Bundesamt
für Sicherheit in der
Informationstechnik

Ein IT-Grundschutzprofil für den Mittelstand

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik
Referat I.1.4 Systemsicherheit, Grundschutz
Postfach 200363
53133 Bonn
Tel:+49 (0) 1888-95820
E-Mail: gshb@bsi.bund.de
Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

In der heutigen Geschäftswelt werden nahezu alle Prozesse durch Informationstechnologie (IT) unterstützt. Beispiele hierfür sind die Textverarbeitung am Arbeitsplatz oder die Steuerung der Produktion im produzierenden Gewerbe. Gleichzeitig führt dies auch zu Abhängigkeiten, da Fehler, die bei der Informationsverarbeitung entstehen, direkte Folgen für die Institution haben. Fällt z. B. die Produktionssteuerung aus oder werden fehlerhafte Produktionsdaten erzeugt, kann dies direkte Auswirkungen auf vertraglich zugesicherte Liefertermine oder die Qualität der gelieferten Produkte haben. Gibt es Störungen z. B. bei den Arbeitsplatzsystemen der Mitarbeiter aus, geht Arbeitszeit verloren.

Die Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten bzw. der Informationstechnik ist damit ein wichtiges Ziel zur Aufrechterhaltung der Geschäftsprozesse und Abwehr von Schäden. Damit dieses Ziel schnell und effektiv erreicht werden und Gefahren identifiziert und durch geeignete Sicherheitsmaßnahmen abgewendet werden können, wird ein IT-Sicherheitskonzept erstellt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit der im IT-Grundschutzhandbuch [GSHB] beschriebenen Methode eine wirkungsvolle und einfach handhabbare Möglichkeit zur Erstellung eines IT-Sicherheitskonzepts zur Verfügung. Das GSHB kann von den Internetseiten des BSI kostenlos unter http://www.bsi.de/gshb/downloads/ heruntergeladen werden. Durch die softwaretechnische Unterstützung mittels verschiedener am Markt erhältlicher Grundschutz-TOOLs (vgl. auch [GSTOOL]) kann die Erstellung eines IT-Sicherheitskonzepts effizient durchgeführt werden.

In vorliegendem Dokument wird anhand eines Beispiels einer mittelgroßen Institution systematisch ein IT-Sicherheitskonzept nach dem IT-Grundschutzhandbuch des BSI [GSHB] erstellt. Es werden konkrete Sicherheitsaspekte detailliert erläutert, die beim Einsatz von Informationstechnologie zu beachten sind. Ausgehend von der beispielhaft dargestellten

Institution wird gezeigt, wie die einzelnen Arbeitsschritte der IT-Grundschutz-Methodik unter Zuhilfenahme des GSTOOL angewendet werden. In Kapitel 2 werden zunächst die Rahmenbedingungen, unter denen das Profil angewendet werden kann, erläutert. Der in diesem Dokument als Beispiel dienende IT-Verbund wird in Kapitel 3 beschrieben. In den Kapiteln 5 bis 9 werden die einzelnen Schritte einer IT-Sicherheitskonzeption aufgeführt. Kapitel 10 erläutert die Aspekte einer Zertifizierung mittels IT-Grundschutz Zertifikat und in Kapitel 11 ist eine exemplarische Sicherheits-Leitlinie für eine mittelgroße Institution dargestellt.

Zur Vorbereitung wird empfohlen, den *Leitfaden IT-Sicherheit* [LEITF] zu lesen. Das vorliegende Dokument setzt die inhaltliche Kenntnis des Leitfadens voraus.

Um die beispielhaft durchgeführten Schritte bei der Erstellung der Sicherheitskonzeption für die mittelgroße Institution mit dem GSTOOL nachvollziehen zu können, besteht die Möglichkeit von der Internetseite des BSI eine kostenlose 30-Tage-Lizenz des GSTOOL herunterzuladen (www.bsi.bund.de/gstool/down.htm). Sie finden dort ebenfalls eine Datenbank zum GSTOOL mit den im vorliegenden Dokument beschriebenen Beispielen einschließlich einer Installationsanleitung.

2 Rahmenbedingung des Profils

In den folgenden Abschnitten werden die Rahmenbedingungen beschrieben, unter denen das in diesem Dokument verwendete Grundschutz-Profil auf den IT-Verbund einer mittelgroßen Institution anwendbar ist. Abschnitte, die mit der am linken Rand abgebildeten Grafik gekennzeichnet sind, weisen darauf hin, dass bei der Sicherheitskonzeption die Unterstützung durch ein Grundschutz-Tool (GSTOOL) möglich ist. Der Einsatz des GSTOOL ist zwar nicht explizit vorgeschrieben, er wird jedoch empfohlen, da hierdurch die Umsetzung des GSHB erheblich vereinfacht wird. In diesem Dokument wird die Vorgehensweise daher an vielen Stellen durch Beispiele aus dem GSTOOL verdeutlicht. Die den Beispielen zugrundeliegende Datenbank des GSTOOL ist über die Internetseiten des BSI erhältlich.

Wird das GSHB manuell, d.h. ohne GSTOOL umgesetzt, ist an vielen Stellen die tabellarische Erfassung von Informationen erforderlich. Im nachfolgenden Dokument sind Punkte, die bei einer manuellen Vorgehensweise zu beachten sind bzw. Hinweise durch das Tabellensymbol an der linken Seite gekennzeichnet.

2.1 Erläuterung zum Schutzbedarf

Da das GSHB nach einem Baukastenprinzip aufgebaut ist, lassen sich mit seiner Hilfe IT-Sicherheitskonzepte einfach erstellen. Dieses Prinzip erlaubt es dem Anwender, einen Soll-Ist-Vergleich zwischen empfohlenen und bereits realisierten Maßnahmen durchzuführen. Stellt man bei diesem Vergleich fehlende oder noch nicht umgesetzte Maßnahmen fest, so ist dies ein Hinweis auf Sicherheitsdefizite, welche durch die in den Bausteinen empfohlenen Maßnahmen behoben werden sollten.

Generell orientiert man sich bei der Auswahl von einzuführenden IT-Schutzmaßnahmen am Wert der zu schützenden Daten, so dass die Wirt-

schaftlichkeit der IT-Sicherheit gewährleistet wird. In diesem Sinne sollen Maßnahmen, die von einer Institution für die Einrichtung und Aufrechterhaltung der IT-Sicherheit ergriffen werden, stets *angemessen* sein. Daher werden IT-Sicherheitsmaßnahmen erst dann eingeführt, nachdem man sich über den Schutzbedarf der eigenen IT und der auf ihr gespeicherten und verarbeiteten Daten bewusst geworden ist. Bei der Ermittlung und individuellen Bewertung des Schutzbedarfs wird man dabei methodisch durch das GSHB und technisch durch das GSTOOL unterstützt.

Die im GSHB aufgeführten Maßnahmen sind stets Standardsicherheitsmaßnahmen, welche die für die jeweiligen Bausteine nach dem Stand der Technik umzusetzenden Maßnahmen zur Erreichung einer angemessenen Sicherheit beschreiben. Teilweise wird mit diesen Maßnahmen auch bereits ein höherer Schutzbedarf abgedeckt, dennoch sind sie in den jeweiligen Bereichen das Minimum dessen, was vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist.

Ziel der in einem ersten Schritt durchzuführenden Schutzbedarfsfeststellung (vgl. Kapitel 2.2 [GSHB]) ist es daher, für jede erfasste Komponente des IT-Verbunds (IT-Anwendung, IT-System, Raum und Übertragungsstrecke) zu entscheiden, welchen Schutzbedarf sie bezüglich der Grundwerte der IT-Sicherheit - Vertraulichkeit, Integrität und Verfügbarkeit - tatsächlich besitzt. Dieser orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Komponente verbunden sind und wird in die drei Kategorien „normal“, „hoch“ und „sehr hoch“ unterteilt. Zur Einstufung in diese Kategorien werden individuell für den betrachteten IT-Verbund die Auswirkungen hinsichtlich der Schadensszenarien

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

- finanzielle Auswirkungen

betrachtet und abgeschätzt.

Die Methodik des GSHB zur Schutzbedarfsfeststellung wird detailliert in diesem Dokument in Kapitel 5.4 an einem Beispiel erläutert.

2.2 Rechtliche Rahmenbedingungen

Verstöße gegen Gesetzte, Richtlinien oder Vorschriften wie auch die Nichteinhaltung von Verträgen können sowohl aus dem Verlust der Verfügbarkeit, der Vertraulichkeit sowie der Integritätsverletzung resultieren. Die Bewertung eines Schadens und die Definition von Schutzmaßnahmen ist damit u.a. von den rechtlichen Konsequenzen für die Institution abhängig. Die nachfolgenden Ausführungen stammen aus [LEITF] und geben das Thema der rechtlichen Rahmenbedingungen sehr gut wieder.

„Während der vergangenen Jahre wurden mehrere Rechtsvorschriften erlassen, aus denen sich zu Fragen der IT-Sicherheit unmittelbare Handlungs- und Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens ableiten lassen. Diese Regelungen gelten oft nicht nur für Aktiengesellschaften sondern auch für die Rechtsform der GmbH. Dies ist in der Öffentlichkeit allerdings noch nicht hinreichend bekannt.

In diesem Zusammenhang wird immer wieder auf das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) hingewiesen. Das KonTraG ist ein sog. Artikelgesetz und ergänzt bzw. ändert verschiedene Gesetze wie das Handelsgesetzbuch und das Aktiengesetz. Insbesondere die Forderung nach einem Risikomanagement für Kapitalgesellschaften – d.h. für Aktiengesellschaften und GmbH – sind im KonTraG enthalten.

Im Einzelnen kann eine Institution von folgenden Regelungen betroffen sein:

*Im **Aktiengesetz** wird festgelegt, dass ein Vorstand persönlich haftet, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG).*

*Geschäftsführern einer GmbH wird im **GmbH-Gesetz** „die Sorgfalt eines ordentlichen Geschäftsmannes" auferlegt (§ 43 Abs. 1 GmbHG), welches ähnliche Folgerungen für das Risikomanagement beinhaltet wie für Vorstände nach dem Aktiengesetz.*

Die im Aktiengesetz genannten Pflichten eines Vorstands gelten auch im Rahmen des Handelsgesetzbuches (§ 317 Abs. 4 HGB). Weiterhin verpflichtet das Handelsgesetzbuch Abschlussprüfer zu prüfen, „ob die Risiken der künftigen Entwicklung zutreffend dargestellt sind" (§ 317 Abs. 2HGB).

Die oben genannten Formulierungen klingen für den juristischen Laien teilweise recht allgemein und unverbindlich. Hieraus lassen sich jedoch konkrete Verpflichtungen an die Gewährleistung eines angemessenen IT-Sicherheitsniveaus in der eigenen Institution ableiten. IT-Sicherheitsvorfälle können massive wirtschaftliche Schäden verursachen und ggf. den Bestand einer Institution gefährden.

*Für bestimmte Berufsgruppen wie Ärzte, Rechtsanwälte oder Angehörige sozialer Berufe gibt es darüber hinaus Sonderregelungen im **Strafgesetzbuch**, die Freiheitsstrafen vorsehen, wenn vertrauliche Angaben von Patienten, Mandanten bzw. Klienten ohne deren ausdrückliche Einwilligung öffentlich gemacht werden (§ 203 StGB). Ein fahrlässiger Umgang mit Informationstechnik kann diesen Tatbestand unter Umständen bereits erfüllen.*

Belange des Verbraucherschutzes werden in verschiedenen Gesetzen behandelt. Die Verwendung von Informationstechnik, die Nutzung des Internets oder von Telekommunikationsdiensten werden zum Teil sehr genau geregelt. Einschlägig sind z. B.: Gesetz zur Nutzung von Telediensten, Telekommunikationsgesetz, Mediendienste-Staatsvertrag, Urheberrecht sowie verschiedene Richtlinien auf EU-Ebene.

Der Umgang mit personenbezogenen Daten wird in den Datenschutzgesetzen des Bundes und der Länder, dem Gesetz über den Datenschutz bei Telediensten, der Telekommunikations-Datenschutzverordnung sowie teilweise in den bereits aufgezählten Gesetzen geregelt.

Auch Banken sind verpflichtet, bei der Kreditvergabe IT-Risiken des Kreditnehmers zu berücksichtigen, was sich unmittelbar auf die angebotenen Konditionen auswirken wird (Stichwort: Basel II).

Die für die jeweilige Institution geltende Rechtslage muss jedoch individuell durch einen Experten geklärt werden, die oben gemachten Angaben können daher nur als Hinweis angesehen werden!"

Die genannten rechtlichen Rahmenbedingungen machen es für einen Institutsleiter erforderlich, sich mit der Thematik *IT-Sicherheit* auseinander zu setzen und zu prüfen, ob die in der Institution umgesetzten IT-Sicherheitsmaßnahmen ausreichend sind und ggf. neue Sicherheitsmaßnahmen zu definieren. Das GSHB liefert hierfür eine Vorgehensweise, mit der fehlende Sicherheitsmaßnahmen identifiziert und erforderliche Sicherheitsmaßnahmen umgesetzt werden können. Der folgende Abschnitt beschreibt, wer in diesen Prozess eingebunden ist, welche Verantwortlichkeiten entstehen und gibt einen Überblick über die Vorgehensweise.

2.3 Verantwortlichkeiten und Vorgehensweise

Das GSHB beschreibt die verschiedenen Aktivitäten, die innerhalb einer Institution im Zusammenhang mit der Umsetzung von Maßnahmen zur IT-Sicherheitskonzeption durchzuführen sind (vgl. Kapitel 2 [GSHB]). Im GSHB werden verschiedene, in den Sicherheitsprozess eingebundene Rollen beschrieben. Das GSHB unterscheidet insbesondere die Rollen des **Institutsleiters**, des **IT-Sicherheitsbeauftragten**, des **IT-Verantwortlichen (Administrator)** und des **IT-Benutzers**.

Der Institutsleiter ist für die Benennung eines Mitarbeiters als IT-Sicherheitsbeauftragten zuständig und zeichnet sich übergeordnet für alle Belange innerhalb der Institution verantwortlich.

Gemäß der Methodik des GSHB ist der IT-Sicherheitsbeauftragte für die Abstimmung der Sicherheits-Leitlinie mit dem Institutsleiter und für die Erstellung des **IT-Sicherheitskonzepts** verantwortlich; d.h. er koordiniert die Erstellung eines IT-Sicherheitskonzepts für die Institution. Gleichzeitig ist er Haupt-Ansprechpartner in Fragen der IT-Sicherheit.

Die IT-Verantwortlichen übernehmen die Pflege und Wartung von IT-Systemen und IT-Anwendungen und sorgen für die Umsetzung der festzulegenden technischen Maßnahmen.

Die IT-Benutzer sind die Anwender der IT-Systeme. Ihre Tätigkeit wird durch IT-Anwendungen unterstützt. Die IT-Benutzer liefern dem IT-Sicherheitsbeauftragten bei der Erstellung des IT-Sicherheitskonzepts Informationen über den Schutzbedarf der einzelnen Komponenten und werden auf die Einhaltung der festgelegten Regelungen verpflichtet. Bei der tatsächlichen Durchführung der Arbeiten ist eine Zuweisung der o.g. Rollen zu Mitarbeitern erforderlich.

Die bei der Erstellung eines IT-Sicherheitskonzepts nach GSHB durchzuführenden Tätigkeiten sind in Kapitel 2 [GSHB] definiert und umfassen die nachfolgenden Phasen (siehe Abbildung 1), die zeitlich nacheinander ausgeführt werden. Ausgenommen ist Phase 2, die schon vor Beendigung der ersten Phase gestartet werden kann. Die Durchführung aller sieben Phasen nimmt erfahrungsgemäß bei einem IT-Verbund der betrachteten Größenordnung etwa ein Jahr in Anspruch. Der Zeitraum kann verkürzt werden, wenn z. B. bereits Vorbereitungen getroffen worden sind und Erfahrungen von Mitarbeitern, etwa in der Einschätzung der Schutzbedürftigkeit von IT-Anwendungen, vorliegen. Die Dauer der einzelnen Phasen ist stark unterschiedlich und hängt von den individuellen Gegebenheiten innerhalb der Institution ab.

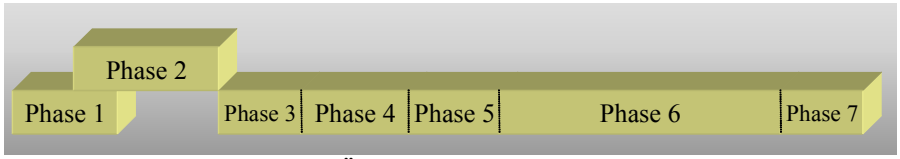


Abbildung 1: Übersicht der Umsetzungsphasen

Phase 1: *Initiierung des IT-Sicherheitsprozesses (vgl. Kapitel 2.0 [GSHB])*

Für die Phase 1 zeichnet die Institutsleitung verantwortlich, sie beinhaltet die Definition des betrachteten IT-Verbundes (also die Festlegung des Geltungsbereichs), der IT-Sicherheits-Leitlinie (M 2.192 [GSHB]) und die Einrichtung des IT-Sicherheitsmanagements (M 2.193 [GSHB]). Üblich ist es, diese Aufgaben an den IT-Sicherheitsbeauftragten zu delegieren. Dieser stimmt die Sicherheits-Leitlinie mit der Institutsleitung ab und erstellt das IT-Sicherheitskonzept.

Als **Ergebnis** der 1. Phase ist eine Sicherheits-Leitlinie erstellt und der IT-Sicherheitsbeauftragte benannt.

Phase 2: *Durchführung einer IT-Strukturanalyse (vgl. Kapitel 2.1 [GSHB])*

Bei der IT-Strukturanalyse werden die Komponenten des IT Verbundes (IT-Anwendung, IT-System, Raum und Kommunikationsverbindung) erfasst. Die IT-Strukturanalyse kann durch den IT-Sicherheitsbeauftragten unter Zuhilfenahme des GSTOOL durchgeführt werden.

Die Verwendung eines GSTOOL ist jedoch nicht zwingend notwendig. Wird darauf verzichtet, muss die IT-Strukturanalyse manuell unter Verwendung von Formularen und Tabellen erfolgen. Bei der Durchführung ist er auf Informationen der IT-Benutzer und IT-Verantwortlichen angewiesen, welche in die IT-Strukturanalyse mit einzubeziehen sind.

Die IT-Strukturanalyse kann schon begonnen werden, bevor die Sicherheits-Leitlinie erstellt ist. In Abbildung 1 ist daher die zeitliche Überlappung der Bearbeitung beider Phasen dargestellt.

Als **Ergebnis** der 2. Phase ist die Struktur der IT dokumentiert, d.h. alle IT-Systeme, deren Benutzer und Verantwortlichen sowie Standorte und auf ihnen laufenden Anwendungen sind bekannt und dokumentiert. Somit ist ein Überblick über die IT-Landschaft der Institution vorhanden.

Phase 3: *Durchführung einer Schutzbedarfsfeststellung (vgl. Kapitel 2.2 [GSHB])*

Die Vorgehensweise zur Schutzbedarfsfeststellung wird in Kapitel 6 detailliert erläutert. Die Schutzbedarfsfeststellung wird durch den IT-Sicherheitsbeauftragten durchgeführt. Sie beginnt mit einer auf den IT-Verbund angepassten Definition der Schutzbedarfskategorien, die in der Institution abgestimmt ist.

Die erforderlichen Informationen zur Bestimmung des Schutzbedarfs werden durch Befragung der IT-Benutzer ermittelt. Auch dieser Vorgang wird durch das GSTOOL unterstützt. Da insbesondere die IT-Benutzer und IT-Verantwortlichen den Schutzbedarf der von ihnen be- und verarbeiteten Daten und genutzten Systeme einschätzen können, ist der IT-Sicherheitsbeauftragte auf die Mitarbeit der IT-Benutzer und IT-Verantwortlichen angewiesen. Daher müssen diese unbedingt bei der Schutzbedarfsfeststellungen mit einbezogen werden.

Als **Ergebnis** dieser Phase ist für jedes in Phase 2 aufgenommene IT-System, jede IT-Anwendung, jeden IT-Raum und für die Kommunikationsverbindungen der Schutzbedarf festgelegt.

Phase 4: *Modellierung nach IT-Grundschutz (vgl. Kapitel 2.3 [GSHB])*

Die Modellierung nach IT-Grundschutz (Phase 4) wird durch den IT-Sicherheitsbeauftragten unter Zuhilfenahme des GSTOOL

durchgeführt. Dabei wird der IT-Verbund mittels Bausteinen des GSHB nachgebildet. Die Modellierung sollte durch die IT-Verantwortlichen unterstützt werden.

Als **Ergebnis** erhält man das Grundschutz-Modell des betrachteten IT-Verbunds.

Phase 5: *Durchführung des Basis-Sicherheitsscheck (vgl. Kapitel 2.4 [GSHB])*

Die Durchführung des Basis-Sicherheitsscheck wird durch den IT-Sicherheitsbeauftragten unter Verwendung des GSTOOL durchgeführt. Hier wird ermittelt, ob die in der Modellierung beschriebenen Maßnahmen „umgesetzt“, „teilweise“, „nicht umgesetzt“ oder „entbehrlich“ sind. Die Erfassung der umgesetzten Maßnahmen kann an die IT-Verantwortlichen delegiert werden. In jedem Fall ist eine enge Kooperation mit den IT-Verantwortlichen nötig.

