab. Bei IT-Systemen, die aufgrund von Verteilungseffekten herabgestuft wurden, muss hier jedoch explizit beachtet werden, dass sich der Schutzbedarf der zugrunde liegenden Kommunikationsverbindungen entsprechend der Anwendungseinstufungen wieder erhöhen kann, falls nicht auch hier entsprechende Redundanz vorhanden ist.

Die Dokumentation des Schutzbedarfs der Kommunikationsverbindungen findet sich in Tabelle 8.

4.4 Räume und Gebäude

Der Schutzbedarf der Räume und Gebäude leitet sich von den dort betriebenen IT-Systemen, aufbewahrten Datenträgern und Dokumenten ab. Dies geschieht ebenfalls nach dem Maximum-Prinzip.

Die Ableitung des Schutzbedarfs der Räume und Gebäude von den IT-Systemen findet sich in Tabelle 9.

4.5 Beispiel Schutzbedarfsfeststellung

4.5.1 Schutzbedarf der IT-Anwendungen

Beispiel:

Tabelle 5: Schutzbedarf der IT-Anwendungen

Nr.	***Bezeichnung***	***Pbez. Daten***	***Grundwert***	***Schutzbedarf***	***Begründung***
A120	*E-Mail*	*X*	*VT*	*hoch*	*personenbezogene Daten enthalten*
			IN	*normal*	*Fehler werden schnell erkannt und haben keine Folgen*
			VF	*hoch*	*Ausfälle bis zu einer Woche sind unproblematisch – Gehälter können per Abschlag überwiesen werden*

4.5.2 Schutzbedarf der IT-Systeme

Beispiel:

Tabelle 6: Schutzbedarf der IT-Systeme

Nr.	*Bezeichnung*	*Anh. Anw.*	*Grundwert*	*Schutzbe-darf*	*Begründung*
S001	*Domänencon-troller*	*A001*	*VT*	*hoch*	*Maximumprinzip*
			IN	*normal*	*Maximumprinzip*
			VF	*hoch*	*Verteilungseffekt, da Redundanz vor-handen*

4.5.3 Schutzbedarf der Netze/ Kommunikationsstrecken

Beispiel:

Tabelle 7: Schutzbedarf der Netze/ Kommunikationsstrecken

Nr.	*Bezeichnung*	*Abh. Syst.*	*K1*	*K2*	*K3*	*K4*	*K5*
K001	*Client-LAN*	*C001, C002, C003*	*X*	*X*	*X*		

Bedeutung der Kategorien

- K1 = Außenverbindung
- K2 = hohe Vertraulichkeit
- K3 = hohe Integrität
- K4 = hohe Verfügbarkeit
- K5 = keine Übertragung

4.5.4 Schutzbedarf der Räume und Gebäude

Beispiel:

Tabelle 8: Schutzbedarf der Räume und Gebäude

Nr.	*Bezeichnung*	*Anh. Syst.*	*Grundwert*	*Schutzbedarf*	*Begründung*
G001	*Hauptgebäude*	*C001, C002, C003*	*VT*	*hoch*	*Maximumprinzip*
			IN	*normal*	*Maximumprinzip*
			VF	*normal*	*Verteilungseffekt, da Redundanz vorhanden*

5 MODELLIERUNG NACH IT-GRUNDSCHUTZ

Für die Definition der im betrachteten Informationsverbund umzusetzenden IT-Sicherheitsmaßnahmen werden die IT-Grundschutz-Kataloge des BSI verwendet. Diese sind nach dem IT-Grundschutz-Schichtenmodell (siehe Abbildung 5) in die folgenden Schichten unterteilt:

- B 1: Übergreifende Aspekte der Informationssicherheit
- B 2: Sicherheit der Infrastruktur
- B 3: Sicherheit der IT-Systeme
- B 4: Sicherheit im Netz
- B 5: Sicherheit in Anwendungen

