MODELLIERUNGSVORSCHRIFT

Version 1.0

EVANGELISCHE KIRCHE IN DEUTSCHLAND

INHALTSVERZEICHNIS

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 anzuwenden. 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.

KONTAKT

Evangelische Kirche in Deutschland

Koordinierungsstelle-IT@ekd.de

Herrenhäuser Straße 12

30419 Hannover

Telefon: +49 511 2796 0

Telefax: +49 511 2796 700

HiSolutions AG

info@hisolutions.com

www.hisolutions.com

Bouchéstraße 12

12435 Berlin

Telefon: +49 30 533 289 0

Telefax: + 49 30 533 289 900

Theodor-Heuss-Ring 23

50668 Köln

Telefon: +49 221 771 09-550