Ergebnisbericht der Arbeitsgruppe Muster IT-Sicherheitskonzepte

Evangelische Kirche
in Deutschland

Herausgeber
Evangelische Kirche in Deutschland (EKD)
Herrenhäuser Str. 12 – 30419 Hannover
Telefon: 0800/5040602
Email: info@ekd.de
www.ekd.de
April 2016
Download: www.ekd.de/EKD-Texte/muster_IT_Sicherheitskonzepte.html
Weitere Informationen: Koordinierungsstelle-IT@ekd.de
Bildnachweis: Getty Images/iStock

Verantwortlich: Arbeitsgruppe Muster-IT-Sicherheitskonzepte
Mitglieder der Arbeitsgruppe:
Harald Aulenbacher (Kirchenamt der EKD), Stefan Haas (Evangelische Landeskirche Baden), Lars Karrock, Evangelische Kirche in Hessen und Nassau), Andrea Niemeyer (Kirchenamt der EKD), Daniel Piasecki (Evangelisch-Lutherische Kirche Norddeutschland), Fabian Spier (Evangelisch-luterhische Landeskirche Hannover), Dr. Sascha Tönnies (Der Beauftragte für den Datenschutz der EKD) Michael Werker (Diakonie Schleswig-Holstein), Julian Wijnmaalen (Kirchenamt der EKD)

Begleitende Beratung:
HiSolutions AG, Bouchestraße 12 – 12435 Berlin
Telefon: 030/533 289-0
www.hisolutions.com
Email: info@hisolutions.com

Inhalt

Muster-IT-Sicherheitskonzept für mittlere und große Einrichtungen

Vorschläge für ein Schulungskonzept IT-Sicherheit

BDFI Musterformular

Tool-Unterstützung IT-Grundschutz

Schutzbedarfskategorien

Schutzbedarfsfestellung

Modellierungsvorschrift

Gefährdungskatalog

Risikoanalyse-Template

1. Ergebniszusammenfassung

1.1 Ausgangslage

Die Evangelische Kirche in Deutschland (EKD) mit ihren kirchlichen und diakonischen Einrichtungen verfügt in verschiedenen Bereichen über eine Vielzahl schützenswerter Daten, die zu einem beträchtlichen Teil auch eines hohen Schutzbedarfes bedürfen.

In der Vergangenheit hat sich die Evangelische Kirche bereits vielfach mit dem Schutz dieser Daten beschäftigt. Die Erkenntnisse sind in die auf der Synode 2012 der EKD verabschiedete Novellierung des Datenschutzgesetzes der EKD (DSG-EKD) eingeflossen. Diese ist seit dem 1. Januar 2013 in Kraft.

Mit dieser Novellierung wurde erstmals für alle kirchlichen Stellen die Verpflichtung zur Einhaltung der IT-Sicherheit festgelegt und normiert. Das DSG-EKD gilt unmittelbar für alle Gliedkirchen und teilweise, je nach deren Organisationsform, auch für die Werke und Einrichtungen der Diakonie. Bestandteil dieser Regelung ist es, dass für jede kirchliche Stelle ein IT-Sicherheitskonzept vorhanden sein muss. Zur Unterstützung dieses Prozesses stellt die EKD Muster-IT-Sicherheitskonzepte zur Verfügung.

Die nähere Ausgestaltung wird in einer Rechtsverordnung festgelegt, deren derzeit vorliegender abgestimmter Entwurf von der EKD unter Beteiligung gliedkirchlicher und diakonischer Vertreter unterschiedlicher Bereiche ausgearbeitet wurde. Die Muster-IT-Sicherheitskonzepte werden Bestandteil der Ratsverordnung, die im Jahr 2015 verabschiedet werden soll. Die Einhaltung dieser Zeitvorgaben geht einher mit der zurzeit erarbeiteten Erweiterung des kommunalen Datenaustausches im kirchlichen Meldewesen um das Modul Staat/Kirche (OSCI-XMeld-Verfahren). Die Aufnahme der Kirchen in dieses sichere und verlässliche Datenaustauschverfahren erfordert eine entsprechende kirchliche Regelung. Diese soll mit der Verordnung zur IT-Sicherheit geschaffen werden und baldmöglichst in Kraft treten.

In der Diakonie prüfen Wirtschaftsprüfer bereits im Rahmen der Jahresabschlussprüfung die IT-Systeme.

1.2 Vorgehensweise zur Entwicklung der Muster-IT-Sicherheitskonzepte

Die Mindestanforderungen der Muster-IT-Sicherheitskonzepte sind entsprechend der Ratsverordnung unter Berücksichtigung der örtlichen Gegebenheiten von den zuständigen kirchlichen Stellen einzuhalten. Diese sollen so rechtzeitig zur Verfügung gestellt werden, dass darauf zum Zeitpunkt der Erstellung der IT-Sicherheitskonzepte der einzelnen kirchlichen Stellen zurückgegriffen werden kann.

Für die Erarbeitung dieser Muster-IT-Sicherheitskonzepte hat das Kirchenamt der EKD eine Arbeitsgruppe gebildet. In dieser Gruppe sind neben der Kompetenz aus dem Bereichen IT und IT-Sicherheit der EKD, den Gliedkirchen und der Diakonie auch die mittlere Ebene eines Kirchenkreises sowie der Beauftragte für den Datenschutz der EKD vertreten. Die Arbeitsgruppe wird durch Vertreter der HiSolutions AG unterstützt.

Als spezialisiertes Beratungsunternehmen für Informationssicherheit und Datenschutz verfügt die HiSolutions AG über umfangreiche Erfahrungen und Experten auf diesem Gebiet. So ist die HiSolutions AG an den größten Grundschutzzertifizierungen mittels Vorbereitung oder Durchführung beteiligt gewesen. Mit der Erstellung mehrerer Standards und Bausteine für das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das Beratungshaus den IT-Grundschutz maßgeblich mit geprägt. Es werden neun zertifizierte IT-Grundschutz-Auditoren und sechs zertifizierte IS-Revisoren beschäftigt.

Aufgrund der Heterogenität der Einrichtungen in Kirche und Diakonie werden zwei unterschiedliche Muster für kleine sowie für mittlere und große kirchliche und diakonische Einrichtungen benötigt. Für die Erarbeitung der Inhalte wurden 3 Workshops durchgeführt. Dabei wurden, die im nachfolgenden Kapitel aufgeführten und in Kapitel 2 vertiefend beschriebenen Ergebnisse diskutiert und in jeweils finale Versionen überführt.

1.3. Struktur der Ergebnisdokumente

Folgende Ergebnisdokumente sind verfügbar:

Tabelle 1: Ergebnisdokumente

Beschreibung	Dokumentenname
Der vorliegende übergreifende Ergebnisbericht	Ergebnisbericht.pdf
Anlage A: Muster-IT-Sicherheitskonzept für kleine Einrichtungen	A_Muster klein.pdf
Anlage B: Muster-IT-Sicherheitskonzept für mittlere und große Einrichtungen	B_Muster groß.pdf
Anlage C1: Vorschläge für ein Schulungskonzept IT-Sicherheit	C1_Schulungskonzept.pdf
Anlage C2: BfDI Musterformular: „Dienstanweisung über die Nutzung elektronischer Kommunikations-systeme am Arbeitsplatz“	C2_Musterformular BfDI.pdf
Anlage C3: Tool-Unterstützung IT-Grundschutz	C3_Produktvorstellung-GS-Tool-Alternativen.pdf
Anlage C4: Abgestimmte Schutzbedarfskategorien	C4_Schutzbedarfskategorien.pdf
Anlage C5: Beispielhafte Schutzbedarfsfeststellung Personalwesen EKD Meldewesen EKD Finanzwesen EKD Patientendaten Diakonie	C5_Schutzbedarfsfeststellung.pdf
Anlage C6: Modellierungsvorschrift der IT-Grundschutz-Kataloge zur Anwendung von Bausteinen auf Informationsverbünde	C6_Modellierungsvorschrift.pdf
Anlage C7: Gefährdungskatalog zur Risikoanalyse nach BSI 100-3	C7_Gefährdungskatalog.pdf
Anlage C8: Template zur Durchführung einer Risikoanalyse nach BSI 100-3.	C8_Risikoanalyse-Template.pdf

Nachfolgendes Schaubild stellt die Abdeckung und die Anwendungsbereiche der Ergebnisdokumente dar.

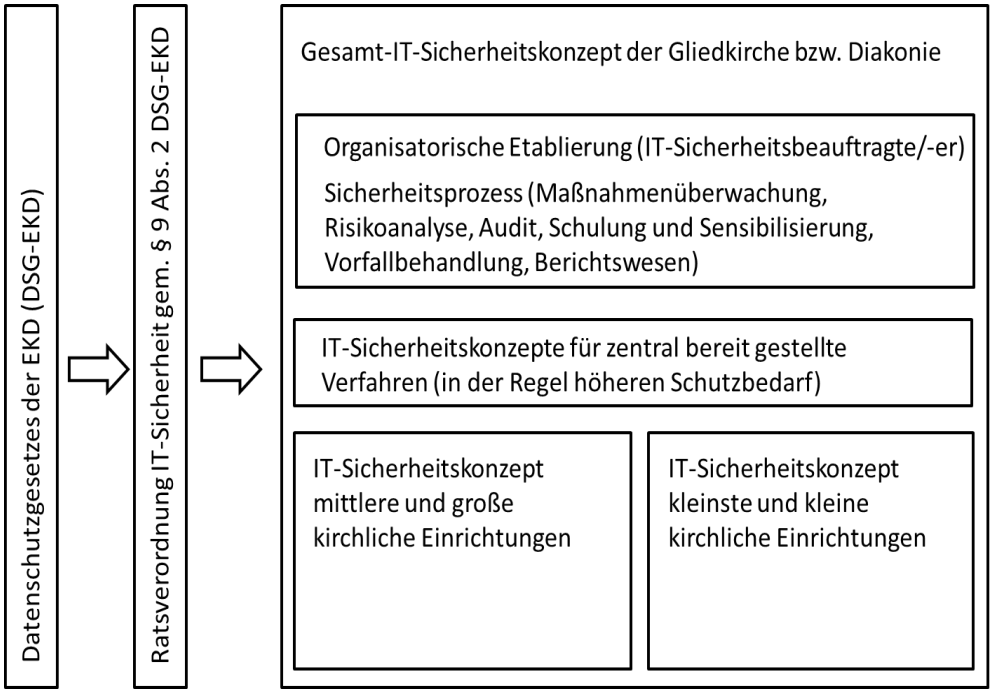


Abbildung 1: Gesamtabdeckung und Anwendung der Ergebnisdokumente

2. Leistungsbeschreibung

2.1 Muster-IT-Sicherheitskonzept kleine kirchliche Einrichtungen

Bei der Ausarbeitung dieses Musters war die Anforderung, den BSI-Grundschutz mit den bei diesen Einrichtungen vorhandenen Kapazitäten umzusetzen. 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.

Es ist aber unbedingt zu beachten, dass bei der Verarbeitung von Daten mit hohem und sehr hohem Schutzbedarf auch in kleinen Einrichtungen immer die Erstellung von IT-Sicherheitskonzepten gemäß dem Muster für mittlere und große Einrichtungen erforderlich ist.

Zunächst wurden auf Grund der in den BSI IT-Grundschutzkatalogen zu findenden Bausteine die relevanten Themengebiete für kleinste und kleine kirchliche Einrichtungen zusammengestellt. Danach wurde die Chance für die Anwendung vor Ort ohne das Vorhandensein sachkundigen Personals gemeinsam durch alle Anwesenden analysiert und im Ergebnis auf das Mindestmaß konsolidiert.

Ferner wurde der Vorschlag angenommen, am Ende des Muster-IT-Sicherheitskonzeptes eine Checkliste anzubieten, welche sowohl der eigenen Prüfung des Grades der Berücksichtigung aller gestellten Anforderungen vor Ort als auch, sofern in der jeweiligen kirchlichen Einrichtung gewünscht, die Möglichkeit eines minimalen Berichtswesens an die übergeordnete kirchliche Organisationseinheit bietet.

Im Ergebnis liegt ein Gesamtdokument vor, welches nach einer einleitenden Sensibilisierung die Anforderungen an ein Mindestmaß der IT-Sicherheit für die Zielgruppe benennt und eine Checkliste anbietet.

2.2 Muster-IT-Sicherheitskonzept mittlere und große kirchliche Einrichtungen

Mittlere und große Einrichtungen werden wie folgt definiert: diese Einrichtungen verfügen über eigenes geschultes IT-Personal oder Externe sowie 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. auch Dienstleistungen, die durch Outsourcing betrieben werden.

Darüber hinaus ist grundsätzlich immer nach dem Muster für mittlere und große kirchliche Einrichtungen vorzugehen, wenn eigenständig Daten mit hohem und sehr hohem Schutzbedarf verarbeitet werden.

Bei der Ausarbeitung dieses Musters war von vorn herein erkennbar, dass grundsätzlich die Vorgehensweise der BSI Standards 100-2 und 100-3 als Mindestmaß umzusetzen ist. Da dabei jedoch häufig eine Einstiegshürde vorhanden und nicht sofort das anzustrebende Ergebnis erkennbar ist, wurde in den Workshops ein Dokument als Muster-IT-Sicherheitskonzept mit jeweils erläuternden Beispielen und einer Kapitelstruktur des Vorgehens bei seiner Erstellung bereitgestellt.

2.3 „Bauplan“ Anwendung Muster-IT-Sicherheitskonzept mittlere und große kirchliche Einrichtungen

Der Bauplan ist ein Dokument, welches den Aufbau eines IT-Sicherheitskonzeptes grafisch darstellt.

2.4 Konzept zur Umsetzung von Schulung und Sensibilisierung

Um IT-Sicherheit erfolgreich umzusetzen sind Schulungen und Sensibilisierungen erforderlich. Nur auf diese Weise lässt sich langfristig eine Sicherheitskultur im Bereich der EKD, ihrer Gliedkirchen, gliedkirchlichen Zusammenschüsse, Diakonischen Werke und Einrichtungen etablieren. Dazu wurde ein Konzept erarbeitet, welches in Bezug auf die verschiedenen Zielgruppen, Empfehlungen zu Themen und Vorgehensweisen enthält und für die praktische Umsetzung auf allen Ebenen geeignet ist.

2.5 Präsentation mit einer Empfehlung zur Tool-Auswahl

Insbesondere bei der Umsetzung von IT-Sicherheitskonzepten in mittleren und großen kirchlichen Einrichtungen wird die Anwendung der Vorgehensweise nach den BSI Standards 100-2 und 100-3 oft hilfreich durch Werkzeuge unterstützt. Es wurde eine Gegenüberstellung der gängigen und geeigneten Tools mit den jeweiligen Leistungsmerkmalen erstellt.

2.6 Beispielhafte Schutzbedarfsfeststellung

Während der Workshops wurde für die Verfahren und Datenarten Meldewesen, Personalwesen, Finanzwesen und für Patientendaten der Diakonie eine Schutzbedarfsfeststellung beispielhaft durchgeführt.

Die Ergebnisse sind den Ergebnisdokumenten mit dem eindeutigen Vermerk „Muster“ hinzugefügt, da sie einen Überblick über die möglichen Ergebnisse einer Schutzbedarfsfeststellung illustrieren. Diese beispielhafte Schutzbedarfsfeststellung darf nicht ohne vorherige Überprüfung und Anpassung an die eigene Situation verwendet werden.

Muster-IT-Sicherheitskonzept für kleine Einrichtungen

1. Einleitung

Alle kirchlichen Einrichtungen[1] sind für IT-Sicherheit verantwortlich. Informations- und Kommunikationstechnik (IT) ist in heutiger Zeit ein unverzichtbares Instrument zur Erfüllung von Aufgaben kirchlicher Stellen im Bereich der evangelischen Kirchen und ihrer Diakonie. IT-Sicherheit stellt einen Teil der Informationssicherheit dar. Diese umfasst die Sicherheit von IT-Systemen und der darin gespeicherten Daten durch Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit).

Die Vorgaben des Datenschutzes sind im EKD-Datenschutzgesetz (DSG-EKD) in der Novellierung aus dem Jahre 2013 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").

Alle Beschäftigten sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten. [Bitte Verweis auf die Anlage der konkreten Landeskirche einfügen][2]

Alle Mitarbeitenden und sonstige relevante Personen (extern Beschäftigte und Projektmitarbeiter) werden systematisch und zielgruppengerecht zu Datenschutzfragen sensibilisiert und zum Umgang mit personenbezogenen Daten geschult.

Es sind technisch-organisatorische Verfahren gemäß § 9 Absatz 1 DSG-EKD zu entwickeln, um die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht in bestehende Bestandsverzeichnisse sicherzustellen.

Somit müssen auch die kleinen kirchlichen Einrichtungen Maßnahmen zur Informationssicherheit umsetzen. Mit dieser Richtlinie und der im Anhang enthaltenen Checkliste zur Informationssicherheit soll diesen Organisationen ein Werkzeug an die Hand gegeben werden. Dieses Dokument muss regelmäßig fortgeschrieben und mit der/dem zuständigen IT-Sicherheitsbeauftragte/-en abgestimmt werden. Es bietet sich an, die Regelungen und die Checkliste quartalsweise oder in kürzeren Intervallen, mindestens aber einmal im Jahr zu überprüfen und ggf. anzupassen. Hierbei muss man sich der Tatsache bewusst sein, dass IT-Sicherheit kein statischer Zustand ist, sondern sich in einem stetigen Prozess fortentwickelt.

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.

---

1 siehe § 1 Absatz 2 DSG-EKD

2 Gelbe Textpassagen in eckigen Klammern sind von der jeweiligen Einrichtung mit Angaben, die für ihren Geltungsbereich zutreffen, auszufüllen.

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.

2. Sensibilisierung der Mitarbeitenden

Besonders wichtig ist die Sensibilisierung aller relevanten Mitarbeitenden. Nur mit informierten und achtsamen Mitarbeitenden können Sicherheitsmaßnahmen wirksam umgesetzt und eventuelle Sicherheitsvorfälle rechtzeitig erkannt werden.

Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, müssen Maßnahmen zu dessen Behebung ergriffen werden. Häufig ist es notwendig, die betroffenen IT-Systeme oder Standorte zu isolieren, um die Auswirkung des Sicherheitsvorfalls einzudämmen. Die Behebung von Sicherheitsvorfällen muss ausführlich dokumentiert werden.

Ein Beispiel für eine Sensibilisierung der Mitarbeitenden „Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz“ befindet sich im Anhang C2 BFDI Musterformular.

3. Datensicherungskonzept

Computersysteme und Datenträger (z. B. Festplatten, Speicherkarten) können ausfallen oder manipuliert werden. Durch Verlust oder Veränderungen von gespeicherten Daten können mitunter gravierende Schäden verursacht werden. Durch regelmäßige Datensicherungen werden Schäden durch Ausfälle von Datenträgern, Schadsoftware oder Manipulationen an Datenbeständen nicht verhindert, deren Auswirkungen können aber minimiert werden.

Die zu sichernden Daten und Anwendungen (hauptsächlich dezentral) müssen aufgelistet und jeweils einem Verantwortlichen zugordnet werden.

Backup-Datenträger müssen einerseits im Bedarfsfall schnell verfügbar sein, andererseits sollten sie räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden. Somit sind sie auch bei Notlagen, wie z. B. Brand oder Hochwasser verfügbar.

Hinweis: Das zusätzliche Speichern auf einem vorzugsweise verschlüsselten USB-Stick könnte eine Datensicherung darstellen.

4. Schutz vor Schadprogrammen

Wenn IT-Systeme mit Schadsoftware (Viren, Würmer, Trojanische Pferde usw.) befallen werden, kann dies die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und der darauf gespeicherten Daten gefährden.

Es muss auf jedem IT-System (z. B. PC, Laptop) ein Viren-Schutzprogramm installiert werden. Automatische Updates müssen aktiviert sein. Dabei muss sichergestellt werden, dass auch die mobilen Endgeräte ausreichend geschützt sind.

Infizierte IT-Systeme müssen unverzüglich von allen Datennetzen getrennt und dürfen bis zur vollständigen Bereinigung nicht mehr produktiv genutzt werden.

Auf allen IT-Systemen müssen für die Betriebssysteme sowie für alle installierten Treiber und Programme zeitnah die jeweils hierfür veröffentlichten sicherheitsrelevanten Updates und Patches eingespielt werden. Dies gilt besonders für Programme, mit denen auf Fremdnetze zugegriffen wird (z. B. Webbrowser).

5. Regelungen für Hard- und Software

Für den sicheren Einsatz von IT-Systemen und IT-Anwendungen ist es erforderlich, dass Abläufe und Vorgänge, die diese IT-Systeme berühren, so gestaltet werden, dass das angestrebte Niveau der Informationssicherheit erreicht bzw. beibehalten wird.

Alle Mitarbeitenden müssen darüber informiert werden, dass nur explizit von der Einrichtung freigegebene und korrekt lizensierte Standardsoftware eingesetzt werden darf.

Es darf nur solche Software eingesetzt werden, für die noch regelmäßig Sicherheitsupdates und -patches ausgeliefert werden.

Durch eine geeignete Benutzerkonten- und Rechteverwaltung wird sichergestellt, dass nur diejenigen Personen Zugriff auf IT-Systeme, Applikationen und Informationen haben, die aufgrund ihrer Aufgaben dazu berechtigt sind.

Bei der normalen Nutzung der Clients darf nicht mit administrativen Rechten (Admin-Benutzer) gearbeitet werden. Dies ist nur zu administrativen Tätigkeiten zulässig, die unbedingt von normalen Aufgaben getrennt durchzuführen sind.

Um sicherzustellen, dass nur Befugte auf Systeme und Informationen zugreifen können, ist es wichtig, dass sich die Mitarbeitenden vor der Nutzung per Passwort authentisieren müssen. Die Benutzer müssen über die dafür notwendigen Regelungen und deren Anwendung sowie deren Hintergründe explizit informiert werden.

Das Passwort bei IT-Systemen muss aus mindestens 8 Zeichen bestehen. Es muss sich aus Klein- und Großbuchstaben, sowie aus Zahlen oder Sonderzeichen zusammensetzen.

Bei der Beendigung von Arbeitsverhältnissen ist die geordnete Über- und Rückgabe der Geräte und Daten sicherzustellen.

Das sichere Löschen und Vernichten von Daten auf Datenträgern (z.B. Server, Clients, Netzkomponenten, Smartphones) muss vor der Aussonderung oder vor einer Weitergabe der Datenträger und Geräte vorgenommen werden. [Referenz auf Liste mit empfohlenen Werkzeugen und Tools der Landeskirche]

6. Büroraum / Lokaler Arbeitsplatz

Der Büroraum ist ein Raum, in dem sich eine oder mehrere Personen aufhalten, um dort der Erledigung ihrer Aufgaben nachzugehen. Diese Aufgaben können (auch IT-unterstützt) aus den verschiedensten Tätigkeiten bestehen: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen.