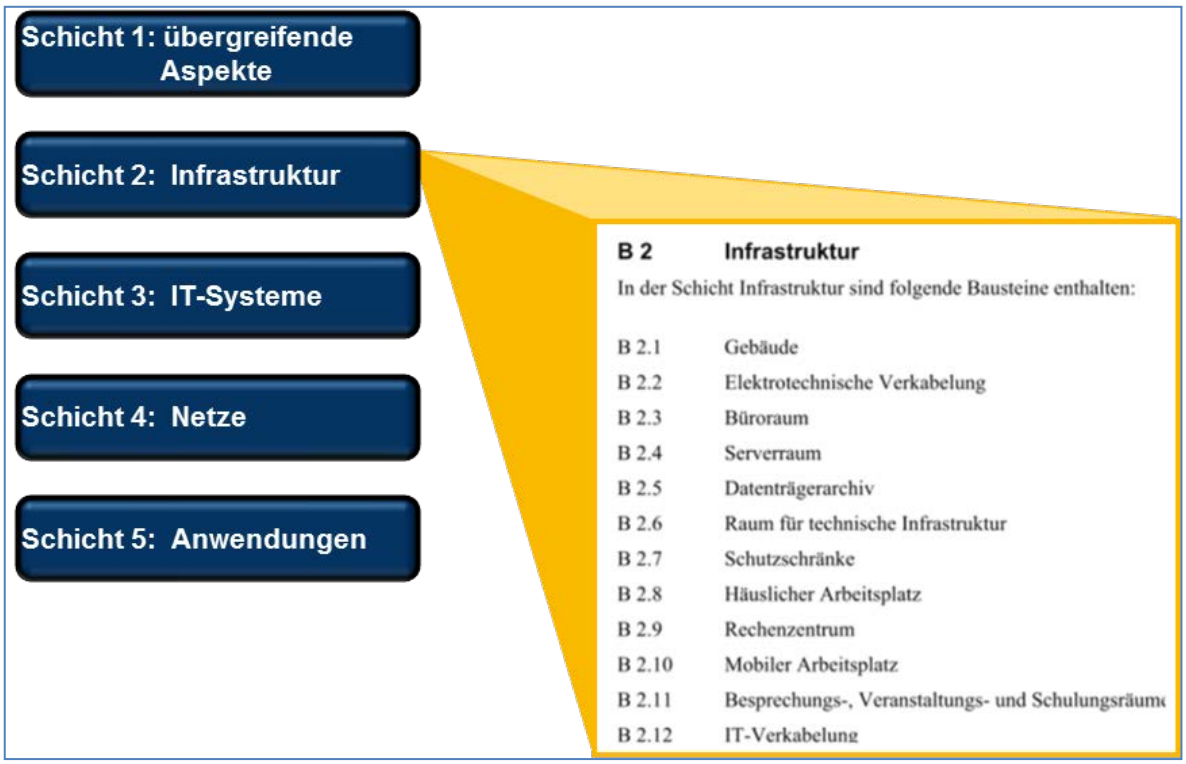

Abbildung 4: Auswahl der Bausteine aus dem IT-Grundschutzkatalog

Für den betrachteten Informationsverbund gilt es, die relevanten Bausteine auszuwählen, auf deren Basis im weiteren Verlauf mögliche Sicherheitsmaßnahmen definiert werden.

Generell wird die Auswahl der Bausteine von zwei Faktoren bestimmt, die gemeinsam in die Betrachtung einbezogen werden müssen:

- Eine Reihe von Bausteinen wird durch die Methodik des IT-Grundschutzes zwangsweise, ohne Bezugnahme auf die Gegebenheiten der hier durchgeführten Untersuchung, vorgeschrieben (siehe Pflichtbausteine beschrieben in den IT-Grundschutzkatalogen).

- Die restlichen Bausteine werden spezifisch gewählt, um spezielle Aspekte des betrachteten Informationsverbundes zu modellieren. Ein Verzicht auf einen dieser Bausteine hätte zur Folge, dass die durch diese Bausteine behandelten Aspekte nicht oder nur unvollständig dargestellt würden, so dass sich lokale Fehler und/oder Sicherheitslücken ergeben können (siehe Pflichtbausteine beschrieben in den IT-Grundschutzkatalogen).

5.1 Auswahl der relevanten IT-Grundschutz-Bausteine

Einen Überblick über die ausgewählten Bausteine mit der Zuordnung zu den Zielobjekten gibt Tabelle 10. Generell gibt es unterschiedliche Typen von Grundschutzbausteinen. Zum einen gibt es Pflichtbausteine, die immer anzuwenden sind (siehe „Pflicht“ in Tabelle 10). Weitere Bausteine müssen angewendet werden, wenn eine bestimmte Bedingung erfüllt ist (siehe „Ja“ in Tabelle 10).

Diese Bedingungen gemäß BSI IT-Grundschutz-Kataloge werden im Dokument C6 Modellierungsvorschrift mitgeliefert. Zudem gibt es auch Bausteine, die nur dann angewendet werden müssen, wenn eine spezielle Anwendung, ein spezielles IT-System, Art des Netzes oder Art der Infrastruktur eingesetzt wird.

5.2 Beispiel Modellierung

Beispiel:

Tabelle 9: Relevante Grundschutz-Bausteine

Baustein	***Relevanz***	***Zielobjekt(e)***	***Begründung***
Schicht 1 – Übergeordnete Aspekte			
B 1.0 Sicherheitsmanagement	*Pflicht*	*Informationsverbund*	
B 1.1 Organisation	*Pflicht*	*Informationsverbund*	
B 1.2 Personal	*Pflicht*	*Informationsverbund*	
B 1.3 Notfallmanagement	*ja*	*Informationsverbund*	
B 1.4 Datensicherungskonzept	*Pflicht*	*Informationsverbund*	
B 1.5 Datenschutz	*nein*	*-*	*Der Datenschutz-Baustein ist hier nicht zwingend anzuwenden, da der Datenschutz an anderer Stelle adressiert wird.*
B 1.6 Schutz vor Schadprogrammen	*ja*	*Informationsverbund*	
B 1.7 Kryptokonzept	*nein*		
B 1.8 Behandlung von Sicherheitsvorfällen	*ja*	*Informationsverbund*	
B 1.9 Hard- und Software Management	*Pflicht*	*Informationsverbund*	
B 1.10 Standardsoftware	*Pflicht*	*Informationsverbund*	
B 1.11 Outsourcing	*nein*	*-*	*nicht relevant, da kein Outsourcing vorhanden*
B 1.12 Archivierung	*nein*	*-*	*nicht relevant, da keine Archivierung vorhanden*
B 1.13 Sensibilisierung und Schulung zur Informationssicherheit	*Pflicht*	*Informationsverbund*	
B 1.14 Patch- und Änderungsmanagement	*ja*	*Informationsverbund*	
B 1.15 Löschen und Vernichten von Datenträgern	*Pflicht*	*Informationsverbund*	