Bei IT-Anwendungen, die einen hohen oder sehr hohen Schutzbedarf besitzen, können die Grundschutz-Sicherheitsmaßnahmen ggf. nicht ausreichend sein. In diesem Fall ist eine ergänzenden Sicherheitsanalyse (vgl. Kapitel 2.5 [GSHB]) durch den IT-Sicherheitsbeauftragten durchzuführen und durch die IT-Verantwortlichen zu unterstützen.

Das **Ergebnis** der 5. Phase ist eine Liste, die insbesondere Auskunft über den Umsetzungsstatus der geforderten Standardsicherheitsmaßnahmen gibt.

Phase 6: *Realisierung von IT-Sicherheitsmaßnahmen (vgl. Kapitel 2.5 [GSHB])*

Anschließend werden die erforderlichen Sicherheitsmaßnahmen umgesetzt. Die Komplexität dieser Phase, die darin besteht, festzulegen, welche Maßnahmen zwingend umgesetzt werden müssen und auf welche verzichtet werden kann, macht die Organisa-

tionsform einer Arbeitsgruppe mit verschiedenen Teams sinnvoll. Der IT-Sicherheitsbeauftragte übernimmt in diesem Fall die Leitung der Arbeitsgruppe und koordiniert die einzelnen Tätigkeiten der Teams. Teilweise wird der IT-Sicherheitsbeauftragte hierbei durch das GSTOOL unterstützt.

Ein Realisierungsplan (Projektplan) sowie die umgesetzten Standardsicherheitsmaßnahmen stellen das Ergebnis der 6. Phase dar.

Phase 7: *Zertifizierung*

Für die grundschutzkonforme Erstellung des Sicherheitskonzepts des definierten IT-Verbunds kann abschließend ein IT-Grundschutz-Zertifikat (vgl. [GSZERT]) ausgestellt werden.

Mit Hilfe dieses Zertifikats wird bestätigt, dass alle erforderlichen Maßnahmen nach dem IT-Grundschutzhandbuch realisiert wurden.

Voraussetzung für die Vergabe eines IT-Grundschutz-Zertifikats ist eine Überprüfung, ob die festgelegten Anforderungen erfüllt werden. Diese Überprüfung wird von einem lizenzierten IT-Grundschutz-Auditor durchgeführt. Das Ergebnis der Überprüfung ist ein Auditreport, der dem BSI als Zertifizierungsstelle vorgelegt wird. Auf der Grundlage des Auditreports entscheidet die Zertifizierungsstelle über die Vergabe des IT-Grundschutz-Zertifikats. Diese Zertifikate werden auf der Internetseite des BSI veröffentlicht.

Um den Weg bis zum IT-Grundschutz-Zertifikat durch das BSI zu erleichtern, definiert das BSI zwei Vorstufen zum eigentlichen IT-Grundschutz-Zertifikat:

- die Selbsterklärung „IT-Grundschutz Einstiegsstufe“ und
- die Selbsterklärung „IT-Grundschutz Aufbaustufe“.

Die Selbsterklärungen können von einem Zeichnungsbefugten einer Institution ohne Beteiligung Dritter gegenüber dem BSI abgegeben werden. Diese Selbsterklärungen werden auf der Internetseite des BSI veröffentlicht. Falls bei der Durchführung des Audits für eine Selbsterklärung ein lizenzierter IT-Grundschutz-Auditor beteiligt wurde, kann dieser die Selbsterklärung mit einem Testat bestätigen (vgl. [GSZERT]).

Die Durchführung der Arbeiten in den dargestellten Phasen wird vom IT-Sicherheitsbeauftragten als Projekt organisiert. Dies bedeutet, dass er für diese Aufgaben von seinem Arbeitgeber ausreichend Arbeitszeit zur Verfügung gestellt bekommt und die Zuarbeit anderer Mitarbeiter (z. B. IT-Anwender, IT-Verantwortliche) zu den erforderlichen Zeitpunkten gesichert ist.

Im folgenden Kapitel 3 wird der IT-Verbund einer mittelgroßen Institution beispielhaft beschrieben. Dieses Beispiel wird verwendet, um die skizzierten Phasen zur Erstellung eines Sicherheitskonzepts nach der Methodik des GSHB und mit Unterstützung des GSTOOL detailliert zu erläutern.

3 Definition und Abgrenzung des IT-Verbundes

Dieser Abschnitt beschreibt beispielhaft zunächst den IT-Verbund der Institution aus der Sicht des Institutsleiters – also aus einer organisatorischen Sicht. Die Beschreibung des IT-Verbundes aus der Sicht des GSHB erfolgt in Kapitel 5 (Strukturanalyse).

Netzplan

In der nachfolgenden Abbildung 2 sind die Systeme und deren Vernetzung der einzelnen Abteilungen aufgeführt. Der Netzplan orientiert sich am Organigramm der Institution und beinhaltet sämtliche IT-Komponenten.

Jedem Mitarbeiter (IT-Benutzer) steht an seinem Arbeitsplatz ein eigenes Telefon zur Verfügung; der Übersichtlichkeit halber sind diese im Netzplan nicht gesondert aufgeführt. Ein Telefax und Anrufbeantworter stehen zentral bei der Sekretärin des Institutsleiters zur Verfügung.

Drucker und Fotokopierer befinden sich in einem zentralen Kopierraum. Zusätzlich sind die Arbeitsplätze des Institutsleiters, der Sekretärinnen, sämtlicher Abteilungsleiter und des Qualitätsmanagement (QM) / Sicherheitsbeauftragten mit einem eigenen Drucker ausgestattet. Aufgrund der Abteilungsgröße steht den Mitarbeitern der Abteilung Produktion ein zusätzlicher Abteilungsdrucker zur Verfügung.

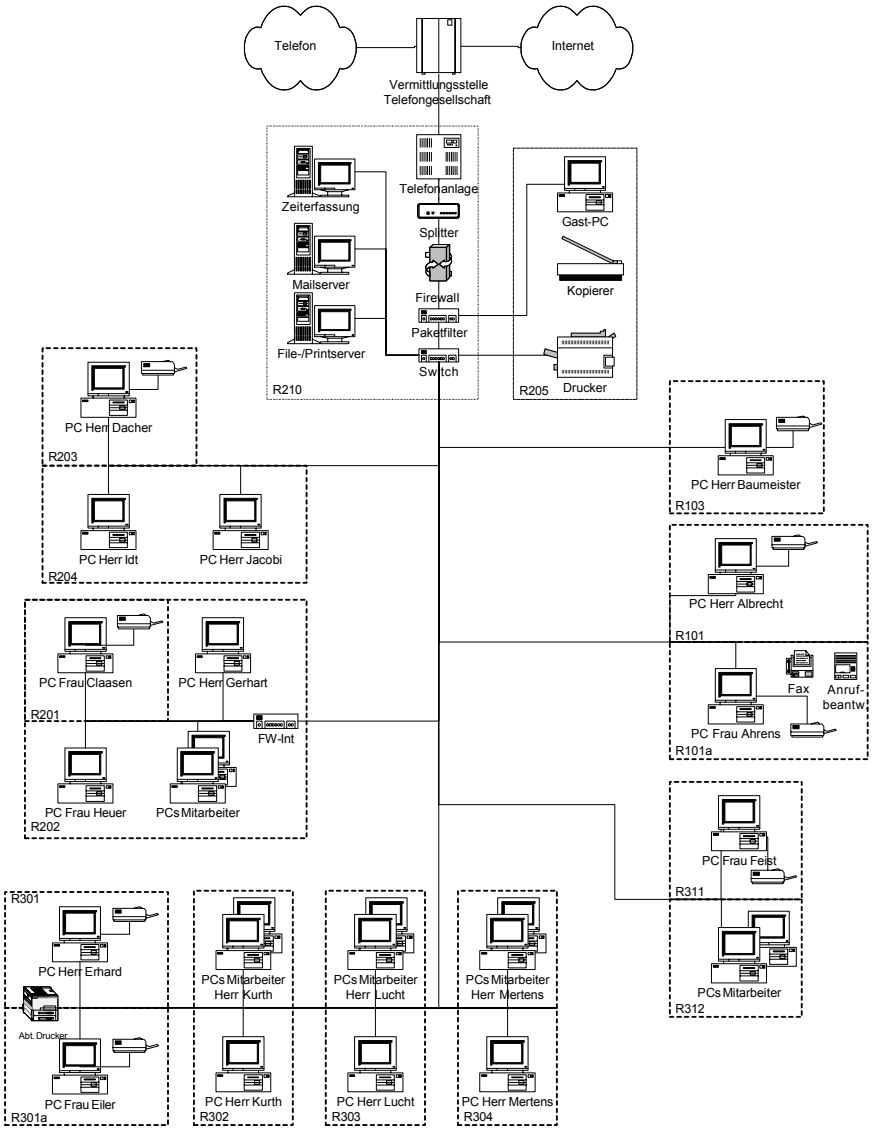


Abbildung 2: mittlerer IT-Verbund

IT-Systeme und IT-Anwendungen

Innerhalb der Institution wird versucht, sämtliche Arbeitsplatzsysteme der Institution soweit wie möglich einheitlich zu halten; dies reduziert den Administrationsaufwand der einzelnen Systeme erheblich. Daher ist jeder „Standard-PC“ der Institution grundsätzlich mit einem Windows 2000 Betriebssystem und einer Office-Lösung (Textverarbeitung, Tabellenkalkulation, Präsentations- und Grafiksoftware) ausgestattet. Eine Übersicht über die vorhandenen IT-Systeme und den Anwendungen findet sich in Anhang A.

IT-Räume

Die Räumlichkeiten der Institution befinden sich im dritten Stock eines Bürogebäudes, welches von verschiedenen Unternehmen genutzt wird. Die Büroräume sind angemietet und bieten die üblichen infrastrukturellen Möglichkeiten. Die einzelnen Räume werden sowohl als Büros, wie auch zur Unterbringung der IT-Infrastruktur verwendet.

Kommunikationsverbindungen

Alle PCs und Server besitzen ein eigenes Netzwerkkabel zum Switch. Genauso besitzen die TK-Endgeräte und das DSL-Modem je eine eigene Leitung zur TK-Anlage. Die Leitungen sind in den vorhandenen Kabelkanälen verlegt.

Die einzige Außenverbindung ist die Anbindung der TK-Anlage zu einer Nebenstelle der Telefongesellschaft, welche gleichzeitig auch Internetprovider der Institution ist.

Bis auf den Abteilungsdrucker der Abteilung Produktion und den zentralen Drucker im Kopierraum sind alle Drucker direkt mit ihrem jeweiligen PC verbunden. Die zentralen Drucker sind als Netzwerkdrucker am Switch angeschlossen.

Organigramm / Personal

In Anhang B ist zur weiteren Illustration das Organigramm der Institution dargestellt. Sie ist in vier Abteilungen (Organisation / Finanzen, IT, Produktion und Labor) gegliedert, die wiederum aus einzelnen fachlichen Teams bestehen. Die Abteilung „Labor“ besteht aus genau einem Team und ist daher nicht weiter unterteilt. Der Institutsleiter steht den Abteilungen vor und koordiniert deren Aktivitäten.

Der Institutsleiter ist Personalvorgesetzter der Abteilungsleiter sowie des QM- und Sicherheitsbeauftragten. Die Abteilungsleiter sind die Personalvorgesetzten der Mitarbeiter in ihren Abteilungen. Teamleiter üben ausschließlich fachliche Verantwortung aus.

Die Rolle des Vertriebs ist in die Abteilung Produktion eingegliedert und wird durch dessen Abteilungsleiter ausgeübt. Neben dem Institutsleiter hat der Abteilungsleiter Produktion eine Sekretärin.

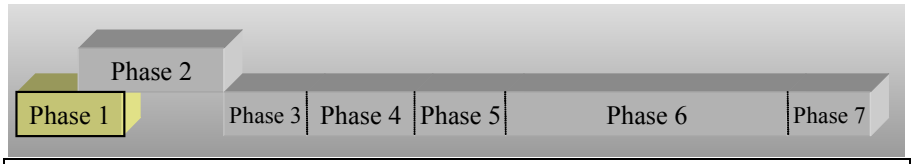
Für das Qualitätsmanagement und das Thema Sicherheit existiert eine eigene Stabsstelle (QM-Beauftragter / Sicherheitsbeauftragter), die direkt dem Institutsleiter unterstellt ist. Der Sicherheitsbeauftragte hat die Aufgabe, die Sicherheit sensibler Informationen zu gewährleisten und die Sicherheitskonzeption durchzuführen.

Die gesamte IT-Infrastruktur wird durch die Abteilung IT betrieben. Fachlich sind verschiedene Mitarbeiter für Serversysteme und Internet sowie Clients verantwortlich. Im Rahmen der Erstellung eines Sicherheitskonzepts nach GSHB sind die Mitarbeiter der Abteilung IT die IT-Verantwortlichen für die IT-Systeme.

Bei der Erstellung eines Sicherheitskonzepts nach GSHB in einer Institution werden von allen Mitarbeitern einer Institution verschiedene Rollen ausgeübt. Die Gesamtverantwortung für die Umsetzung obliegt hierbei dem Sicherheitsbeauftragten (Herr Baumeister), er ist für alle IT-Sicherheitsfragen in der Institution zuständig. Hierzu gehören insbesondere die Erstellung der Sicherheits-Leitlinie und des Sicherheitskonzepts. Die IT-Benutzer (alle Mitarbeiter) werden in ihren Tätigkeiten durch IT-

Systeme (vgl. Anhang A) unterstützt, wohingegen es die Aufgabe der IT-Verantwortlichen ist, den Betrieb der IT-Systeme sicherzustellen. Die Rolle der IT-Verantwortlichen wird in der exemplarischen Institution durch die Abteilung IT und deren Mitarbeiter (Herr Idt, Herr Jacobi) wahrgenommen.

4 Sicherheits-Leitlinie und Sicherheitskonzept



Verantwortlich	IT-Sicherheitsverantwortlicher
Einzubeziehen	Institutsleitung
	Abteilungsleitung
Zeitlicher Aufwand	ca. 1 Monat

Die Initiierung des Sicherheitsprozesses bildet die erste Phase in der Umsetzung des GSHB. Zu diesem Zeitpunkt wird ein Projektteam gebildet und der IT-Sicherheitsbeauftragte als Projektleiter bestimmt. Die Ressourcen zur erfolgreichen Durchführung des Projekts müssen von der Geschäftsführung zur Verfügung gestellt werden. In den ersten Phasen ist hierunter die zeitweise Freistellung von Mitarbeitern zur Unterstützung des Projektleiters zu verstehen. Finanzbudgets zur Anschaffung oder Erweiterung von IT-Sicherheitskomponenten werden ggfs. erst in späteren Projektphasen benötigt. Es ist die Aufgabe des Projektleiters zu diesem Zeitpunkt die Entscheidung darüber, welche Ressourcen zur Verfügung gestellt werden, für die Geschäftsführung vorzubereiten.

Die erste Aufgabe besteht in der Erstellung einer Sicherheits-Leitlinie. Der IT-Sicherheitsbeauftragte hat die Aufgabe mit der Geschäftsleitung abzustimmen und darauf aufbauend die Erstellung eines Sicherheitskonzepts zu koordinieren. Im Anschluss daran hat er für die dauerhafte Einhaltung des erreichten Sicherheitsniveaus der Institution Sorge zu tragen.

4.1 Sicherheits-Leitlinie

Die Sicherheits-Leitlinie definiert das innerhalb des Geltungsbereiches (IT-Verbundes) angestrebte Sicherheitsniveau. Sie definiert daher zunächst den IT-Verbund, in dem die Sicherheits-Leitlinie gültig ist und die von der Institution angestrebten Sicherheitsziele sowie die verfolgte Sicherheitsstrategie.

Die Festlegung der Eckpunkte einer IT-Sicherheits-Leitlinie erfolgt am effizientesten im Rahmen von Workshops mit Vertretern der Institutsleitung und den Abteilungsleitern. Es ist die Aufgabe des IT-Sicherheitsbeauftragten die Workshops zu moderieren, um die relevanten Aspekte (Geltungsbereich/IT-Verbund, Sicherheitsziele, Sicherheitsstrategie) zu erarbeiten.

Die Sicherheits-Leitlinie ist somit Anspruch und Aussage zugleich. Hiermit wird das zu erreichende „Ziel“ (Sicherheitsniveau) der Institution festgelegt. Die Institutsleitung unterrichtet alle Mitarbeiter über diese Sicherheits-Leitlinie und weist darauf hin, dass deren Einhaltung für die Institution von hoher Bedeutung und für die Mitarbeiter verbindlich ist.

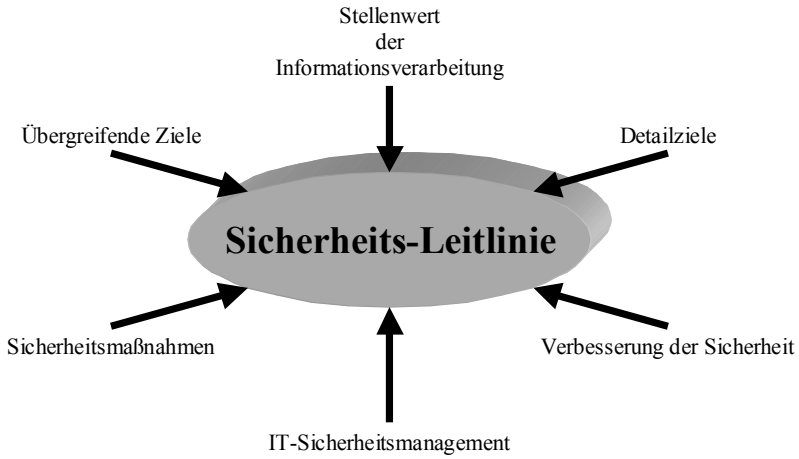


Abbildung 3: Aspekte einer Sicherheits-Leitlinie

In einer IT-Sicherheits-Leitlinie werden von der Institution folgende Kernaspekte (siehe Abbildung 3) betrachtet:

- *Allgemeines*

  In der IT-Sicherheits-Leitlinie wird der Geltungsbereich festgelegt. Dies kann entweder die gesamte Institution (wie im Beispiel aus Kapitel 3) oder ein Institutsteil (z. B. eine Abteilung oder Filiale) sein.

  Die Institutsleitung verabschiedet die IT-Sicherheits-Leitlinie als für alle Mitarbeiter verbindliches Dokument innerhalb der Institution und macht auf eventuelle Folgen von Verstößen aufmerksam.

- *Stellenwert der Informationsverarbeitung*

  Der Stellenwert der Informationsverarbeitung für den festgelegten Geltungsbereich wird dokumentiert. Hierdurch wird argumentiert, weshalb IT-Sicherheit für die Institution relevant ist.

Die in dem vorliegenden Dokument betrachtete Institution ist insbesondere in ihrer Produktionsabteilung für die Aufrechterhaltung ihrer Geschäftstätigkeit auf reibungslos funktionierende IT-Systeme angewiesen.

- *Übergreifende Ziele*

  Die Institution definiert übergreifende Sicherheitsziele. Hierbei kommen z. B. die Gewährleistung von Verfügbarkeit, Vertraulichkeit und Integrität zum Tragen. Weiterhin kann auf Einhaltung von Gesetzen, Richtlinien und geltenden Regelungen Bezug genommen werden.

  Im betrachteten IT-Verbund wird z. B. besonderer Wert auf die Vertraulichkeit der Produktionsdaten gelegt, da diese ihm im Vergleich zu Konkurrenzunternehmen wirtschaftliche Vorteile sichern.

- *Detailziele*

  Ausgehend von den spezifischen Aktivitäten des Geltungsbereichs werden die übergreifenden – und allgemein gehaltenen – Ziele detailliert.

- *IT-Sicherheitsmanagement*

  Die Organisation der Sicherheit innerhalb des Geltungsbereichs wird definiert. Hier werden insbesondere Rollen und Verantwortlichkeiten der einzelnen Funktionen festgelegt.

- *Sicherheitsmaßnahmen*

  Auf abstraktem Niveau werden übergeordnete Sicherheitsmaßnahmen bereits in der Sicherheitspolitik definiert. Solche Ziele können z. B. der Einsatz von Firewallsystemen bei der Internetanbindung oder von Virenschutzsystemen sein. Auf technische Details wird in der Sicherheits-Leitlinie nicht eingegangen.

- *Verbesserung der Sicherheit*

  Da Sicherheit ein Prozess ist, wird bereits in der Sicherheitspolitik festgehalten, wie das erreichte Sicherheitsniveau aufrecht erhalten wird.

Das BSI hat unter [MURI] Musterrichtlinien und Beispielkonzepte zur Verfügung gestellt. In Kapitel 10 befindet sich eine aus [MURI] abgeleitete beispielhafte Sicherheits-Leitlinie, wie sie für die hier betrachtete Institution verwendet werden kann.