Fenster und Türen sind zu verschließen, wenn ein Raum nicht besetzt ist. Büroräume müssen so ausgestattet sein, dass schutzbedürftige Datenträger und Dokumente weggeschlossen werden können. Dazu müssen beispielsweise verschließbare Schreibtische, Rollcontainer oder Schränke vorhanden sein.

Alle Mitarbeitenden müssen darauf hingewiesen werden, dass auch in Büroräumen die vorhandenen IT-Geräte, Zubehör, Software oder Daten ausreichend gegen Diebstahl, Zerstörung und Veränderungen geschützt werden.

In Büros mit Publikumsverkehr sind Diebstahlsicherungen zum Schutz von IT-Systemen (z. B. Laptops) einzusetzen, da andernfalls die Gefahr besteht, dass solche Geräte in einem unbewachten Augenblick abhandenkommen.

7. Mobiler Arbeitsplatz

Ein mobiler Arbeitsplatz kann auch z. B. von Telearbeitern, freien Mitarbeitern oder Selbstständigen sowie von Ehrenamtlichen genutzt werden. Bei einem mobilen Arbeitsplatz kann die infrastrukturelle Sicherheit nicht so vorausgesetzt werden, wie sie in einer Büroumgebung innerhalb der Räumlichkeiten einer Institution anzutreffen ist.

Dienstliche Aufgaben werden häufig auch an wechselnden Arbeitsplätzen und in unterschiedlichen Umgebungen durchgeführt. Die dabei verarbeitenden Informationen müssen angemessen geschützt werden (z. B. durch Sperren des Bildschirms oder Anbringen eines Sichtschutzes).

Die Leistungsfähigkeit von mobilen IT-Systemen wie beispielsweise Laptops, Handys und PDAs wächst ständig und lässt es zu, große Mengen geschäftsrelevanter Informationen außerhalb der Räume der jeweiligen Institution zu bearbeiten. Dabei ist zu beachten, dass meist die infrastrukturelle Sicherheit nicht der einer Büroumgebung entspricht.

An mobilen Arbeitsplätzen sollten weder dienstliche Unterlagen noch mobile IT-Systeme unbeaufsichtigt bleiben. Sie sollten zumindest gegen einfache Wegnahme gesichert, z. B. mit einer Diebstahlsicherung versehen oder in Schränke geschlossen werden.

Beim Einsatz mobiler Geräte sind die Festplatten der Rechner grundsätzlich immer zu verschlüsseln.

8. Arbeitsplatz-Rechner

Als Arbeitsplatz-Rechner wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt.

Eine Bildschirmsperre muss eingerichtet werden, die sich sowohl manuell vom Benutzer aktivieren lässt, als sich auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch aktiviert.

Alle Mitarbeitenden sind dazu zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

E-Mails müssen verschlüsselt von und zu Mail-Servern übertragen werden (z. B. mittels SSL/TLS). Die entsprechenden Einstellungen bei E-Mailprogrammen (SSL/TLS) sind standardmäßig vorzunehmen.

Ein Laptop oder Notebook ist ein IT-System mit einer transportfreundlichen, kompakten Bauform, welches aufgrund dieser mobil genutzt werden kann. Ein Laptop ist ein vollwertiger Arbeitsplatz-Rechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden.

Bei diesen Geräten sind die Festplatten grundsätzlich zu verschlüsseln.

Zugriffe von einem Laptop von außerhalb auf das interne Netz müssen abgesichert erfolgen (über SSL/TLS oder VPN verschlüsselt).

9. Mobiltelefon / Smartphone

Mobiltelefone bzw. Smartphones sind inzwischen alltäglicher Bestandteil der kirchlichen Kommunikationsinfrastruktur geworden. Neben herkömmlichen Telefongesprächen bieten die Geräte meist noch eine Vielzahl an zusätzlichen Funktionen wie das Verschicken von SMS, MMS, E-Mails, die Nutzung des Internets über WLAN oder Mobilfunk. Zudem existieren auch Apps, wie z. B. Whatsapp oder Threema, die Funktionalitäten zur Datenübertragung ermöglichen.

Verlorene Geräte müssen über den Mobilfunkanbieter umgehend gesperrt werden.

Es muss sichergestellt werden, dass die Sicherheitsmechanismen von Mobiltelefonen (z. B. Eingabe einer PIN oder eines Passworts, Fingerabdruck, etc.) genutzt werden.

Bei der Verwendung von Mobiltelefonen muss entschieden werden, ob und wie zusätzliche Dienste wie MMS, Bluetooth oder WLAN genutzt werden dürfen. Nicht benötigte Dienste sollten deaktiviert werden.

Vertrauliche Daten, wie personenbezogene Daten oder Zugangsdaten zum Netz der Institution, sind prinzipiell nicht auf den Geräten zu speichern. Eine unumgängliche Speicherung auf dem Gerät (inklusive Speicherkarte) muss ausschließlich in verschlüsselter Form erfolgen. Das Senden von vertraulichen Daten ist nur über gesicherte, von der kirchlichen Organisation bereitgestellte Transportwege erlaubt [Bitte Verweis auf vorhandene Transportwege einfügen]. Nicht dazu gehören z. B. Skype, Whatsapp oder private E-Mail.

10. Netzwerke

Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose lokale Netze aufzubauen oder bestehende drahtgebundene Netze zu erweitern. WLANs können aufgrund der einfachen Installation nicht nur dauerhaft, sondern auch für temporär zu installierende Netze, wie z. B. für Veranstaltungen, verwendet werden.

Die Kommunikation im WLAN sowie im Power-LAN muss verschlüsselt werden. Für WLAN ist WPA2 zu verwenden. Für Power-LAN ist mindestens eine Verschlüsselung mit AES-128 zu verwenden.

Es wird empfohlen die kryptographischen Schlüssel für den Zugriff auf ein WLAN zufällig zu wählen und diese regelmäßig zu wechseln. Voreingestellte Standardpasswörter sind vor Inbetriebnahme unbedingt zu wechseln.

Bei der Aussonderung von WLAN-Komponenten müssen die Authentifizierungsinformationen für den Zugang zum WLAN und andere erreichbare Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert werden. Hierzu ist die Komponente auf die Werkseinstellung zurückzusetzen.

11. Mobile Datenträger

Mobile Datenträger werden für eine Vielzahl von Zwecken eingesetzt, beispielsweise für den Datentransport, die Speicherung von Daten oder die mobile Datennutzung. Es gibt eine Vielzahl verschiedener Varianten von mobilen Datenträgern. Hierzu gehören unter anderem Disketten, externe Festplatten, CD-ROMs, DVDs, Magnetbänder und USB-Sticks.

Die Mitarbeitenden müssen über die Risiken in Hinblick auf mobile Datenträger und über die erforderlichen Sicherheitsmaßnahmen informiert werden.

Bei mobilen Datenträgern besteht ein hohes Verlust- und Diebstahlsrisiko. Damit die Daten nicht in falsche Hände geraten, sind die Dateien oder besser die gesamten mobilen Datenträger zu verschlüsseln. Insbesondere vertrauliche Dateien auf mobilen Datenträgern müssen zwingend verschlüsselt werden. Dazu bietet sich z. B. die freie Software 7zip mit AES-256 Bit Verschlüsselung an.

Hinweis: Um den Aufwand durch eine zusätzliche Software zu minimieren, sollte bevorzugt auf Lösungen zur Hardwareverschlüsselung zurückgegriffen werden (verschlüsselte USB-Sticks oder Festplatten).

12. Internetnutzung

Das Internet als wichtiges Informations- und Kommunikationsmedium ist aus dem Arbeitsalltag nicht mehr wegzudenken. In den meisten Organisationen ist die Nutzung von E-Mail, Informationsangeboten, Internet-Dienstleistungen, Online-Banking und Online-Shopping selbstverständlich. Gleichzeitig muss verhindert werden, dass durch die Anbindung der eigenen Geräte an das Internet für die Organisation nicht akzeptable Risiken entstehen.

Alle Mitarbeitenden sollten über das Potential, aber auch die Risiken der Internet-Nutzung informiert sein. Sie müssen wissen, welche Rahmenbedingungen bei der Nutzung von Internet-Diensten zu beachten sind. Dazu gehört insbesondere, dass sie die Regeln kennen, um Dienste sicher zu nutzen und sich korrekt im Internet zu verhalten, beispielsweise in (Web-)Blogs oder sozialen Netzwerken (z. B. Facebook, Twitter). Es sollten hierzu die bereits bekannten kirchlichen und diakonischen Regelungen genutzt werden [Bitte vorhandene Regelung einfügen].

Bei vielen Internet-Diensten müssen sich die Benutzer mittels Benutzernamen und Passwort authentisieren. Dabei sind die allgemeinen Regeln zur sicheren Verwendung von Passwörtern (siehe Hard- und Software) einzuhalten. Wichtig ist insbesondere, dass die Passwörter nicht leicht zu erraten sind. Es sind für verschiedene Internet-Dienste verschiedene Passwörter zu verwenden. Vor allem sind dafür keine Passwörter zu nutzen, die für IT-Systeme oder IT-Anwendungen innerhalb der kirchlichen und diakonischen Einrichtungen verwendet werden.

13. Checkliste für kleine Organisationen

Die folgende Checkliste dient als Umsetzungshilfe für die Prüfung und Dokumentation des Umsetzungszustandes der Sicherheitsmaßnahmen für kleine Einrichtungen. Die Checkliste kann ebenso als Nachweis der Bemühungen zur Umsetzung der IT-Sicherheit verwendet werden.

Nr.	Frage	Referenz	Umgesetzt
1.	Werden neue Mitarbeitende bei der Einstellung auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen?	Kap. 1	□
2.	Sind die wichtigen Schlüsselpositionen durch einen Vertreter besetzt?	Kap. 1	□
3.	Haben alle Mitarbeitenden eine Verpflichtung zur Wahrung des Datengeheimnisses unterschrieben?	Kap. 2	□
4.	Werden Backup-Datenträger in einem gesonderten Raum aufbewahrt?	Kap. 3	□
5.	Sind auf allen Clients Virenschutzprogramme installiert?	Kap. 4	□
6.	Werden Betriebssysteme und Anwendungen regelmäßig aktualisiert?	Kap. 4	□
7.	Gibt es eine Checkliste für Mitarbeitende zur Beendigung des Arbeitsverhältnisses?	Kap. 5	□
8.	Gibt es eine Benutzer- und Rechteverwaltung für IT-Systeme und Anwendungen?	Kap. 5	□
9.	Gibt es Passwortregelungen für IT-Systeme und Anwendungen und werden diese umgesetzt?	Kap. 5	□
10.	Werden alle Mitarbeitenden über die Regelungen zur Nutzung von Standardsoftware informiert?	Kap. 5	□
11.	Wird ausschließlich Software aus vertrauenswürdigen Quellen installiert?	Kap. 5	□
12.	Gibt es regelmäßige Kontrollen bezüglich der installierten Software?	Kap. 5	□
13.	Sind auf Clients und Servern automatische Updates aktiviert?	Kap. 5	□
14.	Gibt es spezielle Handlungsanweisungen und Tools zum Löschen und Vernichten von Daten?	Kap. 5	□
15.	Sind Türen und Fenster in der Regel verschlossen, wenn die Mitarbeitenden nicht am Platz sind?	Kap. 6	□

Nr.	Frage	Referenz	Umgesetzt
16.	Sind in den Büros verschließbare Schreibtische oder Schränke vorhanden?	Kap. 6	□
17.	Gibt es in Büros mit Publikumsverkehr Diebstahlsicherungen für IT-Systeme?	Kap. 6	□
18.	Sind am mobilen Arbeitsplatz verschließbare Schreibtische oder Schränke vorhanden?	Kap. 7	□
19.	Gibt es Regelungen welche dienstlichen Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen?	Kap. 7	□
20.	Ist auf allen Clients die Bildschirmsperre aktiviert?	Kap. 8	□
21.	Ist der Zugriff von mobilen Laptops auf das LAN per VPN abgesichert?	Kap. 8	□
22.	Ist die Verschlüsselung von E-Mail-Kommunikation zwischen Client und Server aktiviert?	Kap. 8	□
23.	Ist bei allen Mobiltelefonen/Smartphones die Eingabe der Geräte-PIN aktiviert?	Kap. 9	□
24.	Werden alle vertraulichen Daten nur verschlüsselt auf Mobiltelefonen/Smartphones oder Speicherkarten gespeichert?	Kap. 9	□
25.	Wird bei WLAN das Verschlüsselungsverfahren WPA2 eingesetzt?	Kap. 10	□
26.	Werden die Schlüssel für den WLAN-Zugriff regelmäßig gewechselt?	Kap. 10	□

Glossar

Begriff	Erläuterung
WPA2	Wi-Fi Protected Access 2 (WPA2) ist die Implementierung eines Sicherheitsstandards für Funknetzwerke.
AES-128	AES steht für Advanced Encryption Standard. Dies ist ein Verschlüsselungsstandard mit einer Schlüssellänge von 128 Bit.
TLS/SSL	Transport Layer Security (TLS) ist ein Protokoll zur Verschlüsselung von Datenübertragungen im Internet - weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL).
VPN	Virtual Private Network (VPN) ist ein privates (in sich geschlossenes) Rechnernetz, das auf einer öffentlichen Netzwerk-Infrastruktur aufgebaut ist.
Patch	Ein Patch ist ein in der Regel kleineres Softwareupdate bzw. eine kleinere Softwarekorrektur.

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 festgelegt, 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 2: 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, Kundeninformationen),

-Abrechung 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:

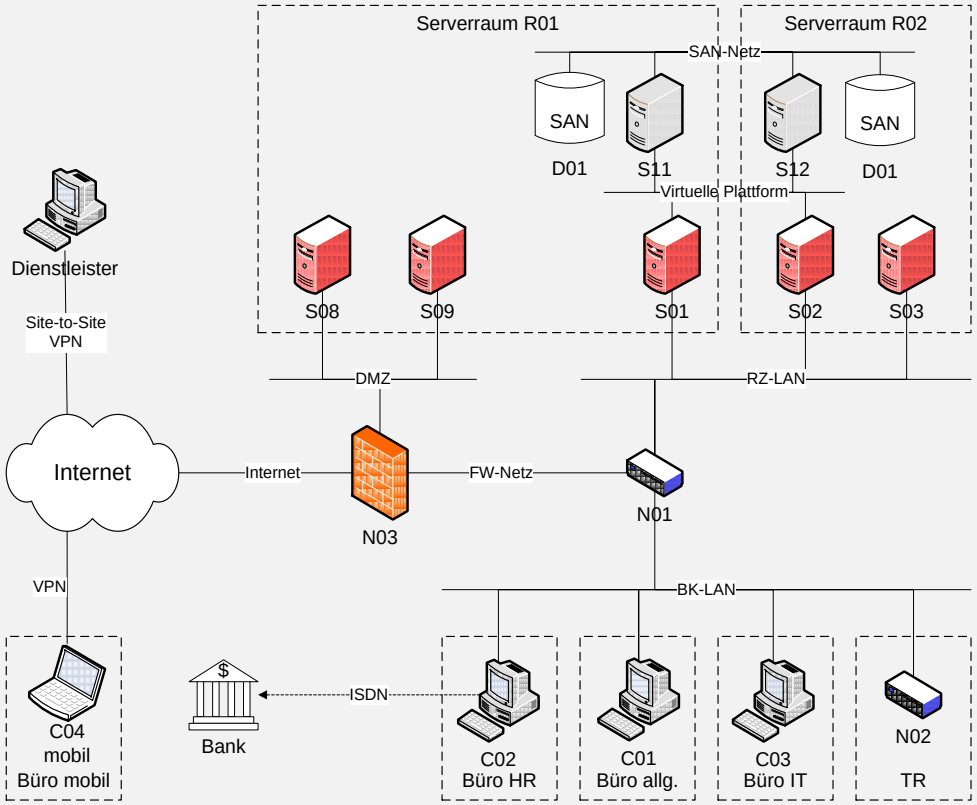


Abbildung 3: Betrachteter IT-Verbund

3.4.2 Wesentliche IT-Anwendungen und IT-Systeme

Beispiel:

Zu den zentralen Fachverfahren gehören:

- Personalwesen
- Finanzwesen
- Bürokommunikation

Beispiel:

Tabelle 2: Anwendungen

Nr.	*Bezeichnung*	*Art*	*Anwender*
A100	*Bürokommunikation*	*Softwarepaket MS-Office*	*Alle*
A101	*Personaldatenverarbeitung mit MS Office*	*Softwarepaket MS-Office*	*Personalsach-bearbeiter / 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*	*Rechnungs-wesen*

Beispiel:

Tabelle 3: 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 4: 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 5: 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[3] aufgeführte Anwendung der Schutzbedarf in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit zu dokumentieren und zu begründen (siehe Abbildung). Dies geschieht dadurch, dass man für jedes dieser Schutzziele abschätzt, welche Schäden durch seine Verletzung eintreten könnten.

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 4: 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

[3] 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.

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 6: Schutzbedarf der IT-Anwendungen

Nr.	*Bezeichnung*	*Pbez. Daten*	*Grundwert*	*Schutzbedarf*	*Begründung*
A120	*E-Mail*	*X*	*VT*	*hoch*	*Personen-bezogene 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 7: Schutzbedarf der IT-Systeme

Nr.	*Bezeichnung*	*Anh. Anw.*	*Grundwert*	*Schutzbedarf*	*Begründung*
S001	*Domänen-controller*	*A001*	*VT*	*hoch*	*Maximumprinzip*
			IN	*normal*	*Maximumprinzip*
			VF	*hoch*	*Verteilungseffekt, da Redundanz vorhanden*

4.5.3 Schutzbedarf der Netze/ Kommunikationsstrecken

Beispiel:

Tabelle 8: 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 9: 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

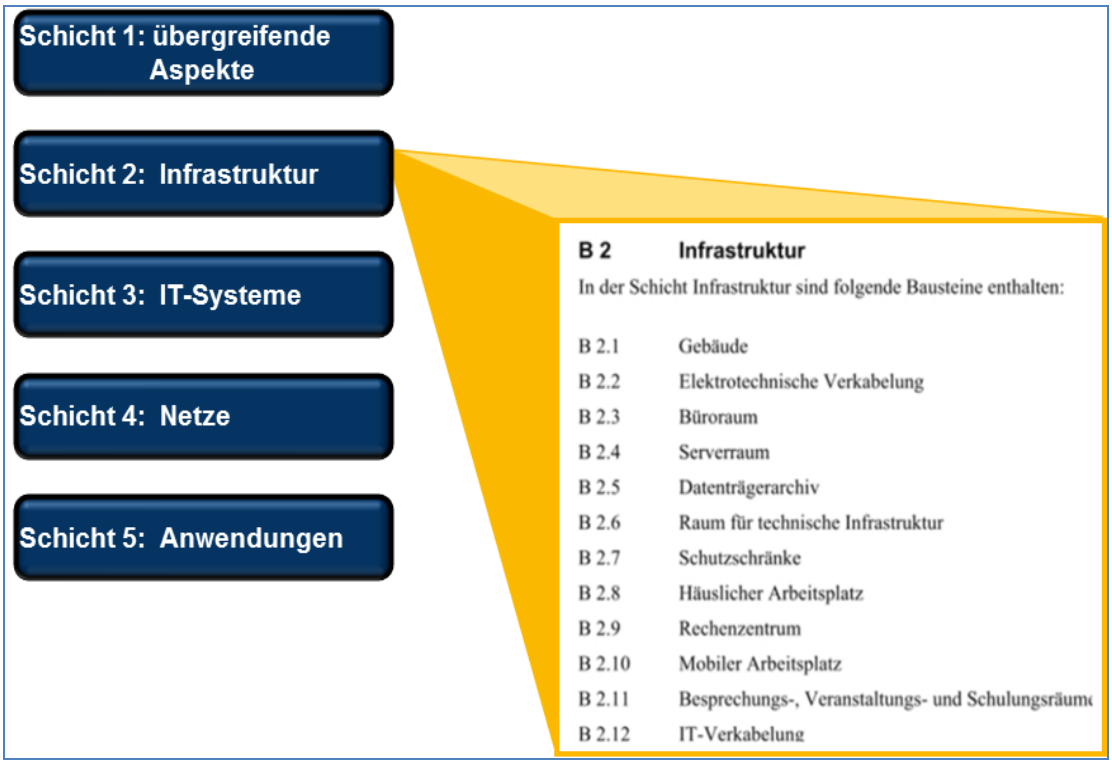


Abbildung 5: Auswahl der Bausteine aus dem IT-Grundschutzkatalog

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 10: 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.

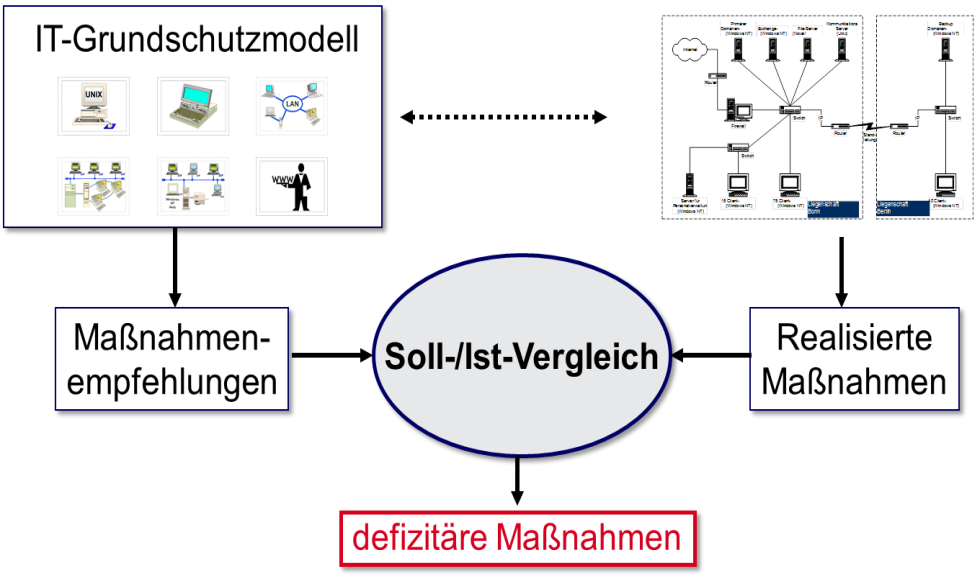


Abbildung 6: Der Basis-Sicherheitscheck zeigt mittels Soll-/Ist-Vergleich Defizite auf Maßnahmen der IT-Grundschutz-Kataloge haben verschiedene Wertigkeiten.

Tabelle 11: 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.
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 12: 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 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 13: 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 14: 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 15: 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 16: 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 17: 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.

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).

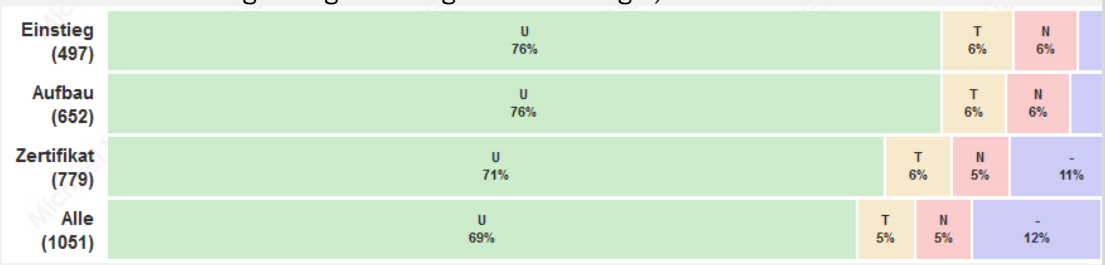


Abbildung 7: Umsetzungsgrad der Maßnahmen

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.