B 1.16 Anforderungsmanagement	*Pflicht*	*Informationsverbund*	
Schicht 2 – Infrastruktur			
B 2.1 Allgemeines Gebäude	*Pflicht*	*Hannover (GEB 1)*	
B 2.1 Allgemeines Gebäude	*Pflicht*	*Berlin (GEB 2)*	
B 2.2 Elektrotechnische Verkabelung	*Pflicht*	*Hannover (GEB 1)*	
B 2.3 Büroraum / Lokaler Arbeitsplatz	*ja*	*BL 1.05 – BL 1.63*	
B 2.4 Serverraum	*ja*	*HN 1.01*	
B 2.5 Datenträgerarchiv	*ja*	*HN 1.16*	
B 2.6 Raum für technische Infrastruktur	*ja*	*HN 1.02*	
B 2.7 Schutzschränke	*nein*		
B 2.8 Häuslicher Arbeitsplatz	*nein*		
B 2.9 Rechenzentrum	*ja*	*BL 1.04, BL 1.64*	
B 2.10 Mobiler Arbeitsplatz	*nein*		
B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume	*ja*		
B 2.12 IT-Verkabelung	*Pflicht*	*Berlin (GEB 2)*	
Schicht 3 – IT-Systeme			
B 3.101 Allgemeiner Server	*Pflicht*	*Alle Server*	
B 3.102 Server unter Unix	*ja*	*Unix-Server (S4, S5, S6, S7, S9, S10, S11, S13, S14)*	
B 3.107 S/390- und zSeries-Mainframe	*nein*		
B 3.108 Windows Server 2003	*ja*	*Windows-Server (insbes. S1, S2, S8)*	
B 3.109 Windows Server 2008	*ja*	*Windows-Server (insbes. S1, S2, S8)*	
B 3.201 Allgemeiner Client	*Pflicht*	*Alle Clients*	
B 3.202 Allgemeines nicht vernetztes IT-System	*nein*		

B 3.203 Laptop	*nein*		
B 3.204 Client unter Unix	*nein*		
B 3.208 Internet-PC	*nein*		
B 3.209 Client unter Windows XP	*ja*		
B 3.210 Client unter Windows Vista	*nein*		
B 3.211 Client unter Mac OS X	*nein*		
B 3.212 Client unter Windows 7	*nein*		
B 3.301 Sicherheitsgateway (Firewall)	*ja*	*N1, N2*	
B 3.302 Router und Switches	*ja*	*N3 – N10*	
B 3.303 Speichersysteme und Speichernetze	*ja*		
B 3.304 Virtualisierung	*nein*		
B 3.305 Terminalserver	*nein*		
B 3.401 TK-Anlage	*ja*	*Informationsverbund*	
B 3.402 Faxgerät	*nein*		
B 3.404 Mobiltelefon	*ja*	*Informationsverbund*	
B 3.405 PDA	*ja*	*Informationsverbund*	
B 3.406 Drucker, Kopierer und Multifunktionsgeräte	*Pflicht*	*Informationsverbund*	
Schicht 4 – Netze			
B 4.1 Heterogene Netze	*hoher Schutzbedarf*	*Standort Außendorf*	
B 4.2 Netz- und Systemmanagement	*hoher Schutzbedarf*	*Standort Außendorf*	
B 4.3 Modem	*nein*		
B 4.4 VPN	*häufig fehleranfällig*	*VPN-Verbindung*	
B 4.5 LAN-Anbindung eines IT-Systems über ISDN	*nein*		
B 4.6 WLAN	*nein*		

B 4.7 VoIP	*nein*		
B 4.8 Bluetooth	*ja*	*Informationsverbund*	
Schicht 5 – Anwendungen			
B 5.2 Datenträgeraustausch	*ja*	*Informationsverbund*	
B 5.3 Groupware	*ja*	*Informationsverbund*	
B 5.4 Webserver	*ja*	*A008, A009*	
B 5.5 Lotus Notes/Domino	*nein*		
B 5.6 Faxserver	*nein*		
B 5.7 Datenbanken	*ja*	*A010, A012*	
B 5.8 Telearbeit	*ja*	*Informationsverbund*	
B 5.9 Novell eDirectory	*nein*		
B 5.12 Microsoft Exchange/Outlook	*ja*	*A005*	
B 5.13 SAP System	*ja*	*A007, A008*	
B 5.14 Mobile Datenträger	*Pflicht*	*Informationsverbund*	
B 5.15 Allgemeiner Verzeichnisdienst	*ja*	*A001*	
B 5.16 Active Directory	*ja*	*A001*	
B 5.17 Samba	*nein*		
B 5.18 DNS-Server	*ja*		
B 5.19 Internet-Nutzung	*ja*	*Informationsverbund*	
B 5.20 OpenLDAP	*nein*		
B 5.21 Webanwendungen	*nein*		
B 5.22 Protokollierung	*nein*		

6 BASIS-SICHERHEITSCHECK

Der Basis-Sicherheitscheck ist ein Organisationsinstrument, welches einen schnellen Überblick über das vorhandene Sicherheitsniveau bietet. Mit Hilfe von Interviews wurde der Status quo des bestehenden Informationsverbunds in Bezug auf den Umsetzungsstatus für jede relevante Maßnahme mit „entbehrlich“, „ja“, „teilweise“ oder „nein“ erfasst (siehe Abbildung 5).