4.2 IT-Sicherheitskonzept

Die Erstellung des IT-Sicherheitskonzeptes wird als IT-Sicherheitskonzeption bezeichnet und besteht aus den Phasen Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, Basissicherheitscheck und Realisierung (siehe Abbildung 4), die in den nachfolgenden Kapiteln beschrieben sind. Die Dokumentation der Ergebnisse dieser Phasen bilden das IT-Sicherheitskonzept

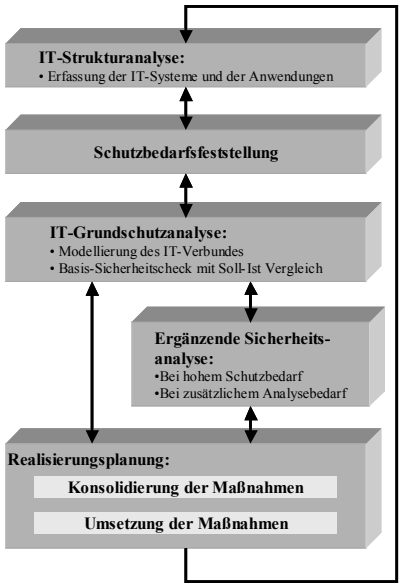
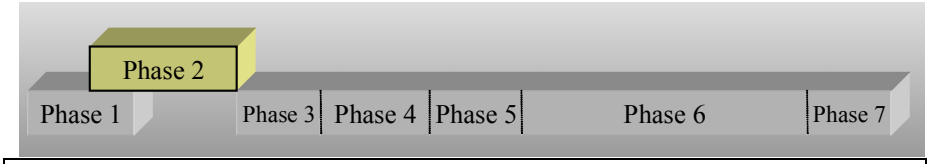


Abbildung 4: Prozess der IT-Sicherheitskonzeption

Diese Dokumentation des IT-Sicherheitskonzeptes kann mit Hilfe des GSTOOL erfolgen, welches die Möglichkeit bietet, die relevanten Reports aus den erfassten Daten zu generieren.

Das IT-Sicherheitskonzept muss hierbei nicht die gesamte Institution umfassen, sondern kann auch sinnvolle Teilbereiche betreffen. Ein IT-Sicherheitskonzept für z. B. eine einzelne Abteilung innerhalb einer Institution ist somit möglich und kann sinnvoll sein und als Ausgangspunkt für ein umfassendes IT-Sicherheitskonzept dienen, wenn die Institution eine komplexere IT-Infrastruktur besitzt.

5 Strukturanalyse



Verantwortlich	IT-Sicherheitsverantwortlicher
Einzubeziehen	IT-Verantwortliche
Zeitlicher Aufwand	ca. ½ Monat

Im Rahmen der IT-Strukturanalyse (vgl. Kapitel 2.1 [GSHB]) wird der IT-Verbund vollständig erfasst und alle Komponenten berücksichtigt. In der betrachteten Institution wird die IT-Strukturanalyse vom IT-Sicherheitsbeauftragten mit Unterstützung durch die IT-Verantwortlichen durchgeführt. Für die betrachtete Institution wird hierfür ein Zeitraum von ca. 2 Wochen veranschlagt.

Die IT-Strukturanalyse besteht hierbei aus den drei Schritten:

Schritt 1 Auswertung eines Netzplans

Die IT-Strukturanalyse beginnt bei der Auswertung und Aktualisierung des Netzplanes (beispielsweise in Form eines Netztopologieplans, vgl. Kapitel 3). Ein Netzplan ist eine graphische Übersicht über die eingesetzten Komponenten und deren Vernetzung, bei dem gleichwertige Komponenten zusammengefasst (gruppiert) sind.

Bei der Auswertung des Netzplanes werden zusätzlich die wesentlichen Kommunikationsverbindungen zwischen den IT-Systemen sowie die Außenverbindungen erfasst.

Schritt 2 Erhebung der IT-Systeme

Zu erfassen sind sowohl die vernetzten als auch die nicht-vernetzten IT-Systeme, also insbesondere auch solche, die nicht im zuvor betrachteten

Netzplan aufgeführt sind. IT-Systeme, die bei der Bereinigung des Netzplans zu einer Gruppe zusammengefasst worden sind, können als ein Objekt behandelt werden. Auch bei den IT-Systemen, die nicht im Netzplan aufgeführt sind, ist zu prüfen, ob sie sinnvoll zusammengefasst werden können.

Gleichzeitig mit der Erfassung der IT-Systeme werden zusätzlich auch die IT-Benutzer und IT-Verantwortlichen des jeweiligen Systems erfasst, so dass zur Erfassung des Personals kein gesonderter Arbeitsschritt erforderlich ist.

Schritt 3 Erfassung der IT-Anwendungen und der zugehörigen Informationen

Zur Reduzierung des Aufwands werden nur die jeweils wichtigsten auf den betrachteten IT-Systemen laufenden oder in naher Zukunft geplanten IT-Anwendungen erfasst. Im nachfolgenden Abschnitt 5.3 werden Beispiele zur Vorgehensweise anhand des betrachteten IT-Verbunds gegeben.

Diese im Rahmen der IT-Strukturanalyse erforderlichen Schritte, werden in den nachfolgenden Abschnitten näher erläutert.

In Kapitel 5.4 werden die einzelnen Schritte mit Hilfe des GSTOOL beispielhaft durchgeführt. Steht kein GSTOOL zur Verfügung, müssen die Informationen papierhaft – z. B. in Form einer Tabelle – erfasst werden. Hilfsmittel zur tabellarischen Erfassung dieser Informationen hat das BSI unter [GSHILF] zur Verfügung gestellt. Diese Hilfsmittel können als Alternative zum GSTOOL genutzt werden, um die IT-Strukturanalyse durchzuführen.

5.1 Netzplan

Der Netzplan wird in einem nächsten Schritt aktualisiert und dabei um fehlende Komponenten (z. B. nicht-vernetzte Rechner) erweitert (*aktualisierter Netzplan*).

Gruppierung / Komplexitätsreduktion

Durch Gruppierung ähnlicher Komponenten kann die Komplexität der dargestellten Infrastruktur reduziert werden. Eine Zusammenfassung der Komponenten aus dem in Kapitel 3 dargestellten IT-Verbund wie z. B. den Standard-PC mit Spezialsoftware ergibt die in Abbildung 5 dargestellte Situation. Die dargestellten Systeme bestehen jeweils aus dem Standard-PC mit Windows 2000 Betriebssystem und einer Office-Umgebung. Zusätzlich sind die Systeme mit einer für den jeweiligen Tätigkeitsbereich des Anwenders erforderlichen Spezialsoftware ausgestattet. Es handelt sich also jeweils um einen Standard-PC mit Spezialsoftware, so dass diese Systeme zu einer PC-Gruppe „PC MA“ (PC Mitarbeiter) zusammengefasst werden können.

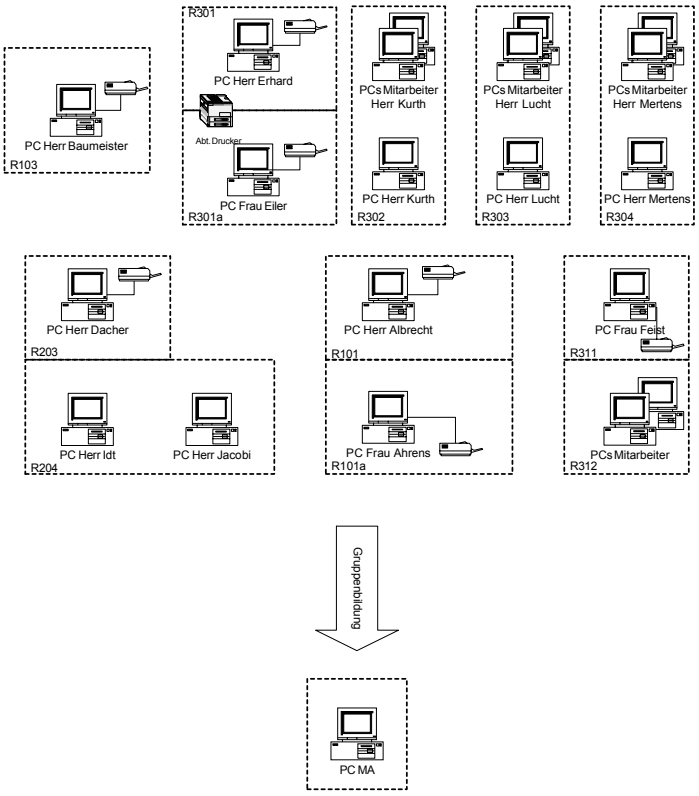


Abbildung 5: Komplexitätsreduktion durch Gruppenbildung

Aus einer konsequent durchgeführten Gruppenbildung (Abbildung 5) aller Systeme des IT-Verbundes resultiert der in Abbildung 6 dargestellte *bereinigte* Netzplan. Hierbei wurden die PCs der Mitarbeiter (Abteilungsleiter, Teamleiter, Sekretärinnen und Institutsleiter sowie IT-Sicherheits und QM-Beauftragter) zur Gruppe der „PC MA“ wie oben beschrieben zusammengefasst. Die Gruppe „PC Projekt A“ beinhaltet Systeme der Abteilung Produktion und IT, die gemeinsam an einem Projekt arbeiten, bei dem ein erhöhter Bedarf an Verfügbarkeit auf die Projektergebnisse erforderlich ist.

Diese Gruppe wurde organisationsübergreifend definiert. Als Ausgangspunkt diente hierbei der gemeinsame hohe Schutzbedarf bzgl. der Verfügbarkeit, der vom Schutzbedarf der restlichen Systeme abweicht. Damit ist die Bildung einer separaten Gruppe sinnvoll.

Die in der Institution vorkommenden Kommunikationsverbindungen sind textuell im Netzplan hervorgehoben.

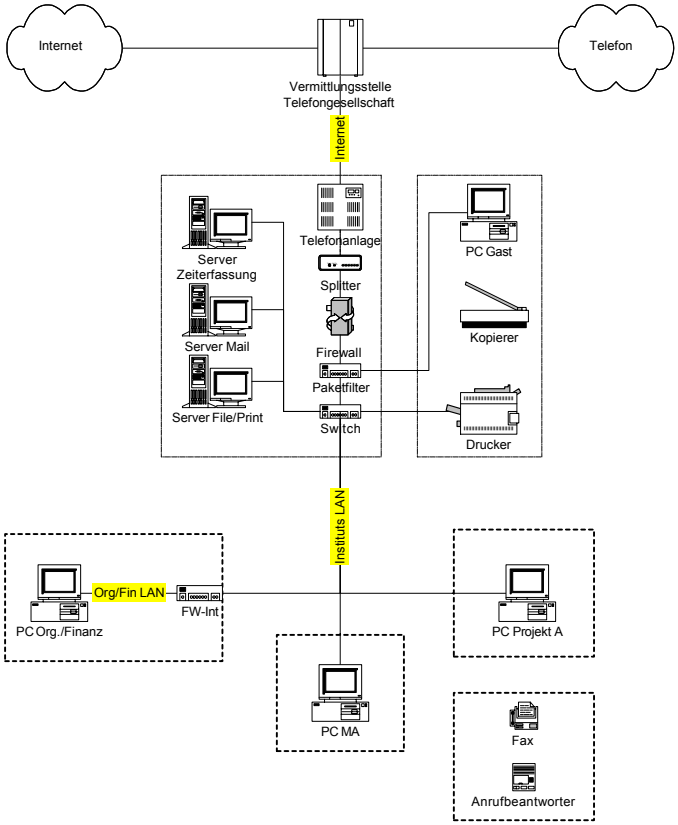


Abbildung 6: bereinigter Netzplan

Dieser bereinigte Netzplan bildet die Grundlage für die anschließend durchzuführenden Schritte der IT-Strukturanalyse *Erhebung der IT-Systeme* und *Erfassung der IT-Anwendungen*. Das Ergebnis dieser Erhebung ist in der Tabelle in Anhang A dargestellt.

5.2 Erhebung der IT-Systeme

Auf Grundlage des bereinigten Netzplans werden die einzelnen IT-Systeme innerhalb des IT-Verbunds erfasst. Falls sich der IT-Sicherheitsbeauftragte entscheidet, eine tabellarische Erfassung ohne Unterstützung eines GSTOOL durchzuführen, bietet es sich an, die Spaltenüberschriften entsprechend der nachfolgenden Auflistung zu wählen:

- Eindeutige Bezeichnung/Kürzel (z. B. die Inventarnummer) des Systems,
- Name des Systems (z. B. entsprechend der Gruppenbezeichnung des bereinigten Netzplans),
- Typ des Systems / Plattform (z. B. Client/PC unter Windows 2000),
- bei gruppierten Systemen die Anzahl zusammengefasster Systeme,
- Status des Systems (in Betrieb/Test/Planung/Reparatur),
- Standort des Systems (beispielsweise Gebäude- und Raumnummer, bei größeren Serverräumen zusätzlich Standort innerhalb des Raums),
- Nutzer und zuständiger Administrator des Systems sowie
- Art der Netzanbindung und die Netzadresse.

Es bietet sich hierfür an, die in Anhang A dargestellte Tabelle als Ausgangspunkt zu nutzen und die Tabelle um die o.g. Spalten zu erweitern.

Zur Erfassung der Nutzer werden anhand des Organigramms unterschiedliche Benutzergruppen definiert (vgl. Kapitel 3.2 [GSHB]) und den in Kapitel 2.3 genannten Rollen zugewiesen. Benutzer, die identische oder ähnli-

che Funktionen innerhalb der Institution wahrnehmen und ähnliche IT-Systeme und Anwendungen nutzen, werden zu einer Benutzergruppe zusammengefasst (vgl. Kapitel 5.4).

Bei der Bildung von Personengruppen lassen sich z. B. die Mitarbeiter einer Abteilung oder eines Teams oft gut zu einer Gruppe zusammenfassen, da sie vergleichbare IT-Systeme und Anwendungen nutzen.

Das GSTOOL kann bei der Erhebung der einzelnen Daten als Hilfsmittel eingesetzt werden. Die Erfassung von IT-Systemen mit dem GSTOOL wird in Kapitel 5.4.1 erläutert.

Die direkt an die PCs angeschlossenen Drucker (z. B. Parallel-/ USB-Port) werden nicht als eigenständige Komponenten erfasst, sondern sind aus Sicht des GSHB lediglich ein Teil des jeweiligen PCs. Diese Information wird als Notiz zum jeweiligen Zielobjekt erfasst.

Nachdem die IT-Systeme erfasst wurden, sieht das GSHB nun die Erfassung der IT-Anwendungen vor.

5.3 IT-Anwendungen

IT-Systeme werden genutzt, um IT-Anwendungen zu betreiben. Im 3. Schritt der IT-Strukturanalyse werden die im IT-Verbund eingesetzten Anwendungen erfasst. Hierbei wird ausgehend von den im vorangegangenen Schritt aufgenommenen IT-Systemen festgehalten, welche IT-Anwendungen auf den einzelnen Systemen (bzw. Gruppen von Systemen) laufen.

Es werden die jeweils wichtigsten auf den betrachteten IT-Systemen laufenden IT-Anwendungen erfasst.

Das GSHB kann nicht nur bereits vorhandene, sondern darüber hinaus für die Konzeption und Auswahl von Standardsicherheitsmaßnahmen neu geplanter IT-Systeme genutzt werden. Hierfür werden in diesem Schritt ge-

plante IT-Anwendungen erfasst. Die Vorgehensweise des GSHB entspricht dann der Erstellung eines Entwicklungskonzeptes (vgl. Kapitel 2.3 [GSHB]). Im Falle einer angestrebten Zertifizierung durch das BSI ist die Erfassung geplanter IT-Anwendungen jedoch nicht sinnvoll, da nur vorhandene Systeme und Anwendungen zertifiziert werden können.

Im Sinne einer effizienten Durchführung kann auf eine vollständige Erfassung aller Anwendungen verzichtet werden, wenn sichergestellt ist, dass zumindest diejenigen IT-Anwendungen des jeweiligen IT-Systems erfasst werden,

- deren Daten bzw. Informationen und Programme den höchsten Bedarf an Vertraulichkeit haben,
- deren Daten bzw. Informationen und Programme den höchsten Bedarf an Integrität besitzen und
- die die kürzeste tolerierbare Ausfallzeit (höchster Bedarf an Verfügbarkeit) haben.

Auf die Erfassung einer Anwendung, die nur sporadisch von einem Anwender genutzt wird, kann beispielsweise verzichtet werden, wenn sie kein wesentlicher Bestandteil der Tätigkeitsausübung ist und die verarbeiteten Daten kein hohes Maß an Integrität und Vertraulichkeit bedürfen. Bei der Erfassung der Anwendungen muss daher immer beurteilt werden, welche Art Daten verarbeitet werden und wie abhängig der Benutzer bei seiner Tätigkeitsausübung von der Anwendung ist.

Um dies sicherzustellen, müssen die IT-Benutzer und IT-Verantwortlichen im Rahmen der Erfassung mit einbezogen werden. Erfasst werden hierbei:

- eine Beschreibung und Kurzbezeichnung der Anwendung,
- die betroffenen IT-Systeme sowie
- die Information darüber, ob mit der Anwendung personenbezogene Daten gespeichert und/oder verarbeitet werden.

Auch diese Erfassung kann mit dem GSTOOL durchgeführt werden. Die Erfassung einer IT-Anwendung mit dem GSTOOL ist in Kapitel 5.4.4 erläutert.

Werden die Daten tabellarisch erfasst, bietet es sich neben den drei o.g. Punkten an, Spalten für die Erfassung des Schutzbedarfs hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität mit in der Tabelle vorzusehen, da diese Informationen in Phase 3 (Schutzbedarfsfeststellung) benötigt werden.

Mit diesem Schritt ist die Phase 2 – IT-Strukturanalyse – abgeschlossen und eine genaue Übersicht über die vorhandene IT-Infrastruktur ist erstellt. Alle IT-Systeme, IT-Anwendungen, Räume, Kommunikationsverbindungen und Personengruppen wurden erfasst und es ist dokumentiert

- welche IT-Systeme und IT-Anwendungen in der Institution vorkommen,
- welche Personen die IT-Anwendungen und IT-Systeme nutzen (IT-Benutzer) und pflegen/warten (IT-Verantwortliche) sowie
- wo die IT-Systeme aufgestellt und welche wesentlichen Kommunikationsverbindungen vorhanden sind.

In Phase 3 (Kapitel 6) – Schutzbedarfsfeststellung – wird der Schutzbedarf der IT-Komponenten bestimmt.

Das nachfolgende Kapitel 5.4 stellt die IT-Strukturanalyse unter Zuhilfenahme des GSTOOL dar. Wird die IT-Strukturanalyse nicht werkzeugunterstützend durchgeführt, bietet es sich an Tabellen zu erstellen, mit denen die angegebenen Informationen - wie erläutert - sinngemäß erfasst werden können.

5.4 Strukturanalyse mittels GSTOOL

Dieses Kapitel enthält anhand des GSTOOL erläuterte Beispiele der einzelnen Schritte der IT-Strukturanalyse. Da mit dem GSTOOL neben den IT-Systemen und IT-Anwendungen auch Personen(gruppen), Räume und Kommunikationsverbindungen erfasst werden, unterscheiden sich die einzelnen Schritte leicht von der in den vorangegangenen Abschnitten dargestellten Vorgehensweise des GSHB. Die Vorgehensweise des GSHB sieht eine Erfassung von Personen(-gruppen), Räumen und Kommunikationsverbindungen nicht explizit vor, diese Informationen werden vielmehr implizit erfasst. Aus diesem Grund ist im GSHB kein separater Schritt für die Erfassung dieser Informationen vorhanden. Die Vorgehensweise mit dem GSTOOL macht jedoch die strukturierte Erfassung dieser Informationen erforderlich und wird nachfolgend als eigener Schritt mit erwähnt. Die Vorgehensweise im GSTOOL besteht aus dem „Erfassen“ (von Komponenten) und der „Verknüpfung“ erfasster Komponenten miteinander. Diese Vorgehensweise ist in der folgenden Abbildung 7 dargestellt.

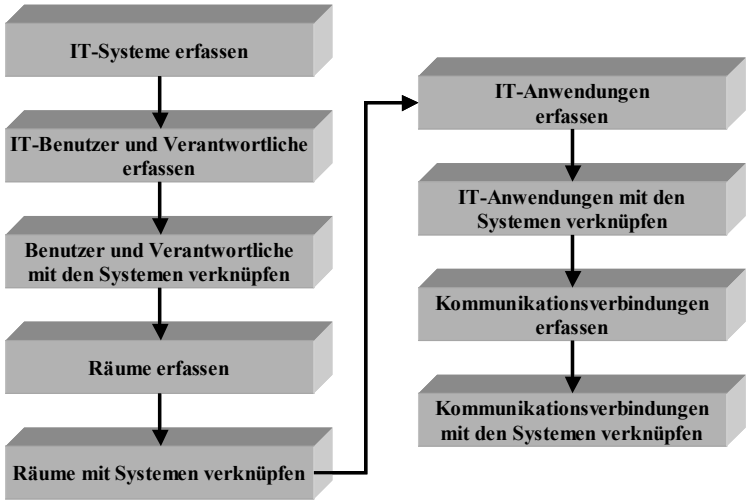


Abbildung 7: Vorgehensweise mit GSTOOL

Das Ergebnis der IT-Strukturanalyse ist jedoch identisch mit der manuellen Vorgehensweise.

5.4.1 Erfassung der IT-Systeme mit dem GSTOOL

Im GSTOOL werden die Informationen zu einem IT-System als Zielobjekt **IT-System** eingepflegt (vgl. Kapitel 3.2 [GSTHB]). Abbildung 8 stellt die für die Gruppe der Mitarbeiter-PCs in diesem Schritt (PC MA) einzutragenden Daten dar.