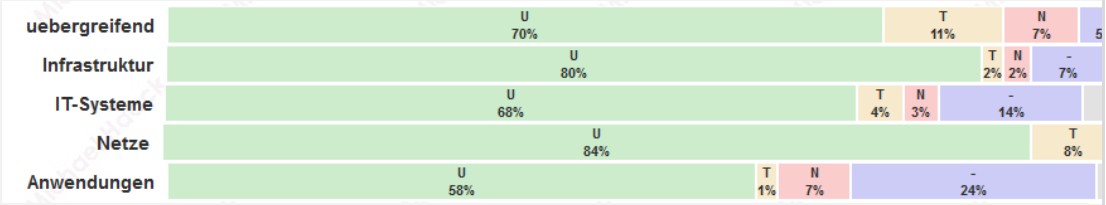


Abbildung 8: Umsetzungsgrad der Maßnahmen nach Schichten

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.

Referenzdokumente (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

Vorschläge für ein Schulungs-konzept IT-Sicherheit

1. Allgemeines

1.1 Rahmenbedingungen / Ausgangslage

Die Evangelische Kirche in Deutschland EKD hat mit der Novellierung ihres Datenschutzgesetzes (DSG-EKD) sowie dem Erlass einer Ratsverordnung zur IT-Sicherheit sich, die Gliedkirchen, die gliedkirchlichen Zusammenschlüsse sowie die ihnen zugeordneten kirchlichen und diakonischen Werke und Einrichtungen zur Einhaltung der IT-Sicherheit und zur Erstellung, Umsetzung und Fortschreibung von IT-Sicherheitskonzepten verpflichtet.

1.2 Zielsetzung und Gegenstand

Um eine zielgerichtete und effiziente Erstellung und Umsetzung des IT-Sicherheitskonzeptes zu unterstützen, soll dieses Schulungskonzept Verantwortliche der wesentlichen Zielgruppen Wissen vermitteln und sie bezüglich IT-Sicherheit sensibilisieren.

1.3 Akzeptanzmanagement

Akzeptanzmanagement soll ermöglichen, dass das Thema IT-Sicherheit und die IT-Sicherheitskonzepte in den verschiedenen Einrichtungen verankert und gelebt werden. Ziel ist hierbei die Vermittlung der Sinnhaftigkeit von IT-Sicherheit sowie der Formulierung und des Einsatzes von IT-Sicherheitskonzepten.

Akzeptanzmanagement beantwortet die Frage, was würde die verschiedenen Mitarbeitergruppen dazu bewegen, Sicherheit einzuhalten. Der Erfahrung nach spielen zwei wichtige Faktoren die Hauptrolle:

- Der Bezug zur eigenen Arbeit (oder zum Privatleben) muss stets hergestellt werden: Bsp.: Handhabung von Passwörtern.
- Der Bezug zur eigenen Verantwortung muss stets hergestellt werden, z. B.: Was ist meine Rolle, meine Aufgabe? Daraus ergibt sich, welche Daten ich benutze: die Klassifizierung. Wer klassifiziert, der schützt!

2. Zielgruppen

Das Identifizieren und Schulen verschiedener Zielgruppen ist von enormer Bedeutung, damit eine Wissensvermittlung zielgerichtet und effizient durchgeführt werden kann.

Beim Workshop der Projektgruppe zur IT-Sicherheit im Mai 2014 wurden die folgenden zu adressierenden Zielgruppen identifiziert:

- Ehrenamtliche
- Angestellte (Verwaltung)
- Angestellte (Gemeinde/Basis)
- IT-Mitarbeiter
- Führungskräfte (Theologen, Juristen und sonstige Führungskräfte aus der Verwaltung)

2.1 Ehrenamtliche

Die Ehrenamtlichen sind eine sehr wichtige Zielgruppe und stellen zahlenmäßig die größte Gruppe aller Mitarbeitenden der evangelischen Kirche. Aufgrund der hohen Zahl von Ehrenamtlichen kann in der Regel die Wissensvermittlung nur in Bezug auf die durch den Ehrenamtlichen wahrgenommene Aufgabe durchgeführt werden.

2.2 Angestellte (Gemeinde/Basis)

Die Angestellten der Gemeinden haben mitunter sehr enge Berührungspunkte mit IT-Anwendungen und den damit verarbeiteten Daten. Eine kontinuierliche Wissensvermittlung unter Beachtung der dezentralen Standortgegebenheiten ist ratsam, damit das Wissen weiter vertieft und eine Sensibilisierung nachhaltig stattfinden kann.

2.3 Angestellte (Verwaltung)

Die Angestellten der Kirchenverwaltungen arbeiten täglich mit IT-Anwendungen und den damit verarbeiteten Daten. Eine kontinuierliche Wissensvermittlung vor Ort in der eigenen Verwaltung ist ratsam, damit das Wissen weiter vertieft und eine Sensibilisierung nachhaltig stattfinden kann.

2.4 IT-Mitarbeiter

IT-Mitarbeiter sorgen in der Regel für die Umsetzung des IT-Sicherheitskonzepts auf technischer und auch organisatorischer Ebene.

Damit IT-Mitarbeiter zielgerichtet und effektiv das IT-Sicherheitskonzept umsetzen können, sollte eine intensive Wissensvermittlung erfolgen.

2.5 Führungskräfte

Mit Führungskräften sind Theologen, Juristen und sonstiges Führungskräfte in der Regel aus der Verwaltung gemeint. Ein IT-Sicherheitskonzept ist nur dann erfolgreich, ein bestimmtes Sicherheitsniveau zu erreichen, wenn die Führungskräfte eindeutig die Notwendigkeit verstehen, hinter den Maßnahmen stehen, sie selbst vorleben sowie diese aktiv auch von ihren Mitarbeitern einfordern.

Gerade bei Führungskräften ist es wichtig, ein grundlegendes Verständnis für die oft sehr abstrakt und hochtechnisch erscheinenden Maßnahmen des IT-Sicherheitskonzeptes zu erreichen. Zudem sollte den Führungskräften deutlich gemacht werden, dass die Ziele der IT-Sicherheit wichtig für die Organisation sind.

3. Methoden

In diesem Kapitel werden die Methoden der Wissensvermittlung skizziert, die in einem Schulungsprogramm zur Anwendung kommen. Im Folgenden werden die hier aufgezählten Methoden erläutert:

- Präsentation zum IT-Sicherheitsmanagement von externen Experten
- Kombinierter Vortrag zu Datensicherheit und IT-Sicherheit
- Schulung IT-Sicherheitskonzept inklusive Workshop
- E-Learning
- Handzettel zur IT-Sicherheit

3.1 Präsentation zum IT-Sicherheitsmanagement von externen Experten

Präsentationen haben im Allgemeinen den Vorteil, dass die Zielgruppen das Thema bzw. die Inhalte sehen und zusätzlich durch den Vortragenden hören. Diese Präsentation sollte inhaltlich alle wesentlichen Aspekte zur Informationssicherheit mit Beispielen beinhalten. Eine Präsentation von externen Experten wird an dieser Stelle empfohlen, damit durch dessen Expertise Gespräche mit den Zielgruppen über die Sicherheitsthemen gefördert wird. Des Weiteren wird ebenfalls durch Externe die Sicht auf IT-Sicherheit geschärft, was die interne IT weniger einem Rechtfertigungsdruck aussetzt. Eine Veranstaltung von mindestens einem halben Tag ist zu empfehlen.

Bei der Aufbereitung der Themen ist besonders darauf zu achten, einen nicht technischen aber sehr aggregierten Blick einzunehmen.

3.2 Kombinierter Vortrag zu Datensicherheit und IT-Sicherheit

Besonders Angestellte aus Gemeinden und der Verwaltung sollten in dieser Veranstaltung einen Einblick in die Datenschutzanforderungen in der EKD und auch in Maßnahmen der IT-Sicherheit bekommen. Für die Übermittlung des Wissens wird eine Powerpoint-Präsentation vorgeschlagen und für eine dezentrale Schulung sollte ein E-Learning-Tool (= E-Learning-Plattform, siehe Abbildung 9) in Betracht gezogen werden. Für den kombinierten Vortrag ist mindestens ein halber Tag anzusetzen. Das E-Learning sollte quartalsweise erfolgen.

3.3 Schulung IT-Sicherheitskonzept

Das Knowhow, um ein Sicherheitskonzept nach dem Muster IT-Sicherheitskonzept zu erstellen, sollte den IT-Mitarbeitern, die für IT-Sicherheitsbelange zuständig sind, durch eine Schulung vermittelt werden. Dabei ist das theoretische Wissen durch einen Experten mithilfe von Präsentationen darzulegen und durch praktische Übungen zu ergänzen. Es wird empfohlen den Teilnehmerkreis von mindestens 8 bis maximal 15 Schulungsteilnehmern zu beschränken.

Aufbauempfehlung für eine Schulung zum IT-Sicherheitskonzept:

1. Tag: Theoretische Wissensvermittlung

2. Tag: Wiederholung und Vertiefung der Theorie anhand von Praxisbeispielen

3. Tag: Toolschulung (zur Durchführung des IT-Sicherheitskonzeptes) mit prakt. Übungen.

3.4 E-Learning

Das Nutzen einer E-Learning Plattform ist eine moderne Art der nachhaltigen und günstigen Wissensvermittlung.

Im Bereich der IT-Sicherheit sind bisher leider nur wenige solcher Plattformen verfügbar. Eine günstige und ausgereifte Plattform ist „open beware“[4]. Diese Web-Plattform (siehe Abbildung 9) bietet eine Auswahl an wichtigen Themen:

- E-Mail
- Viren
- Passworte
- Internet
- Vertrauliche Daten
- Mobile Geräte
- Am Arbeitsplatz

Es ist möglich diese Themen weiter zu entwickeln und somit auf spezifische Belange der evangelischen Kirche einzugehen.

Abbildung 9: E-Learning Plattform „open beware"

4 Siehe http://www.bdg.de/beware/open-beware/index.html (Stand: 25.5.2014)

3.5 Handzettel zur IT-Sicherheit

Zur weiteren Informationsvermittlung eignen sich Handzettel bzw. Informationsblätter. Auf diesen A-4 großen Seiten können bestimmte Themen aus dem großen Bereich der IT-Sicherheit vertieft, oder auch anwenderspezifisch und individuell auf die jeweilige Einrichtung abgestimmt, vermittelt werden. Eine Weitergabe des Wissens bzw. der Handzettel ist hier weniger aufwendig, da diese als E-Mail oder als ausgedrucktes Papier verteilt werden kann. Um die Zielgruppen nicht mit Sicherheitsinformationen zu überfordern, ist zu empfehlen, nicht mehr als zwei solcher Blätter im Jahr zu verteilen.

Die Abbildung 9 stellt ein Beispiel zum Thema Informationsklassifizierung dar.

Was macht eigentlich ein Informationseigentümer?

Informationen sind wertvolle Güter für ein Unternehmen. Sie entscheiden über Erfolg und Verlust. Daher sollten sensible Daten besonders geschützt werden. Doch wer entscheidet, welche Daten besonders sensibel/geschäftskritisch sind?

Welche Aufgaben hat der Informationseigentümer?

Der Informationseigentümer ist der Ersteller einer Information bzw. aus Unternehmenssicht der erste, der eine Information von Externen (z.B. Kunde, Dienstleiser) erhält. Seine Aufgabe ist es die geschäftliche Relevanz der Information anhand der Schutzziele zu bewerten.

Wonach sind die Informationen zu bewerten?

Die typischen Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit. Je Schutzziel ist eine unternehmensweite definierte Klasse zu wählen. (siehe Richtlinie zum IT-Sicherheitsmanagement)

Vertraulichkeit: Wie hoch ist der Schutzbedarf der Informationen hinsichtlich Ihrer Geheimhaltung?

Integrität: Wie wichtig ist die Unverfälschtheit/Ursprünglichkeit von Informationen?

Verfügbarkeit: Welche zeitlichen Anforderungen werden hinsichtlich eines berechtigten Zugriffs auf Informationen und Systeme gestellt?

Die Bewertung wird durch einen Klassifizierungsbogen als Hilfsmittel erleichtert. Aus Gründen der Praktikabilität sollten Informationen vor ihrer Klassifizierung zu Gruppen zusammengefasst werden. Die Bewertung von einzelnen Informationen muss dann nur in Ausnahmefällen erfolgen.

Was geschieht mit der Klassifizierung?

Die Klassifizierung der Informationen dient der effizienten Anwendung von Sicherheitsmaßnahmen. Alle Informationen und die sie verarbeitenden IT-Systeme können somit entsprechend ihres Schutzbedarfs geschützt werden. Bspw. sollten vertrauliche Kundendaten besser geschützt werden als frei zugängliche Geschäftsdaten. Der für die Verwaltung und Verarbeitung der Information zuständige Mitarbeiter oder Dienstleister (der sogenannte Informationstreuhänder oder Informationsbesitzer) ist für die Einhaltung der Vorgaben des Informationseigentümers zuständig.

Wie wird der Schutzbedarf angepasst?

Eine Höherstufung ist durch jeden Mitarbeiter oder durch den Datenschutzbeauftragten möglich. Dabei sind der Informationseigentümer sowie der Informationstreuhänder zu informieren, welche die Höherstufung veranlassen. Eine Rückstufung ist nur in Rücksprache mit dem Informationseigentümer bzw. bei personenbezogenen Daten mit dem Datenschutzbeauftragten möglich.

Welche Maßnahmen sind für schutzbedürftige Informationen anzuwenden?

- Kennzeichnungspflicht entsprechend der Einstufung der Vertraulichkeit
- Verschlüsselung bei Speicherung auf Datenträgern bzw. beim Versand über E-Mail, Fax oder Post
- Geheimhaltungsverpflichtung bzw. Zustimmung des Eigentümers bei Weitergabe an Dritte
- Beschränkung von Zugriffs- und Vervielfältigungsrechten
- Sicheres Verfahren zur Vernichtung bzw. Löschung
- Berücksichtigung in der Notfallplanung bzw. proaktive Maßnahmen

Wo finde ich weitere Informationen?

Weitere Informationen zur Informations-eigentümerschaft und Klassifizierung können in der Richtlinie zum Sicherheitsmanagement nachgelesen werden.

Abbildung 10: Beispielhafter Handzettel zur Informationsklassifizierung

3.6 Weitere Sensibilisierungsmaßnahmen

Zur Unterstützung der oben genannten Methoden, sollten weitere Sensibilisierungsmaßnahmen eingeführt werden, damit die Aufmerksamkeit bei den Zielgruppen aufrechterhalten wird. Dazu eignen sich bspw.

- Newsletter per E-Mail,
- Flyer über die sichere Passwortgestaltung,
- Passwortkarten zur Hinterlegung von sicheren Passwörtern,
- Plakate mit speziellen Sicherheitsthemen,
- Notizzettel mit Sicherheitsempfehlungen,
- Sicherheitsrätsel mit Gewinnspiel.

Abbildung 11: Beispielhafte Passwortkarte zur einfachen Erstellung und Nutzung von Passwörtern mit entsprechender Güte

4. Themen

4.1 IT-Sicherheit (allgemein)

Die Inhalte zur IT-Sicherheit sind nach der jeweiligen Zielgruppe zu wählen. Damit sollten für Ehrenamtliche und Angestellte eher Themen zugeschnitten werden, welche die Anwendung der IT-Sicherheit betrifft. Dies sind u.a. Themen wie

- Informationen zur Anwendung der jeweiligen Richtlinien,
- Erstellen und Hinterlegen von Passwörtern,
- sichere IT-Nutzung.

4.2 IT-Sicherheitsmanagement

Die IT-Mitarbeitenden, welche bei der Umsetzung des Sicherheitskonzepts mitwirken sowie Verantwortung tragen, sollten neben den allgemeinen und o.g. Sicherheitsthemen in die Vorgehensweise nach BSI IT-Grundschutz geschult werden. Die folgenden Themen sind dabei zu berücksichtigen:

- Standards und Kataloge im IT-Grundschutz
- Aufbau und Struktur
- IT-Grundschutz-Vorgehensweise:
    - Definition Informationsverbund
    - IT-Strukturanalyse
        - Komplexitätsreduktion
        - Erhebung der IT-Systeme
        - Erhebung der Antworten
        - Erhebung der Netze
        - Erhebung der Standorte
        - Netzplanerhebung
    - Schutzbedarfsfeststellung
    - Modellierung
        - Schichtenprinzip
        - Bausteinaufbau und -struktur
    - Basissicherheitschecks
    - ergänzende Sicherheitsanalyse
    - Risikoanalyse

4.3 Verantwortung von Führungskräften

Für Führungskräfte gelten neben den allgemeinen Sicherheitsthemen als Anwender besonders Themen in Bezug auf deren Beitrag und Verantwortung.

Dabei sind die Themen so zu gestalten, dass die Führungskräfte an das Thema IT-Sicherheit herangeführt und darauf aufbauend auf deren Belange vertieft werden.

Dabei sollten folgende Inhalte thematisiert werden:

- IT-Sicherheit
  - Was ist unter IT-Sicherheit zu verstehen?
  - Aus welchen Gründen sollte IT-Sicherheit umgesetzt werden (Stellenwert der IT-Sicherheit)?
  - Welche Motivationen / Hintergründe existieren IT-Sicherheit einzuhalten und stetig weiter zu entwickeln?
- Grundlagen zur Vorgehensweise nach BSI IT-Grundschutz
- Vorteile einer Zertifizierung nach BSI IT-Grundschutz
- Sicherheitsziele
- Beteiligung der Führungskräfte beim Managementprozess IT-Sicherheit
- Sicherheitsrisiken und deren Analyse
- Führungskräfte als Vorbildfunktion

4.4 Pflichten der Mitarbeitenden

Zu den Pflichten der Mitarbeiter gehört der verantwortungsvolle Umgang mit der IT. In den folgenden Themen sind alle Mitarbeitenden sinnvollerweise zu sensibilisieren:

- 10 goldenen Regeln zur IT-Sicherheit
- Richtlinien,
- Datenschutz,
- Sicherheitsvorfall,
- Soziale Netzwerke,
- Mobile Geräte,
- Social Engineering am Telefon.

Auch ein Hinweis auf das Organisationsverschulden bei mangelhafter Umsetzung der IT-Sicherheit durch die Mitarbeitenden sollte gegeben werden.

4.5 Herleitung von Risiken

Das Thema der Herleitung von Risiken für die kirchlichen Organisationen ist am besten durch die Vermittlung der Risikoanalyse-Grundlagen zu vermitteln. Hier sind die folgenden Aspekte zu adressieren:

- Bestimmung sowie Unterschiede zu Gefährdung und Risiko
- Ermitteln von Gefährdungen
- Gefährdungsbewertung – von der Gefährdung zum Risiko
- Risikobehandlung
- OPTIONAL: Risikoanalyse nach BSI Standard 100-3

4.6 Aufwand und Nutzen

Eine Abschätzung von Aufwänden für die Durchführung eines IT-Sicherheitskonzeptes ist nicht trivial und hängt immer von der Größe und dem Umfang des betrachteten Informationsverbundes sowie auch entscheidend vom Wissen der Verantwortlichen und Administratoren zur IT-Sicherheit ab.

Ein thematischer Aspekt einer Schulung zur Durchführung eines IT-Sicherheitskonzeptes sollte auch immer je nach Organisation eine ungefähre Einschätzung und Evaluierung möglicher Aufwände sowie eine Abwägung von Aufwand und Nutzen beinhalten.

5. Schulungsprogramm

Die folgende Tabelle 18 gibt eine Empfehlung zu einem möglichen Schulungsprogramm.

Tabelle 18: Schulungsprogramm

	Ehren-amtliche	Angestellte (Gemeinden/ Basis)	Angestellte (Verwaltung)	IT-Mitarbeitende	Führungskräfte
Präsentation zum IT-Sicherheitsmanagement				X	X
Kombinierter Vortrag zu Datensicherheit und IT-Sicherheit		X	X		
Schulung IT-Sicherheits-konzept		X		X	
E-Learning	X	X	X		
Handzettel zur IT-Sicherheit	X	X	X	X	X
Weitere Sensibilisierungs maßnahmen	X	X	X	X	

BFDI Musterformular

Musterdienstanweisung/-vereinbarung

Diese Musterdienstanweisung/-vereinbarung ist eine aktualisierte Zusammenfassung u.g. Muster und dem Versuch geschuldet, eine adäquate und transparente Formulierung als Beispiel zur Verfügung zu stellen.

Hinweise: Das Muster kann sowohl als kollektive Regelung (Dienstvereinbarung / Betriebsvereinbarung, Dienstanweisung / Arbeitsanordnung) wie auch als einzelvertragliche Vereinbarung im öffentlichen Bereich wie im nicht-öffentlichen Bereich verwendet werden. Der Wortlaut ist jeweils entsprechend anzupassen.

- Bei behördlichen Vereinbarungen nicht vergessen, die landesdatenschutz-rechtlichen §§ entsprechend zu beachten und einzufügen.
- Zu ersetzende/ergänzende Texte und Hinweise sind kursiv unterstrichen formatiert bzw. durch ..... gekennzeichnet.
- Nicht zutreffende Passagen (z. B. Firewall des Netzbetreibers) je nach Bedarf bitte entsprechend anpassen.
- Alternative 1 und 2 können beliebig ausgestaltet werden, jedoch sollte dabei an die Anpassungen der erforderlichen Hinweise (Protokollierung, TKG etc.) gedacht werden.
- Bei Löschungen oder ergänzend eingefügten Absätzen auf die Verweise innerhalb des Textes achten.
- Regelungen für behörden-/unternehmensfremde Beschäftigte (Leiharbeiter, Fremdfirmen) sind in den Verträgen entsprechend anzupassen.

Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz

Zwischen ..... (nachfolgend Kürzel Behörde / Dienststelle / Unternehmen)

und ..... (nachfolgend Beschäftigte / Personalvertretung)

wird die folgende Dienstanweisung / Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz abgeschlossen:

1. Geltungsbereich und Zweckbestimmung

Diese Dienstanweisung / Dienstvereinbarung regelt die Grundsätze für den Zugang und die Nutzung der Internetdienste im / bei Kürzel und gilt für alle Beschäftigten, auch für behörden- / unternehmensfremde Beschäftigte (z. B. Leiharbeiter oder Beschäftigte von Fremdfirmen die bei der Behörde / dem Unternehmen tätig sind).

Ziel dieser Vereinbarung ist die Herstellung der Transparenz der Nutzungsbedingungen und der Maßnahmen zur Protokollierung und Kontrolle, die Sicherung der Persönlichkeitsrechte der Beschäftigten und die Gewährleistung des Schutzes ihrer personenbezogenen Daten.