Durch die Identifizierung von noch nicht oder nur teilweise umgesetzten Maßnahmen wurden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Geschäftsprozesse und der Informationstechnik aufgezeigt. Die Dokumentation aller nicht oder nur teilweise umgesetzten Maßnahmen befindet sich im Software-Tool bzw. im Anhang dieses IT-Sicherheitskonzeptes.

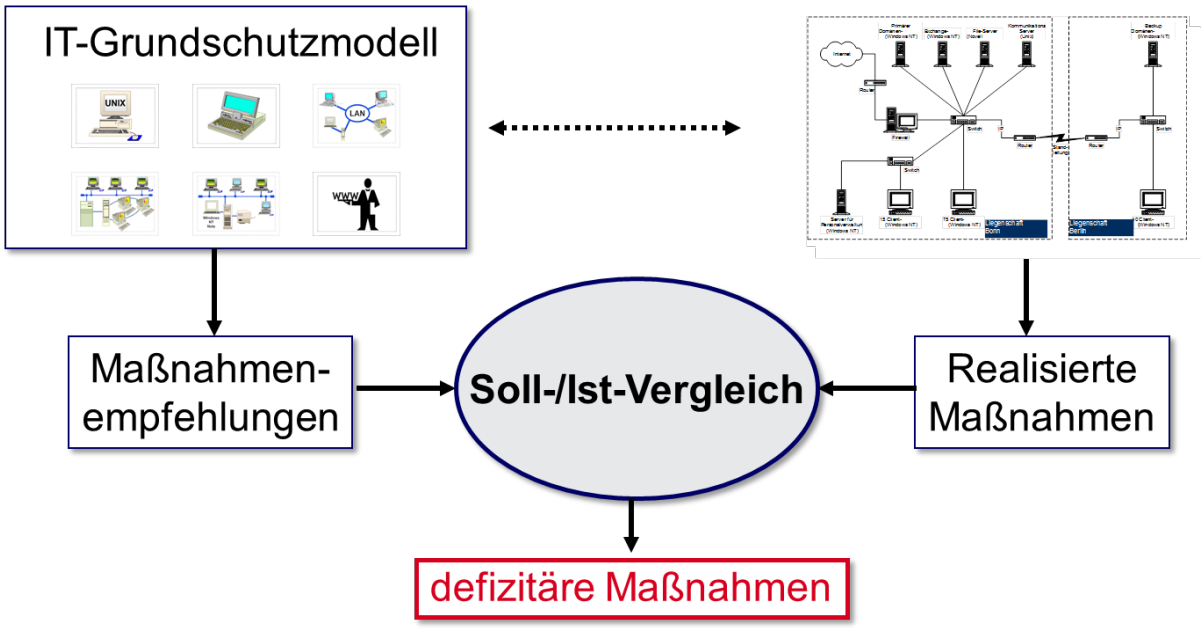

Abbildung 5: Der Basis-Sicherheitscheck zeigt mittels Soll-/Ist-Vergleich Defizite auf Maßnahmen der IT-Grundschutz-Kataloge haben verschiedene Wertigkeiten.

Tabelle 10: Die Siegelstufen geben eine Priorität der Maßnahmenumsetzung vor

Kennzeichnung	**Bedeutung**
A (Einstieg)	Unabdingbare Standardsicherheitsmaßnahmen; die Umsetzung ist für alle drei Stufen der IT-Grundschutz-Qualifizierung erforderlich.
B (Aufbau)	Wichtigste Standardsicherheitsmaßnahmen; die Umsetzung ist für die Aufbaustufe und für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz erforderlich.

Kennzeichnung	Bedeutung
C (Zertifikat)	Diese Maßnahmen sind für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz darüber hinaus erforderlich.
Z (zusätzlich)	Die Umsetzung dieser zusätzlichen Sicherheitsmaßnahmen sollte zur Steigerung der Informationssicherheit erfolgen (zum Beispiel bei hohem Schutzbedarf), ist jedoch zur Qualifizierung nach IT-Grundschutz nicht erforderlich.
W (Wissen)	Diese Maßnahmen dienen der Vermittlung von Grundlagen und Kenntnissen, die für das Verständnis und die Umsetzung der anderen Maßnahmen hilfreich sind. Sie müssen weder für ein Auditor-Testat noch für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz geprüft werden.

6.1 Beispiel Basis-Sicherheitscheck

Beispiel:

Tabelle 11: Defizitare Maßnahmen

Baustein	***Maßnahme***	***Bemerkung (T – teilweise, N – nein)***
B 1.6 Schutz vor Schadprogrammen	*M 4.84 Nutzung der BIOS-Sicherheitsmechanismen (A)*	*(T) Ein BIOS-Passwort ist nicht flächendeckend vergeben. Bei neuen Installationen wird dies durchgängig gemacht, so dass diese Maßnahme im Laufe der Zeit immer weiter umgesetzt sein wird.*
B 1.8 Behandlung von Sicherheitsvorfällen	*M 6.67 Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle (Z)*	*(T) Spezielle Detektionsmaßnahmen (IDS, IPS) kommen nicht zum Einsatz. Die Auswertung von Protokollen erfolgt durch die einzelnen Teilthemen (Server, Clients, Netzwerk etc.) und wird ggf. in die Lagebesprechung - und damit zum IT-SiBe - berichtet.*
B 1.9 Hard- und Software-Management	*M 4.84 Nutzung der BIOS-Sicherheitsmechanismen (A)*	*(T) Ein BIOS-Passwort ist nicht flächendeckend vergeben. Bei neuen Installationen wird dies durchgängig gemacht, so dass diese Maßnahme im Laufe der Zeit immer weiter umgesetzt sein wird.*
B 1.9 Hard- und Software-Management	*M 5.150 Durchführung von Penetrationstests (Z)*	*(T) Penetrationstests werden sporadisch gemacht. Wurde längere Zeit u. a. wegen der Unsicherheit mit "Hacker-Paragraf" nicht gemacht. Sollte nun aber wieder angegangen werden.*
B 1.9 Hard- und Software-Management	*M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation (Z)*	*(T) Verschlüsselung wird fallweise in den Bereichen, wo es sinnvoll oder erforderlich ist, verwendet. Bei Einwahlverbindungen (VPN) wird IPSec verwendet. Bei internen Netzwerkübergängen wird mittelfristig eine Verschlüsselung mittels Hardwareboxen eingeführt.*
B 1.14 Patch- und Änderungsmanagement	*M 2.429 Erfolgsmessung von Änderungsanforderungen (Z)*	*(T) Mit der vollständigen Einbindung der Server und Clients in WSUS und dem damit verbundenen Rollout-Prozess über mehrere Schritte mit Zwischentests wird eine implizite Erfolgsmessung umgesetzt sein.*

B 2.4 Serverraum	*M 1.31 Fernanzeige von Störungen (Z)*	*(T) USV-Störungen der Haus-Anlage werden zum Leitstand gemeldet. Die Störungsanzeige vor der Lampertz-Zelle wird täglich kontrolliert. Aus dem Serverraum werden keine Störungen weitergemeldet.*
B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume	*M 2.204 Verhinderung ungesicherter Netzzugänge (A)*	*(N) In den Besprechungsräumen werden externe Gäste derzeit uneingeschränkt im Etagen-LAN zugelassen. Eine Einführung von Radius basierter Port-Security (NAC bzw. NAP) ist noch für 2015 geplant (siehe Netzwerkkonzept).*
B 3.101 Allgemeiner Server	*M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (A)*	*(T) Patches werden nur sporadisch ausgerollt. Derzeit wird ein WSUS-System zur Patch-Bereitstellung (sowohl für Clients als auch für Server) umgesetzt. Das Konzept zum Patchmanagement ist bereits vorhanden.*
B 3.301 Sicherheitsgateway (Firewall)	*M 5.71 Intrusion Detection und Intrusion Response Systeme (Z)*	*(N) Intrusion Detection und Intrusion Response Systeme sind nicht installiert. Es sollte geprüft werden, in wieweit und welche Art von IDS bzw. IPS einsetzbar sind.*

7 ERGÄNZENDE SICHERHEITSANALYSE

Die Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bieten im Normalfall einen angemessenen und ausreichenden Schutz. Bei hohem oder sehr hohem Schutzbedarf sind jedoch zusätzliche oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich. Dies gilt auch, wenn besondere Einsatzbedingungen vorliegen oder wenn Komponenten verwendet werden, die nicht mit den existierenden Bausteinen der IT-Grundschutz-Kataloge abgebildet werden können. Hierzu ist zunächst im Rahmen einer ergänzenden Sicherheitsanalyse zu entscheiden, ob für die jeweils betroffenen Bereiche eine Risikoanalyse durchgeführt werden muss.

Die ergänzende Sicherheitsanalyse stellt sicher, dass die nicht (vollständig) abgedeckten Risiken ermittelt werden. Solche Risiken sind insbesondere dann wahrscheinlich, wenn

- Komponenten mit hohem oder sehr hohem Schutzbedarf existieren oder
- Zielobjekte nur unzureichend durch IT-Grundschutzbausteine abgedeckt sind oder
- Zielobjekte in Einsatzszenarien betrieben werden, die im IT-Grundschutz nicht vorgesehen sind.

Bei allen Zielobjekten, für die nicht (vollständig) abgedeckte Risiken identifiziert wurden, muss eine Entscheidung herbeigeführt werden, ob dieses Risiko weiter zu betrachten ist.

Die folgende Tabelle 13 zeigt diejenigen Objekte, für die im Rahmen der erweiterten Sicherheitsanalyse entschieden wurde, dass keine erweiterte Risikoanalyse durchzuführen ist. Die Entscheidung muss nachvollziehbar begründet werden.