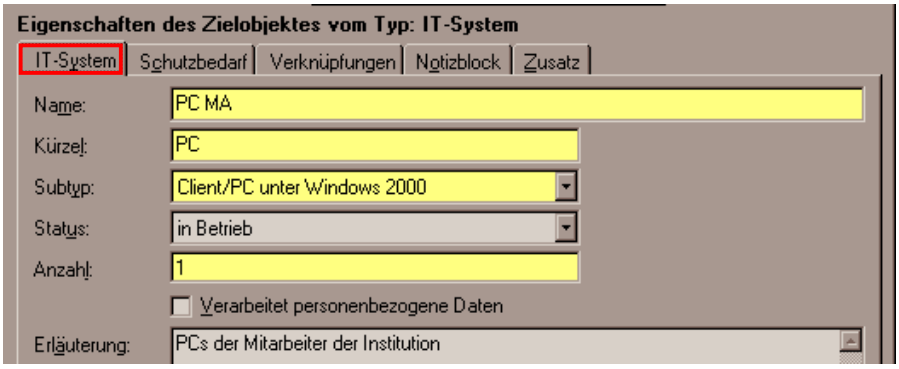


Abbildung 8: IT-System-Gruppe der Mitarbeiter-PCs

Mit den übrigen Gruppen innerhalb des IT-Verbunds wird identisch verfahren, so dass nach Aufnahme aller Gruppen im Zielobjekt IT-System die in Abbildung 9 wiedergegebene Übersicht im GSTOOL existiert.

Insgesamt besteht der in Kapitel 3 dargestellte IT-Verbund aus 12 Gruppen von IT-Systemen.

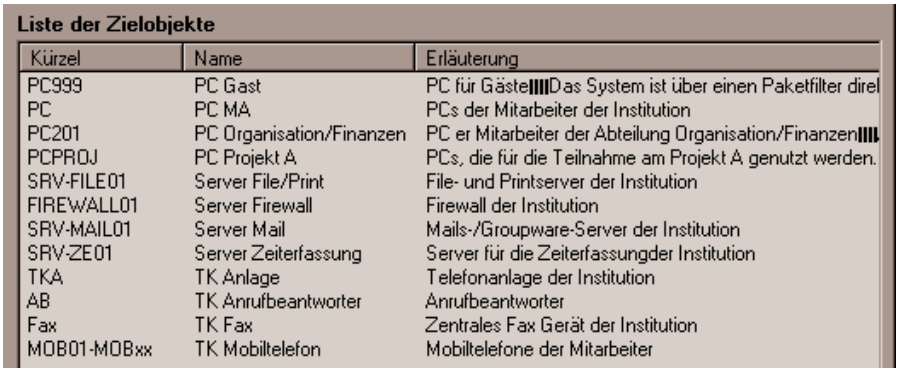


Abbildung 9: Liste erfasster IT-Systeme

Nachdem alle IT-Systeme erfasst wurden müssen die IT-Benutzer, IT-Verantwortlichen und die Räume der Systeme erfasst werden.

5.4.2 Erfassung von IT-Benutzern und IT-Verantwortlichen

Auch Benutzergruppen werden im GSTOOL als eigenes Zielobjekt aufgefasst. Exemplarisch sind in Abbildung 10 gemäß der im GSTOOL benutzten Terminologie die Eigenschaften des Zielobjekts (Benutzergruppe) MA Mitarbeiter dargestellt. Die Benutzergruppe besteht in diesem Fall aus allen Mitarbeitern der Institution ohne die Mitarbeiter der Abteilung Organisation/Finanzen, die aufgrund des Umgangs mit sensiblen Daten in einer separaten Gruppe eingegliedert wurden.

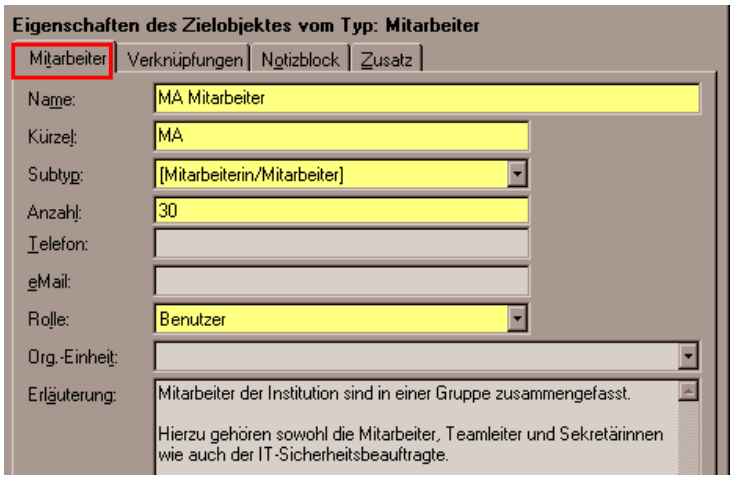


Abbildung 10: Definition der Benutzergruppe MA Mitarbeiter

Anschließend werden die erfassten Mitarbeiter mit den erfassten IT-Systemen verknüpft (vgl. Kapitel 4.2 [GSTHB]).

In Abbildung 11 ist die Zuordnung exemplarisch dargestellt. Hierbei ist die Verknüpfung des PC MA mit den Mitarbeiter als IT-Benutzer und einem Mitarbeiter IT als Administrator dargestellt.

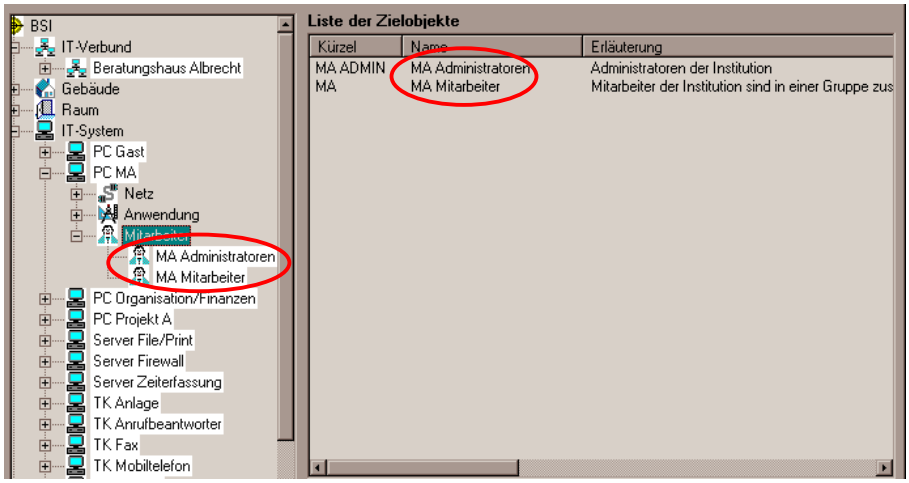


Abbildung 11: Verknüpfung des PC MA mit den Mitarbeitern der Institution und dem Mitarbeiter IT als Administrator

5.4.3 Erfassung von IT-Räumen

Nachdem die IT-Benutzer und IT-Verantwortlichen festgelegt sind, muss der Standort des Systems festgehalten werden. Das GSTOOL betrachtet IT-Räume als ein eigenes Zielobjekt. Für jeden Raum der Institution werden dabei folgende Daten erfasst:

- Bezeichnung des Raums,
- Raumnummer,
- Raumtyp (Büroraum, Datenträgerarchiv, häuslicher Arbeitsplatz, Rechenzentrum, Schutzschrank, Serverraum oder Technikraum).

In Abbildung 12 ist die Erfassung der Büroräume der Mitarbeiter des in Kapitel 3 dargestellten IT-Verbundes anhand des GSTOOL dargestellt.

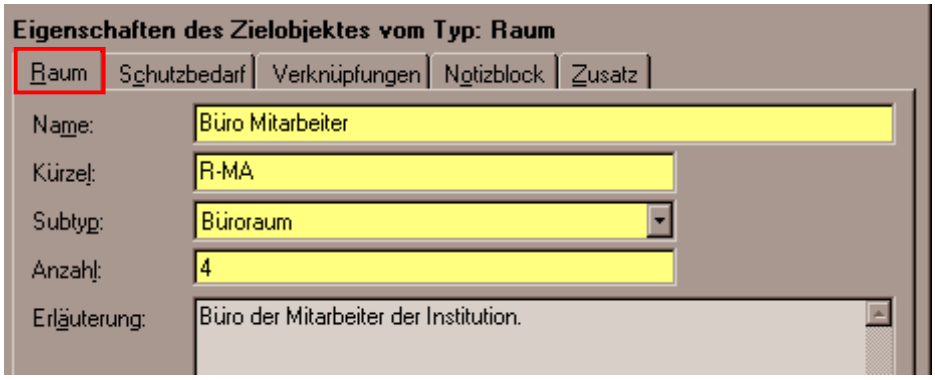


Abbildung 12: Erfasster Raum des IT-Sicherheitsbeauftragten

Die Möglichkeit Räume zu Raumgruppen zusammen zu fassen, wurde hierbei intensiv genutzt. Bei der Betrachtung des IT-Verbundes aus Kapitel 3 ist aufgefallen, dass – bis auf die Räume der Abteilung Organisation/Finanzen – alle Büroräume der Mitarbeiter zusammengefasst werden können. Die Büroräume der Mitarbeiter der Abteilung Organisation/Finanzen können nicht mit den Räumen der übrigen Mitarbeiter gruppiert werden, da hier personenbezogene Daten verarbeitet werden.

Nachdem die Räume bzw. Raumgruppen erfasst wurden, wird dieser mit den IT-Systemen verknüpft (vgl. Kapitel 4.2 [GSTHB]), die in diesem Raum aufgestellt sind.

Nachdem die IT-Systeme erfasst und die Mitarbeiter sowie Räume den IT-Systemen zugeordnet wurden, erfordert der nächste Schritt der IT-Strukturanalyse gemäß GSTOOL die Erfassung der einzelnen IT-Anwendungen.

5.4.4 Erfassung der IT-Anwendungen mit dem GSTOOL

Mit dem GSTOOL werden eine Bezeichnung der Anwendung sowie ein Kürzel und der Typ der Anwendung (Datenbank/Datenträgeraustausch/E-

Mail/Faxserver/Lotus Notes/Novell eDirectory/WWW-Dienst oder Allgemeine Anwendung) erfasst. Die Office-Anwendung des beispielhaften IT-Verbundes wird z. B. wie in Abbildung 13 dargestellt, mit dem GSTOOL erfasst.

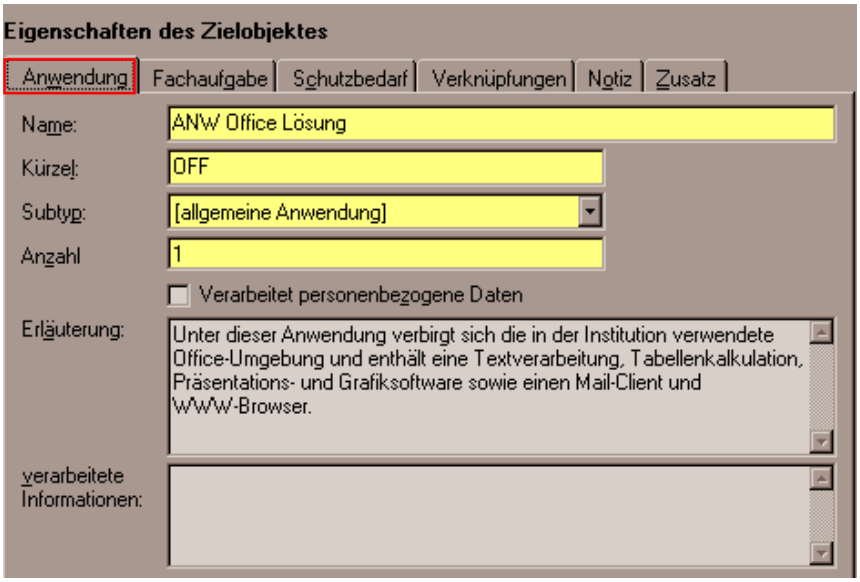


Abbildung 13: Erfasste IT-Anwendung „Office Lösung“

Die Anwendungen zur Zeiterfassung und Arbeitszeitauswertung nehmen hierbei eine Sonderrolle ein, da mit ihr personenbezogene Daten verarbeitet werden. Dies ist wie in Abbildung 14 dargestellt, im GSTOOL besonders zu vermerken.

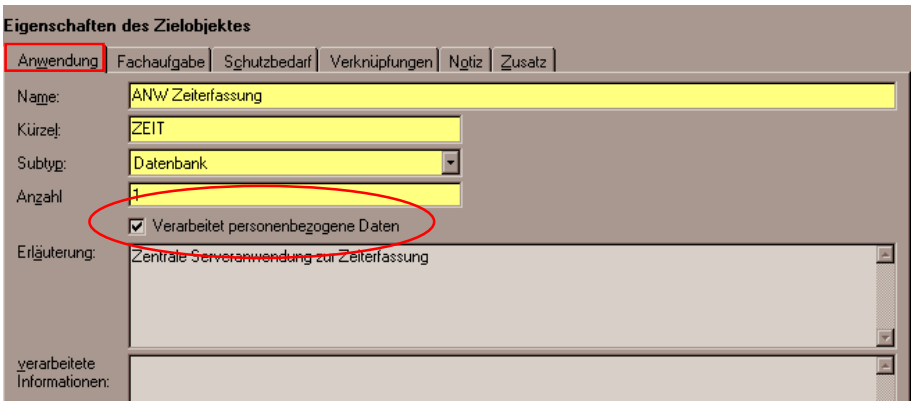


Abbildung 14: IT-Anwendung, die personenbezogene Daten verarbeitet

Mit den übrigen Gruppen der Anwendungen wird bei der Erfassung ebenso vorgegangen, so dass nach Aufnahme aller Gruppen von Anwendungen die in Abbildung 15 gezeigte Aufstellung im GSTOOL existiert.

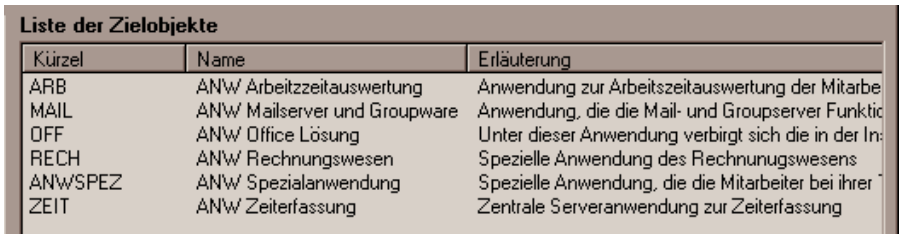


Abbildung 15: Liste aller erfassten IT-Anwendungen

Insgesamt werden in dem in Kapitel 3 dargestellten IT-Verbund sechs Gruppen von Anwendungen eingesetzt. Die von den Mitarbeitern für die Ausübung ihrer Tätigkeiten genutzte Anwendung wird in der Gruppe „*ANW Spezialanwendung*“ zusammengefasst. Unter diese Gruppe fallen damit z. B. das in der Abteilung Produktion genutzte Projektmanagement-Tool oder die Softwareentwicklungs-Werkzeuge im Labor. Im Anschluss an die Erfassung der Anwendung ist es erforderlich, die erfassten Anwen-

dungen den IT-Systemen zuzuordnen. Im GSTOOL werden die Anwendungen mit den Systemen „verknüpft“ (vgl. Kapitel 4.2 [GSTHB]).

5.4.5 Kommunikationsverbindungen mit dem GSTOOL

Die Methodik des GSHB sieht die Betrachtung und Erfassung der Kommunikationsverbindungen erst während der Schutzbedarfsfeststellung (siehe Kapitel 6) vor. Bei einer toolgestützten Vorgehensweise bietet es sich jedoch an, die Kommunikationsverbindungen bereits während der IT-Strukturanalyse zu erfassen. Wie auch bei den IT-Räumen betrachtet das GSTOOL auch IT-Verbindungen als eigenes Zielobjekt.

Abbildung 16 stellt die mit Hilfe des GSTOOL erfasste Internetanbindung dar.

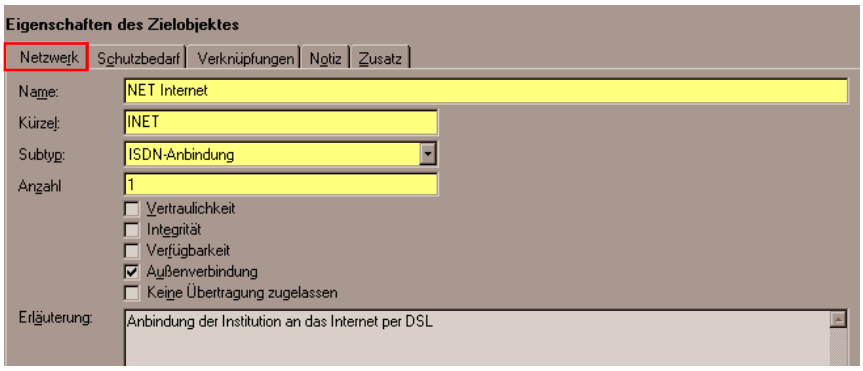


Abbildung 16: Erfasste (kritische) Internetanbindung

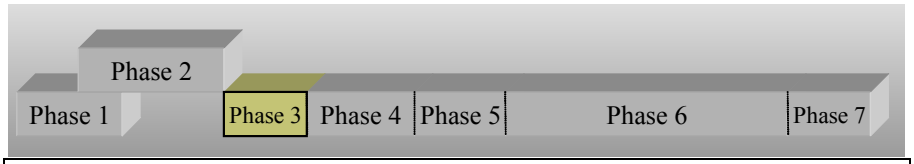
Das GSTOOL besitzt derzeit keinen Subtyp DSL, so dass unter Verwendung von Kapitel 8 [GSHB] ein geeigneter Baustein für die Internetanbindung ausgewählt werden muss. Als geeignet für die Darstellung der Internetanbindung erscheint der in Kapitel 8.4 aus [GSHB] beschriebene Baustein *LAN-Anbindung eines IT-Systems über ISDN*, so dass dieser zunächst als Typ verwendet wird.

Nachdem alle Verbindungen erfasst wurden, müssen diese mit den IT-Systemen verknüpft werden (vgl. Kapitel 4.2 [GSTHB]).

Ebenso wird mit allen übrigen IT-Systemen verfahren. Jeder interne PC wird somit mit dem Instituts-LAN verknüpft. Die TK-Anlage und das Faxgerät werden in gleicher Weise mit dem ISDN-Netz verknüpft. Die Firewall wird hierbei sowohl mit dem Instituts-LAN als auch mit dem Internet verknüpft, da sie die Übergabestelle bildet. Der PC Organisation/Finanzen wird mit dem NET ORG/FIN verknüpft und der Gast PC mit dem NET Gast.

Das Ergebnis dieses Schritts ist die Zuordnung der Kommunikationsverbindung zu jedem IT-System.

6 Schutzbedarfsfeststellung



Verantwortlich	IT-Sicherheitsverantwortlicher
Einzubeziehen	Institutsleitung
	IT-Verantwortliche
	IT-Benutzer
Zeitlicher Aufwand	ca. ½ Monat

Das Ziel der Schutzbedarfsfeststellung (Vorgehensweise siehe Abbildung 17) ist die Bestimmung des Schutzbedarfs für alle Komponenten des IT-Verbunds. Da der Schutzbedarf meist nicht exakt quantifizierbar ist, beschränkt sich das GSHB auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien – „normal“, „hoch“ und „sehr hoch“ – unterteilt wird.

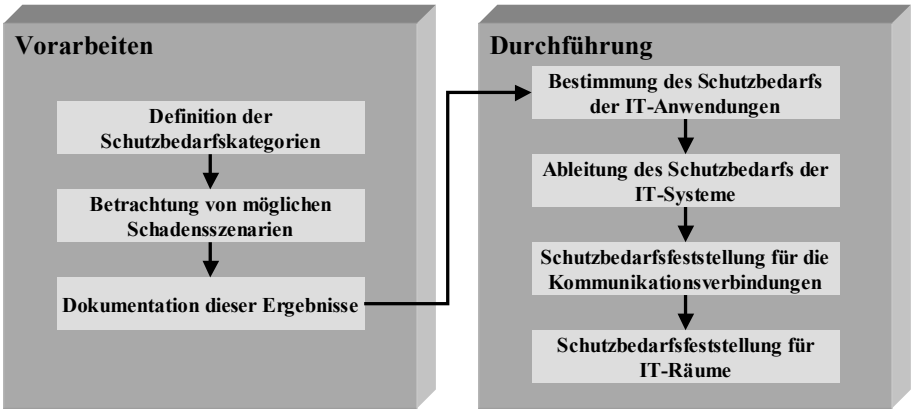


Abbildung 17: Vorgehensweise der Schutzbedarfsfeststellung

Der IT-Sicherheitsbeauftragte benötigt für die Durchführung dieser Aufgabe insbesondere die Unterstützung der IT-Anwender, da diese am besten die Schutzbedürftigkeit der von ihnen gespeicherten und verarbeiteten Daten einschätzen können. Der IT-Sicherheitsbeauftragte wird in Gesprächen mit den Anwendern die Schutzbedarfsfeststellung durchführen. In der Institution wird der IT-Sicherheitsbeauftragte stellvertretend für die IT-Anwender mit den Abteilungsleitern die Bewertung durchführen.

Nachfolgend werden die einzelnen Schritte der Schutzbedarfsfeststellung anhand des exemplarischen IT-Verbundes aus Kapitel 3 erläutert.