2. Organisatorische Grundsätze

(1) Die elektronischen Kommunikationssysteme stehen den Beschäftigten als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung.

(2) Die Absicherung des Zuganges zum Internet wird durch eine Firewall des Netzbetreibers / der Behörde / des Unternehmens sichergestellt. Die Installation und Konfiguration von Web-Browsern, die IT-fachliche Betreuung der Beschäftigten sowie die Administration ihrer Internetberechtigungen erfolgt durch die Behörde / Dienststelle / Abteilung.

(3) Arbeitsplätze mit einem Internetzugang müssen wirksam durch Virenschutzprogramme vor Schadsoftware gesichert werden. Diese Programme dürfen durch Beschäftigte nicht eigenständig manipuliert oder deaktiviert werden. Gleiches gilt für den Einsatz von Filterprogrammen, die den Zugriff auf Angebote mit rechtswidrigen oder strafbaren Inhalten sperren, sowie für alle Sicherheitsprogramme und -einstellungen.

Wenn vorhanden, Hotline oder Ansprechpartner für Störungen angeben.

3. Zulässigkeit der Nutzung

a) Alternative 1

(1) Die private Nutzung ist unter dem Vorbehalt des Widerrufs in geringfügigem Umfang zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden und die private Nutzung keine negativen Auswirkungen auf die Bewältigung der Arbeitsaufgaben hat.

(2) Das Abrufen von Informationen oder Inhalten, die für die Behörde / das Unternehmen Kosten verursachen, ist für den Privatgebrauch unzulässig. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftliche Zwecke verfolgt werden.

(3) Private E-Mails dürfen grundsätzlich nur über die Nutzung Webmail-Dienste versandt und empfangen werden. Über die dienstlichen E-Mail-Adressen eingehende private E-Mails sind wie private schriftliche Post zu behandeln. Eingehende private, aber fälschlich als Dienstpost behandelte E-Mails sind den betreffenden Beschäftigten unverzüglich nach Bekanntwerden ihres

privaten Charakters zur alleinigen Kenntnis zu geben. Private E-Mails sind von Beschäftigten als solche zu kennzeichnen.

(4) Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Protokollierung und Kontrolle gemäß Nr. 7 und 8 dieser Vereinbarung erstrecken sich auch auf den Bereich der privaten Nutzung des Internetzugangs. Die Beschäftigten erklären durch die private Nutzung des Internetzugangs seine Einwilligung in die Protokollierung und Kontrolle Nr. 7 und 8 dieser Vereinbarung für den Bereich der privaten Nutzung.

b) Alternative 2

(1) Der Internetzugang und das E-Mail-System werden nur für die dienstliche Nutzung zur Verfügung gestellt, jegliche private Nutzung ist untersagt.

(2) Über die dienstlichen E-Mail-Adressen eingehende private E-Mails sind wie private schriftliche Post zu behandeln. Eingehende private, aber fälschlich als Dienstpost behandelte E-Mails sind den betreffenden Beschäftigten unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben. Private E-Mails sind von Beschäftigten nach Kenntnisnahme des privaten Charakters unverzüglich zu löschen.

(3) Wird bei den in Nr. 7 und 8 aufgeführten Maßnahmen eine Zuwiderhandlung gegen die Vorschrift des Absatzes 2 Satz 3 festgestellt, dürfen die Daten ohne vorherige Einsichtnahme der in Nr. 7 Abs. 4 genannten Personen von diesen Personen gelöscht werden.

a) und b)

(*) Dokumente, die personenbezogene oder andere sensible Daten beinhalten, dürfen nicht unverschlüsselt übertragen werden.

(*) Das Abrufen und Ausführen von Dateien oder Programmen aus und im Internet ist nur von und bei den vom IT-Verantwortlichen bekannt gegebenen Anbietern gestattet, soweit deren Inhalte für den dienstlichen Gebrauch benötigt werden. Urheberrechtlich geschützte Dateien, für die keine Lizenz vorhanden ist, dürfen nicht abgerufen und gespeichert werden. Ermöglicht die Berechtigung der Beschäftigten das Abrufen und die Installation von Treibern, Setup-Programmen oder ähnlicher systemeingreifender Software, ist das vorher vom zuständigen IT-Verantwortlichen genehmigen zu lassen. Das Ausführen von aktiven Inhalten (z. B. Makros) in heruntergeladenen Dokumenten ist nur bei als vertrauenswürdig gekennzeichneten Anbietern gestattet. Die Einstellungen in den zugehörigen Anwendungen werden vom IT-Verantwortlichen vorgenommen.

(*) Das Abrufen von für die Behörde / das Unternehmen kostenverursachenden Informationen oder Inhalten aus dem Internet ist bei der zuständigen Behörde / Dienststelle / Abteilung zu beantragen und bedarf der Genehmigung durch den ..... bzw. durch den jeweiligen Dienststellen- / Abteilungs- / Fachbereichsleiter.

(*) Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen über sogenannte Remote-Anwendungen bzw. Terminal-Emulationen sind grundsätzlich nicht zugelassen. Sollte dienstlicher Bedarf für Remote-Zugriffe bzw. Terminal-Emulationen bestehen, sind diese bei dem IT-Verantwortlichen unter Angabe der Gründe zu beantragen.

(*) Die Internet-Telefonie und Bildtelefonie sind grundsätzlich nicht zugelassen. Ausnahmen für den dienstlichen Gebrauch sind beim IT-Verantwortlichen zu beantragen und nur mit der dafür zur Verfügung gestellten Software zulässig.

(*) Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse der jeweiligen Beschäftigten nicht mehr für diesen zur weiteren Nutzung zur Verfügung. Die Beschäftigten sind angehalten, ihre außerbetrieblichen Kommunikationspartner über diesen Umstand zu informieren. Dienstliche E-Mails werden an zur Aufrechterhaltung des Dienstbetriebes zuständige Beschäftigte weitergeleitet. Ist ein privater Charakter des Inhaltes dieser weitergeleiteten E-Mail

ersichtlich, ist die E-Mail ohne weitere Kenntnisnahme des Inhaltes durch die jeweiligen Beschäftigten zu löschen. Eine Weiterleitung erfolgt nicht.

(*) Aus Wirtschaftlichkeits- oder IT-Sicherheitsgründen kann die Internetnutzung beschränkt werden. Dies kann beispielsweise folgendes beinhalten:

- Sperrung bestimmter Dienste der Internetnutzung,
- Reduzierung auf bestimmte Internetanschlüsse,
- Beschränkung des Massendatentransfers oder des Speicherplatzes.

4. Verhaltensgrundsätze

(1) Grundsätzlich gelten die Regelungen der „Dienstanweisung für die Nutzung des IT-Systems“ der Behörde / des Unternehmens.

(2) Die Beschäftigten haben jede Nutzung des Internets zu unterlassen, die geeignet ist, den Interessen der Dienststelle / des Unternehmens oder deren/dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Behördennetzes / Unternehmensnetzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften und die „Dienstanweisung für die Nutzung des IT-Systems“ verstößt. Dies gilt vor allem für

- das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen,
- die Nutzung des Internets zur Erledigung privater Rechtsgeschäfte, insbesondere die Nutzung von Zahlungsfunktionen (Onlinebanking, Internetversandhandel, eBay o.ä.) oder
- die Nutzung von Onlinespieleplattformen.

Abrufen und Aufrufen heißt auf im Netz vorhandene Informationen mit IT-Systemen der Behörde / des Unternehmens zugreifen.

Verbreiten heißt einer Vielzahl von Personen oder einem unbestimmten Personenkreis über Internet-Dienste unter Verwendung von IT-Systemen der Behörde / des Unternehmens anbieten.

Anbieten ist nur der für Presse- und Öffentlichkeitsarbeit zuständigen Stelle oder der nach der Geschäftsverteilung für Veröffentlichungen zuständigen Stelle bzw. nur mit deren Genehmigung gestattet.

(3) Zur Überprüfung der Einhaltung der Regelungen dieser Vereinbarung werden regelmäßige nicht-namensbezogene Stichproben (ohne Identifizierungsmerkmale) in den Protokolldateien durchgeführt (vgl. Nr. 7 Abs. 4). Ergänzend wird eine Übersicht über das jeweilige Gesamtvolumen des ein- und ausgehenden Datenverkehrs erstellt.

(4) Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.

5. Information und Schulung der Beschäftigten

Die Beschäftigten werden durch die Dienststelle / Abteilung über die besonderen Datensicherheitsprobleme bei der Nutzung der elektronischen Kommunikationssysteme unterrichtet. Sie werden für den sicheren und wirtschaftlichen Umgang mit diesen Systemen qualifiziert und über die einschlägigen Rechtsvorschriften informiert.

6. Verantwortlichkeit

Die Verantwortung für die Beachtung der vorgenannten Festlegungen und Hinweise obliegt den zuständigen Stellen sowie den jeweiligen Beschäftigten. Diese haben insbesondere auch sicherzustellen, dass eine Nutzung des Internets durch Unbefugte vom Arbeitsplatz aus nicht erfolgt.

Hinweis: Trotz des Einsatzes von Firewall oder Systemen und Software zum Schutz vor Schadsoftware ist das Ausspähen und Manipulieren von Daten durch Dritte nicht mit absoluter Sicherheit ausgeschlossen.

7. Protokollierung und Kontrolle

(1) Alle eingehenden E-Mails werden durch eine Firewall, einen Spam-Filter sowie Virenscanner geprüft. Einzelheiten der Filterung sind unter folgender Adresse einsehbar:

Link auf das im Intranet verfügbare Dokument und ggf. auf Besonderheiten

(2) Die Verkehrsdaten für den Internetzugang werden mit Angaben von

- Datum / Uhrzeit,
- Adressen von Absender und Empfänger (z. B. IP-Adressen)
- Benutzeridentifikation (z. B. bei der Verwendung eines Proxy-Servers)
- der aufgerufenen Webseiten und
- übertragener Datenmenge

protokolliert.

(3) Die Protokolle nach Absatz 2 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler
- Gewährleitung der Systemsicherheit
- Optimierung des Netzes
- statistischen Feststellung des Gesamtnutzungsvolumens
- Stichprobenkontrollen gemäß Absatz 4 und
- Auswertungen gemäß Nr. 8 dieser Vereinbarung (Missbrauchskontrolle)

verwendet.

Betreffende §§ aus den Landesgesetzen / Verwaltungsvorschriften einfügen

(4) Die Protokolle werden durch einen von der Behörden- / Abteilungs- / Unternehmensleitung schriftlich beauftragten Mitarbeiter regelmäßig stichprobenhaft hinsichtlich der aufgerufenen Websites, aber nicht personenbezogen, gesichtet und in aggregierter Form, also ohne Nennung von Namen und anderen Identifizierungsmerkmalen, ausgewertet. Die Auswertung der Übersicht des Gesamtdatenvolumens erfolgt monatlich ebenfalls durch diesen Mitarbeiter. Der/Die (behördliche) Datenschutzbeauftragte wird beteiligt, wenn er/sie dies wünscht.

(5) Der Zugriff auf die Protokolldateien gemäß Absatz 3 ist auf den von der Behörden- / Abteilungs- / Unternehmensleitung beauftragten Mitarbeiter begrenzt. Dieser hat eine entsprechende Verpflichtungserklärung zum Datenschutz unterschrieben. Darüber hinaus ist er hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf die strafrechtlichen Konsequenzen bei Verstößen hingewiesen worden.

(6) Die Protokolldaten werden nach 30 Tagen automatisch gelöscht.

Erforderlichkeit und Datensparsamkeit gilt bei der Löschfrist zu beachten.

a) Hinweis zu Alternative 1

Kontrolle und Auswertung von personenbezogenen Protokollen können sich auch auf die private Kommunikation erstrecken. Deshalb soll jeder Beschäftigte, der Internetdienste für private Zwecke nutzen möchte, eine persönliche Erklärung unterschreiben, mit der er in mögliche Eingriffe in das Fernmeldegeheimnis einwilligt, die mit den in Satz 1 genannten Maßnahmen verbunden sind, und die weiteren Rahmenbedingungen der Privatnutzung anerkennt. Einen entsprechenden Formulierungsvorschlag enthält der Anhang 1 dieser Musterdienstanweisung.

8. Maßnahmen bei Verstößen / Missbrauchsregelung

(1) Bei Verdacht auf missbräuchliche oder unerlaubte Nutzung des Internetzugangs (hervorgerufen beispielsweise durch ein erhöhtes Gesamtdatenvolumen oder auch die Kenntnisnahme nicht zulässiger im Internet angebotener Inhalte) gemäß Nr. 3 und 4 dieser Vereinbarung durch einen Mitarbeiter erfolgt unter Beteiligung des/der (behördlichen) Datenschutzbeauftragten eine Überprüfung des Datenverkehrs durch ..... und dem nach Nr. 7 Abs. 4 beauftragten Mitarbeiter. Sind weitere Untersuchungsmaßnahmen (z. B. Offenlegung der IP-Adresse des benutzten Arbeitsplatzes oder weitere Überprüfungen) notwendig, werden diese von den in Satz 1 genannten Personen veranlasst. Auf der Basis dieser Untersuchung wird ein Bericht erstellt, der dem Betroffenen ausgehändigt wird. Dieser ist anschließend dazu zu hören.

(2) Im Übrigen gelten die einschlägigen Regelungen des Disziplinar- bzw. Tarifrechts.

(3) Ist aufgrund der stichprobenhaften nicht-personenbezogenen Kontrollen bzw. der Auswertung der Übersicht des Datenvolumens eine nicht mehr tolerierbare Häufung von offensichtlich privater Nutzung des Internetzugangs zu erkennen, so werden innerhalb von einer zu setzenden Frist von zwei Wochen nach der Anhörung die Stichproben weiterhin nicht-personenbezogen durchgeführt. Ergeben diese Stichproben bzw. die Auswertung der Übersicht des Datenvolumens keine Änderung im Nutzungsverhalten, so werden die Protokolle der folgenden zwei Wochen durch die in Absatz 1 genannten Personen stichprobenhaft personenbezogen ausgewertet. Hierbei wird wie im Falle des Verdachts einer missbräuchlichen Nutzung (Abs. 1) vorgegangen. Zu den Verfahren nach Satz 1 und Satz 2 erfolgt eine entsprechende vorherige schriftliche Mitteilung an alle Beschäftigten, so dass deren Kenntnisnahme über die Maßnahmen gewährleistet werden kann.

(4) Ein Verstoß gegen diese Dienstanweisung kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

(5) Die Dienststellen- / Abteilungs- / Unternehmensleitung behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs im Einzelfall zu untersagen.

9. Grundsätze für eine Nutzung behörden- / unternehmensfremder Kommunikationssysteme

(1) Diese Vereinbarung gilt auch für Beschäftigte, die ihre Tätigkeiten direkt bei Kunden der Behörde / des Unternehmens ausführen. In diesen Fällen sind für eine zulässige Nutzung des Internetzuganges vorrangig die Regelungen des Kunden zu beachten.

(2) Die Regelungen in

- Nr. 2 Abs. 3 (Schutz vor Schadsoftware, Manipulation/Deaktivierung von Programmen und weiteres),
- Nr. 3 Abs. 2 (Abrufen von kostenpflichtigen Informationen und weiteres) und Abs. 5 bis 9 (Umfang der erlaubten Abrufe, Speicherung und Nutzung) sowie

- Nr. 4 Abs. 2 (Unterlassung der Nutzung zum Schaden der Behörde / des Unternehmens und weitere)

bleiben unberührt.

10. Änderungen und Erweiterungen

(1) Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden der Personalvertretung und dem behördlichen Datenschutzbeauftragten mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden.

11. Inkrafttreten

(1) Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von zwei Wochen gekündigt werden. Im Falle einer Kündigung ist jede private Nutzung des Internetzuganges, auch der Empfang und das Versenden privater E-Mails über die dienstliche E-Mail-Adresse bis zum Abschluss einer neuen Vereinbarung untersagt.

(2) Alle Beschäftigten bestätigen schriftlich die Kenntnisnahme. Ein Abdruck der Vereinbarung wird ihnen zusammen mit einer Kopie der Bestätigung ausgehändigt.

.....	.....
Ort, Datum	Ort, Datum
.....	.....
Personalvertretung	Behörde / Geschäftsleitung

Erklärung zur Nutzung der dienstlichen E-Mail-Adresse und des dienstlichen Internetzugangs (Anhang 1)

Ich habe die „Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz“ zur Kenntnis genommen.

× *nur ankreuzen, wenn zutreffend*

◯ Ich möchte den Internetzugang in dem von der Dienstanweisung erlaubten Umfang auch privat nutzen. Ich verpflichte mich, dabei diese Dienstanweisung, sonstige Bestimmungen sowie die allgemeinen Gesetze einzuhalten und für private E-Mails ausschließlich über Webmail-Dienste zu nutzen.

◯ Mir ist bekannt, dass technisch nicht zwischen dienstlicher und privater Nutzung unterschieden wird. Ich bin daher damit einverstanden, dass

- unter den in Nr. 7 der Dienstanweisung genannten Voraussetzungen auch Daten meiner privaten Nutzung, die dem Fernmeldegeheimnis nach Art. 10 Grundgesetz und § 88 Telekommunikationsgesetz unterliegen, protokolliert und auswertet sowie
- unter Auswertung dieser Protokolle festgestellte Verstöße gemäß Nr. 8 der Dienstanweisung ggf. dienst-, arbeits- und u.U. auch strafrechtliche Konsequenzen haben können.

◯ Für den Fall der ausnahmsweise privaten Inanspruchnahme der dienstlichen E-Mail-Adresse und des dienstlichen Internetzuganges willige ich darin ein, dass auch insoweit

- eine Protokollierung und Kontrolle nach Nr. 7 dieser Dienstanweisung erfolgt,
- eine Spamfilterung nach Nr. 7 dieser Dienstanweisung erfolgt,
- im Einzelfall eine Einsichtnahme in E-Mails erfolgen kann, wenn dies zur Aufklärung tatsächlicher Anhaltspunkte für einen Verstoß gegen die Verhaltensgrundsätze nach Nr. 4 der Dienstanweisung unerlässlich ist; bei nicht erkennbar als privat gekennzeichneten E-Mails auch, wenn dies zur Aufrechterhaltung des Dienstbetriebes technisch bzw. zur Abwicklung des Dienstbetriebes durch meinen dienstlichen Vertreter unverzichtbar ist.

◯ Ich habe Kenntnis, dass die Verfügbarkeit und Integrität der genannten Systeme nicht gesichert sind, also ausnahmsweise die Möglichkeit besteht, dass E-Mails nicht oder verspätet zugestellt werden.

◯ Mir ist bekannt, dass ich im Falle einer privaten Nutzung der dienstlichen E-Mail-Adresse meine Kommunikationspartner darauf hinzuweisen habe, dass es sich um ein dienstliches E-Mail-Postfach handelt und auch bei einer privaten Nutzung die Bedingungen nach Nr. 7 und 8 (Protokollierung, Missbrauchsregelung) der Dienstanweisung gelten bzw. die private Nutzung untersagt ist.

b) Hinweis zu Alternative 2

"...die Bedingungen nach Nr. 3, 7 und 8 der Dienstanweisung"

.....	.....
Ort, Datum	Ort, Datum
.....	.....
Beschäftigte	Behörde / Personalvertretung / Geschäftsleitung

Beizufügende Anhänge

Artikel 10 Grundgesetz

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird, und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

Tool-Unterstützung IT-Grundschutz

Tool-Unterstützung IT-Grundschutz

Produktvergleich

Andreas Floß, Senior Consultant
Ronny Frankenstein, Senior Manager

HISOLUTIONS

Zusammenfassung

Die folgende Präsentation stellt 4 Software-Tools zur Dokumentation der IT-Sicherheitskonzepte nach BSI IT-Grundschutz vor. Für jedes Tool werden die wesentlichen Features dargestellt. Es wurden betrachtet:

- HiScout der Firma HiScout GmbH,
- i-Doit der Firma synetics GmbH,
- CRISAM der Firma calpana business consulting GmbH sowie
- verinice. der Firma SerNet GmbH.

Alle Tools sind entsprechend den Vorgaben des BSI geeignet das IT-Sicherheitskonzept zu dokumentieren. Es gibt verschiedene Anwendungsbereiche und z.T. auch Zusatzfunktionen, die für eine Entscheidung zum Einsatz in den Einrichtungen maßgeblich sein können.

Technische Unterschiede in der Implementierung (Clientsoftware, Webanwendung) sind ebenfalls bei der Tool-Auswahl zu berücksichtigen.

Abschließend wird ein Vergleich der wichtigen Features und Zusatzfunktionen gegeben, der den jeweiligen Einrichtungen bei der Auswahl helfen soll.