Beispiel:

Tabelle 12: Ergebnis der ergänzenden Sicherheitsanalyse

Zielobjekte	***Begründung gegen die Risikoanalyse***
A220 IT-Betrieb allgemein	*Da es sich hierbei nicht um eine Anwendung im Sinne von Software handelt, reicht es aus, die Risikoanalyse für die zugeordneten IT-Systeme durchzuführen.*
A480 Gebäudeleittechnik	*Da es sich hierbei nicht um eine Anwendung im Sinne von Software handelt, reicht es aus, die Risikoanalyse für die zugeordneten IT-Systeme durchzuführen.*
A485 Betrieb TK-Anlagen	*Da es sich hierbei nicht um eine Anwendung im Sinne von Software handelt, reicht es aus, die Risikoanalyse für die zugeordneten IT-Systeme durchzuführen.*
A900 Personalverwaltung	*Die Anwendung wird extern durch EXTERN betrieben. Die ergänzende Risikoanalyse ist daher nicht notwendig.*
A903 CMS und Web (EXTERN)	*Die Anwendung wird extern durch EXTERN betrieben. Die ergänzende Risikoanalyse ist daher nicht notwendig.*
C01 Client in der IT-Abteilung	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit und Integrität. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
C09 Client in der Personalabteilung	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit und Integrität. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
N01 Backbone-Switche	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit und Integrität. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
N02 Switche LAN	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit und Integrität. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
N03 Switche DMZ	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit und Integrität. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*

Zielobjekte	*Begründung gegen die Risikoanalyse*
N04 Router DSL Zugang	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit und Integrität. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
N05 Router MPLS-Netze	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit und Integrität. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
K00 Internet	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit und Integrität. Da aber kein direkter Einfluss auf die Vertraulichkeit und Integrität im Internet möglich ist, kann auf eine ergänzende Risikoanalyse verzichtet werden.*
K10 WLAN	*Hoher Schutzbedarf nur bezüglich Integrität. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
S721 POP3-Proxy	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
S806 Printserver	*Hoher Schutzbedarf nur bezüglich Vertraulichkeit. Da aber keine vertraulichen Daten lokal gespeichert werden, sind die Standardmaßnahmen ausreichend. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
T04 Smart Phone	*Smart Phone ist bereits für hohen Schutzbedarf ausgelegt. Auf eine ergänzende Risikoanalyse kann daher verzichtet werden.*
U01 Drucker Standard Netzwerk	*Normale Standard-Netzwerkdrucker haben keine Permanent-Speicher, in denen kontinuierlich Informationen gesammelt werden.*

Abkürzungsverzeichnis

Objekte im Modell

Abkürzung	Erläuterung
Axxx	Anwendungen
Cxx	IT-Systeme / Clients
Sxxx	IT-Systeme / Speicher
Dxx	IT-Systeme / Speichersysteme (SAN, NAS)
Nxx	IT-Systeme / Netzwerkkomponenten (Router, Switches, Krypto-Boxen)
Txx	IT-Systeme / TK-Anlagen, Mobiltelefone, PDAs
Uxx	IT-Systeme / Drucker, Kopierer, Multifunktionsgeräte
Kxx	Kommunikationsverbindungen
Gxx	Infrastruktur / Gebäude
Rxx	Infrastruktur / Räume

8 RISIKOANALYSE

Ziel der Risikoanalyse nach dem BSI-Standard 100-3 (siehe [Ref-03] und [Ref-04]) ist, die vorhandenen Risiken durch eine Risikobehandlung auf ein verträgliches/akzeptables Maß (Restrisiko) zu reduzieren.

Die Risikoanalyse besteht aus den folgenden Schritten:

- Erstellen des Gefährdungskataloges
- Darstellen der Ergebnisse der Risikoanalyse
- Verantwortung der Organisationsleitung

8.1 Erstellen des Gefährdungskataloges

Im ersten Schritt werden die relevanten Risiken für das Zielobjekt herausgearbeitet. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen, die so genannten elementaren Gefährdungen (siehe Anlage C7 Gefährdungskatalog) verwendet.

Nicht alle potentiell möglichen Gefährdungen, welche im Gefährdungskatalog benannt sind, müssen untersucht werden, insbesondere wenn Gefährdungen durch eine besondere Technologie, ein spezielles Produkt oder einen besonderen Anwendungsfall bedingt sind oder in üblichen Einsatzszenarien nur unter sehr speziellen Voraussetzungen zu einem Schaden führen oder sehr gute Fachkenntnisse, Gelegenheiten und Mittel eines Angreifers voraussetzen. Für die IT-Sicherheit relevante Gefährdungen sind solche, die zu einem nennenswerten Schaden führen können und die im vorliegenden Anwendungsfall und Einsatzumfeld realistisch sind.

Deshalb werden in einem zweiten Schritt alle Gefährdungen gestrichen, welche außerhalb des Zielobjektes existieren und nicht durch Sicherheitsmaßnahmen des Zielobjektes beeinflusst werden können. Beispiele dafür sind Gefährdungen wie Feuer und Wasser oder Einfluss durch Großereignisse im Umfeld.

8.2 Ergebnisse der Risikoanalyse

Aus den verbleibenden Gefährdungen können sich Risiken ergeben. Deshalb werden abschließend die verbleibenden Gefährdungen mit den bisherigen bereits umgesetzten Maßnahmen auf eine ausreichende Risikominimierung hin untersucht und bewertet.

Die Prüfung erfolgt anhand des IT-Sicherheitskonzepts und folgender Prüfkriterien:

- **Mechanismenstärke** - Wirken die in den Standard-Sicherheitsmaßnahmen empfohlenen Schutzmechanismen der jeweiligen Gefährdung ausreichend stark entgegen?
- **Zuverlässigkeit** - Können die vorgesehenen Sicherheitsmechanismen nicht zu leicht umgangen werden?
- **Vollständigkeit** - Bieten die Standard-Sicherheitsmaßnahmen Schutz gegen alle Aspekte der jeweiligen Gefährdung?