6.1 Vorarbeiten

Vor der eigentlichen Schutzbedarfsfeststellung müssen die Schutzbedarfskategorien voneinander abgegrenzt werden. Anschließend werden konkrete Schadensszenarien (*Was wäre wenn? - Szenarios*) betrachtet. Es bietet sich an, diese Vorarbeiten im Rahmen von Workshops mit der Institutsleitung zu erarbeiten. Die Vorbereitung des Workshops wird üblicherweise vom

IT-Sicherheitsbeauftragten vorgenommen. Die Ergebnisse des Workshops sollten in Form von Schutzbedarfskategorien als Teil der Sicherheitsdokumentation festgehalten werden.

6.1.1 Phase 1: Definition der Schutzbedarfskategorien

Zunächst werden die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ definiert. Als Rahmen dient hierbei die folgende Einstufung:

normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein.
sehr hoch	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Die einzelnen Schutzbedarfskategorien müssen hinsichtlich des Verlusts von Vertraulichkeit, Integrität oder der Beeinträchtigung der Verfügbarkeit, die für eine IT-Anwendung einschließlich ihrer Daten entstehen können, konkretisiert werden, so dass die adäquate Schutzbedarfskategorie im Einzelfall ausgewählt werden kann. Die Schäden lassen sich typischerweise den folgenden Schadensszenarien zuordnen:

- **Beeinträchtigung des informationellen Selbstbestimmungsrechts**

  Das informationelle Selbstbestimmungsrecht eines Benutzers sollte durch IT-Anwendungen nicht beeinträchtigt werden. Zudem muss ein Missbrauch personenbezogener Daten ausgeschlossen sein.

  Die in Kapitel 3 dargestellte Institution besitzt für die Verwaltung der Personaldaten eine eigene Abteilung. Da es sich hierbei um personenbezogene Daten handelt und der Missbrauch ausgeschlossen sein muss, muss dies bei der Schutzbedarfsfeststellung gesondert berücksichtigt werden.

- **Beeinträchtigung der Aufgabenerfüllung**

  Die Erfüllung der Aufgaben einer Institution kann durch den Verlust der Verfügbarkeit einer IT-Anwendung oder der Integrität der Daten erheblich beeinträchtigt werden. Je nach Umfang der Einschränkungen der angebotenen Dienstleistungen und der zeitlichen Dauer ist die Schwere des Schadens unterschiedlich zu bewerten.

  In der Institution aus Kapitel 3 würde z. B. ein Ausfall des internen Fileservers die Aufgabenerfüllung beeinträchtigen. Eine Folge könnte die verspätete Auslieferung von Dokumenten an die Kunden der Institution sein. Dies ist in Abhängigkeit von evtl. vereinbarten Vertragsstrafen bei der Schutzbedarfsfeststellung zu berücksichtigen.

- **Verstoß gegen Gesetze/Vorschriften/Verträge**

  Verstöße gegen Gesetze, Vorschriften oder Verträge können sowohl aus dem Verlust der Vertraulichkeit als auch der Integrität und der Verfügbarkeit resultieren. Der Umfang der sich hieraus möglicherweise ergebenden rechtlichen Konsequenzen für die Institution erlaubt eine Bewertung der Schadensgröße.

  Ein Verstoß gegen einen Vertrag kann bereits dann eintreten, wenn zugesagte Liefertermine nicht eingehalten werden können.

- **Beeinträchtigung der persönlichen Unversehrtheit**

  Falls die Fehlfunktion einer IT-Anwendung oder eines IT-Systems zu einer Verletzung einer Person führt oder sogar Invalidität bzw. Tod zur Folge haben kann, ist die Einstufung der Schadenshöhe am direkten persönlichen Schaden zu messen.

  Ein derartiger Fall tritt beispielsweise in der Medizintechnik auf, bei der durch Fehlfunktionen in IT-gestützten Systemen (z. B. Narkosesystemen, Bestrahlungsapparate) Menschenleben gefährdet sind.

- **Negative Außenwirkung**

  Ansehens- oder Vertrauensverlust oder allgemeine negative Außenwirkungen können durch Verlust einer der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit in einer IT-Anwendung entstehen.

  Die Höhe des Schadens orientiert sich hierbei an der Schwere des Vertrauensverlustes oder des Verbreitungsgrades der Außenwirkung.

  Für die in Kapitel 3 dargestellte Institution wäre es beispielsweise unhaltbar, wenn Informationen über im Kundenauftrag durchgeführte Projekte und deren Ergebnisse an die Öffentlichkeit gelangen.

- **Finanzielle Auswirkungen**

  Wird die Vertraulichkeit schutzbedürftiger Daten verletzt, werden solche Daten unbefugt verändert oder stehen für die Ausübung der Geschäftstätigkeit der Institution wichtige Daten nicht oder nicht rechtzeitig zur Verfügung, so ergeben sich hieraus unmittelbare oder mittelbare finanzielle Schäden. Das GSHB nennt hierfür folgende Beispiele:

  - unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,
  - Manipulation von finanzwirksamen Daten in einem Abrechnungssystem,
  - Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste,
  - Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen,
  - Ausfall eines Buchungssystems einer Reisegesellschaft,
  - Ausfall eines E-Commerce-Servers,
  - Zusammenbruch des Zahlungsverkehrs einer Bank,
  - Diebstahl oder Zerstörung von Hardware.

Bei der Ermittlung der Schadenshöhe ist zu berücksichtigen, dass sich die Höhe des Gesamtschadens aus den direkt und indirekt entstehenden Kosten zusammensetzt (Sachschäden, Schadenersatzleistungen und Kosten für zusätzlichen Aufwand wie z. B. Wiederherstellung).

Damit man eine für die betrachtete Institution gültige Abgrenzung der einzelnen Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ erhält, sollten die Grenzen für die einzelnen Schadensszenarien bestimmt und schriftlich festgehalten werden.

Nachfolgend werden konkrete Beispiele für die *Finanziellen Auswirkungen* gegeben. Im Beispiel werden die finanziellen Auswirkungen am Umsatz der Institution festgemacht. Möglich ist auch die Definition fester monetärer Grenzen (z. B. zwischen 50 EUR und 250 EUR). Wesentlich ist hierbei, dass die Institution entscheidet, welche Schadenshöhe verkraftbar ist und wann ein existenzbedrohender Schaden vorliegt:

Finanzielle Auswirkungen	
normal	Es entstehen der Institution finanzielle Schäden in Höhe von maximal 1% eines durchschnittlichen monatlichen Umsatzes.
hoch	Es entstehen der Institution finanzielle Schäden in Höhe von 1%-10% eines durchschnittlichen monatlichen Umsatzes.
sehr hoch	Es entstehen der Institution finanzielle Schäden in Höhe von über 10% eines durchschnittlichen monatlichen Umsatzes.

Tabelle 1: Abgrenzung von Schutzbedarfskategorie

Im Gespräch mit der Geschäftsführung wurden die obigen Grenzen für die Einstufung in Schadenskategorien für finanzielle Schäden festgelegt. Eine Bestimmung konkreter Werte (Einstufung von finanziellen Schäden über 100.000 Euro als ‚sehr hoch') hat man vermieden, um diese nicht in regelmäßigen oder unregelmäßigen Abständen neu festlegen zu müssen. Bei einer Veränderung der geschäftlichen Situation könnte der einmal festgelegte konkrete Wert für die Einstufung in eine Kategorie nicht mehr zutreffend sein. So würde etwa bei einem Auftragsrückgang auch der Umsatz sinken

und dazu führen, dass bereits ein finanzieller Schaden von 50.000 Euro sehr kritisch für den Fortbestand des Unternehmens wäre. Andererseits werden alle Mitarbeiter über die monatliche Geschäftsentwicklung unterrichtet, so dass die vorgenommene Kategorisierung ausreichend konkret ist.

Die angegebenen Schadensauswirkungen werden in den nächsten Schritten der Schutzbedarfsfeststellung genutzt, um den Schutzbedarf von IT-Anwendungen und IT-Systemen zu bestimmen. In der nächsten Phase werden Schadensszenarien betrachtet.

6.1.2 Phase 2: Ermittlung von Schadensszenarien

Zur Ermittlung der Schadensszenarien werden die maximalen Schäden und Folgeschäden betrachtet, die aus dem Verlust der Grundwerte der IT-Sicherheit entstehen können. Die potenziellen materiellen oder ideellen Schäden werden in realistischen Schadensszenarien aus Sicht der Anwender beschrieben. Der Schutzbedarf der IT-Anwendung wird hieraus abgeleitet (vergl. Kapitel 6.2) und bestimmt sich aus der Höhe der möglichen Schäden. Zur Bewertung werden die Verantwortlichen und die Benutzer der betrachteten IT-Anwendung einbezogen, da sie die beste Vorstellung darüber haben, welche Schäden entstehen können.

Die Verfügbarkeit des Systems PC Projekt A aus Kapitel 3 wird beispielsweise als „hoch“ eingestuft. Das Schadensszenario „Ausfall des Systems“ hätte für die Institution Konventionalstrafen zur Folge, da vertraglich ein täglicher Datenabgleich mit dem Auftraggeber vereinbart wurde. Bei Nichteinhaltung dieser Verpflichtung und dem damit verbundenen Verlust ist im Vertrag eine Konventionalstrafe von 50.000 Euro vorgesehen. Zusätzlich müssen die verlorenen Daten rekonstruiert werden, was mit einem Aufwand von 20 Mitarbeitertagen beziffert wird. Allein aufgrund der finanziellen Auswirkungen ist daher die Einstufung ‚hoch’ bzgl. der Verfügbarkeit vorzunehmen.

6.1.3 Phase 3: Dokumentation der Ergebnisse

Bestandteil des Sicherheitskonzepts sind sowohl die Definitionen der Schutzbedarfskategorien (Phase 1) als auch die ermittelten Schadensszenarien (Phase 2). Für die mittlere Institution ergeben sich die nachfolgend gelisteten Schutzbedarfskategorien. Die jeweils für *normalen / hohen / sehr hohen* Schutzbedarf gültigen Formulierungen sind durch ein „/“ voneinander getrennt.

Beeinträchtigung des informationellen Selbstbestimmungsrechts	
normal/ hoch/ sehr hoch	- Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als *tolerabel / bedeutend / nicht akzeptabel* eingeschätzt werden. - Ein möglicher Missbrauch personenbezogener Daten hat *geringe / erhebliche / gravierende* Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der Aufgabenerfüllung	
normal/ hoch/ sehr hoch	- Die Beeinträchtigung würde von den Betroffenen als *tolerabel / nicht tolerabel / existenzbedrohend* eingeschätzt werden. - Die tolerierbare Ausfallzeit beträgt maximal z. B. *12 / 1 bis 12 Stunden / weniger als 1 Stunde*.
Verstoß gegen Gesetze/Vorschriften/Verträge	
normal/ hoch/ sehr hoch	- Verstöße gegen Vorschriften und Gesetze haben *geringfügige / erhebliche / geschäftsschädigende* Konsequenzen - Vertragsverletzungen haben *geringe / hohe / existenzbedrohende* Konventionalstrafen zur Folge.
Beeinträchtigung der persönlichen Unversehrtheit	
normal/ hoch/ sehr hoch	- Eine Beeinträchtigung der persönlichen Unversehrtheit kann *wahrscheinlich / nicht absolut / nicht* ausgeschlossen werden.
Negative Außenwirkung	

normal/ hoch/ sehr hoch	- Es ist eine *geringe bzw. nur interne / breite / überregionale* Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
Finanzielle Auswirkungen	
normal/ hoch/ sehr hoch	- Es entstehen der Institution finanzielle Schäden in Höhe von *weniger als 1% / 1% bis 10% / mehr als 10% eines durchschnittlichen monatlichen Umsatzes*

Zusätzlich werden die Ergebnisse der nachfolgenden Schutzbedarfsfeststellungen der einzelnen Komponenten dokumentiert. Alle Ergebnisse sind als Bestandteil des Sicherheitskonzepts aufzubewahren und bei einer späteren Überprüfung anzupassen bzw. fortzuschreiben.

Die Dokumentation der nachfolgenden Schutzbedarfsfeststellung der IT-Anwendungen kann sowohl mittels des GSTOOL erfolgen, als auch direkt in der tabellarischen Erfassung der IT-Anwendung, in der drei Spalten (Verfügbarkeit, Vertraulichkeit und Integrität) für den Schutzbedarf vorgesehen sind.

6.2 IT-Anwendungen

Die in Abschnitt 6.1.2. definierten Schadensszenarien der IT-Anwendungen einschließlich ihrer Daten werden verwendet, um zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Für jede IT-Anwendung wird festgehalten, welche möglichen Schäden bei einer Beeinträchtigung der IT-Anwendung entstehen können. Der Schutzbedarf orientiert sich direkt an diesen Schadensausmaßen.

Abbildung 18 zeigt die Schutzbedarfsfeststellung der Anwendung „Rechnungswesen“ anhand des GSTOOL. Jeder definierte Schutzbedarf ist hierbei mit einem Kommentar zu versehen, in dem das jeweilige Ergebnis begründet wird. Dieser Kommentar ergibt sich direkt aus den definierten Schadensszenarien.

Das GSTOOL in seiner aktuellen Version unterstützt die Schutzbedarfsklassen „niedrig bis mittel“, „hoch“ und „sehr hoch“. Die Schutzbedarfsklasse „niedrig bis mittel“ ist mit der in diesem Dokument genutzten Schutzbedarfsklasse „normal“ identisch.

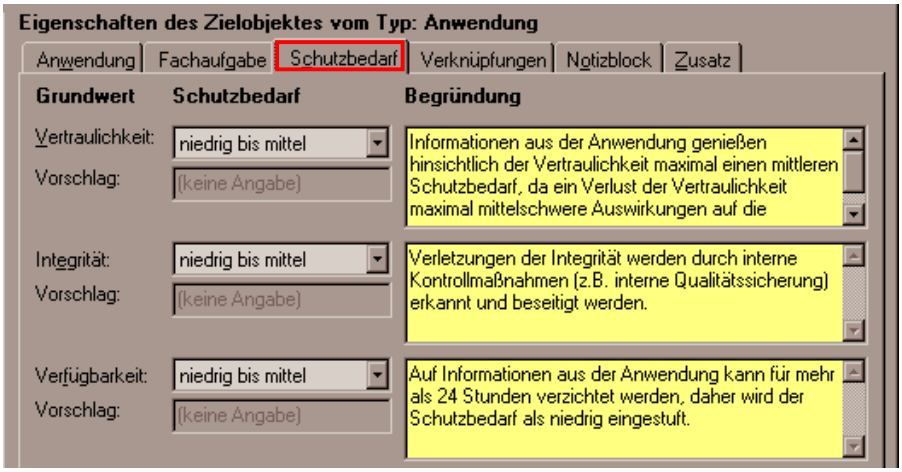


Abbildung 18: Schutzbedarfsfeststellung der Anwendung „Rechnungswesen“

Ebenso wird der Schutzbedarf aller weiteren Anwendungen bestimmt und dokumentiert.

6.3 IT-Systeme

Bei der Ermittlung des Schutzbedarfs der IT-Systeme geht man vom Schutzbedarf der auf diesen laufenden IT-Anwendungen aus. Ausgehend von den in Kapitel 5 ermittelten relevanten IT-Anwendungen wird der Schutzbedarf der IT-Systeme aus den möglichen Schäden im Falle einer Beeinträchtigung der Gesamtheit der betreffenden IT-Anwendungen ermittelt. Hierbei werden die folgenden Vorgehensweisen unterschieden:

1. ***Maximum-Prinzip***

   Der Schutzbedarf eines IT-Systems wird im Wesentlichen aus dem möglichen Schaden bzw. der Summe der möglichen Schäden mit den schwerwiegendsten Auswirkungen bestimmt.

2. ***Beachtung von Abhängigkeiten***

   Der Schutzbedarf eines IT-Systems oder einer IT-Anwendung wird auf ein anderes IT-System/IT-Anwendung übertragen, wenn die Funktionsfähigkeit von anderen IT-Systemen/Anwendungen abhängig ist (z. B. wenn eine Anwendung eine Datenbank eines anderen IT-Systems nutzt).

3. ***Kumulationseffekt***

   Der Schutzbedarf des IT-Systems erhöht sich, wenn mehrere IT-Anwendungen bzw. Informationen auf einem IT-System verarbeitet werden und durch Kumulation mehrere (z. B. kleinere) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entsteht.

4. ***Verteilungseffekt***

   Der Schutzbedarf des IT-Systems verringert sich – z. B. durch Lastverteilung – wenn auf dem IT-System nur unwesentliche Teilbereiche der IT-Anwendung laufen.

Abbildung 19 zeigt die Schutzbedarfsfeststellung des PC des IT-Sicherheitsbeauftragten (PC IT-Sicherheitsbeauftragter) anhand des GSTOOL. Wie bei den IT-Anwendungen ist der definierte Schutzbedarf mit einem Kommentar zu versehen.

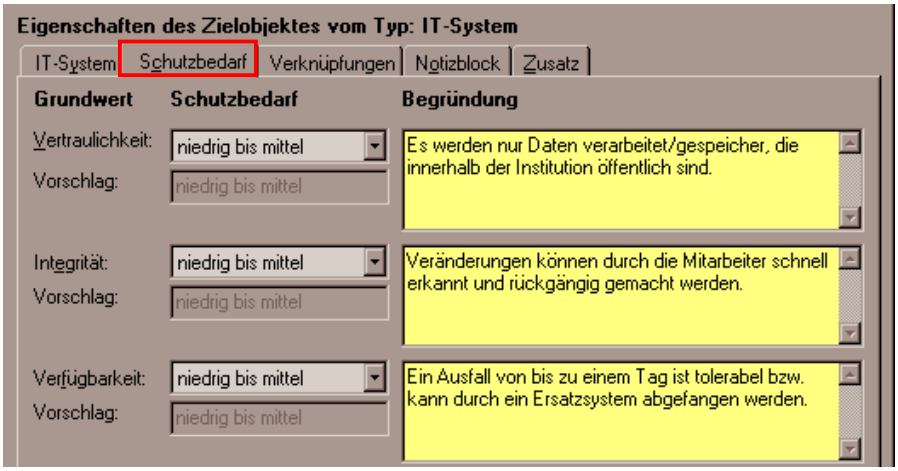


Abbildung 19: Schutzbedarfsfeststellung des PC IT-Sicherheitsbeauftragter

Das GSTOOL unterstützt die Definition des Schutzbedarfs, indem es anhand des Maximum-Prinzips den Schutzbedarf der dem IT-System zugeordneten IT-Anwendungen auf das IT-System ableitet und einen Vorschlag zum Schutzbedarf unterbreitet.

Der vom GSTOOL vorgeschlagene Schutzbedarf ist in jedem Fall zu überprüfen, da eine toolgestützte Schutzbedarfsfeststellung jeweils nur eine der o.g. Vorgehensweisen berücksichtigen kann. Für die IT-Systeme in den verschiedenen Abteilungen lässt sich der IT-Sicherheitsbeauftragte die Einstufung des Schutzbedarfs von den Abteilungsleitern bestätigen.

Ebenso wird der Schutzbedarf aller verbleibenden IT-Systeme bestimmt und dokumentiert.

Im nächsten Schritt wird der Schutzbedarf der vorhandenen Kommunikationsverbindungen bestimmt.

6.4 Kommunikationsverbindungen

Die Schutzbedarfsfeststellung von Kommunikationsverbindungen dient der Identifikation kritischer Verbindungen. Hierbei ist festzustellen, welche Kommunikationsverbindungen kryptographisch abzusichern, redundant auszulegen oder über welche Verbindungen Angriffe durch Innen- und Außentäter zu erwarten sind. Zu jeder Verbindung muss dabei erfasst werden,

- ob es sich um eine Außenverbindung handelt,
- ob die übertragenen Informationen einer hohen Vertraulichkeit bedürfen,
- ob die übertragenen Informationen einer hohen Integrität bedürfen,
- ob die übertragenen Informationen einer hohen Verfügbarkeit bedürfen und
- ob hochschutzbedürftige Informationen übertragen werden dürfen.

Im beispielhaften IT-Verbund aus Kapitel 3 wurde das interne Netz der Abteilung Personal / Finanzen durch eine interne Firewall vom Instituts-LAN separiert. Der Grund hierfür ist die Einschätzung, dass die innerhalb der Abteilung verarbeiteten Personaldaten nicht in das Instituts-LAN gelangen dürfen.

Bei der Erfassung kritischer Kommunikationsverbindungen wird wie folgt vorgegangen: Zunächst werden sämtliche „Außenverbindungen“ als kritische Verbindungen identifiziert und erfasst. Anschließend werden sämtliche Verbindungen erfasst, die von einem IT-System mit hohem oder sehr hohem Schutzbedarf ausgehen. Dadurch werden solche Verbindungen identifiziert, über die hochschutzbedürftige Informationen übertragen werden. Anschließend werden die Verbindungen, über die die hochschutzbedürftigen Daten weiter übertragen werden, erfasst. Abschließend sind die Kommunikationsverbindungen zu identifizieren, über die derlei Informationen nicht übertragen werden dürfen.

Die dabei erfassten Daten können direkt im GSTOOL eingegeben werden. Bei einer nicht toolgestützten Vorgehensweise können diese Informationen tabellarisch dokumentiert oder graphisch im Netzplan hervorgehoben werden.

Die im beispielhaften IT-Verbund vorkommende Internet-Anbindung wird – als Außenverbindung – demnach im GSTOOL als kritische Verbindung erfasst.