HISOLUTIONS

Übersicht der Tools

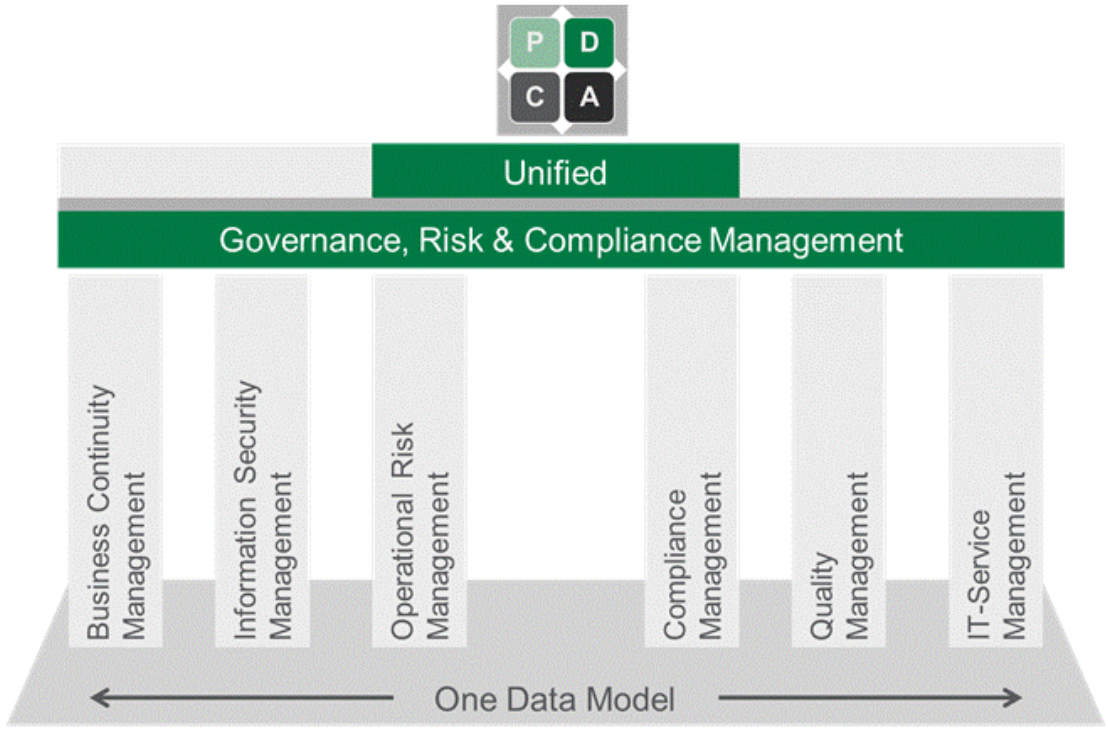
HISOLUTIONS

Produktvorstellung

HiScout

HISOLUTIONS

HiScout GRC Suite



HISOLUTIONS

HiScout

Das HiScout ISM Modul unterstützt die Umsetzung von BSI IT-Grundschutz

- Komplettes ISMS nach BSI 100-1 / 2 / 3
- BCM Modul nach BSI 100-4 / UMRA
- Zertifizierte Grundschutzverbünde durch HiScout
- Flexible Schnittstellen (GS-Tool Import, Metadatenupdate, XML)
- Template-basiertes Reporting
- Browserbasierte Multi-Useranwendung (Zero-Client)
- Vollständige ISO-Konformität (Prozesse, Informationen, Audits, …)

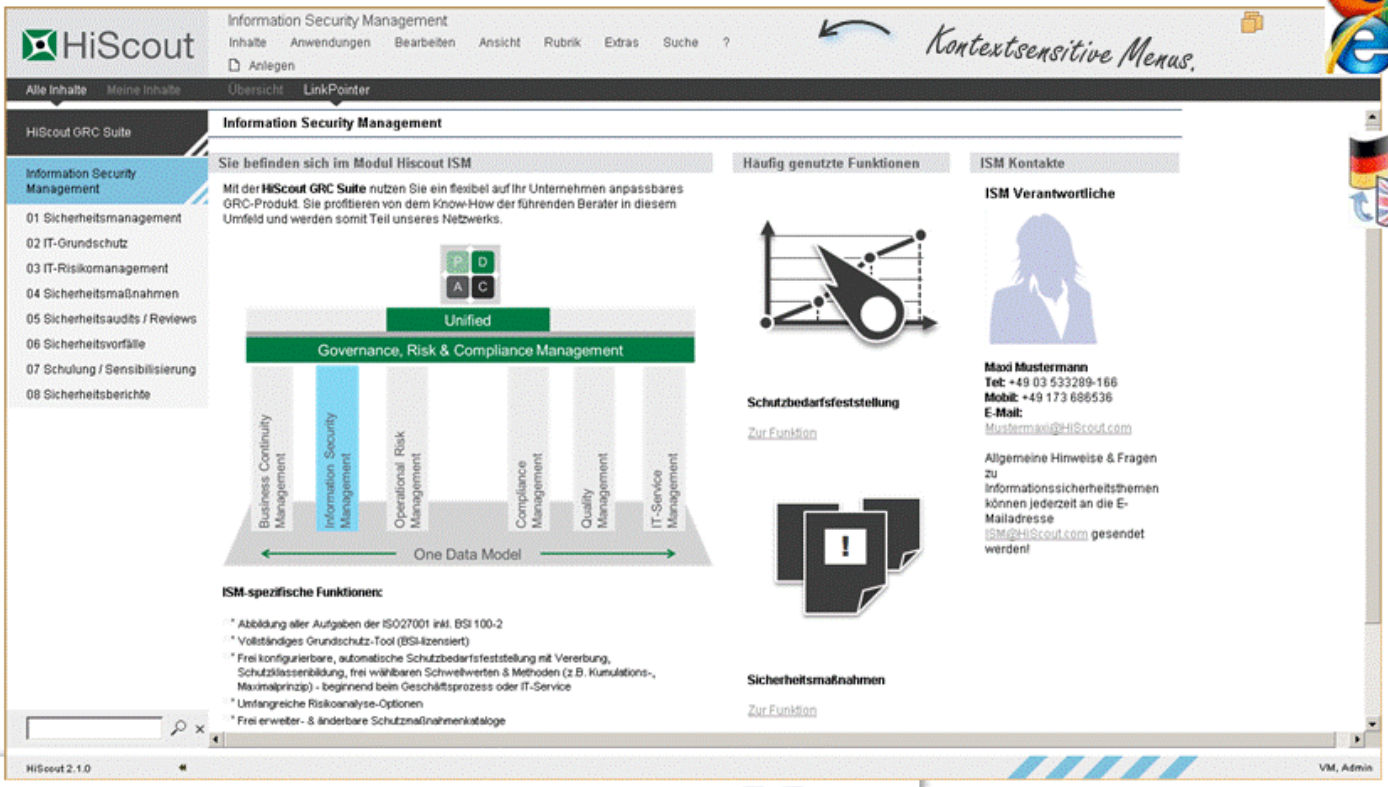
HISOLUTIONS

HiScout

Portalbasierte Weboberfläche

Web-basiert, Zero-Client.

Kontextsensitive Menus.



HISOLUTIONS

HiScout

Anpassungen können ohne technische Eingriffe durch den Benutzer durchgeführt werden

HISOLUTIONS

HiScout

Lizenzmodell

- Lizenzen sind in Abhängigkeit von
  - Umfang Modulauswahl
  - Unternehmens- bzw. Behördengröße
  - Nutzeranzahlen

HISOLUTIONS

Produktvorstellung

i-doit

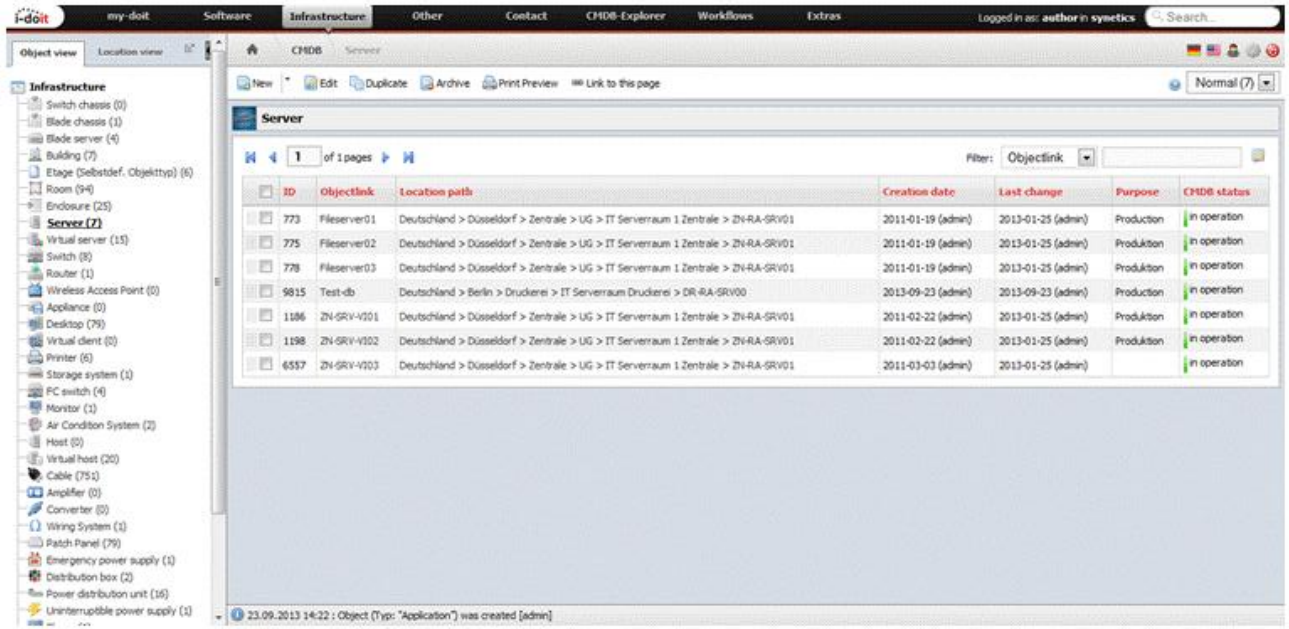
HISOLUTIONS

i-doit – VIVA-Modul (synetics)

- Webbasiert
- Dokumentation komplexer IT-Infrastrukturen
- Basiert auf einer CMBD in Anlehnung an ITIL
- Open- und Pro-Versionen erhältlich
- Erweiterbar durch verschiedene Module
- Kostenpflichtiges Modul VIVA notwendig für IT-Security (ISO, GS)
- Benötigt zwingend i-doit Pro (ab Version 1.1)

HISOLUTIONS

i-doit Benutzeroberfläche

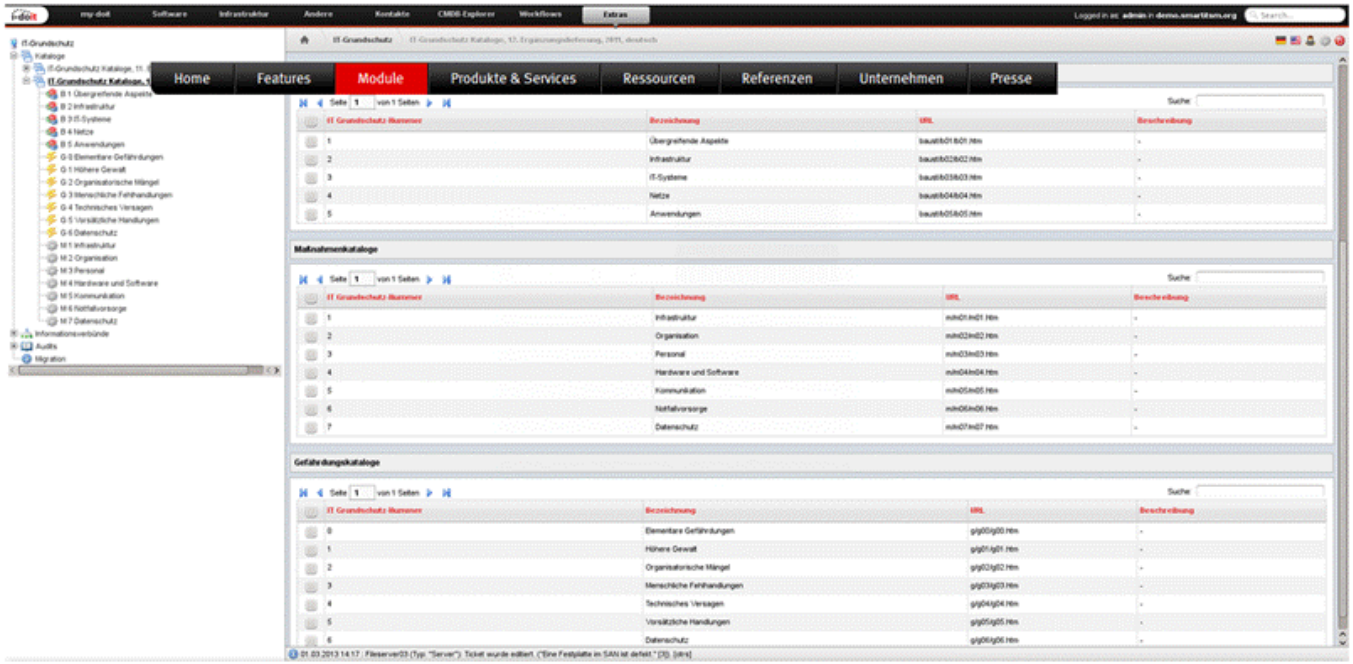


HISOLUTIONS

Zusätzliches Modul ermöglicht die Abbildung von BSI IT-Grundschutz

- Import der aktuellen IT-Grundschutz-Kataloge EL11 (2009) und EL12 (2011)
- Anpassen und Erstellen von Bausteinen, Gefährdungen und Maßnahmen
- Übersichten mit Statusanzeige
- Vollständige Unterstützung BSI-Standard 100-2, 100-3,
- Ausgabe der Referenzdokumentation

i-doit bietet eine Katalogverwaltung zur Pflege BSI IT-Grundschutzkataloge



Im Basis-Sicherheitscheck wird der Umsetzungsstatus dokumentiert

Seite 1 von 1 Seiten Suche:

Status	IT-Grundschutz-Maßnahme	Qualifizierungsstufe	Anmerkungen	Datum der Umsetzung	Umsetzer
	M 2.192 Erstellung einer Leitlinie zur Informationssicherheit	A (Einstieg)	-	05.04.2013	Max Mustermann
	M 2.335 Festlegung der Sicherheitsziele und -strategie	A (Einstieg)	-	05.04.2013	Erika Mustermann
	M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	A (Einstieg)	-	05.04.2013	Erika Mustermann
	M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	A (Einstieg)	-	05.04.2013	Enoch Root
	M 2.195 Erstellung eines Sicherheitskonzepts	A (Einstieg)	-	-	Enoch Root
-	M 2.197 Integration der Mitarbeiter in den Sicherheitsprozess	A (Einstieg)	-	-	-
-	M 2.337 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse	A (Einstieg)	-	-	-
	M 2.338 Erstellung von zielgruppengerechten Sicherheitsrichtlinien	Z (Zusätzlich)	-	-	-
	M 2.339 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit	Z (Zusätzlich)	-	-	-
-	M 2.475 Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten	A (Einstieg)	-	-	-
	M 2.199 Aufrechterhaltung der Informationssicherheit	A (Einstieg)	-	-	Max Mustermann, Erika Mustermann
	M 2.200 Management-Berichte zur Informationssicherheit	C (Zertifikat)	-	-	-
	M 2.201 Dokumentation des Sicherheitsprozesses	C (Zertifikat)	-	-	-
	M 6.16 Abschließen von Versicherungen	Z (Zusätzlich)	-	-	-

i-doit

i-doit unterstützt die Einbindung der CMDB in die Grundschutz-Vorgehensweise

- Vollständige Unterstützung der BSI-Standards 100-2, 100-3
  - Modellierung von Informationsverbünden
  - Ermittlung des Schutzbedarfs
  - Durchführung einer ergänzenden Sicherheitsanalyse
  - Zuordnung von Bausteinen und deren Gefährdungen sowie Maßnahmen
  - Durchführen von BSCs, Umsetzung von Maßnahmen
  - Risikoanalyse von zugeordneten Gefährdungen
- Konzeptionelles Problem: „Zielobjekte“ in CMDB vs. „Zielgruppen“ in VIVA (Einordnung, Vererbung etc.)
- Version 1.0 von Mai 2013, aktuell Version 1.2 von September 2013

HISOLUTIONS

Lizenzmodell

- Das Zusatzmodul VIVA ist zusätzlich zum Basismodul erhältlich.

Fakten und Preise

Der Einsatz des VIVA-Moduls orientiert sich preislich am eingesetzten i-doit Objektpaket und ist sowohl im Rahmen der Kaufversion, als auch für die Subskription verfügbar. Die Konditionen sind dabei ergänzend zum Basispaket zu verstehen.

	einmalig	500er	1.000er	5.000er	unlimitiert
Subskription	1.200,00 €	44,00 €	64,00 €	132,00 €	600,00 €
Kaufversion*	-	1.395,00 €	1.495,00 €	1.595.,00 €	2.990,00 €

*** 3 Jahre Updates und Upgrades inklusive, 10% des Kaufpreises ab dem 4. Jahr für jährliche Wartung**

Alle Preise sind netto und verstehen sich zzgl. der gesetzlich fälligen MwSt

Produktvorstellung

crisam®
DECISION ENGINEERING

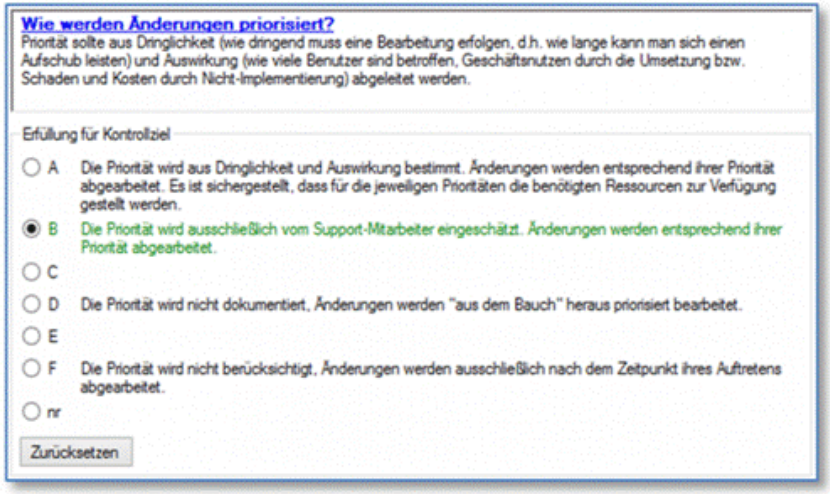
HISOLUTIONS

CRISAM 5

- Hersteller: Calpana Business Consulting (AT)
- CRISAM = „Corporate Risk Application Method“
- Erweiterbar durch Verschiedene Module (Knowledge Pack) u.a.
  - CRISAM ISMS Knowledge Pack
  - CRISAM ISO 27001 Knowledge Pack
  - **CRISAM BSI und GSTOOL Knowledge Pack**
- Benötigt CRISAM Explorer

CRISAM 5 – ISMS Knowledge Pack

- 160 Bausteine und 1.700 Kontrollziele zur Identifikation und Bewertung von IT-Risiken
- Quellen, wie BSI Grundschutz, ISO/IEC 27002, ITIL Version 2 und 3, COBIT und NIST
- Best Practices und Empfehlungen von Herstellern.
- Expertenwissen aus der CRISAM® Community.
- halbjährlichen Zyklus aktualisiert

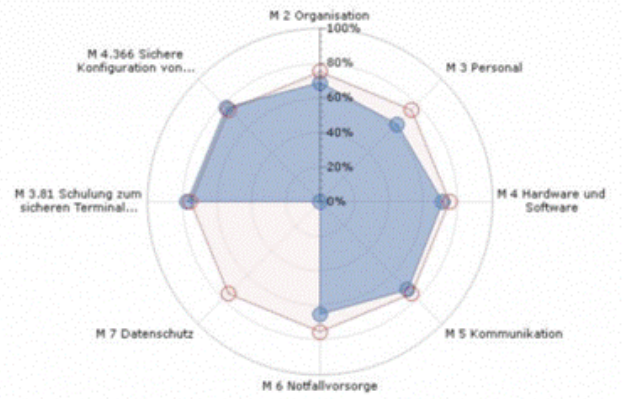


CRISAM 5 – ISO 27001 Knowledge Pack

- Aktuelle Versionen (2005 und 2013) der ISO/IEC 27000 Normenreihe.
- Von Norm geforderte Berichte „Statement of Applicability“ und „Scope Document“
- Compliance Analysebericht um die Konformität Ihres ISMS zu den Normforderungen der ISO/IEC 27001 nachzuweisen und gegenüber 27002 darzustellen
- Unterstützt damit optimal bei der Vorbereitung und (Re-)Zertifizierung
- Auswertung aus CRISAM® ISMS Kontrollen

CRISAM 5 – BSI und GSTOOL Knowledge Pack

- **GSTOOL Import**, um bestehende BSI GSTOOL Daten in das CRISAM Risikomanagement Informationssystem zu übernehmen
- **BSI Compliance Analysebericht**, als Konformitätsnachweis Ihres ISMS nach BSI IT-Grundschutz nachzuweisen
- Unterstützt bei der **Vorbereitung und Zertifizierung** nach BSI IT-Grundschutz-Zertifikat
- Das integrierte Mapping ermöglicht **Auswertungen** aus CRISAM ISMS oder bestehenden **BSI Kontrollen**



Produktvorstellung

verinice.

HISOLUTIONS

verinice.

Verinice.Pro

- IT-Grundschutz, ISO 27001/2, Risikoanalyse nach ISO 27005, IS-Assessments nach VDA Vorgaben, Nachweis von Compliance mit Standards wie IDW PS 330 u. a.
- *Auch* als CMDB verwendbar
- Zentrales IS-Repository, Zentrale Dokumentenablage, Fernzugriff
- VMware-Anbindung möglich
- Mehrbenutzerfähigkeit, Berechtigungskonzept, Directory-Anbindung
- Web-basierter Workflow, Sichere Verbindung (SSL), Mailbenachrichtigungen
- Erstellen einer Verarbeitungsübersicht nach § 4g II i.V.m. § 4e BDSG

HISOLUTIONS

verinice.

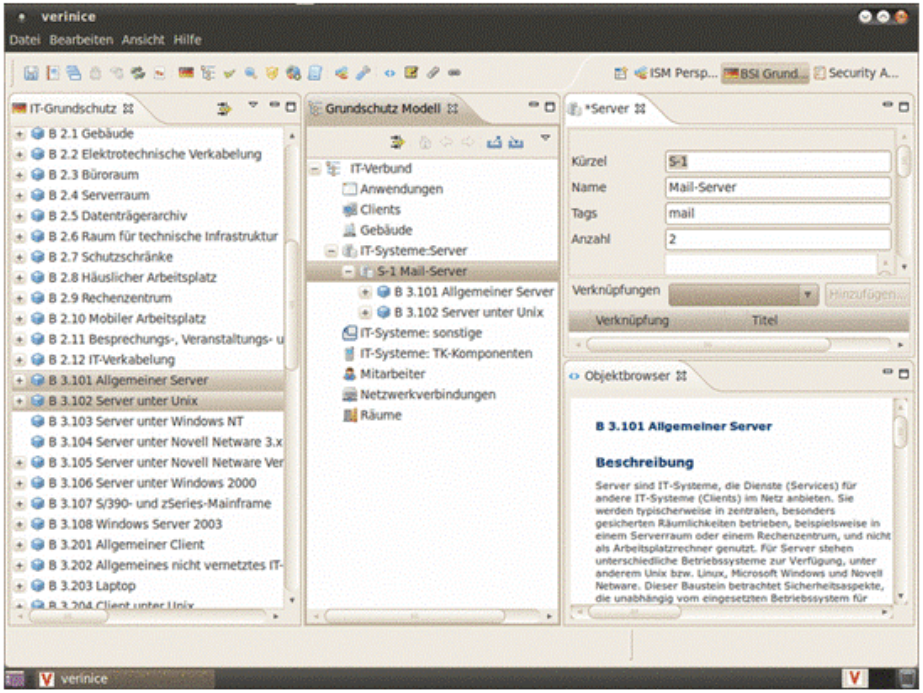
Verinice.Pro

- Import von GS-Tool durch HiSolutions möglich
- Offener Source Code (nicht Server)
- Externe Datenbank (Hibernate: Postgres / Oracle / …),
- Dynamisches Objektmodell (HitroUI)
- BIRT-Reporting
  - Erstellen eigener Reports möglich

HISOLUTIONS

verinice.