Immanent werden bei diesem Vorgehen die einzelnen Risiken mit ihrer Schadenshöhe und Eintrittswahrscheinlichkeit in einer Risikomatrix (vgl. Tabelle 14) gruppiert.

Tabelle 13: Risikomatrix

Eintrittswahr-scheinlichkeit	**Hoch**	Mittleres Risiko	Hohes Risiko	Hohes Risiko
	Mittel	Niedriges Risiko	Mittleres Risiko	Hohes Risiko
	Niedrig	Niedriges Risiko	Niedriges Risiko	Mittleres Risiko
		Niedrig	**Mittel**	**Hoch**
		Schadenshöhe		

Risiken, die in der Risikomatrix im „roten Bereich“ liegen, können Auswirkungen haben, die nicht einfach tolerierbar sind. Entsprechend müssen Maßnahmen für die Risikobehandlung definiert werden, die

- die Wahrscheinlichkeit des Eintretens oder
- die Schadenshöhe bei einem Eintreten

verringern.

Liegt ein Risiko vor, können verschiedene Strategien bei der Auswahl der Maßnahmen zugrunde gelegt werden:

A) **Risiko-Reduktion** durch weitere Sicherheitsmaßnahmen: Die verbleibende Gefährdung wird beseitigt, indem eine oder mehrere ergänzende Sicherheitsmaßnahmen erarbeitet und umgesetzt werden, die der Gefährdung hinreichend entgegenwirken und damit auch das daraus resultierende Risiko minimieren.

B) **Risiko-Vermeidung** durch Umstrukturierung: Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko wird durch Umstrukturierung beseitigt.

C) **Risiko-Übernahme:** Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko werden akzeptiert.

D) **Risiko-Transfer:** Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko wird durch eine Versicherung oder durch andere Vertragsgestaltung (Outsourcing) übertragen.

Die dokumentierte Durchführung der Risikoanalyse gemäß dem BSI Standard 100-3 ist der Anlage C8 Risikoanalyse-Template zu entnehmen. Im Folgenden werden pro verbleibende Gefährdung:

- geeignete Maßnahmen aufgelistet
- Risiken abgeleitet
- Risiken anhand der Qualität des Maßnahmen-Bündels bewertet

Hinweis für zusätzliche Maßnahmen: Z Maßnahmen, Maßnahmen mit „Umsetzung entbehrlich“, „nicht umgesetzt“ und abgeleitet Maßnahmen in Risikobehandlung aufnehmen (A, B, C, D)

Die Tabelle 16 zeigt eine relevante Gefährdung und die resultierenden Risiken, sowie Maßnahmen zur Minimierung der Restrisiken.

8.3 Verantwortung der Organisationsleitung

Die Organisationsleitung entscheidet, dass bestimmte Risiken bekannt sind und getragen werden. Dies wird mit Datum und Unterschrift bestätigt (siehe Tabelle 17).

8.4 Beispiel Risikoanalyse

8.4.1 Erstellen des Gefährdungskatalogs

In der folgenden Tabelle 15 werden die relevanten Gefährdungen für die Anwendung „E-Mail“ aufgelistet. E-Mail hat einen Schutzbedarf von höher als „normal“ nur bei Vertraulichkeit (VT) und Verfügbarkeit (VF).

Beispiel:

Tabelle 14: Auflistung der relevanten elementaren Gefährdungen

Nr.	***Bezeichnung der elementaren Gefährdung***	***Sicherheitsziele***
G 0.15	*Abhören*	*VT*
G 0.16	*Diebstahl von Geräten, Datenträgern oder Dokumenten*	*VT, VF*
G 0.25	*Ausfall von Geräten und Systemen*	*VF*
G 0.28	*Software-Schwachstellen oder -Fehler*	*VT, IN, VF*
G 0.29	*Verstoß gegen Gesetze oder Regelungen*	*VT, IN, VF*
G 0.30	*Unberechtigte Nutzung oder Administration von Geräten und Systemen*	*VT, IN, VF*
G 0.31	*Fehlerhafte Nutzung oder Administration von Geräten und Systemen*	*VT, IN, VF*
G 0.32	*Missbrauch von Berechtigungen*	*VT, IN, VF*
G 0.36	*Identitätsdiebstahl*	*VT, IN, VF*
G 0.40	*Verhinderung von Diensten (*Denial of Service*)*	*VF*
G 0.45	*Datenverlust*	*VF*

8.4.2 Erarbeiten der Risiken

Beispiel:

Tabelle 15: Darstellung der Restrisiken: Switch XY

Gefährdung	G 0.25 Ausfall von Geräten oder Systemen
Vorhandene Maßnahmen	M 1.043 Gesicherte Aufstellung aktiver Netzkomponenten M 2.277 Funktionsweise eines Switches M 2.281 Dokumentation der Systemkonfiguration von Routern und Switches M 2.282 Regelmäßige Kontrolle von Routern und Switches M 4.204 Sichere Administration von Routern und Switches M 4.205 Protokollierung bei Routern und Switches M 6.091 Datensicherung und Recovery bei Routern und Switches M 6.092 Notfallvorsorge bei Routern und Switches
Risiko	Ausfall von IT-Systemen, Gefährdung durch Reinigungs- oder Fremdpersonal
Bewertung	Die bereits umgesetzten Sicherheitsmaßnahmen reduzieren einen Großteil der Risiken. Der Ausfall von Systemen sowie die Gefährdung durch Reinigungs- oder Fremdpersonal und die somit bestehende Möglichkeit der Mutwilligen Zerstörung von Geräten bildet ein Risiko, welches durch die derzeitigen Maßnahmen nicht abgedeckt wird.
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** Schaffung von Redundanz durch Umsetzung der Sicherheitsmaßnahme „M 2.314 Verwendung von hochverfügbaren Architekturen für Server“. **B. Risikovermeidung** **C. Risikoübernahme** **D. D. Risikotransfer**