Bei einer tabellarischen Erfassung der Informationen können kritische Kommunikationsverbindungen beispielsweise direkt im Netzplan gezielt hervorgehoben (andere Farbe, dickere Linien, etc.) werden. Zusätzlich bietet es sich an sowohl die Bezeichnung der Kommunikationsverbindung, als auch eine Begründung, wieso diese als kritisch eingestuft wird, zu dokumentieren.

Mit den übrigen Verbindungen wird identisch verfahren. Im exemplarischen Verbund aus Kapitel 3 sind keine weiteren Kommunikationsverbindungen als kritisch anzusehen.

Im nächsten Schritt wird der Schutzbedarf der vorhandenen IT-Räume bestimmt.

6.5 IT-Räume

Zu IT-Räumen zählen Räume, die ausschließlich dem IT-Betrieb dienen (wie Serverräume, Datenträgerarchive), oder solche, in denen unter anderem IT-Systeme betrieben werden (wie Büroräume). Wenn IT-Systeme statt in einem speziellen Technikraum in einem Schutzschrank untergebracht sind, ist dieser Schutzschrank wie ein Raum zu erfassen.

Um den Schutzbedarf eines IT-Rraumes festzustellen, müssen die im jeweiligen IT-Raum aufgestellten IT-Systeme betrachtet werden. Eine Übersicht, welche IT-Räume relevant sind, wurde bei der IT-Strukturanalyse erfasst.

Zur Bestimmung des Schutzbedarfs der IT-Räume werden die möglichen Schäden der relevanten IT-Systeme in ihrer Gesamtheit betrachtet. Im Wesentlichen wird aus dem möglichen Schaden bzw. der Summe der möglichen Schäden (unter Berücksichtigung des Kumulationseffekts) mit den schwerwiegendsten Auswirkungen der Schutzbedarf eines IT-Systems bestimmt (Maximum-Prinzip).

Das GSTOOL unterstützt hierbei die Vorgehensweise, indem es den Schutzbedarf des Raums aus den ihm zugeordneten IT-Systemen nach dem Maximum-Prinzip ableitet und vorschlägt. Auch hier ist der Vorschlag des GSTOOL zu überprüfen. Alternativ bietet sich eine tabellarisch Erfassung des Schutzbedarfs eines IT-Raumes an. In Abbildung 20 ist die Erfassung des Schutzbedarfs des *Büros MA* dargestellt. Der Schutzbedarf des Raums leitet sich hierbei direkt aus dem einzigen dort befindlichen IT-System ab.

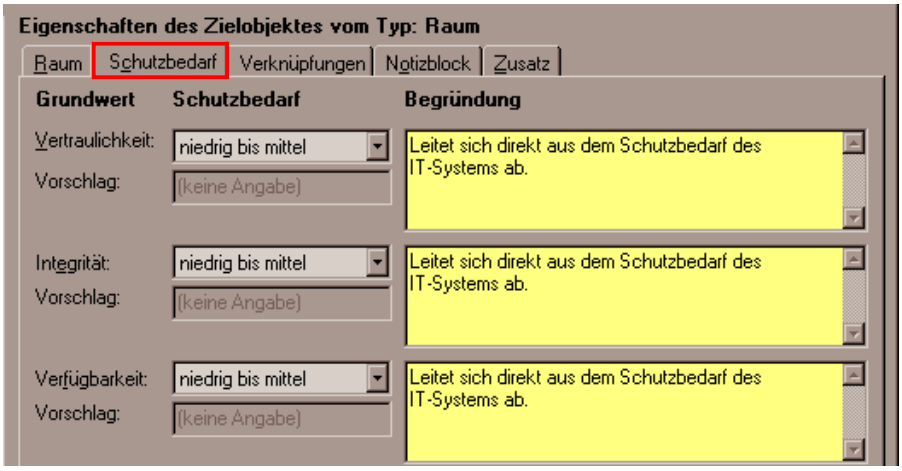


Abbildung 20: Schutzbedarfsfeststellung des Raumes *Büro MA*

Ein Serverraum ist üblicherweise ein Raum, in dem verschiedene IT-Systeme untergebracht sind und bei dem der Schutzbedarf verschiedener Systeme auf den Raum übertragen werden muss. Exemplarisch ist in Ab-

bildung 21 der erfasste Schutzbedarf für den *Raum Server/IT/TK* aus dem exemplarischen Verbund dargestellt.

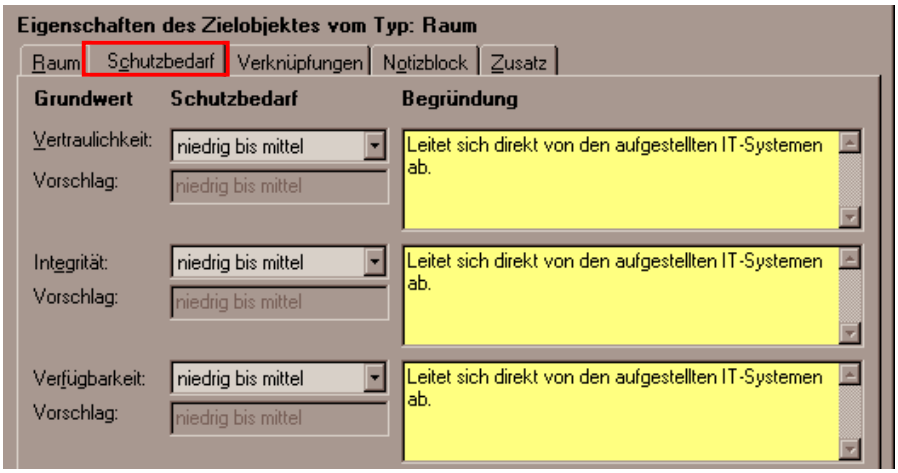


Abbildung 21: Schutzbedarfsfeststellung des Server/IT/TK Raums

Die Schutzbedarfsfeststellung der übrigen Räume erfolgt analog.

Die Schutzbedarfsfeststellung ist mit diesem Schritt abgeschlossen. Sie bietet einen Anhaltspunkt für die weitere Vorgehensweise der IT-Sicherheitskonzeption. Ausgehend von den Ergebnissen wird angenommen, dass

- bei einem „normalen“ Schutzbedarf die Standard-Sicherheitsmaßnahmen nach GSHB im Allgemeinen ausreichend und angemessen sind.
- bei einem „hohen“ Schutzbedarf die Standard-Sicherheitsmaßnahmen nach GSHB einen Basisschutz bilden, aber unter Umständen durch weitergehende Maßnahmen ergänzt werden müssen, um dem Schutzbedarf gerecht zu werden.

- bei einem „sehr hohen“ Schutzbedarf die Standard-Sicherheitsmaßnahmen nach GSHB einen Basisschutz bilden, in der Regel aber nicht allein ausreichen. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer ergänzenden Sicherheitsanalyse ermittelt werden.

Die ergänzende Sicherheitsanalyse wird im folgenden Kapitel genauer erläutert.

6.6 Exkurs: ergänzende Sicherheitsanalyse

In der Regel bieten die im GSHB aufgeführten Standardsicherheitsmaßnahmen einen angemessenen und ausreichenden Schutz.

Die Schutzbedarfsfeststellung kann jedoch ergeben, dass z. B. eine IT-Komponente einen hohen oder sehr hohen Schutzbedarf besitzt. In diesem Fall muss eine höherwertige IT-Sicherheitsmaßnahme ergriffen werden. Welche Maßnahme sich als geeignet erweist, wird nach der Durchführung des Basis-Sicherheitschecks (vgl. Kapitel 8) mittels einer ergänzenden Sicherheitsanalyse bestimmt. Der Aufwand zur Durchführung der ergänzenden Sicherheitsanalyse wird dadurch minimiert, dass man sich auf die sicherheitskritischen Bereiche konzentriert und nicht den gesamten IT-Verbund analysiert. Zu diesem Zweck werden aus den Ergebnissen der Schutzbedarfsfeststellung diejenigen Bereiche extrahiert, die einen hohen oder sehr hohen Schutzbedarf besitzen oder als sicherheitskritisch eingestuft wurden. Hierzu können gemäß GSHB gehören:

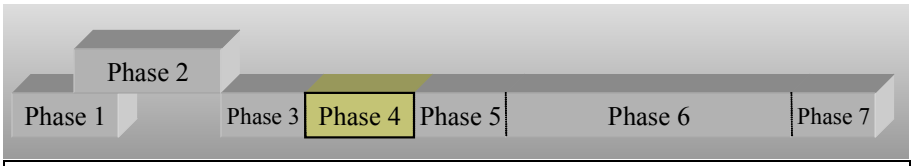
- IT-Systeme mit höherem Schutzbedarf,
- Kommunikationsverbindungen nach außen,
- Kommunikationsverbindungen mit hochschutzbedürftigen Daten,
- Kommunikationsverbindungen, die bestimmte Daten nicht transportieren dürfen und

- IT-Räume mit hohem Schutzbedarf.

Die Vorgehensweise ist im BSI Dokument „Risikoanalyse auf der Basis von IT-Grundschutz“ [GSRISK] ausführlich beschrieben.

Im nächste Schritt der Umsetzung des GSHB wird der IT-Verbund mit den Bausteinen des GSHB modelliert.

7 Modellierung



Verantwortlich	IT-Sicherheitsverantwortlicher
Einzubeziehen	IT-Verantwortliche
Zeitlicher Aufwand	ca. ½ Monat

Der betrachtete IT-Verbund wird nun mit Hilfe der vorhandenen Bausteine des IT-Grundschutzhandbuchs nachgebildet (vgl. Kapitel 2.3 [GSHB]). Der IT-Sicherheitsverantwortliche führt die Modellierung durch. Zur Unterstützung kann er das GSTOOL verwenden. Als Ergebnis dieser Phase erhält man ein IT-Grundschutzmodell des IT-Verbunds, das aus verschiedenen, ggf. auch mehrfach verwendeten Bausteinen des GSHB besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des IT-Verbunds beinhaltet.

Bei der Modellierung des IT-Verbundes bietet es sich an, diese anhand der im GSHB vorgesehenen Gruppierung der IT-Sicherheitsaspekte in einzelne Themen (sog. Schichten) durchzuführen (siehe Abbildung 22).

Das für die Darstellung des nachfolgend beispielhaft modellierten IT-Verbundes verwendete GSTOOL besitzt unterschiedliche Darstellungsmöglichkeiten. Neben einer „Objektsicht“, welche jeder Komponente die ihr zugeordneten Bausteine des GSHB darstellt, gibt es im GSTOOL die „Schichtensicht“, welche die einzelnen Bausteine des GSHB den jeweiligen Schichten des GSHB zugeordnet darstellt. Für die nachfolgenden Abbildungen wurde die „Schichtensicht“ des GSTOOL gewählt.

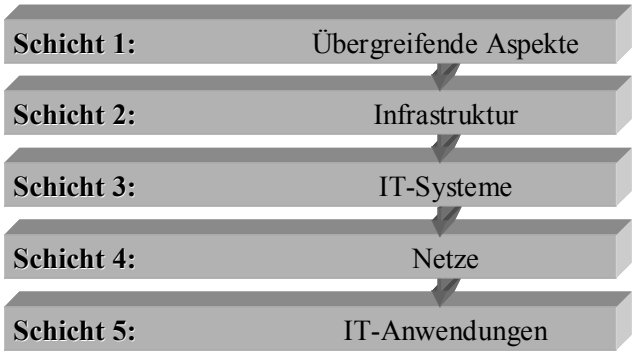


Abbildung 22: Schichtenmodell gemäß GSHB

Schicht 1 – zusammengefasst in [GSHB] (Kapitel 3) – umfasst die übergreifenden IT-Sicherheitsaspekte, die für sämtliche oder große Teile des IT-Verbunds gleichermaßen gelten. Dies betrifft insbesondere übergreifende Konzepte und die daraus abgeleiteten Regelungen. Bausteine der Schicht 1 sind unter anderem IT-Sicherheitsmanagement (Kapitel 3.0 [GSHB]), Organisation (Kapitel 3.1 [GSHB]), Datensicherungskonzept (Kapitel 3.4 [GSHB]) und Computer-Virenschutzkonzept (Kapitel 3.6 [GSHB]).

Schicht 2 – zusammengefasst in [GSHB] (Kapitel 4) – beinhaltet baulich-technischen Gegebenheiten, in der Aspekte der infrastrukturellen Sicherheit zusammengeführt werden. Hierunter fallen insbesondere die Bausteine Gebäude (Kapitel 4.1 [GSHB]), Räume (Kapitel 4.3 [GSHB]), Schutzschränke (Kapitel 4.4 [GSHB]) und häuslicher Arbeitsplatz (Kapitel 4.5 [GSHB]).

Schicht 3 betrifft die einzelnen IT-Systeme des IT-Verbunds, die ggf. in Gruppen zusammengefasst wurden. Hier werden die IT-Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Stand-alone-Systemen behandelt. In die Schicht 3 fallen damit beispielsweise die Bausteine Unix-System (Kapitel 5.2 [GSHB]), tragbarer PC (Kapitel 5.3 [GSHB]), Windows 2000 Server (Kapitel 6.9 [GSHB]) und TK-Anlage (Kapitel 8.1 [GSHB]).

Schicht 4 betrachtet die Vernetzungsaspekte der IT-Systeme, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine Heterogene Netze (Kapitel 6.7 [GSHB]), Netz- und Systemmanagement (Kapitel 6.8 [GSHB]) und Firewall (Kapitel 7.3 [GSHB]).

Schicht 5 schließlich beschäftigt sich mit den eigentlichen IT-Anwendungen, die im IT-Verbund genutzt werden. In dieser Schicht können unter anderem die Bausteine E-Mail (Kapitel 7.4 [GSHB]), WWW-Server (Kapitel 7.5 [GSHB]), Faxserver (Kapitel 8.5 [GSHB]) und Datenbanken (Kapitel 9.2 [GSHB]) zur Modellierung verwendet werden.

Die Modellierung nach GSHB besteht nun darin, für die Bausteine des GSHB zu entscheiden, ob und wie sie zur Abbildung des IT-Verbunds herangezogen werden können. Je nach betrachtetem Baustein können die während der IT-Strukturanalyse erfassten Objekte von unterschiedlicher Art sein: einzelne Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten, usw.

Das Modell - die Zuordnung von Bausteinen zu Zielobjekten - kann dabei entweder mit Hilfe des GSTOOL oder in Form einer Tabelle dokumentiert werden.

Wird die Modellierung anhand des GSTOOL durchgeführt, schlägt das GSTOOL eine Modellierung des IT-Verbundes auf der Basis der während der IT-Strukturanalyse (Phase 2) erhobenen Informationen vor. Die vom GSTOOL vorgeschlagene Modellierung muss jedoch in jedem Fall überprüft und bei Bedarf angepasst werden.

Im Falle, dass der IT-Sicherheitsbeauftragte sich auf den Modellierungsvorschlag des GSTOOL stützt, überprüft er die Zuordnung der vorgeschlagenen Bausteine mit den IT-Verantwortlichen und den IT-Anwendern auf ihre Anwendbarkeit. So muss z. B. die Modellierung des Firewall-Systems aus dem in Kapitel 3 dargestellten IT-Verbund manuell korrigiert werden (vgl. Kapitel 7.3).

Bei einer tabellarischen Dokumentation hält der IT-Sicherheitsbeauftragte

- *die Nummer und Titel des Bausteins*,
- *das Zielobjekt oder die Zielgruppe (Dies kann z. B. die Identifikationsnummer einer Komponente oder einer Gruppe bzw. der Name eines Gebäudes oder einer Organisationseinheit sein.)*,
- *ein Ansprechpartner* und
- *Notizen (z. B. als Begründung oder für weitere Informationen)*

fest. Er nimmt hierfür die Unterstützung von den jeweiligen IT-Verantwortlichen in Anspruch.

Die Anwendung der Bausteine erfolgt – wie beschrieben – anhand des Schichtenmodells. Im ersten Schritt werden die zu den „Übergeordneten Aspekten“ definierten Bausteine angewandt.

7.1 Übergeordnete Aspekte der IT-Sicherheit

Zunächst werden alle übergeordneten und nicht-technischen Aspekte des IT-Verbunds modelliert, die für den gesamten IT-Verbund einheitlich geregelt sein sollten. Dadurch müssen die Bausteine in den meisten Fällen nur einmal für den gesamten IT-Verbund angewendet werden. Die im GSHB als *Pflichtbausteine* bezeichneten Maßnahmen zum IT-Sicherheitsmanagement, zur Organisation des IT-Betriebs sowie zur Schulung und Sensibilisierung des Personals sollten immer angewendet werden.

Zu den übergreifenden Aspekten gehören die nachfolgenden Bausteine. Diese müssen einzeln auf Ihre Relevanz hin geprüft und ggf. auf den Verbund angewandt werden.

Als *Pflichtbausteine* sind die Bausteine *IT-Sicherheitsmanagement* (B3.00), *Organisation* (B3.01), *Personal* (B3.02), *Datensicherungskonzept* (B3.04), *Computer-Virenschutzkonzept* (B3.06), *Hard- und Software-Management*

(B3.09) sowie der Baustein *Standardsoftware* (B9.01) für den gesamten IT-Verbund einmal anzuwenden.

Der Baustein *Notfallvorsorge-Konzept* (B3.03) 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.

Der das *Kryptokonzept* (B3.07) betreffende Baustein ist zu gebrauchen, sobald 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 zur *Behandlung von Sicherheitsvorfällen* (B3.8) muss angewandt werden, 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 IT-Verbunds einen Schaden in den Kategorien hoch oder sehr hoch zur Folge hat.

Der *Outsourcing-Baustein* (B3.10) ist immer dann zu verwenden, wenn IT-Systeme, Anwendungen oder Geschäftsprozesse zu einem externen Dienstleister ausgelagert werden.

Der Baustein zur *Archivierung* (B9.5) ist auf den IT-Verbund anzuwenden, wenn aufgrund interner oder externer Vorgaben eine Langzeitarchivierung elektronischer Dokumente erforderlich ist oder bereits ein System zur Langzeitarchivierung elektronischer Dokumente betrieben wird.

Aus diesen allgemeinen Vorgaben ergibt sich für den in Kapitel 3 dargestellten und im GSTOOL modellierten IT-Verbund das in Abbildung 23 dargestellte konkrete Ergebnis.

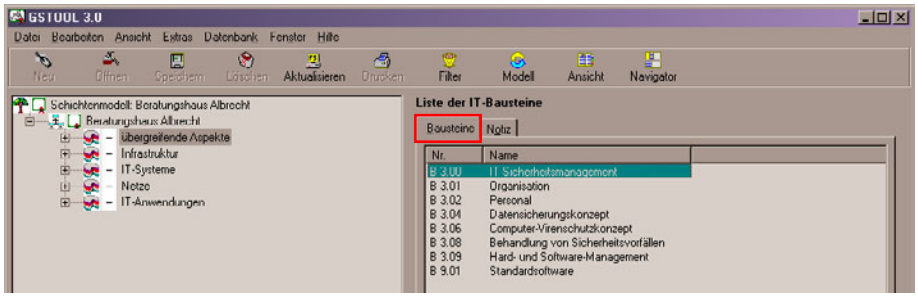


Abbildung 23: Übersicht über Bausteine der Schicht 1

Nicht verwendete Bausteine	
	Begründung
B3.03	Der Baustein zur Notfallvorsorge wurde nicht angewandt, da im IT-Verbund keine Komponente mit hoher Verfügbarkeit vorhanden ist.
B3.07	Der Baustein zum Kryptokonzept wurde nicht angewandt, da keine Komponenten vorhanden sind, die einen hohen Schutzbedarf an Vertraulichkeit oder Integrität besitzen.
B3.10	Dieser Baustein wurde nicht angewandt, da keine Geschäftsprozesse an Externe ausgelagert wurden (Outsourcing).
B9.05	Der Baustein wurde nicht angewandt, da keine Langzeitarchivierung erforderlich und kein derartiges System vorhanden ist.

Die nächste Schicht modelliert die Aspekte der Infrastruktur.

7.2 Infrastruktur

Die im jeweiligen IT-Verbund relevanten baulichen Gegebenheiten werden mit den Bausteinen aus Kapitel 4 [GSHB] modelliert. Auf jedes Gebäude, jeden Raum oder Schutzschrank (bzw. Gruppen dieser Komponenten) wird dabei der jeweils zugehörige Baustein aus dem GSHB angewendet.

Zu den infrastrukturellen Aspekten gehören die nachfolgenden Bausteine. Diese müssen einzeln auf Ihre Relevanz hin geprüft und ggf. auf den IT-Verbund angewandt werden.

Zu den Pflichtbausteinen gehören der Baustein *Gebäude* (B4.01), welcher für jedes Gebäude bzw. jede Gebäudegruppe einmal anzuwenden ist und der Baustein *Verkabelung* (B4.02), welcher in der Regelung einmal pro Gebäude (zusätzlich zum Baustein B4.01) verwendet werden muss. Die übrigen Bausteine (B4.31-B4.6) betreffen Räume innerhalb des Gebäudes und sind je nach Bedarf auf bei den zutreffenden Räume zu verwenden. Hierbei sind bestehende Abhängigkeiten zwischen den Bausteinen (z.B. zwischen B4.31 und B4.32) zu berücksichtigen.