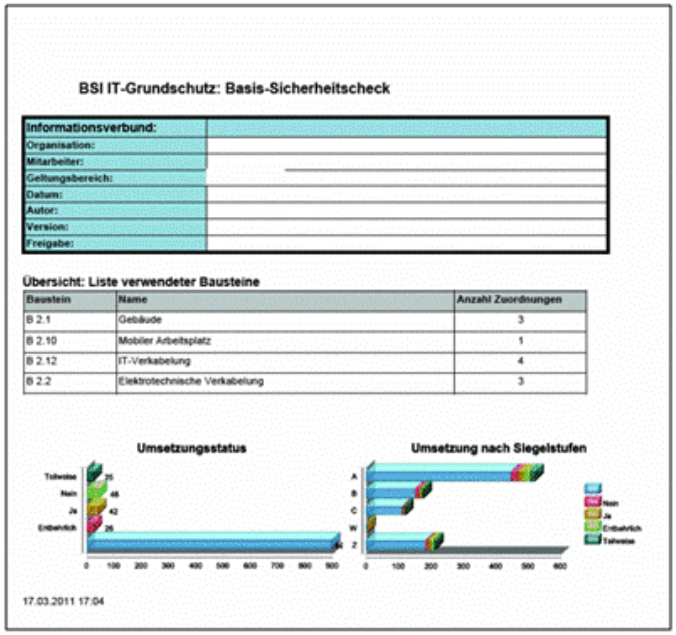
Verinice.Pro bietet deckt das komplette Vorgehen des BSI IT-Grundschutz ab



HISOLUTIONS

verinice.

Verschiedene grafische Darstellungen des ISMS sind möglich



BSI IT-Grundschutz: Basis-Sicherheitscheck

Informationsverbund:	
Organisation:	
Mitarbeiter:	
Geltungsbereich:	
Datum:	
Autor:	
Version:	
Freigabe:	

Übersicht: Liste verwendeter Bausteine

Baustein	Name	Anzahl Zuordnungen
B 2.1	Gebäude	3
B 2.10	Mobiler Arbeitsplatz	1
B 2.12	IT-Verkabelung	4
B 2.2	Elektrotechnische Verkabelung	3

Umsetzungsstatus

Umsetzung nach Siegelstufen

17.03.2011 17:04

Scope / Client: My Company

Date: 17. März 2011

Risk Register

Risk Acceptance Criteria

Category	Tolerable risk level
Confidentiality	7
Integrity	7
Availability	8

The following risk assessment was performed as detailed in the approved risk assessment method and is in accordance with international standard ISO / IEC 27005.
Risk acceptance criteria shown on the left are defined in the risk assessment policy and approved by senior management.

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Integrity: property of protecting the accuracy and completeness of assets
Availability: property of information being accessible and usable upon demand by an authorized entity
(ISO/IEC 27000:2009)

Risk Matrix: Confidentiality

Number of identified Risks

Impact	0	1	2	3
Probability				
0	0	0	0	60
1	0	0	0	3
2	0	0	0	7
3	0	0	3	20
4	0	0	0	2
5	0	0	0	5
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

Table shows the number of identified risks and their severity. See below for classification of probability and business impact levels.

Total Count

HISOLUTIONS

Zusammenfassung

HISOLUTIONS

Die Entscheidung für ein Tool hängt von vielen Faktoren ab

- Spezielle Anforderungen der Organisation?
- Verpflichtende Vorgaben zum Tooleinsatz?
- Wie wichtig ist das verteilte Arbeiten (Webbasiert oder Clientlösung)?
- Komplexität und Bedienerfreundlichkeit der Anwendung?
- Sichere Übertragung möglich?
- Lizenzen / Kosten:
  - Genaue Kenntnisse von Mengengerüsten nötig
  - Synergieeffekte bei Nutzung weiterer Funktionen (BCM, Compliance, CMDB, IT-Servicemanagement, …)?
  - Mieten oder kaufen?
  - Wie viel Support gewünscht?
  - Verhandlungen mit Herstellern…

HISOLUTIONS

Zusammenfassung I: Wesentliche Features

Parameter	HiScout	verinice.PRO	i-doit Pro inkl. VIVA	CRISAM 5.0
Fokus	Governance Risk and Control	Information Security Management	Assetmanagement	Governance Risk and Control
Client-Technologie	webbasiert (SSL)	Rich Client (Java)	webbasiert (SSL)	Rich Client / webbasiert
Berechtigungskonzept	++	+	+	++
Erweiterbar durch Module	++	-	o	++
Eigene Berichte	++	++	o	++
Handling / Einarbeitungszeit	-	++	o	+
Übersichten mit Statusanzeige (Cockpit)	+	o	+	++
Lernkurve	+	+	++	+
Kosten	6000-9000€ (nach Organisationsgröße)	freie Version (nur 1 User) oder 1700€/Jahr	2400-4600€ oder 270-800/Jahr (nach Anzahl Objekte)	nicht bekannt (je nach Anzahl der User)

HISOLUTIONS

Zusammenfassung II: weitere Features

Parameter	HiScout	verinice.PRO	i-doit Pro inkl. VIVA	CRISAM 5.0
Server-Technologie	Windows Server, SQL Server, ASP.NET	Java (Tomcat), Postgres/My-SQL (auch als VMware-Appl.)	Apache, MySQL, PHP	Windows Server,SQL Server, ASP.NET
ISO 2700x und IT-Grundschutz	+	+	+	+
Vom BSI akkreditiert für IT-Grundschutz	+	+	+	+
Mappings zu ISO 27001/2	+	-	-	+
Anpassung von Bausteinen	+	+	+	+
Zentrale Dokumentenablage	++	+	+	+
Workflows	++	+	+	++
Import / Export	+	+	+	++
Offener Sourcecode	-	o (nur Client)	- (nur i-doit open)	-
Individuelle Anpassung nötig	-	o	o	-
Produktreife	+	++	-	+
Optionaler Support	+	+	+	+

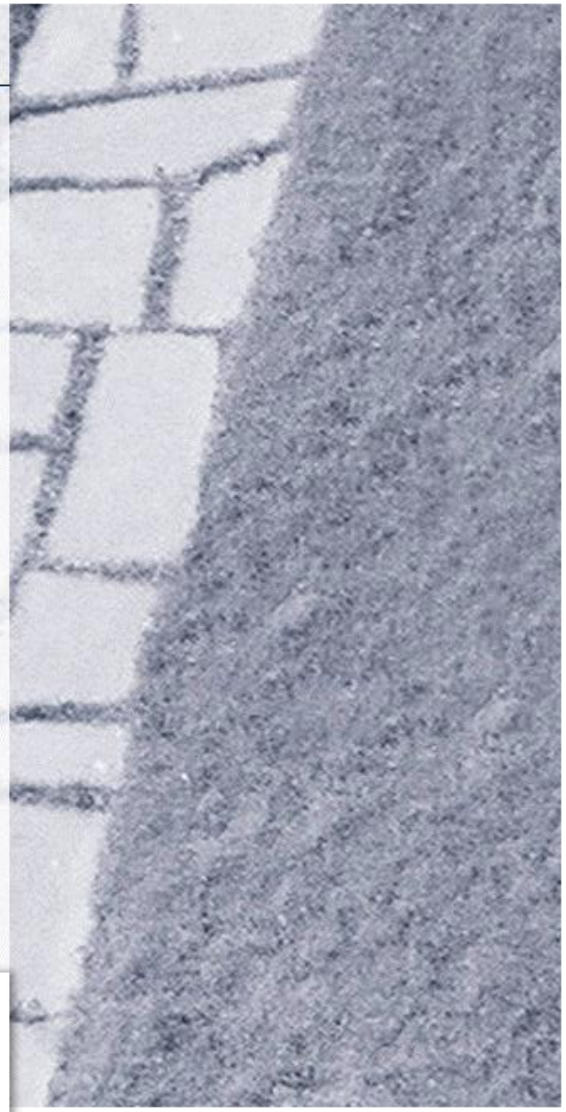
HISOLUTIONS

Kontakt

HiSolutions AG

Bouchéstraße 12
12435 Berlin
www.hisolutions.com
+49 30 533 289 0

Ronny Frankenstein
Senior Manager
Produkt Manager BSI IT-Grundschutz / ISO 27001
Datenschutz- und IT-Sicherheitsbeauftragter
frankenstein@hisolutions.com



HISOLUTIONS

Schutzbedarfskategorien

Beschreibung Schutzbedarfskategorien

Diese Schutzbedarfskategorien wurden von der Arbeitsgruppe zur Bereitstellung der Muster-IT-Sicherheitskonzepte am 28.3.2014 abgestimmt. Diese Schutzbedarfskategorien gelten als Empfehlung und können im IT-Sicherheitskonzept zur Bestimmung des Schutzbedarfs (siehe Kapitel 4 des Muster-IT-Sicherheitskonzepts für mittlere und große Einrichtungen) verwendet werden. Meldedaten, die seitens des Staates (kommunale Meldebehörden) an die Kirchen (Rechenzentren) geliefert werden, sind hinsichtlich Vertraulichkeit und Integrität grundsätzlich in die Schutzbedarfskategorie hoch einzustufen. Patienten- und Klientendaten fallen in der Regel unter die Schutzbedarfskategorie sehr hoch (§ 203 StGB) oder hoch.

Schutzbedarf „normal“:
1. Verstoß gegen Gesetze/Vorschriften/Verträge
Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen (innerkirchliche Vorschriften). Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts (personenbezogene Daten bzw. Datenschutz)
Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. Es handelt sich um personenbezogene Daten, deren Missbrauch einen einzelnen Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann, z. B. Daten über Vertragsbeziehungen, Höhe des Einkommens, etwaige Sozialleistungen, Ordnungswidrigkeiten.
3. Beeinträchtigung der persönlichen Unversehrtheit
Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung
Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
5. Negative Innen- oder Außenwirkung
Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen
Der finanzielle Schaden bleibt für die Institution tolerabel. Oder der zu erwartende direkte Schaden ist kleiner als 50.000 €.

Schutzbedarf „hoch“:
1. Verstoß gegen Gesetze/Vorschriften/Verträge
Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen (z. B. Strafverfahren). Vertragsverletzungen mit hohen Konventionalstrafen.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts (personenbezogene Daten bzw. Datenschutz)
Im Falle der erheblichen Beeinträchtigung handelt es sich z. B. um Daten zur Unterbringung in Anstalten, Straffälligkeit, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Insolvenzen. Hierunter fallen auch alle besonderen personenbezogenen Daten gemäß DSG-EKD. Sämtliche Daten, die die Privatsphäre betreffen, wie Schulden und Pfändungen, dienstliche Beurteilungen, Insolvenzen, Ansehensverluste betroffener Personen und/oder kirchlicher Stellen.
3. Beeinträchtigung der persönlichen Unversehrtheit
Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung
Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung
Eine breite Ansehens- oder Vertrauensbeeinträchtigung, d.h. innerhalb der Evangelische Kirche in Deutschland, ihrer Gliedkirchen und ihrer gliedkirchlichen Zusammenschlüsse sowie die ihnen zugeordneten kirchlichen und diakonischen Werke und Einrichtungen, ist zu erwarten.
6. Finanzielle Auswirkungen
Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend. Oder der zu erwartende direkte Schaden ist größer als 50.000 € und kleiner als 500.000 €.

Schutzbedarf „sehr hoch“:
1. Verstoß gegen Gesetze/Vorschriften/Verträge
Fundamentaler Verstoß gegen Vorschriften und Gesetze. Daten, die besonderen rechtlichen Verschwiegenheitsbeschränkungen unterliegen und deren Preisgabe einen Straftatbestand darstellen. Vertragsverletzungen, deren Haftungsschäden ruinös sind.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts (personenbezogene Daten bzw. Datenschutz)
Eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen ist möglich. Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann (Stichwort: physische Existenz), z. B. Adressen von verdeckten Ermittlern, Adressen von Personen, die mögliche Opfer einer Straftat sein können. Hochsensible Daten, wie die Unterbringung in Anstalten und Einrichtungen, Daten zur Intimsphäre, zu Straftaten, zu erzieherischen Maßnahmen, Pflegedaten oder Daten von Berufsgeheimnisträgern gemäß § 203 StGB oder ein breiter öffentlicher Ansehensverlust.
3. Beeinträchtigung der persönlichen Unversehrtheit
Es besteht Gefahr für Leib und Leben.
4. Beeinträchtigung der Aufgabenerfüllung
Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung
Eine Ansehens- oder Vertrauensbeeinträchtigung innerhalb der Kirchen und in der Beziehung zu den öffentlichen Behörden auf allen regionalen Ebenen ist denkbar. Ein mindestens landesweiter Vertrauensverlust ist zu erwarten.
6. Finanzielle Auswirkungen
Der finanzielle Schaden ist für die Institution existenzbedrohend. Oder der zu erwartende direkte Schaden übersteigt die Grenze von 500.000€.

Schutzbedarfsfeststellung

Muster zur Schutzbedarfsfeststellung

Die folgenden Schutzbedarfsfeststellungen wurden von der Arbeitsgruppe Muster IT-Sicherheitskonzepte der EKD unter Mithilfe von Experten aus den jeweiligen Fachbereichen beispielhalft erarbeitet. Somit stellt dies nur ein Muster dar, das zur Orientierung für die Erstellung eines IT-Sicherheitskonzeptes (siehe Kapitel 4: Schutzbedarfsfeststellung im Muster-IT-Sicherheitskonzept für mittlere und große Einrichtungen) zur Verfügung gestellt wird.

Personalwesen

Schutzziel „Vertraulichkeit“ PERSONALWESEN	
Schadenszenario	**Schutzbedarf**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Normal** Verletzung des Datenschutzes bei Mitarbeitendendaten.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Hoch** Inhalt der Daten (z. B. Daten zur Unterbringung in Anstalten, Straffälligkeit, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Insolvenzen) kann zu einer Beeinträchtigung des informationellen Selbstbestimmungsrechts führen.
Beeinträchtigung der persönlichen Unversehrtheit	**Normal** Kein Schaden möglich.
Beeinträchtigung der Aufgabenerfüllung	**Hoch** Einzelne Betroffene sehen Schaden möglicherweise als nicht tolerabel an.
Negative Innen- oder Außenwirkung	**Hoch** Ein breiter Vertrauensverlust ist zu befürchten.
Finanzielle Auswirkungen	

Schutzziel „Integrität“ PERSONALWESEN	
Schadenszenario	**Schutzbedarf**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Normal** Keine Schäden durch Integritätsverlust zu erwarten.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Hoch** Eine Beeinträchtigung ist durch Integritätsverlust von Sozialdaten zu erwarten.
Beeinträchtigung der persönlichen Unversehrtheit	**Normal** Es sind keine Schäden durch Integritätsverlust zu erwarten.
Beeinträchtigung der Aufgabenerfüllung	**Normal** Es sind keine Schäden durch Integritätsverlust zu erwarten.
Negative Innen- oder Außenwirkung	**Normal** Durch Integritätsverlust sind nur tolerable Schäden zu erwarten.
Finanzielle Auswirkungen	**Hoch** Eventuelle Klagen von Betroffenen durch fehlerhafte Personalauswahl sind möglich.

Schutzziel „Verfügbarkeit“ PERSONALWESEN	
Schadenszenario	**Schutzziel**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Normal** Nur geringfügige Konsequenzen durch Verstöße zu erwarten.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Normal** Keine Beeinträchtigung des Betroffenen zu erwarten.
Beeinträchtigung der persönlichen Unversehrtheit	**Hoch** Eine Beeinträchtigung des Betroffenen kann nicht ausgeschlossen werden (z. B. keine Überweisung des Gehalts).
Beeinträchtigung der Aufgabenerfüllung	**Hoch** Einzelne Personen würden es nicht als tolerabel einschätzen (z. B. Ausfall der Zeiterfassung).
Negative Innen- oder Außenwirkung	**Hoch** Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten (z. B. Ausfall in kirchlichem Rechenzentrum).
Finanzielle Auswirkungen	**Hoch** Reparaturkosten von über 50.000€ könnten entstehen.

Meldewesen

Schutzziel „Vertraulichkeit“ MELDEWESEN	
Schadenszenario	**Schutzbedarf**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Hoch** Bei Verstoß gegen das Meldegesetz droht ein Zugriffsentzug auf Meldedaten.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Hoch** Besonders sensible Daten (z. B. sexuelle Orientierung) können erhebliche Konsequenzen für den Betroffenen haben.
Beeinträchtigung der persönlichen Unversehrtheit	**Hoch** Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden (wegen Sperrvermerk).
Beeinträchtigung der Aufgabenerfüllung	**Normal** Es sind keine Auswirkungen zu erwarten.
Negative Außenwirkung	**Hoch** Die Veröffentlichung von Meldedaten ist nicht unmittelbar existenzbedrohend.
Finanzielle Auswirkungen	**Normal** Direkte Strafzahlungen sind tolerierbar.

Schutzziel „Integrität“ MELDEWESEN	
Schadenszenario	**Schutzbedarf**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Normal** Keine Änderung von sensiblen Meldewesendaten zu erwarten.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Normal** Der Verlust des Sperrvermerkes ist tolerierbar.
Beeinträchtigung der persönlichen Unversehrtheit	**Hoch** Bei Verlust des Sperrvermerkes kann die Beeinträchtigung der persönlichen Unversehrtheit nicht absolut ausgeschlossen werden.
Beeinträchtigung der Aufgabenerfüllung	**Normal** Große Fehler würden schnell erkannt werden.
Negative Innen- oder Außenwirkung	**Normal** Keine wesentlichen Schäden zu erwarten.
Finanzielle Auswirkungen	**Normal** Finanzielle Auswirkungen sind tolerabel.

Schutzziel „Verfügbarkeit“ MELDEWESEN	
Schadenszenario	**Schutzziel**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Normal** Keine Anforderungen vorhanden.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Normal** Kein Schaden möglich.
Beeinträchtigung der persönlichen Unversehrtheit	**Normal** Kein Schaden möglich.
Beeinträchtigung der Aufgabenerfüllung	**Normal** Kein Schaden möglich, da ein Ausfall des Meldewesens größer 24 h vertretbar ist.
Negative Innen- oder Außenwirkung	**Normal** Kein Schaden möglich.
Finanzielle Auswirkungen	**Normal** Auswirkungen sind tolerierbar.

Finanzwesen

Schutzziel „Vertraulichkeit“ FINANZWESEN	
Schadenszenario	**Schutzbedarf**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Normal** Es sind nur geringe Strafen zu erwarten.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Normal** Es ist keine Beeinträchtigung zu erwarten, da keine besonderen personenbezogenen Daten vorhanden sind.
Beeinträchtigung der persönlichen Unversehrtheit	**Normal** Eine Beeinträchtigung ist ausgeschlossen.
Beeinträchtigung der Aufgabenerfüllung	**Normal** Es ist keine Beeinträchtigung zu erwarten.
Negative Innen- oder Außenwirkung	**Normal** Es ist kein breiter Ansehensverlust zu befürchten.
Finanzielle Auswirkungen	

Schutzziel „Integrität“ FINANZWESEN	
Schadenszenario	**Schutzbedarf**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Hoch** Ein Verstoß gegen Gesetze kann erhebliche Konsequenzen bedeuten.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Normal** Keine Beeinträchtigung möglich.
Beeinträchtigung der persönlichen Unversehrtheit	**Normal** Keine Beeinträchtigung möglich.
Beeinträchtigung der Aufgabenerfüllung	**Hoch** Eine Beeinträchtigung ist von einzelnen Betroffenen zu erwarten.
Negative Innen- oder Außenwirkung	**Hoch** Eine negative Außenwirkung ist kirchenweit und in einzelnen Fällen landesweit zu erwarten. Diese sind nicht existenzbedrohend.
Finanzielle Auswirkungen	**Hoch** Hohe finanzielle Auswirkungen sind zu erwarten.

Schutzziel „Verfügbarkeit“ FINANZWESEN	
Schadenszenario	**Schutzziel**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Hoch** Ein Verstoß kann erhebliche Konsequenzen haben (z. B. Zahlung von Steuern und Sozialabgaben).
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Normal** Eine Beeinträchtigung erscheint nicht möglich.
Beeinträchtigung der persönlichen Unversehrtheit	**Hoch** Eine Beeinträchtigung des Betroffenen kann nicht ausgeschlossen werden (z. B. keine Überweisung des Gehalts).
Beeinträchtigung der Aufgabenerfüllung	**Hoch** Nur einige Betroffene werden beeinträchtigt. Eine Ausfallzeit ist bis zu 24h noch tolerierbar.
Negative Innen- oder Außenwirkung	**Hoch** Es ist eine negative innerkirchliche Wirkung zu erwarten.
Finanzielle Auswirkungen	**Hoch** Hohe Sanktionen bei fehlenden Steuerzahlungen und Sozialabgaben.

Diakonie

Schutzziel „Vertraulichkeit“ DIAKONIE	
Schadenszenario	**Schutzbedarf**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Sehr hoch** Es gibt besondere rechtliche Verschwiegenheitsbeschränkungen (z. B. Gesundheitsdaten, Patientendaten, ärztliche Schweigepflicht).
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Sehr hoch** Es existieren Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann.
Beeinträchtigung der persönlichen Unversehrtheit	**Hoch** Eine Gefährdung von Leib und Leben kann nicht ausgeschlossen werden.
Beeinträchtigung der Aufgabenerfüllung	**Hoch** Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt.
Negative Innen- oder Außenwirkung	**Sehr hoch** Eine Ansehens- oder Vertrauensbeeinträchtigung innerhalb der Kirchen und in der Beziehung zu den öffentlichen Behörden auf allen regionalen Ebenen ist denkbar. Es ist mit einem mindestens landesweiten Vertrauensverlust zu rechnen.
Finanzielle Auswirkungen	**Hoch** Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend (kleiner 500.000€).

Schutzziel „Integrität“ DIAKONIE	
Schadenszenario	**Schutzbedarf**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Normal** Keine Vertragsverletzungen bekannt.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Normal** Eine Beeinträchtigung der informationellen Selbstbestimmung ist eher unwahrscheinlich.
Beeinträchtigung der persönlichen Unversehrtheit	**Hoch** Eine Beeinträchtigung der persönlichen Unversehrtheit kann in Einzelfällen nicht ausgeschlossen werden.
Beeinträchtigung der Aufgabenerfüllung	**Hoch** Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt werden.
Negative Innen- oder Außenwirkung	**Normal** Verletzungen der Integrität werden vermutlich nicht nach außen

Schutzziel „Integrität“ DIAKONIE	
Schadenszenario	**Schutzbedarf**
	dringen.
Finanzielle Auswirkungen	**Normal** Keine großen finanziellen Auswirkungen bei Verletzung der Integrität zu erwarten.

Schutzziel „Verfügbarkeit“ DIAKONIE	
Schadenszenario	**Schutzziel**
Verstoß gegen Gesetze / Vorschriften / Verträge	**Normal** Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Normal** Es sind keine Beeinträchtigung zu erwarten.
Beeinträchtigung der persönlichen Unversehrtheit	**Hoch** Eine Beeinträchtigung kann nicht absolut ausgeschlossen werden.
Beeinträchtigung der Aufgabenerfüllung	**Hoch** Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt werden. Eine Ausfallzeit von mehr als 24h kann zu Beeinträchtigungen führen.
Negative Innen- oder Außenwirkung	**Normal** Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	**Normal** Der finanzielle Schaden bleibt für die Institution tolerabel (kleiner als 50.000€).

Modellierungsvorschrift

1. Allgemeines

Die in diesem Dokument beschriebenen Modellierungsvorschriften sind dem BSI IT-Grundschutzkatalogen des Bundesamts für Sicherheit in der Informationstechnik entnommen. Für die Erstellung von IT-Sicherheitskonzepten (siehe Kapitel 5 im Muster-IT-Sicherheitskonzept für mittlere und große Einrichtungen) sind diese Modellierungsvorschriften als Empfehlung anzusehen, von denen auch begründet abgewichen werden kann.