8.4.3 Erklärung der Organisationsleitung

Beispiel:

Tabelle 16: Erklärung der Organisationsleitung über Kenntnis der Risiken

Hiermit wird seitens der kirchlichen Organisation bestätigt, dass die zuvor genannten Risiken bekannt sind und – bis zu ihrer etwaigen Abstellung – getragen werden.

Hannover, den 2.6.2014	*Max Mustermann*
_____	_____
Ort, Datum	Unterschrift Max Mustermann

9 MANAGEMENTBERICHT

Im Managementbericht werden die Ergebnisse des IT-Sicherheitskonzepts dargestellt.

9.1 Beispiel Managementbericht

Beispiel:

Das vorliegende IT-Sicherheitskonzept für die Mustereinrichtung beschreibt den Status der IT-Sicherheit und gibt Handlungsanweisungen zur weiteren Senkung der Risiken. Die Untersuchung des aktuellen Status wurde nach Vorgaben des BSI durchgeführt und mit Hilfe des Tools [SOFTWARE] dokumentiert. Nach der Erfassung der Anforderungen an die IT wurde anhand des Baustein-Katalogs des BSI die Maßnahmenumsetzung geprüft. Einen groben Überblick über das Ergebnis gibt die folgende Abbildung 7*.*

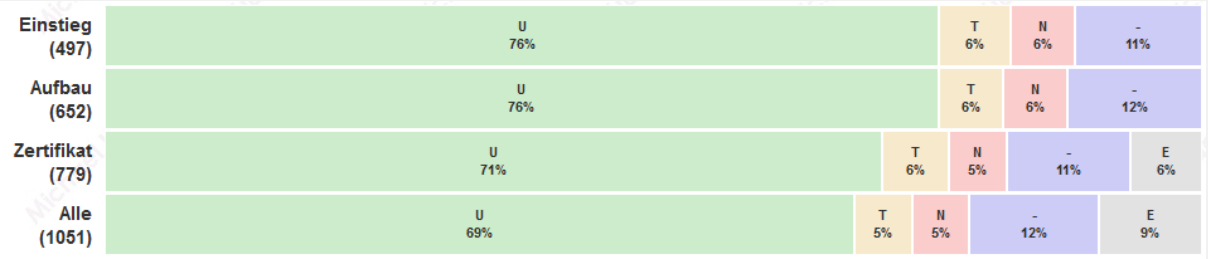

Abbildung 6: Umsetzungsgrad der Maßnahmen

Insgesamt wurden 1051 Maßnahmen aus dem IT-Grundschutz-Katalogen untersucht. Davon sind 69% umgesetzt, 5% teilweise umgesetzt und 5% nicht umgesetzt. 12% der Maßnahmen sind bei der Mustereinrichtung entbehrlich. Bezogen auf die zertifizierungsrelevanten Maßnahmen ergibt sich sogar ein Umsetzungsgrad von 71%. Die folgende Abbildung 8 *zeigt den Umsetzungsgrad nach den einzelnen Schichten des IT-Grundschutzes.*

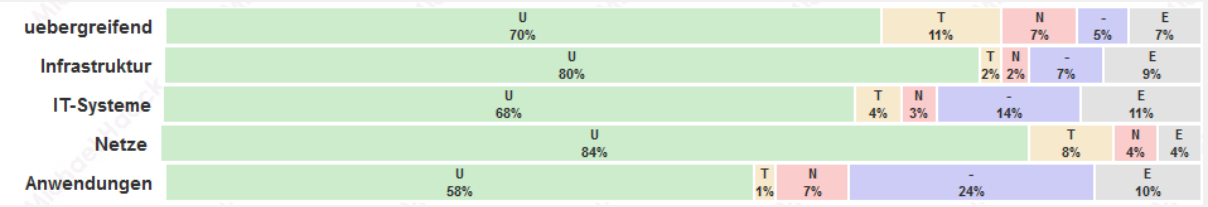

Abbildung 7: Umsetzungsgrad der Maßnahmen nach Schichten

Wesentliche Mängel

- Eine gesamthafte aktuelle Liste aller IT-Systeme mit deren Einsatzzweck ist nicht vorhanden

Der Gesamtstatus der IT-Sicherheit ist als befriedigend zu bewerten. Der definierte Informationsverbund erfüllt die Voraussetzungen für eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz noch nicht.

REFERENZZDOKUMENTE (EXTERN)

[Ref-01] BSI-Standard 100-1, Managementsysteme für Informationssicherheit, Version 1.5, Mai 2008

[Ref-02] BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 2.0, Mai 2008

[Ref-03] BSI-Standard 100-3, Risikoanalysen auf der Basis von IT-Grundschutz, Version 2.5, Mai 2008

[Ref-04] Ergänzung zum BSI-Standard 100-3, Version 2.5, August 2011