Für jeden der Bausteine aus Schicht 2 ist aufgrund seines Anwendungsbereiches (siehe Kapitel 2.3 [GSHB]) zu entscheiden, ob dieser auf den IT-Verbund angewandt werden muss. Existiert beispielsweise ein separater Raum, in dem Datenträger aufbewahrt werden, muss der Baustein 4.33 angewandt werden. Die Bausteine der Infrastruktur-Schicht des in Kapitel 3 dargestellten IT-Verbunds sind in Abbildung 24 dargestellt.

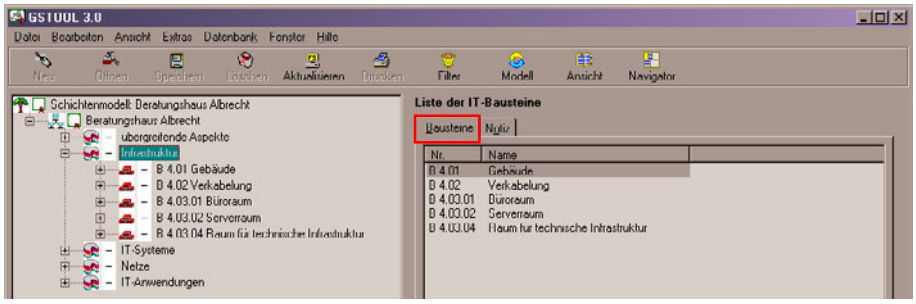


Abbildung 24: Übersicht über angewandte Bausteine der Schicht 2

Nicht verwendete Bausteine	
	Begründung
B4.4	Der Baustein ist nicht anwendbar, da innerhalb des IT-Verbundes keine Schutzschränke vorhanden sind.

B4.5	Der Baustein ist nicht anwendbar, da innerhalb des IT-Verbundes keine häuslichen Arbeitsplätze genutzt werden.
B4.6	Der Baustein behandelt ein Rechenzentrum, welches in diesem Verbund nicht existiert. Dieser Baustein ist somit nicht anwendbar.

Dem Raum Server/IT/TK (Abbildung 25, Darstellung anhand des Objektmodells) wurde hierbei zusätzlich der Baustein B4.34 (Raum für technische Infrastruktur) zugeordnet, da in ihm Verteilerkästen aufgestellt sind. Bei einer schriftlichen Erfassung müssen die entsprechenden Informationen in der Tabelle aufgenommen werden.

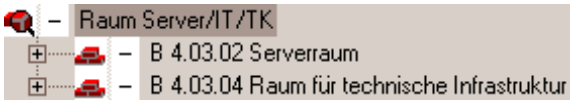


Abbildung 25: Modellierter Raum Server/IT/TK

Im nächsten Schritt werden die Aspekte der IT-Systeme (Schicht 3) betrachtet und modelliert.

7.3 IT-Systeme

Bei der Modellierung der IT-Systeme werden Sicherheitsaspekte z. B. für Server- und Client-Computer, Hosts, Terminals, etc. abgedeckt.

Zu den Bausteinen dieser Schicht gehören beispielsweise der Baustein *Servergestütztes Netz* (B6.01), welcher auf IT-Systeme anzuwenden ist, die als Server Dienste im Netz anbieten. Hierbei sind verschiedene Abhängigkeiten zu beachten. Z. B. ist Baustein B6.01 zusätzlich zu den Betriebssystemspezifischen Serverbausteinen (z. B. Baustein Windows 2000 Server B6.09) anzuwenden, da in ihm betriebssystemunabhängige Sicherheitsaspekte betrachtet werden.

Für jeden der Bausteine zu den IT-Systemen ist zu entscheiden, ob dieser auf den IT-Verbund angewandt werden muss. Die Bausteine der Schicht 3

des hier beispielhaft dargestellten IT-Verbunds sind in Abbildung 26 dargestellt.

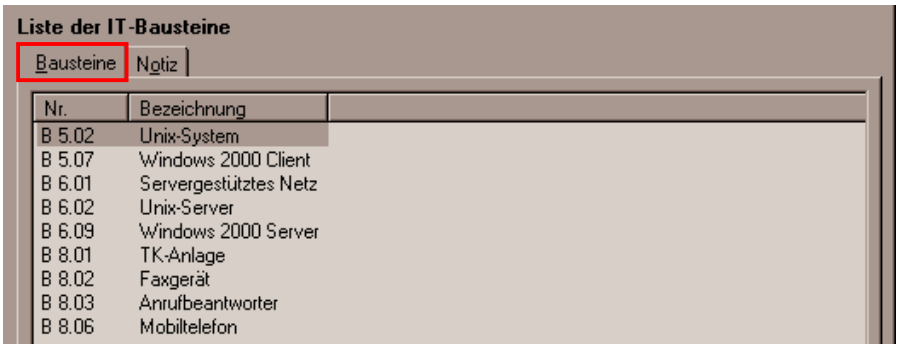


Abbildung 26: Übersicht über angewandte Bausteine der Schicht 3

Dem Server Firewall (Abbildung 27) wurden hierbei die Bausteine B5.02 und B7.03 (Baustein aus der Schicht 4 (IT-Netze)) zugeordnet, da dieser auf einem Unix-System basiert und die Funktionalität einer Firewall wahrnimmt. Das GSTOOL weist dem Server Firewall automatisch den Baustein B7.03 (Firewall) zu. Dies ist jedoch für den in Kapitel 3 dargestellten IT-Verbund nicht ausreichend, da der Firewall Server auf einem Unix-System basiert. Dem GSTOOL fehlt diese zusätzliche Information, so dass der Baustein B5.02 dem Firewall Server manuell zugewiesen werden muss.

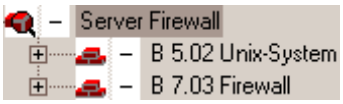


Abbildung 27: Modellierter Server Firewall

Nachfolgend werden die Aspekte der IT-Netze betrachtet und modelliert.

7.4 IT-Netze

Dieser Abschnitt behandelt die Sicherheitsaspekte der Kommunikationsnetze.

Bausteine dieser Schicht sind beispielsweise der Baustein *Heterogene Netze* (B6.07), welcher auf jedes Teilnetz einmal angewendet wird und somit als quasi-Pflichtbaustein angesehen werden kann. Der Baustein *LAN-Anbindung eines IT-Systems über ISDN* (B8.04) kann verwendet werden, wenn eine Internetanbindung per ISDN oder DSL realisiert ist.

Für jeden Baustein der Schicht 4 ist auch hier zu entscheiden, ob dieser auf den IT-Verbund angewandt werden muss. Die Bausteine der Schicht 4 des in Kapitel 3 dargestellten IT-Verbunds sind in Abbildung 28 dargestellt.

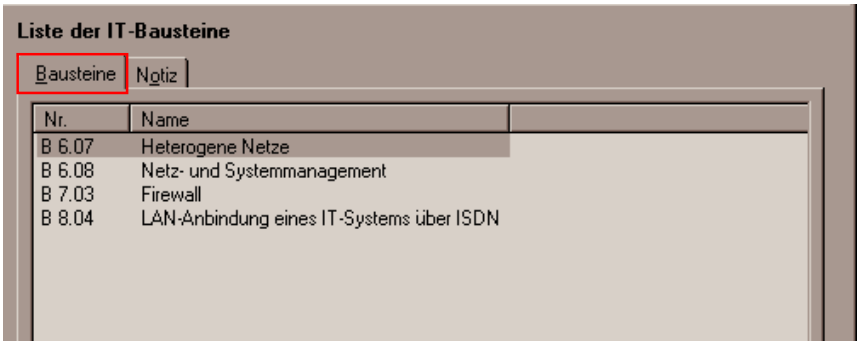


Abbildung 28: Übersicht über angewandte Bausteine der Schicht 4

Die mittels eines DSL-Anschluss realisierte Internetanbindung (Abbildung 29) wurde hierbei mit dem Baustein B8.04 (LAN-Anbindung eines IT-Systems über ISDN) modelliert, da derzeit noch kein Baustein für DSL vorhanden ist.

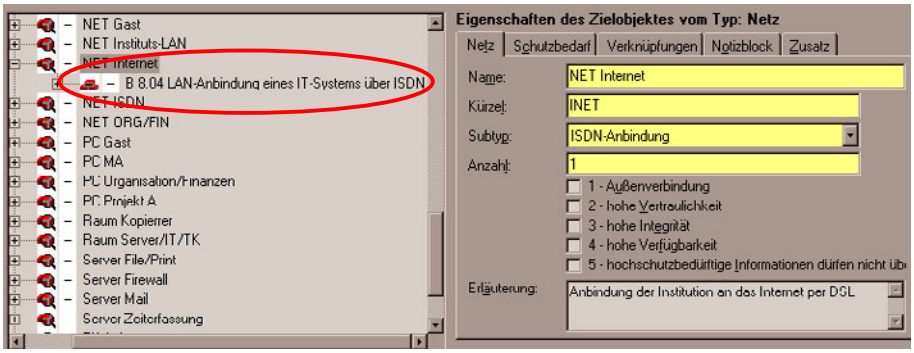


Abbildung 29: Mit ISDN-Baustein (anstelle DSL) modellierte Internetanbindung

Abschließend werden im nächsten Schritt die Aspekte der IT-Anwendungen betrachtet und modelliert.

7.5 IT-Anwendungen

Bei der abschließenden Modellierung der IT-Anwendungen des IT-Verbunds ist darauf zu achten, dass die Sicherheit der Anwendungen unabhängig von den IT-Systemen und Netzen betrachtet wird. Dies liegt darin begründet, dass z. B. viele IT-Anwendungen häufig als Client-Server-Applikationen realisiert sind und die Server selbst meist wieder auf nachgegeschaltete Systeme, wie beispielsweise Datenbanken, zugreifen.

Relevante Bausteine der Schicht 5 (IT-Anwendungen) sind insbesondere die Bausteine *Datenbanken* (B9.05), welcher pro Datenbanksystem oder Gruppe solcher angewendet wird und der Baustein *E-Mail* (B7.04), welcher auf jedes E-Mail System anzuwenden ist.

Für jeden der Bausteine der Schicht 5 ist zu entscheiden, ob dieser auf den IT-Verbund angewandt werden muss. Die Bausteine der Schicht 5 des in Kapitel 3 dargestellten IT-Verbunds sind in Abbildung 30 dargestellt.

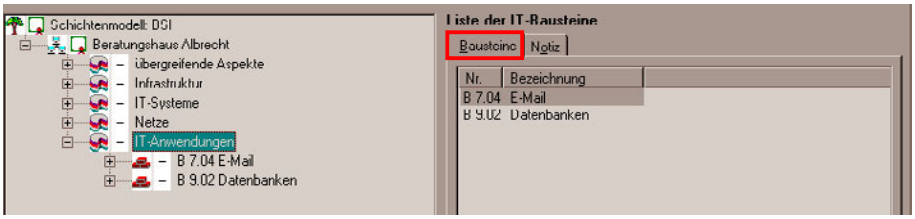


Abbildung 30: Übersicht über angewandte Bausteine der Schicht 4

Im exemplarischen IT-Verbund werden die Bausteine B7.04 (E-Mail) und B9.02 (Datenbanken) der Schicht 5 angewandt. Der Baustein B9.01 (Standardsoftware) wird in Schicht 1 angewandt und modelliert insbesondere die eingesetzte Office-Anwendung.

Der Baustein B9.02 (Datenbanken) wird für die Zeiterfassung angewendet, welche eine Datenbanklösung zur Speicherung der Informationen einsetzt. Auch wenn die genutzte Datenbank eng mit der Anwendung verknüpft ist und wenig Anpassungsmöglichkeiten zulässt – u.a. ist hierdurch meist die Gewährleistung des Herstellers gefährdet - macht die Berücksichtigung der im Baustein genannten Maßnahmen und Gefährdungen Sinn.

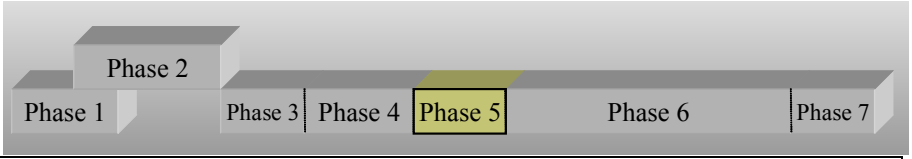
Abschließend bietet sich eine Überprüfung der Modellierung auf Vollständigkeit und Lücken an. Hierzu sollte erneut der Netzplan oder eine vergleichbare Übersicht über den IT-Verbund herangezogen und die einzelnen Komponenten systematisch durchgegangen werden. Jede Komponente sollte entweder einer Gruppe zugeordnet oder einzeln modelliert worden sein.

Wichtig ist, dass alle Hard- und Software-Komponenten in technischer Hinsicht nachgebildet und die zugehörigen organisatorischen, personellen und infrastrukturellen Aspekte vollständig abgedeckt sind.

Für den Fall, dass die Modellierung nicht vollständig durchführbar ist, weil entsprechende Bausteine im GSHB fehlen, müssen die Komponenten durch ähnliche Bausteine nachgebildet werden (vgl. z. B. die Vorgehensweise bei der Internetanbindung aus dem IT-Verbund des Kapitel 3 und dessen Modellierung in Kapitel 7.4).

Damit ist Phase 4, die Modellierung des IT-Verbunds, abgeschlossen. Nun wird überprüft, welche der durch das GSHB vorgegebenen Maßnahmen bereits umgesetzt sind und welche noch umgesetzt werden müssen (Basis-Sicherheitscheck).

8 Basissicherheitscheck



Verantwortlich	IT-Sicherheitsverantwortlicher
Einzubeziehen	IT-Verantwortliche
Zeitlicher Aufwand	ca. 1-2 Monat(e)

Der Basissicherheitscheck (vgl. Kapitel 2.5 [GSHB]) hat das Ziel festzustellen, welche der durch das GSHB vorgegebenen Standardsicherheitsmaßnahmen nicht oder nicht ausreichend umgesetzt sind. Die in der vorangegangenen Phase durchgeführte Modellierung wird dabei als Prüfplan für den Soll-Ist-Vergleich genutzt. Verantwortlich für diese Phase zeichnet sich erneut der IT-Sicherheitsbeauftragte, welcher gemeinsam mit den IT-Verantwortlichen entscheiden muss, ob die einzelnen Standardsicherheitsmaßnahmen entsprechend der Vorgaben aus dem GSHB umgesetzt sind.

Der Basissicherheitscheck besteht aus drei Schritten:

Schritt 1 Organisatorische Vorbereitungen

Im ersten Schritt werden insbesondere die relevanten Ansprechpartner für den Soll-Ist-Vergleich ausgewählt und vorhandene Dokumente gesichtet.

Schritt 2 Durchführung des Soll-Ist-Vergleichs

Durchführung des eigentlichen Soll-Ist-Vergleichs mittels Interviews und stichprobenartiger Kontrollen.

Schritt 3 Dokumentation der Ergebnisse

Die Ergebnisse des Soll-Ist-Vergleichs einschließlich der erhobenen Begründungen werden dokumentiert.

8.1 Organisatorische Vorbereitungen

Die organisatorischen Vorbereitungen haben das Ziel, die verantwortlichen Ansprechpartner für die einzelnen verwendeten Bausteine zu identifizieren. Zusätzlich dient eine Sichtung vorhandener Dokumente (z. B. vorhandene Systemdokumentation, System- und Sicherheitskonzepte, QM-Dokumentation etc.) der Vorbereitung des nachfolgenden Soll-Ist Vergleichs, da hiermit bereits umgesetzte Maßnahmen schon jetzt identifiziert werden können. Hierdurch wird der nachfolgende Aufwand reduziert.

Als erstes wird die hausinterne Dokumentation, die IT-sicherheitsrelevante Abläufe regelt, gesichtet. Diese Dokumente können bei der Ermittlung bereits umgesetzter Standardsicherheitsmaßnahmen – insbesondere bei Fragen nach bestehenden organisatorischen Regelungen – hilfreich sein. Zur Bestimmung der richtigen Ansprechpartner ist zu klären, wer für den Inhalt der Dokumente zuständig ist.

Auswahl der geeigneten Interviewpartner

Für die Auswahl der geeigneten Interviewpartner sollte zunächst für jeden in der Modellierung genutzten Bausteine ein Hauptansprechpartner festgelegt werden.

- Bei den Bausteinen der Schicht 1 „Übergeordnete Aspekte“ ergibt sich ein geeigneter Ansprechpartner in der Regel direkt aus der im Baustein behandelten Thematik. Beispielsweise sollte für den Baustein 3.2 „Personal“ ein Mitarbeiter der zuständigen Personalabteilung als Ansprechpartner ausgewählt werden.

- Im Bereich der Schicht 2 „Infrastruktur“ sollte die Auswahl geeigneter Ansprechpartner in Abstimmung mit der Hausverwaltung vorgenommen werden.
- In Bausteinen der Schicht 3 „IT-Systeme“, Schicht 4 „Netze“ und Schicht 5 „IT-Anwendungen“ werden in den zu prüfenden Sicherheitsmaßnahmen verstärkt technische Aspekte behandelt. In der Regel kommt daher der Administrator der entsprechenden Schicht als Ansprechpartner in Frage.

Bei der Anwendung des GSTOOL können die Ansprechpartner direkt im GSTOOL vorgehalten und dokumentiert werden (Abbildung 31). Bei tabellarischer Dokumentation ist zu jedem Baustein vorzuhalten, welche Ansprechpartner gewählt wurden.

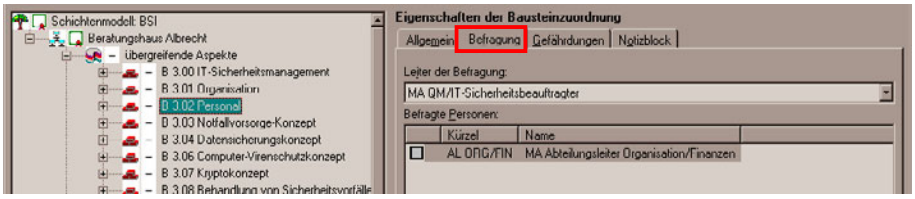


Abbildung 31: Definition der Ansprechpartner zu Baustein 3.2 (Personal)

Nachdem alle Ansprechpartner festgelegt und Interviewtermine koordiniert sind, werden im folgenden Schritt die umgesetzten Standardsicherheitsmaßnahmen identifiziert.

8.2 Durchführung des Soll-Ist-Vergleichs

Die Durchführung des Soll-Ist-Vergleichs findet auf der Basis von Interviews mit den festgelegten Ansprechpartnern statt. Mit dem entsprechenden Ansprechpartner wird für jeden Baustein ermittelt, ob die erforderlichen Standardsicherheitsmaßnahmen „entbehrlich“, „umgesetzt“, „teilweise umgesetzt“ oder „nicht umgesetzt“ sind.

Eine Maßnahme kann dabei als „entbehrlich“ angesehen werden, wenn die entsprechenden Gefährdungen mit anderen adäquaten Maßnahmen entgegengewirkt wird (z. B. durch Maßnahmen, die nicht im IT-Grundschutzhandbuch aufgeführt sind, aber dieselbe Wirkung erzielen oder durch höherwertige Maßnahmen des IT-Grundschutzhandbuchs), oder die Maßnahmenempfehlungen nicht relevant sind (z. B. weil Dienste nicht aktiviert wurden). Eine als „entbehrlich“ eingestufte Maßnahme bedarf in jedem Fall einer ausführlichen Begründung.

Die Maßnahme M 2.229 (Planung des Active Directory) ist beispielsweise im Baustein B6.09 (Windows 2000 Server) vorgesehen. Wird auf dem System jedoch kein Active Directory genutzt, kann die Maßnahme als entbehrlich eingestuft werden.

Vorbereitung der Interviews

Der Interviewer (also in der Regel der IT-Sicherheitsbeauftragte) sollte die einzelnen Maßnahmen inhaltlich kennen und verstehen. Dies macht es erforderlich, dass er sich bereits vor dem Interview mit den relevanten Maßnahmen auseinandersetzt, um so durch gezielte Fragen den Umsetzungsstand der einzelnen Maßnahmen beurteilen zu können.

Durchführung der Interviews

Bei den Interviews bietet es sich an, dem Ansprechpartner den Inhalt der Maßnahmenempfehlung zu erläutern. Zur Vorbereitung verschafft sich der Fragesteller ausreichende inhaltliche Kenntnis der Bausteine. Die Erfassung des Umsetzungsgrads der einzelnen Maßnahmen eines Bausteins erfolgt hierbei idealerweise während des Interviews anhand der Formulare aus [GSHILF] oder direkt im GSTOOL.

8.3 Dokumentation der Ergebnisse

Die Dokumentation der Ergebnisse erfolgt bereits während der Interviews entweder direkt im GSTOOL oder papierhaft und muss anschließend bereinigt werden. Hierzu werden die Ergebnisse des Interviews entweder durch die im GSTOOL vorhandenen oder anhand der ausgefüllten Formulare aus [GSHILF] geprüft und ggf. ergänzt. Es bietet sich an, die endgültige Fassung erneut mit dem jeweiligen Ansprechpartner abzustimmen, um Missverständnisse und Unkorrektheiten zu vermeiden und um die Ergebnisse zu konsolidieren.

Bei Standardsicherheitsmaßnahmen, die nicht umgesetzt sind, muss mit dem Ansprechpartner festgelegt werden, bis wann die entsprechende Maßnahme umsetzbar ist und welche Aufwände und ggf. Kosten anfallen. Als entbehrlich eingestufte Maßnahmen müssen begründet werden.