2. Übergeordnete Aspekte

Der Baustein B 1.0 Sicherheitsmanagement ist für den gesamten Informationsverbund einmal an-zuwenden. Ein funktionierendes Informationssicherheitsmanagement ist die wesentliche Grundlage für die Erreichung eines angemessenen Sicherheitsniveaus. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

Der Baustein B 1.1 Organisation muss für jeden Informationsverbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden Informationsverbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

Der Baustein B 1.2 Personal muss für jeden Informationsverbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden Informationsverbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

Der Baustein B 1.3 Notfallmanagement ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Verfügbarkeit haben oder wenn größere IT-Systeme bzw. umfangreiche Netze betrieben werden. Bei der Bearbeitung des Bausteins ist besonderes Augenmerk auf diese Komponenten zu richten. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

Der Baustein B 1.4 Datensicherungskonzept ist für den gesamten Informationsverbund einmal anzuwenden.

Der Baustein B 1.5 Datenschutz dient für Anwender in Deutschland zur Orientierung, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert werden, bei denen eine Verarbeitung und sonstige Nutzung personenbezogener oder -beziehbarer Daten erfolgt. Dabei sollte dann geprüft werden, ob der Baustein nicht nur auf einzelne Informationsverbünde oder Verfahren, sondern auf die gesamte Institution anzuwenden ist.

Der Baustein B 1.6 Schutz vor Schadsoftware ist für den gesamten Informationsverbund einmal anzuwenden.

Der Baustein B 1.7 Kryptokonzept ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Vertraulichkeit oder Integrität haben, oder wenn bereits kryptographische Verfahren im Einsatz sind.

Der Baustein B 1.8 Behandlung von Sicherheitsvorfällen ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf einen der drei Grundwerte haben, oder wenn der Ausfall des gesamten Informationsverbunds einen Schaden in den Kategorien hoch oder sehr hoch zur Folge hat. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

Der Baustein B 1.9 Hard- und Software-Management muss für jeden Informationsverbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden Informationsverbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

Der Baustein B 1.10 Standardsoftware ist zumindest einmal für den gesamten Informationsverbund anzuwenden. Gibt es innerhalb des Informationsverbunds Teilbereiche mit unterschiedlichen Anforderungen oder Regelungen für die Nutzung von Standardsoftware, sollte Baustein B 1.10 auf diese Teilbereiche jeweils getrennt angewandt werden.

Der Baustein B 1.11 Outsourcing ist zumindest dann anzuwenden, wenn die folgenden Bedingungen alle erfüllt sind: IT-Systeme, Anwendungen oder Geschäftsprozesse werden zu einem externen Dienstleister ausgelagert, und die Bindung an den Dienstleister erfolgt auf längere Zeit, und durch die Dienstleistung kann die Informationssicherheit des Auftraggebers beeinflusst werden, und im Rahmen der Dienstleistungen erbringt der Dienstleister auch regelmäßig nennenswerte Tätigkeiten im Bereich Informationssicherheitsmanagement. Gibt es in einem Informationsverbund verschiedene ausgelagerte Komponenten bei unterschiedlichen Dienstleistern, ist der Baustein für jeden externen Dienstleister einmal anzuwenden. Für die Anwendung dieses Bausteins gelten besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

Der Baustein B 1.12 Archivierung ist auf den Informationsverbund anzuwenden, wenn aufgrund interner oder externer Vorgaben eine Langzeitarchivierung elektronischer Dokumente erforderlich ist oder bereits ein System zur Langzeitarchivierung elektronischer Dokumente betrieben wird.

Der Baustein B 1.13 IT-Sicherheitssensibilisierung und -schulung ist für den gesamten Informationsverbund einmal anzuwenden.

Der Baustein B 1.14 Patch- und Änderungsmanagement ist zumindest bei größeren Informationsverbünden anzuwenden, also wenn größere IT-Systeme bzw. umfangreiche Netze betrieben werden. Bei kleineren und wenig komplexen Informationsverbünden reicht die Umsetzung von M 2.221 Änderungsmanagement aus.

Der Baustein B 1.15 Löschen und Vernichten von Daten ist für den gesamten Informationsverbund einmal anzuwenden.

Der Baustein B 1.16 Anforderungsmanagement ist für den gesamten Informationsverbund einmal anzuwenden.

3. Infrastruktur

Der Baustein B 2.1 Allgemeines Gebäude ist für jedes Gebäude bzw. jede Gebäudegruppe einmal anzuwenden.

Der Baustein B 2.2 Elektrotechnische Verkabelung ist in der Regel einmal pro Gebäude bzw. Gebäudegruppe anzuwenden (zusätzlich zum Baustein B 2.1 Allgemeines Gebäude). Darüber hinaus kann der Baustein B 2.2 auch für einzelne Räume bzw. Raumgruppen, wie beispielsweise Serverräume oder Rechenzentren, angewendet werden, wenn diese Besonderheiten in Bezug auf die elektrotechnische Verkabelung aufweisen. Für die IT-Verkabelung ist zusätzlich der Baustein B 2.12 IT-Verkabelung anzuwenden.

Der Baustein B 2.3 Büroraum / Lokaler Arbeitsplatz ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen sich Mitarbeiter aufhalten, um dort ihre Aufgaben zu erledigen.

Der Baustein B 2.4 Serverraum ist auf jeden Raum oder Bereiche bzw. jede Gruppe von Räumen anzuwenden, in denen Server oder TK-Anlagen betrieben werden. Server sind IT-Systeme, die Dienste im Netz zur Verfügung stellen. Für Räumlichkeiten, auf die der Baustein B 2.9 angewandt wird, muss nicht zusätzlich der Baustein B 2.4 herangezogen werden.

Der Baustein B 2.5 Datenträgerarchiv ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Datenträger gelagert oder archiviert werden.

Der Baustein B 2.6 Raum für technische Infrastruktur ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen technische Geräte betrieben werden, die keine oder nur wenig Bedienung erfordern (z. B. Verteilerschrank, Netzersatzanlage).

Der Baustein B 2.7 Schutzschränke ist auf jeden Schutzschrank bzw. jede Gruppe von Schutzschränken einmal anzuwenden. Schutzschränke können gegebenenfalls als Ersatz für einen dedizierten Serverraum dienen.

Der Baustein B 2.8 Häuslicher Arbeitsplatz ist auf jeden häuslichen Arbeitsplatz bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.

Der Baustein B 2.9 Rechenzentrum ist auf jedes Rechenzentrum einmal anzuwenden. Als Rechenzentrum werden Einrichtungen und Räumlichkeiten bezeichnet, die für den Betrieb einer größeren, zentral für mehrere Stellen eingesetzten Datenverarbeitungsanlage erforderlich sind. Für Räumlichkeiten, auf die der Baustein B 2.9 angewandt wird, muss nicht zusätzlich der Baustein B 2.4 herangezogen werden.

Der Baustein B 2.10 Mobiler Arbeitsplatz ist immer dann anzuwenden, wenn Mitarbeiter häufig nicht mehr nur innerhalb der Räumlichkeiten des Unternehmens bzw. der Behörde arbeiten, sondern an wechselnden Arbeitsplätzen außerhalb. Typische Zielobjekte für den Baustein B 2.10 sind Laptops.

Der Baustein B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume ist auf jeden solchen Raum bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.

Der Baustein B 2.12 IT-Verkabelung ist in der Regel einmal pro Gebäude bzw. Gebäudegruppe anzuwenden (zusätzlich zum Baustein B 2.1 Allgemeines Gebäude). Darüber hinaus kann der Baustein B 2.12 auch für einzelne Räume bzw. Raumgruppen, wie beispielsweise Serverräume oder Rechenzentren, angewendet werden, wenn diese Besonderheiten in Bezug auf die IT-Verkabelung aufweisen. Für die elektrotechnische Verkabelung ist zusätzlich der Baustein B 2.2 Elektrotechnische Verkabelung anzuwenden.

4. IT-Systeme

Der Baustein B 3.101 Allgemeiner Server ist auf jedes IT-System anzuwenden, das Dienste (z. B. Datei- oder Druckdienste) als Server im Netz anbietet.

Der Baustein B 3.102 Server unter Unix ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.

Der Baustein B 3.107 S/390- und zSeries-Mainframe ist auf jeden Großrechner anzuwenden, der vom Typ S/390 oder zSeries ist.

Der Baustein B 3.108 Windows Server 2003 ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.

Der Baustein B 3.109 Windows Server 2008 ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.

Hinweis: Für jeden Server (und auch jeden Großrechner) muss neben dem Betriebssystem-spezifischen Baustein immer auch Baustein B 3.101 Allgemeiner Server angewandt werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte für Server zusammengefasst sind.

Der Baustein B 3.201 Allgemeiner Client ist auf jeden Client anzuwenden. Clients sind Arbeitsplatz-Computer, die regelmäßig oder zumindest zeitweise in einem Netz betrieben werden (im Gegensatz zu Einzelplatz-Systemen).

Der Baustein B 3.202 Allgemeines nicht vernetztes IT-System ist auf jedes Einzelplatz-System anzuwenden. Einzelplatz-Systeme sind Arbeitsplatz-Computer, die gar nicht oder nur in Ausnahmefällen in einem Netz betrieben werden (im Gegensatz zu Clients).

Der Baustein B 3.203 Laptop ist auf jeden mobilen Computer (Laptop) anzuwenden.

Der Baustein B 3.204 Client unter Unix ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.

Der Baustein B 3.208 Internet-PC ist auf jeden Computer anzuwenden, der ausschließlich für die Nutzung von Internet-Diensten vorgesehen ist und nicht mit dem internen Netz der Institution verbunden ist. In diesem speziellen Szenario brauchen keine weiteren Bausteine der IT-Grundschutz-Kataloge auf diesen Computer (bzw. diese Gruppe) angewandt werden.

Der Baustein B 3.209 Client unter Windows XP ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.

Der Baustein B 3.210 Client unter Windows Vista ist auf jedem Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.

Der Baustein B 3.211 Client unter MacOS X ist auf jedem Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.

Der Baustein B 3.212 Client unter Windows 7 ist auf jedem Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.

Hinweis: Für jeden Client muss neben dem Betriebssystem-spezifischen Baustein immer auch entweder Baustein B 3.201 Allgemeiner Client oder Baustein B 3.202 Allgemeines nicht vernetztes IT-System angewandt werden, da in diesen Bausteinen die plattformunabhängigen Sicherheitsaspekte für Clients zusammengefasst sind.

Der Baustein B 3.301 Sicherheitsgateway (Firewall) ist immer anzuwenden, wenn unterschiedlich vertrauenswürdige Netze gekoppelt werden. Ein typischer Anwendungsfall ist die Absicherung einer Außenverbindung (z. B. beim Übergang eines internen Netzes zum Internet oder bei Anbindungen zu Netzen von Geschäftspartnern). Aber auch bei einer Kopplung von zwei

organisationsinternen Netzen mit unterschiedlich hohem Schutzbedarf ist der Baustein anzuwenden, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Entwicklungsabteilung, wenn dort besonders vertrauliche Daten verarbeitet werden.

Der Baustein B 3.302 Router und Switches ist in jedem aktiven Netz, das im vorliegenden Informationsverbund eingesetzt wird, anzuwenden.

Der Baustein B 3.303 Speichersysteme und Speichernetze ist immer dann anzuwenden, wenn für die Datenspeicherung dedizierte Speichersysteme eingesetzt werden. Typische Zielobjekte für diesen Baustein sind NAS-Systeme (Network Attached Storage) und SAN-Systeme (Storage Area Networks).

Der Baustein B 3.304 Virtualisierung ist auf jeden Virtualisierungsserver oder jede Gruppe von Virtualisierungsservern anzuwenden.

Der Baustein B 3.305 Terminalserver ist auf jeden Terminalserver des betrachteten Informationsverbunds anzuwenden.

Der Baustein B 3.401 TK-Anlage ist auf jede TK-Anlage bzw. auf jede entsprechende Gruppe anzuwenden.

Der Baustein B 3.402 Faxgerät ist auf jedes Faxgerät bzw. auf jede entsprechende Gruppe anzuwenden.

Der Baustein B 3.404 Mobiltelefon sollte mindestens einmal angewandt werden, wenn die Benutzung von Mobiltelefonen in der betrachteten Organisation(-seinheit) nicht grundsätzlich untersagt ist. Bestehen mehrere unterschiedliche Einsatzbereiche von Mobiltelefonen (beispielsweise mehrere Mobiltelefon-Pools), so ist der Baustein B 3.404 jeweils getrennt darauf anzuwenden.

Der Baustein B 3.405 PDA sollte mindestens einmal angewandt werden, wenn die Benutzung von PDAs in der betrachteten Organisation(-seinheit) nicht grundsätzlich untersagt ist. Der Baustein B 3.201 Allgemeiner Client muss hier nicht zusätzlich angewandt werden.

Der Baustein B 3.406 Drucker, Kopierer und Multifunktionsgeräte sollte mindestens einmal pro Informationsverbund angewandt werden. Als Multifunktionsgeräte werden dabei Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste.

5. Netze

Der Baustein B 4.1 Heterogene Netze ist in der Regel auf jedes Teilnetz einmal anzuwenden. Falls die Teilnetze klein sind und mehrere Teilnetze in der Zuständigkeit des gleichen Administratoren-Teams liegen, kann es jedoch ausreichend sein, den Baustein B 4.1 auf diese Teilnetze insgesamt einmal anzuwenden.

Der Baustein B 4.2 Netz- und Systemmanagement ist auf jedes Netz- bzw. Systemmanagement-System anzuwenden, das im vorliegenden Informationsverbund eingesetzt wird.

Der Baustein B 4.3 Modem ist auf alle Außenverbindungen anzuwenden, die über Modems realisiert sind.

Der Baustein B 4.4 VPN ist für jede Art von Fernzugriffen auf den Informationsverbund, also interne Netze oder IT-Systeme, einmal anzuwenden. Hierzu gehören Verbindungen über Datennetze, wie z. B. Site-to-Site-, End-to-End- oder Remote-Access-VPNs, und über Telekommunikationsverbindungen, wie z. B. über analoge Wählleitungen, ISDN- oder Mobiltelefonie.

Der Baustein B 4.5 LAN-Anbindung eines IT-Systems über ISDN ist auf alle Außenverbindungen anzuwenden, die über ISDN realisiert sind.

Der Baustein B 4.6 WLAN ist auf alle Kommunikationsnetze anzuwenden, die gemäß der Standardreihe IEEE 802.11 und deren Erweiterungen realisiert sind.

Der Baustein B 4.7 VoIP ist auf alle Kommunikationsnetze anzuwenden, in denen VoIP-Technologie zum Einsatz kommt. Tauschen leitungsvermittelnde TK-Anlagen Informationen untereinander über ein IP-Netz aus, ist der Baustein B 4.7 VoIP ebenfalls anzuwenden.

Der Baustein B 4.8 Bluetooth ist immer dann anzuwenden, wenn Bluetooth für Kommunikationsverbindungen benutzt wird bzw. IT-Komponenten mit Bluetooth-Schnittstellen in der Institution genutzt werden.

6. IT-Anwendungen

Der Baustein B 5.2 Datenträgeraustausch sollte für jede Anwendung einmal herangezogen werden, die als Datenquelle für einen Datenträgeraustausch dient oder auf diesem Wege eingegangene Daten weiterverarbeitet.

Der Baustein B 5.3 Groupware ist auf jedes E-Mail-System (intern oder extern) des betrachteten Informationsverbunds anzuwenden.

Der Baustein B 5.4 Webserver ist auf jeden WWW-Dienst (z. B. Intranet oder Internet) des betrachteten Informationsverbunds anzuwenden.

Der Baustein B 5.5 Lotus Notes ist auf jedes Workgroup-System, das auf dem Produkt Lotus Notes basiert, bzw. auf jede entsprechende Gruppe im Informationsverbund einmal anzuwenden.

Der Baustein B 5.6 Faxserver ist auf jeden Faxserver bzw. auf jede entsprechende Gruppe anzuwenden.

Der Baustein B 5.7 Datenbanken sollte pro Datenbanksystem bzw. pro Gruppe von Datenbanksystemen einmal angewandt werden.

Der Baustein B 5.8 Telearbeit ist bei jedem Telearbeitsplatz bzw. auf jede entsprechende Gruppe anzuwenden.

Der Baustein B 5.9 Novell eDirectory sollte auf jeden Verzeichnisdienst, der mit Hilfe von Novell eDirectory realisiert ist, einmal angewandt werden. Zusätzlich ist immer der Baustein B 5.15 Allgemeiner Verzeichnisdienst anzuwenden.

Der Baustein B 5.12 Exchange/Outlook ist - zusätzlich zu Baustein B 5.3 Groupware - auf jedes Workgroup- oder E-Mail-System anzuwenden, das auf Microsoft Exchange bzw. Outlook basiert.

Der Baustein B 5.13 SAP System ist auf jede Applikation für Geschäftsprozesse (oder Gruppe solcher Applikationen) anzuwenden, die auf Software des Herstellers SAP basiert.

Der Baustein B 5.14 Mobile Datenträger sollte mindestens einmal pro Informationsverbund angewandt werden.

Der Baustein B 5.15 Allgemeiner Verzeichnisdienst sollte - unabhängig vom gewählten Produkt - auf jeden Verzeichnisdienst einmal angewandt werden.

Der Baustein B 5.16 Active Directory sollte auf jeden Verzeichnisdienst, der mit Hilfe von Microsoft Active Directory realisiert ist, einmal angewandt werden. Zusätzlich ist immer der Baustein B 5.15 Allgemeiner Verzeichnisdienst anzuwenden.

Der Baustein B 5.17 Samba ist auf jedem Samba-Server des betrachteten Informationsverbunds anzuwenden.

Der Baustein B 5.18 DNS-Server ist auf jeden im Informationsverbund betriebenen DNS-Server bzw. auf jede Gruppe von DNS-Servern anzuwenden.

Der Baustein B 5.19 Internet-Nutzung ist immer dann anzuwenden, wenn Internet-Dienste vom Arbeitsplatz genutzt werden sollen.

Der Baustein B 5.20 OpenLDAP sollte auf jeden Verzeichnisdienst, der mit Hilfe von OpenLDAP realisiert ist, einmal angewandt werden. Zusätzlich ist immer der Baustein B 5.15 Allgemeiner Verzeichnisdienst anzuwenden.

Der Baustein B 5.21 Webanwendungen ist auf jeden als Webanwendung ausgelegten Web-Dienst (z. B. Intranet oder Internet) des betrachteten Informationsverbunds anzuwenden.

Der Baustein B 5.22 Protokollierung ist zumindest bei größeren Informationsverbünden anzuwenden, also wenn größere IT-Systeme bzw. umfangreiche Netze betrieben werden. Bei kleineren und wenig komplexen Informationsverbünden reicht die Umsetzung von M 2.500 Protokollierung von IT-Systemen aus.

Gefährdungskatalog

1. Allgemeines

Die in diesem Dokument enthaltenen Gefährdungen[5] sind dem BSI IT-Grundschutzkatalogen des Bundesamts für Sicherheit in der Informationstechnik entnommen. Dieser Gefährdungskatalog stellt eine Auswahl an möglichen Gefährdungen für die Risikoanalyse (siehe Kapitel 8: B_Muster groß.docx) eines IT-Sicherheitskonzeptes dar.

[5] Siehe: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Gefaehrdungs-katalog-G0-ElementareGefaehrdungen.pdf

2. Gefährdungskatalog

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheits-ziel
G 0.1	Feuer	I, A
G 0.2	Ungünstige klimatische Bedingungen	I, A
G 0.3	Wasser	I, A
G 0.4	Verschmutzung, Staub, Korrosion	I, A
G 0.5	Naturkatastrophen	A
G 0.6	Katastrophen im Umfeld	A
G 0.7	Großereignisse im Umfeld	C, I, A
G 0.8	Ausfall oder Störung der Stromversorgung	I, A
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A
G 0.12	Elektromagnetische Störstrahlung	I, A
G 0.13	Abfangen kompromittierender Strahlung	C
G 0.14	Ausspähen von Informationen / Spionage	C
G 0.15	Abhören	C
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	C, A
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A
G 0.19	Offenlegung schützenswerter Informationen	C
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	C, I, A
G 0.21	Manipulation von Hard- oder Software	C, I, A
G 0.22	Manipulation von Informationen	I
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I
G 0.24	Zerstörung von Geräten oder Datenträgern	A
G 0.25	Ausfall von Geräten oder Systemen	A
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A
G 0.27	Ressourcenmangel	A
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.32	Missbrauch von Berechtigungen	C, I, A
G 0.33	Personalausfall	A
G 0.34	Anschlag	C, I, A
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheits-ziel
G 0.36	Identitätsdiebstahl	C, I, A
G 0.37	Abstreiten von Handlungen	C, I
G 0.38	Missbrauch personenbezogener Daten	C
G 0.39	Schadprogramme	C, I, A
G 0.40	Verhinderung von Diensten (Denial of Service)	A
G 0.41	Sabotage	A
G 0.42	Social Engineering	C, I
G 0.43	Einspielen von Nachrichten	C, I
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A
G 0.45	Datenverlust	A
G 0.46	Integritätsverlust schützenswerter Informationen	I

Risikoanalyse-Template

Management Summary

Ausgangslage

[Kurzfassung der Beschreibung der Ausgangslage sowie des organisatorischen/technischen Umfelds]

Zusammenfassung der Ergebnisse

A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen

- Zusammenfassung der Maßnahmen aus Kapitel 6

B. Risikovermeidung

- Zusammenfassung der Maßnahmen aus Kapitel 6

C. Risikoübernahme

- Zusammenfassung der Maßnahmen aus Kapitel 6

D. Risikotransfer

- Zusammenfassung der Maßnahmen aus Kapitel 6

1. Allgemeines

Dieses Dokument beschreibt eine Möglichkeit zur Durchführung einer Risikoanalyse, wie im IT-Sicherheitskonzept gefordert wird (siehe Kapitel 8: Muster-IT-Sicherheitskonzept für mittlere und große Einrichtungen). In den folgenden Kapiteln wird eine Risikoanalyse nach dem BSI-Standard 100-3 durchgeführt.

2. Einleitung

Ziel einer Risikoanalyse ist es, die vorhandenen Risiken durch eine Risikobehandlung auf ein verträgliches/akzeptables Maß (Restrisiko) zu reduzieren.

Ein Risiko ist ein mögliches Ereignis mit unerwünschter Wirkung und wird als Produkt von Eintrittswahrscheinlichkeit und Schadenshöhe betrachtet.

Im ersten Schritt werden **die relevanten Risiken** für das Zielobjekt herausgearbeitet. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen, so genannte elementare G0 Gefährdungen (vgl. IT-Grundschutz – G0-Katalog), als Hilfsmittel verwendet. Bei den elementaren Gefährdungen wurde der Fokus darauf gelegt, **tatsächliche Gefahren** zu benennen. Gefährdungen, die überwiegend die fehlende oder unzureichende Umsetzung von Sicherheitsmaßnahmen thematisieren und somit auf indirekte Gefahren verweisen, werden somit bewusst vermieden.

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.

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 19) gruppiert.

Tabelle 19: 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		

In der hier beschriebenen Methodik nach BSI Standard 100-3 werden Eintrittswahrscheinlichkeiten nicht explizit, sondern lediglich implizit im Rahmen der Ermittlung und Bewertung von Gefährdungen betrachtet.

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:

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

3. Gefährdungskatalog G.0 – Festlegung der Relevanz nach dem Sicherheitsziel

Zielobjekt:

Zielobjekt XY

Sicherheitsziel:

Vertraulichkeit (C): Normal, Hoch, Sehr Hoch

Integrität (I): Normal, Hoch, Sehr Hoch

Verfügbarkeit (A): Normal, Hoch, Sehr Hoch

Vorgehensweise:

Reduktion der G.0 Gefährdungen hinsichtlich der Sicherheitsziele

- **Fall 1:** Sicherheitsziele unterschiedlich ausgeprägt
  - Reduzierung hinsichtlich der Sicherheitsziele
  - G.0 Gefährdungen mit normalen Schutzbedarf werden gemäß der Entscheidungen in der ergänzenden Sicherheitsanalyse nicht betrachtet
- **Fall 2:** Sicherheitsziele gleich ausgeprägt
  - Keine Reduktion, alle G.0 Gefährdungen sind relevant
  - Weiter mit Kapitel 4.
- **Fall 3:** Keine relevanten Bausteine vorhanden
  - Keine Reduktion, alle G.0 Gefährdungen sind relevant
  - Weiter mit Kapitel 4.

Tabelle 20: G.0 Gefährdungen

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel
G 0.1	Feuer	I, A
G 0.2	Ungünstige klimatische Bedingungen	I, A
G 0.3	Wasser	I, A
G 0.4	Verschmutzung, Staub, Korrosion	I, A
G 0.5	Naturkatastrophen	A
G 0.6	Katastrophen im Umfeld	A
G 0.7	Großereignisse im Umfeld	C, I, A
G 0.8	Ausfall oder Störung der Stromversorgung	I, A
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A
G 0.12	Elektromagnetische Störstrahlung	I, A
G 0.13	Abfangen kompromittierender Strahlung	C
G 0.14	Ausspähen von Informationen / Spionage	C
G 0.15	Abhören	C
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	C, A
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A
G 0.19	Offenlegung schützenswerter Informationen	C
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	C, I, A
G 0.21	Manipulation von Hard- oder Software	C, I, A
G 0.22	Manipulation von Informationen	I
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I
G 0.24	Zerstörung von Geräten oder Datenträgern	A
G 0.25	Ausfall von Geräten oder Systemen	A
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A
G 0.27	Ressourcenmangel	A
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.32	Missbrauch von Berechtigungen	C, I, A
G 0.33	Personalausfall	A
G 0.34	Anschlag	C, I, A
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A
G 0.36	Identitätsdiebstahl	C, I, A

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel
G 0.37	Abstreiten von Handlungen	C, I
G 0.38	Missbrauch personenbezogener Daten	C
G 0.39	Schadprogramme	C, I, A
G 0.40	Verhinderung von Diensten (Denial of Service)	A
G 0.41	Sabotage	A
G 0.42	Social Engineering	C, I
G 0.43	Einspielen von Nachrichten	C, I
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A
G 0.45	Datenverlust	A
G 0.46	Integritätsverlust schützenswerter Informationen	I

Tabelle 21: Reduzierung G.0 Gefährdungen hinsichtlich des Schutzziels

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel	Relevanz
G 0.1	Feuer	I, A	Ja/Nein
G 0.2	Ungünstige klimatische Bedingungen	I, A	Ja/Nein
G 0.3	Wasser	I, A	Ja/Nein
G 0.4	Verschmutzung, Staub, Korrosion	I, A	Ja/Nein
G 0.5	Naturkatastrophen	A	Ja/Nein
G 0.6	Katastrophen im Umfeld	A	Ja/Nein
G 0.7	Großereignisse im Umfeld	C, I, A	Ja/Nein
G 0.8	Ausfall oder Störung der Stromversorgung	I, A	Ja/Nein
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A	Ja/Nein
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A	Ja/Nein
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A	Ja/Nein
G 0.12	Elektromagnetische Störstrahlung	I, A	Ja/Nein
G 0.13	Abfangen kompromittierender Strahlung	C	Ja/Nein
G 0.14	Ausspähen von Informationen / Spionage	C	Ja/Nein
G 0.15	Abhören	C	Ja/Nein
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A	Ja/Nein
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	C, A	Ja/Nein
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A	Ja/Nein
G 0.19	Offenlegung schützenswerter Informationen	C	Ja/Nein
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	C, I, A	Ja/Nein
G 0.21	Manipulation von Hard- oder Software	C, I, A	Ja/Nein
G 0.22	Manipulation von Informationen	I	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel	Relevanz
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I	Ja/Nein
G 0.24	Zerstörung von Geräten oder Datenträgern	A	Ja/Nein
G 0.25	Ausfall von Geräten oder Systemen	A	Ja/Nein
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A	Ja/Nein
G 0.27	Ressourcenmangel	A	Ja/Nein
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A	Ja/Nein
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A	Ja/Nein
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A	Ja/Nein
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A	Ja/Nein
G 0.32	Missbrauch von Berechtigungen	C, I, A	Ja/Nein
G 0.33	Personalausfall	A	Ja/Nein
G 0.34	Anschlag	C, I, A	Ja/Nein
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A	Ja/Nein
G 0.36	Identitätsdiebstahl	C, I, A	Ja/Nein
G 0.37	Abstreiten von Handlungen	C, I	Ja/Nein
G 0.38	Missbrauch personenbezogener Daten	C	Ja/Nein
G 0.39	Schadprogramme	C, I, A	Ja/Nein
G 0.40	Verhinderung von Diensten (Denial of Service)	A	Ja/Nein
G 0.41	Sabotage	A	Ja/Nein
G 0.42	Social Engineering	C, I	Ja/Nein
G 0.43	Einspielen von Nachrichten	C, I	Ja/Nein
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A	Ja/Nein
G 0.45	Datenverlust	A	Ja/Nein
G 0.46	Integritätsverlust schützenswerter Informationen	I	Ja/Nein

4. Gefährdungskatalog G.0 – Reduktion hinsichtlich der Schadensauswirkung auf das Zielobjekt

Vorgehensweise:

Reduktion der G.0 Gefährdungen hinsichtlich der Schadenswirkung auf das Zielobjekt (Switche)

Tabelle 22: Reduzierte G.0 Gefährdung hinsichtlich der Schadensauswirkung auf das Zielobjekt

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheits-ziel	Schaden möglich?
G 0.1	Feuer	I, A	Ja/Nein
G 0.2	Ungünstige klimatische Bedingungen	I, A	Ja/Nein
G 0.3	Wasser	I, A	Ja/Nein
G 0.4	Verschmutzung, Staub, Korrosion	I, A	Ja/Nein
G 0.5	Naturkatastrophen	A	Ja/Nein
G 0.6	Katastrophen im Umfeld	A	Ja/Nein
G 0.7	Großereignisse im Umfeld	C, I, A	Ja/Nein
G 0.8	Ausfall oder Störung der Stromversorgung	I, A	Ja/Nein
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A	Ja/Nein
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A	Ja/Nein
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A	Ja/Nein
G 0.12	Elektromagnetische Störstrahlung	I, A	Ja/Nein
G 0.13	Abfangen kompromittierender Strahlung	C	Ja/Nein
G 0.14	Ausspähen von Informationen / Spionage	C	Ja/Nein
G 0.15	Abhören	C	Ja/Nein
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A	Ja/Nein
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	C, A	Ja/Nein
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A	Ja/Nein
G 0.19	Offenlegung schützenswerter Informationen	C	Ja/Nein
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	C, I, A	Ja/Nein
G 0.21	Manipulation von Hard- oder Software	C, I, A	Ja/Nein
G 0.22	Manipulation von Informationen	I	Ja/Nein
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I	Ja/Nein
G 0.24	Zerstörung von Geräten oder Datenträgern	A	Ja/Nein
G 0.25	Ausfall von Geräten oder Systemen	A	Ja/Nein
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A	Ja/Nein
G 0.27	Ressourcenmangel	A	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheits-ziel	Schaden möglich?
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A	Ja/Nein
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A	Ja/Nein
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A	Ja/Nein
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A	Ja/Nein
G 0.32	Missbrauch von Berechtigungen	C, I, A	Ja/Nein
G 0.33	Personalausfall	A	Ja/Nein
G 0.34	Anschlag	C, I, A	Ja/Nein
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A	Ja/Nein
G 0.36	Identitätsdiebstahl	C, I, A	Ja/Nein
G 0.37	Abstreiten von Handlungen	C, I	Ja/Nein
G 0.38	Missbrauch personenbezogener Daten	C	Ja/Nein
G 0.39	Schadprogramme	C, I, A	Ja/Nein
G 0.40	Verhinderung von Diensten (Denial of Service)	A	Ja/Nein
G 0.41	Sabotage	A	Ja/Nein
G 0.42	Social Engineering	C, I	Ja/Nein
G 0.43	Einspielen von Nachrichten	C, I	Ja/Nein
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A	Ja/Nein
G 0.45	Datenverlust	A	Ja/Nein
G 0.46	Integritätsverlust schützenswerter Informationen	I	Ja/Nein

5. Reduktion durch vorhandenen Baustein

Vorgehensweise:

Reduktion der G.0 Gefährdungen durch die in vorhandenen Bausteinen bereits umgesetzten Maßnahmen

- Fall 1: Relevante Bausteine vorhanden
  - Verwendung der Kreuzreferenztabelle des entsprechenden Bausteins
  - Reduktion aufgrund vorhandener Gegenmaßnahmen
    - Mechanismenstärke (Durchschnitt über alle Maßnahmen, welche die entsprechende G.0 Gefährdung adressieren)
    - Zuverlässigkeit (Durchschnitt über alle Maßnahmen, welche die entsprechende G.0 Gefährdung adressieren)
    - Vollständigkeit (Durchschnitt über alle Maßnahmen, welche die entsprechende G.0 Gefährdung adressieren)
- Qualität des Maßnahmenbündels ausreichend?
  - Fall 1: Ja, G.0 Gefährdung wird gestrichen
  - Fall 2: Nein, G.0 Gefährdung wird nicht gestrichen
    - Risikoanalyse der G.0 Gefährdung im Kapitel 0.
- Fall 2: Keine relevanten Bausteine vorhanden
  - Verwendung der Kreuzreferenztabelle entfällt bei nicht vorhandenem Baustein
  - nutzerdefinierten Baustein erstellen oder
  - Risikoanalyse der übrigen G.0 Gefährdungen im Kapitel 0.

5.1 Kreuzreferenztabellen der zugehörigen Bausteine

Tabelle 23: Kreuzreferenztabelle des Bausteins "XY"

B XY	Siegelstufe	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins	Spezielle Gefährdung des Bausteins
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			

5.2 Reduktion aufgrund vorhandener Gegenmaßnahmen

Tabelle 24: Bewertung der Reduktion der Gefährdungen aufgrund vorhandener BSI-IT-Grundschutzmaßnahmen aus einem angewendeten Baustein

Nr.	Bezeichnung der elementaren Gefährdung	Maßnahmen-Nr. im Baustein	Qualität des Maßnahmenbündels			Wirksame Gegenmaßnahme vorhanden?
			Mechanismenstärke	Zuverlässigkeit	Vollständigkeit	
G 0.1	Feuer	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.2	Ungünstige klimatische Bedingungen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.3	Wasser	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.4	Verschmutzung, Staub, Korrosion	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.5	Naturkatastrophen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.6	Katastrophen im Umfeld	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.7	Großereignisse im Umfeld	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.8	Ausfall oder Störung der Stromversorgung	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.10	Ausfall oder Störung von Versorgungsnetzen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.11	Ausfall oder Störung von Dienstleistern	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.12	Elektromagnetische Störstrahlung	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.13	Abfangen kompromittierender Strahlung	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.14	Ausspähen von Informationen / Spionage	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.15	Abhören	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.18	Fehlplanung oder fehlende Anpassung	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.19	Offenlegung schützenswerter Informationen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Maßnahmen-Nr. im Baustein	Qualität des Maßnahmenbündels			Wirksame Gegenmaßnahme vorhanden?
			Mechanismenstärke	Zuverlässigkeit	Vollständigkeit	
G 0.21	Manipulation von Hard- oder Software	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.22	Manipulation von Informationen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.23	Unbefugtes Eindringen in IT-Systeme	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.24	Zerstörung von Geräten oder Datenträgern	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.25	Ausfall von Geräten oder Systemen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.26	Fehlfunktion von Geräten oder Systemen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.27	Ressourcenmangel	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.28	Software-Schwachstellen oder -Fehler	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.29	Verstoß gegen Gesetze oder Regelungen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.32	Missbrauch von Berechtigungen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.33	Personalausfall	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.34	Anschlag	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.35	Nötigung, Erpressung oder Korruption	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.36	Identitätsdiebstahl	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.37	Abstreiten von Handlungen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.38	Missbrauch personenbezogener Daten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.39	Schadprogramme	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.40	Verhinderung von Diensten (Denial of Service)	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.41	Sabotage	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.42	Social Engineering	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.43	Einspielen von Nachrichten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Maßnahmen-Nr. im Baustein	Qualität des Maßnahmenbündels			Wirksame Gegenmaßnahme vorhanden?
			Mechanismenstärke	Zuverlässigkeit	Vollständigkeit	
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.45	Datenverlust	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.46	Integritätsverlust schützenswerter Informationen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein

6. Identifikation weiterer Gefährdungen außerhalb vom G.O Gefährdungskatalog

Vorgehensweise:

Identifikation weiterer Gefährdungen durch:

- Brainstorming
- Quellenrecherche und
- Expertenrunden

7. Risikoanalyse Gefährdungskatalog elementare Gefährdungen

Vorgehensweise:

- Geeignete Maßnahmen pro verbleibende Gefährdung auflisten
- Risiken pro verbleibende Gefährdung ableiten
- Bewertung des Risikos anhand der Qualität des Maßnahmen-Bündels pro verbleibende Gefährdung
- Hinweis für zusätzliche Maßnahmen: Z Maßnahmen, Maßnahmen mit „Umsetzung entbehrlich“, „nicht umgesetzt“ und abgeleitet Maßnahmen in Risikobehandlung aufnehmen (A,B,C,D)

G 0.1 Feuer

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.2 Ungünstige klimatische Bedingungen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.3 Wasser

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.4 Verschmutzung, Staub, Korrosion

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.5 Naturkatastrophen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.6 Katastrophen im Umfeld

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.7 Großereignisse im Umfeld

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.8 Ausfall oder Störung der Stromversorgung

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.10 Ausfall oder Störung von Versorgungsnetzen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.11 Ausfall oder Störung von Dienstleistern

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.12 Elektromagnetische Störstrahlung

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.13 Abfangen kompromittierender Strahlung

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.14 Ausspähen von Informationen/Spionage

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.15 Abhören

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.18 Fehlplanung

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.19 Offenlegung schützenswerter Informationen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.21 Manipulation von Hard- oder Software

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.22 Manipulation von Informationen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.23 Unbefugtes Eindringen in IT-Systeme

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.24 Zerstörung von Geräten oder Datenträgern

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.25 Ausfall von Geräten oder Systeme

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.26 Fehlfunktion von Geräten oder Systemen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.27 Ressourcenmangel

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.28 Software-Schwachstellen oder –Fehler

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.29 Verstoß gegen Gesetze oder Regelungen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.32 Missbrauch von Berechtigungen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.33 Personalausfall

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.34 Anschlag

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.35 Nötigung, Erpressung oder Korruption

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.36 Identitätsdiebstahl

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.37 Abstreiten von Handlungen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.38 Missbrauch personenbezogener Daten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.39 Schadprogramme

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.40 Verhinderung von Diensten (Denial of Service)

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.41 Sabotage

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.42 Social Engineering

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.43 Einspielen von Nachrichten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.45 Datenverlust

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

G 0.46 Integritätsverlust schützenswerter Informationen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen B. Risikovermeidung C. Risikoübernahme D. Risikotransfer

Verzeichnisse

Abbildungsverzeichnis

Tabellenverzeichnis

Anlagen-Dokumente

Anlage A	Muster IT-Sicherheitskonzept für kleine Einrichtungen
Anlage B	Muster IT-Sicherheitskonzept für mittlere und große Einrichtungen
Anlage C1	Schulungskonzept IT-Sicherheit
Anlage C2	BFDI Musterformular
Anlage C3	Tool-Unterstützung IT-Grundschutz
Anlage C4	Schutzbedarfskategorien
Anlage C5	Schutzbedarfsfeststellung
Anlage C6	Modellierungsvorschrift
Anlage C7	Gefährdungskatalog
Anlage C8	Risikoanalyse-Template

Konformitätsbestätigung

KONFORMITÄTSBESTÄTIGUNG

MUSTER-IT-SICHERHEITSKONZEPTE DER EKD

Version 1.0

Datum:
Mittwoch, 30.07.2014

Kunde:
EVANGELISCHE KIRCHE IN DEUTSCHLAND (EKD)

HISOLUTIONS

INHALTSVERZEICHNIS

1 ERGEBNISZUSAMMENFASSUNG

1.1 Ausgangslage

Die Evangelische Kirche in Deutschland mit ihren kirchlichen und diakonischen Einrichtungen verfügt in verschiedenen Bereichen über eine Vielzahl schützenwerter Daten, die zu einem beträchtlichen Teil auch eines hohen Schutzbedarfes bedürfen.

In der Vergangenheit hat sich die Evangelische Kirche bereits vielfach mit dem Schutz dieser Daten beschäftigt. Die Erkenntnisse sind in die auf der letzten Synode der EKD verabschiedete Novellierung des Datenschutzgesetzes der EKD (DSG-EKD) eingeflossen. Diese ist seit dem 1. Januar 2013 in Kraft.
Mit dieser Novellierung wurde erstmals für alle kirchlichen Stellen die Verpflichtung zur Einhaltung der IT-Sicherheit festgelegt und normiert. Das DSG-EKD gilt unmittelbar auch für alle Gliedkirchen und teilweise, je nach deren Organisationsform, auch für die Werke und Einrichtungen der Diakonie.

Die nähere Ausgestaltung wird in einer Rechtsverordnung festgelegt, deren derzeit vorliegender abgestimmter Entwurf von der EKD unter Beteiligung gliedkirchlicher und diakonischer Vertreter unterschiedlicher Bereiche ausgearbeitet wurde. Die Verordnung soll im ersten Halbjahr 2014 verabschiedet werden und in Kraft treten.

Bestandteil dieser Regelung ist es, dass für jede kirchliche Stelle ein IT-Sicherheitskonzept vorhanden sein muss. Für die Erstellung dieser Konzepte wurde in der Verordnung festgelegt, dass die EKD Muster-IT-Sicherheitskonzepte zur Verfügung stellt.

1.2 Vorgehen

1.3 Muster-IT-Sicherheitskonzept kleinste und kleine kirchliche Einrichtungen

Bei der Ausarbeitung dieses Musters war die Herausforderung eine angemessene Balance zwischen regulatorischen Anforderungen, den damit einher gehenden Eigeninteressen der EKD in jeder noch so kleinen Einrichtung und einer realistischen Chance der Anwendung zu finden.

Diese Muster-IT-Sicherheitskonzepte basieren auf der Definition der Kategorie 1 der kirchlichen Einrichtung:

Kategorie 1: kleinste und kleine Einrichtung, keine geschultes IT-Personal, minimale Infrastruktur, überwiegend, dezentrale Datenhaltung, z.T. zentrale Anwendungen (Melde-, Finanz- und Personalwesen), z.T. keine ausreichende Angrenzung zu privaten Bereichen (Räume und Geräte), in der Regel keine IT-Standards (Datensicherung, Kennwortregelungen), keine Server.

Das BSI hat auf seinen Webseiten ein "IT-Grundschutz-Profil für eine kleine Institution" veröffentlicht, welches speziell für die Anwendergruppe mit wenig IT-Systemen und geringen Kenntnissen der Informationssicherheit entwickelt worden ist. Analog der Vorgehensweise in diesem IT-Grundschutz-Profil, wurde für die Kategorie 1 ein Muster-IT-Sicherheitskonzept erstellt.

Zunächst wurden auf Grund der in den BSI IT-Grundschutzkatalogen zu findenden Bausteine die relevanten Themengebiete für kleinste und kleine kirchliche Einrichtungen zusammengestellt. Danach

wurde die Chance für die Anwendung vor Ort ohne das Vorhandensein sachkundigen Personals gemeinsam durch alle Anwesenden analysiert und im Ergebnis auf das notwendige Mindestmaß konsolidiert.

1.4 Muster-IT-Sicherheitskonzept mittlere und große kirchliche Einrichtungen

Bei der Ausarbeitung dieses Musters war von vorn herein erkennbar, dass grundsätzlich die Vorgehensweise der BSI Standards 100-2 und 100-3 umzusetzen ist.

Da dabei jedoch häufig eine Einstiegshürde vorhanden ist und nicht sofort das anzustrebende Ergebnis erkennbar ist, wurde in den Workshops einerseits ein Word Dokument als Muster-IT-Sicherheitskonzept mit jeweils erläuternden Beispielen und einer Kapitelstruktur des Vorgehens bei seiner Erstellung bereitgestellt.

Diese Muster-IT-Sicherheitskonzepte basieren auf der Definition der Kategorie 2 der kirchlichen Einrichtung:

Kategorie 2: mittlere bis größere Einrichtung, vorhandene IT-Infrastruktur (Server, Serverraum, Verkabelung), Systemadministration durch eigenes Personal oder Externe, Standards vorhanden aber unterschiedlich ausgeprägt, z.T. outgesourcte Dienstleistungen.

Dieses Muster entspricht weitgehend dem vom BSI veröffentlichten "IT-Grundschutz-Profil für eine mittlere Institution" und "IT-Grundschutz-Profil für eine große Institution".

1.5 Bestätigung der Konformität

Die angefertigten Muster-IT-Sicherheitskonzepte entsprechen in beiden Varianten den Anforderungen nach BSI IT-Grundschutz.

Ronny Frankenstein

Ronny Frankenstein

HISOLUTIONS

KONTAKT

Ronny Frankenstein
Fon +49 30 533 289 0
frankenstein@hisolutions.com

HiSolutions AG
Bouchéstraße 12
12435 Berlin

info@hisolutions.com
www.hisolutions.com
Fon +49 30 533 289 0
Fax +49 30 533 289 900

Niederlassung
Frankfurt am Main
Mainzer Landstraße 50
60325 Frankfurt am Main

Fon +49 30 533 289 0
Fax +49 30 533 289 900

Niederlassung
Köln
Theodor-Heuss-Ring 23
50688 Köln

Fon +49 221 77 109 550
Fax +49 30 533 289 900

Niederlassung
München
Landsberger Str. 302
80687 München

Fon +49 89 904 05 160
Fax +49 30 533 289 900

www.ekd.de