Ist eine dargestellte Maßnahme bereits umgesetzt, so werden Details zur Umsetzung direkt mit dokumentiert, so dass später nachvollzogen werden kann, womit die Umsetzung der Maßnahme begründet wurde.

Fall: Maßnahme ist umgesetzt

Wird das GSHB mittels GSTOOL umgesetzt, bietet es sich an, das Ergebnis der Befragung direkt im Anschluss in das GSTOOL zu übertragen. Abbildung 32 zeigt das Ergebnis einer Befragung an einer Maßnahmen aus der Schicht 1.

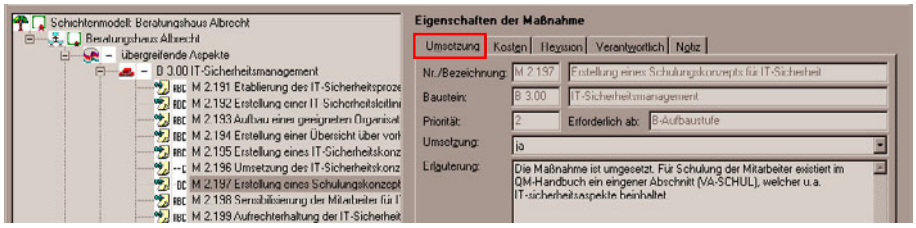


Abbildung 32: Dokumentation des Ergebnisses eines Interviews

Die dargestellte Maßnahme ist bereits umgesetzt (Umsetzung: *Ja*). Details zur Umsetzung werden direkt mit dokumentiert (Erläuterung: *Die Maßnahme ist umgesetzt. Für Schulung der Mitarbeiter existiert im QM-Handbuch ein eigener Abschnitt (VA-SCHUL), welcher u.a. IT-Sicherheitsaspekte beinhaltet*), so dass später nachvollzogen werden kann, womit die Umsetzung der Maßnahme begründet wurde.

Fall: Maßnahme ist entbehrlich

In Abbildung 33 ist eine mit dem GSTOOL als „entbehrlich" eingestufte Maßnahme dargestellt. Die Begründung („*Die Maßnahme wird als entbehrlich angesehen, da es innerhalb der Institution keinen Grund gibt, Arbeitsmittel nach Dienstende zu verschließen. Eine solche Vorgehensweise hätte teilweise behindernde Auswirkungen. Durch verschlossene Büroräume und unterschiedliche Schlüsselkreise wird sichergestellt, dass niemand an Daten gelangt, die für ihn nicht gedacht sind.*") ist hierbei direkt mit angegeben.

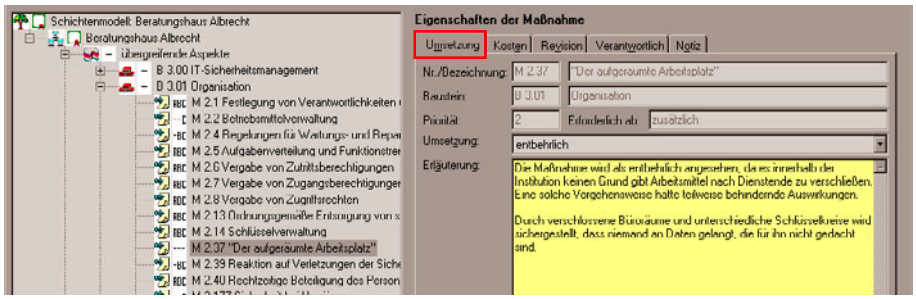


Abbildung 33: Dokumentation einer entbehrlichen Maßnahme

Die Maßnahme wird als entbehrlich angesehen und eine schlüssige Begründung angegeben. Die Angabe einer schlüssigen Begründung ist für eine spätere Auditierung/Zertifizierung zwingend erforderlich. Dem Auditor wird hierdurch die Möglichkeit gegeben, zu entscheiden, ob die Maßnahme tatsächlich entbehrlich ist.

Fall: Maßnahme ist nicht umgesetzt

Bei Maßnahmen die nicht oder nur teilweise umgesetzt sind und deren Umsetzung erforderlich ist, ist gemeinsam mit dem Ansprechpartner eine Kostenschätzung für die Umsetzung zu erstellen. Bei der Nutzung des GSTOOL kann diese Kostenschätzung direkt im GSTOOL vorgenommen werden (Abbildung 34).

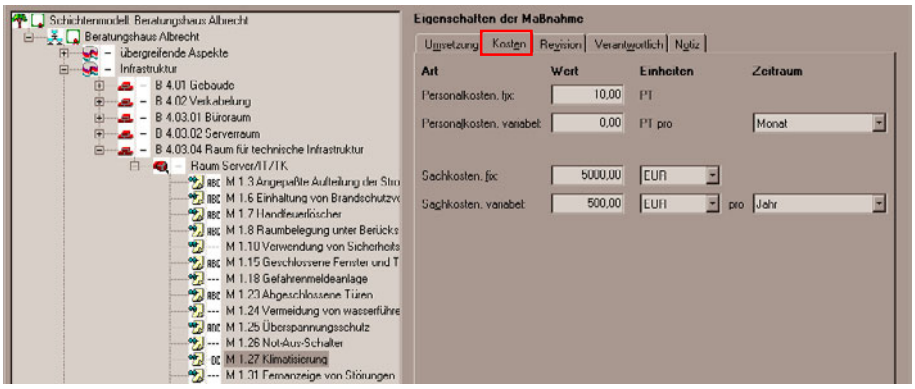


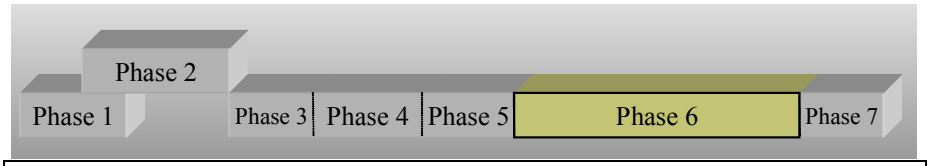
Abbildung 34: Dokumentation einer Kostenschätzung

Im Beispiel wird vom Ansprechpartner für den Serverraum dessen Klimatisierung als nicht ausreichend angegeben. Die internen Personalkosten für die Planung und Realisierung der Erweiterung werden mit 10 PT[1] abgeschätzt. Zusätzlich entstehen Sachkosten in Höhe von 5000 EUR und jährliche Wartungskosten von 500 EUR.

Nachdem für alle Bausteine der Umsetzungsgrad der Maßnahmen festgestellt wurde und eine grobe Schätzung der zu erwartenden Aufwände für die Umsetzung fehlender oder nicht ausreichend umgesetzter Maßnahmen erfolgte, wird in der nächsten Phase die Umsetzung dieser Maßnahmen geplant.

[1] Personentage

9 Realisierung



Verantwortlich	IT-Sicherheitsverantwortlicher
Einzubeziehen	Institutsleitung IT-Verantwortliche IT-Benutzer
Zeitlicher Aufwand	ca. 4-6 Monate

Nun liegen alle Informationen vor, um die Umsetzung der identifizierten fehlenden oder nur teilweise realisierten Standardsicherheitsmaßnahmen zu planen. Sind nur wenige fehlende Maßnahmen identifiziert und bindet deren Umsetzung wenig finanzielle oder personelle Ressourcen, kann oft ad hoc entschieden werden, wer diese Maßnahmen bis wann umzusetzen hat. Dies kann einfach und unkompliziert in den in Phase 6 erstellten Tabellen des Soll-Ist-Vergleichs oder im GSTOOL dokumentiert werden.

Bei vielen umzusetzenden Maßnahmen ist jedoch eine umfangreiche Planung erforderlich, welche die folgenden Schritte umfasst:

Schritt 1 Sichtung der Untersuchungsergebnisse

Aus den Ergebnissen des Basis-Sicherheitschecks werden alle nicht umgesetzten bzw. nur teilweise umgesetzten Maßnahmen einschließlich ihrer Prioritäten extrahiert und in einer Tabelle zusammengefasst.

Bei einer Vorgehensweise mit GSTOOL kann dieses Ergebnis als Bericht erzeugt werden.

Schritt 2 Konsolidierung der Maßnahmen

Die ausgewählten Maßnahmen müssen eventuell noch weiter konkretisiert bzw. an die organisatorischen und technischen Gegebenheiten der Institution angepasst werden. Die IT-Sicherheitsmaßnahmen sollten auf Eignung hin überprüft werden. Sie müssen vor den möglichen Gefährdungen wirksam schützen und in der Praxis umsetzbar sein, dürfen also z.B. nicht die Abläufe behindern oder andere Sicherheitsmaßnahmen schwächen.

Schritt 3 Kosten- und Aufwandsschätzung

Budget zur Umsetzung von IT-Sicherheitsmaßnahmen steht nicht in unbeschränktem Umfang zur Verfügung. Daher ist für jede zu realisierende Maßnahme festzuhalten, welche Investitionskosten und welcher Personalaufwand benötigt werden. Hierbei wird zwischen einmaligen und wiederkehrenden Investitionskosten bzw. Personalaufwänden unterschieden.

Es bietet sich an, die Kosten- und Aufwandschätzung gemeinsam mit den jeweiligen IT-Verantwortlichen zu erstellen, da diese über ausreichende Erfahrungen verfügen.

Schritt 4 Festlegung der Umsetzungsreihenfolge der Maßnahmen

Wenn Ressourcen (finanziell und personell) für die sofortige Umsetzung sämtlicher Maßnahmen fehlen, muss die Reihenfolge der Maßnahmenumsetzung festgelegt werden. Dabei sollten folgende Aspekte berücksichtigt werden:

- Die Priorität einer Maßnahme spiegelt wider, in welcher zeitlichen Reihenfolge die Maßnahme umzusetzen ist.
- Bei einigen Maßnahmen ergibt sich durch logische Zusammenhänge eine zwingende zeitliche Reihenfolge. So sind zwar die Maßnahmen M 2.25 Dokumentation der Systemkonfiguration und M 2.26 Ernennung eines Administrators und eines Vertreters beide

sehr wichtig, aber ohne Administrator kann M 2.25 kaum umgesetzt werden.

- Manche Maßnahmen erzielen eine große Breitenwirkung, manche jedoch nur eine eingeschränkte lokale Wirkung. Oft ist es sinnvoll, zuerst auf die Breitenwirkung zu achten.
- Es gibt Bausteine, die auf das angestrebte Sicherheitsniveau einen größeren Einfluss haben, als andere. Maßnahmen eines solchen Bausteins sollten bevorzugt behandelt werden, insbesondere wenn hierdurch Schwachstellen in hochschutzbedürftigen Bereichen beseitigt werden. So sollten immer zunächst die Server abgesichert werden (z. B. durch Umsetzung des Bausteins 6.2 Unix-Server) und dann erst die angeschlossenen Clients.
- Bausteine mit auffallend vielen fehlenden Maßnahmen repräsentieren Bereiche mit vielen Schwachstellen. Sie sollten ebenfalls bevorzugt behandelt werden.

Die Umsetzungsreihenfolge kann auch durch eine angestrebte Zertifizierung beeinflusst werden (vgl. Kapitel 10). Wird eine Zertifizierung angestrebt, bietet es sich an, zunächst diejenigen Maßnahmen umzusetzen, die für eine Selbsterklärung Einstiegsstufe erforderlich sind, anschließend werden die für eine Selbsterklärung Aufbaustufe erforderlichen Maßnahmen umgesetzt und abschließend die für das IT-Grundschutz-Zertifikat erforderlichen Maßnahmen.

Schritt 5 Festlegung der Verantwortlichkeit

Nach der Bestimmung der Reihenfolge für die Umsetzung der Maßnahmen wird festgelegt, wer bis wann welche Maßnahmen zu realisieren hat. Dabei ist darauf zu achten, dass der Verantwortliche ausreichende Fähigkeiten und Kompetenzen zur Umsetzung der Maßnahmen besitzt, dass ihm die erforderlichen Ressourcen zur Verfügung gestellt werden und er die Umsetzung der Maßnahme bzw. den Stand der Umsetzung an den IT-Sicherheitsverantwortlichen meldet.

Durch regelmäßige Status-Berichte kann der IT-Sicherheitsverantwortliche den Fortschritt der Umsetzung überwachen und ggf. zusätzliche Maßnahmen initiieren.

Schritt 6 Realisierungsbegleitende Maßnahmen

Parallel zur Umsetzung der einzelnen Maßnahmen bietet es sich an, die Betroffenen über die Umsetzung zu informieren. Hierzu eignen sich Sensibilisierungsmaßnahmen, die darauf zielen, betroffene Mitarbeiter

- für die Belange der IT-Sicherheit zu sensibilisieren,
- über die Notwendigkeit und die Konsequenzen der Maßnahmen zu unterrichten und
- zu schulen, so dass diese die neuen IT-Sicherheitsmaßnahmen korrekt um- und einsetzen.

Die Mitarbeiter sollten möglichst frühzeitig in die Planungen mit einbezogen werden: Sie sind es, die mit den neuen Maßnahmen „leben" müssen.

Der Institutsleiter der in Kapitel 3 dargestellten Institution setzt die Sicherheits-Leitlinie offiziell in Kraft und stellt sie anschließend den Mitarbeitern der Institution vor. Er erläutert den Mitarbeitern die Inhalte und Ziele und macht die Notwendigkeit der Umsetzung des GSHB deutlich.

Durch regelmäßige Informationsveranstaltungen werden die Mitarbeiter über den Fortgang der Umsetzung auf dem Laufenden gehalten.

Nach der Realisierung und Einführung der neuen IT-Sicherheitsmaßnahmen sollte durch den IT-Sicherheitsbeauftragten geprüft werden, ob die notwendige Akzeptanz der Mitarbeiter vorhanden ist. Stellt sich heraus, dass die neuen Maßnahmen nicht akzeptiert werden, ist ein Misserfolg vor-

programmiert. Die Ursachen sind herauszuarbeiten und ggf. ist eine zusätzliche Aufklärung der Betroffenen einzuleiten.

Die Umsetzung von Passwortregeln ist oft ein Problem, da die Mitarbeiter häufig einfache Passworte wählen. Durch einen Passwort-Cracker kann sehr schnell deutlich gemacht werden, dass gute Passworte für die Gesamtsicherheit wesentlich sind!

Aufrechterhaltung der Sicherheit

Die Aufrechterhaltung der Sicherheit ist ein ständiger Prozess (Abbildung 35) und nicht mit dem einmaligen Durchlaufen der Phasen 1-7 abgeschlossen. Mit der Umsetzung der Maßnahmen ist daher lediglich der erste Durchlauf des Prozesses beendet. Der IT-Sicherheitsbeauftragte muss den Prozess weiter aufrecht erhalten und ständig die ordnungsgemäße Umsetzung der Maßnahmen und Einhaltung der Richtlinien überwachen. Bei Veränderungen im IT-System sind die geänderten oder neu hinzugefügten Komponenten bzgl. der Einhaltung von IT-Sicherheitsmaßnahmen zu prüfen. Dieser Prozess wird vom IT-Sicherheitsbeauftragten initiiert.

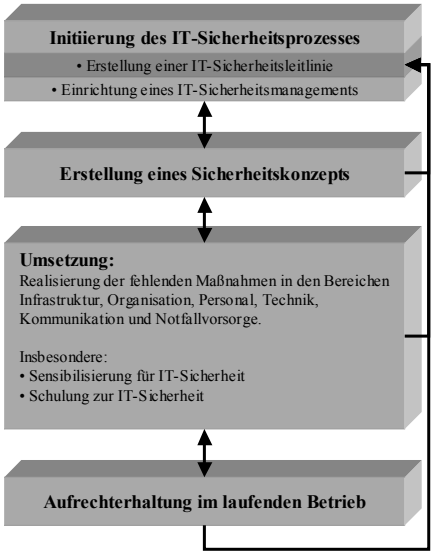
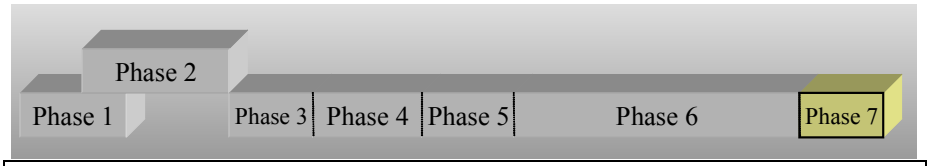


Abbildung 35: Darstellung des Sicherheitsprozesses

Weiterhin ist der IT-Sicherheitsbeauftragte für die Aktualisierung der einzelnen Dokumente und erhobenen Daten verantwortlich. Hierzu bietet es sich z. B. an, turnusmäßig mit den in Phase 4 identifizierten Ansprechpart-

nern die jeweils relevanten Dokumente auf Vollständigkeit und Aktualität hin zu prüfen.

10 Zertifizierung



Verantwortlich	IT-Sicherheitsverantwortlicher
Einzubeziehen	Auditor
	Institutsleitung
	IT-Verantwortliche
	IT-Benutzer
Zeitlicher Aufwand	ca. ½ Monat

Die Umsetzung der im IT-Grundschutzhandbuch GSHB beschriebenen Standardsicherheitsmaßnahmen kann mittels eines vom BSI ausgegebenen IT-Grundschutz Zertifikats nach außen transparent gemacht werden (vgl. [GSZERT]). Aufgrund der ständigen Aktualisierung und Erweiterung des IT-Grundschutzhandbuchs bleiben die aufgeführten Standardsicherheitsmaßnahmen praktisch auf der Höhe der Zeit.

Ausprägungen der IT-Grundschutz-Qualifizierung

Derzeit hat das BSI drei verschiedene Ausprägungen der IT-Grundschutz-Qualifizierung definiert. Diese drei Ausprägungen erlauben es einer Institution schrittweise ein IT-Grundschutz-Zertifikat – dieses stellt den höchsten Grad an Vertrauenswürdigkeit und das höchste Sicherheitsniveau dar – zu erreichen. Die Gültigkeit einer Qualifizierung und die Möglichkeit einer Verlängerung ist von der jeweiligen Stufe abhängig.

Stufe 1: Selbsterklärung „IT-Grundschutz Einstiegsstufe“

Gültigkeit:	2 Jahre
Verlängerbar:	Nicht für denselben IT-Verbund

Die IT-Grundschutz-Qualifizierung in der Einstiegsstufe wird erreicht, wenn die Institution lediglich die unabdingbaren Standard-Sicherheitsmaßnahmen des IT-Grundschutzhandbuchs umgesetzt hat und einen Audit-Report, der die Prüfergebnisse dokumentiert, nach dem BSI-Zertifizierungsschema erstellt hat. Bei Bedarf kann das BSI Einsicht in den Audit-Report der Institution nehmen. Das durch die Selbsterklärung „IT-Grundschutz Einstiegsstufe“ dargestellte Sicherheitsniveau ist das geringste der drei Ausprägungen.

Stufe 2: Selbsterklärung „IT-Grundschutz Aufbaustufe“

Gültigkeit:	2 Jahre
Verlängerbar:	Nicht für denselben IT-Verbund

Voraussetzung für die Selbsterklärung „IT-Grundschutz Aufbaustufe“ ist, dass die Institution die wichtigsten Standard-Sicherheitsmaßnahmen des IT-Grundschutzhandbuchs umgesetzt hat. Wie auch bei der Einstiegsstufe muss die Institution einen Audit-Report entsprechend dem BSI-Zertifizierungsschema erstellen. Das BSI kann Einsicht in den Audit-Report nehmen.

Die notwendigen Vorarbeiten und Erhebungen der Stufen 1 und 2 können dabei sowohl von Dritten als auch von Mitarbeitern der eigenen Institution erfolgen. Die Selbsterklärung wird darauf basierend von einem zeichnungsbefugten Vertreter der Institution abgegeben.

Stufe 3: IT-Grundschutz-Zertifikat

Gültigkeit:	2 Jahre
Verlängerbar:	Ja

Innerhalb der drei Ausprägungen der IT-Grundschutz-Qualifizierung stellt das IT-Grundschutz-Zertifikat den höchsten Grad an Vertrauenswürdigkeit und das höchste Sicherheitsniveau dar. Das Zertifikat wird durch Zertifizie-

rungsstellen vergeben, die für die Vergabe des IT-Grundschutz-Zertifikats akkreditiert sind. Voraussetzung ist, dass die Umsetzung der im IT-Grundschutzhandbuch beschriebenen und im vorliegenden Fall relevanten Standard-Sicherheitsmaßnahmen durch einen lizenzierten Auditor bestätigt ist.

Entscheidend bei der Interpretation der drei Ausprägungen der IT-Grundschutz-Qualifizierung ist, dass die Einstiegs- und die Aufbaustufe zwar ein definiertes niedriges, jedoch noch kein ausreichendes Sicherheitsniveau gemäß IT-Grundschutzhandbuch festlegen. Sie dienen als Meilensteine bis zur Erreichung des IT-Grundschutz-Zertifikats. Nur das IT-Grundschutz-Zertifikat attestiert die Realisierung eines „umfassenden IT-Grundschutzes".

Die erreichte Qualifizierungsstufe ist mit davon abhängig, wie vollständig die Standarsicherheitsmaßnahmen umgesetzt sind. Die im GSHB genannten Standardsicherheitsmaßnahmen werden für die drei Ausprägungen wie folgt gekennzeichnet:

- »A« Die Umsetzung dieser Maßnahme ist für alle Stufen der IT-Grundschutz-Qualifizierung erforderlich (unabdingbare Maßnahme).
- »B« Die Umsetzung dieser Maßnahme ist für die Aufbaustufe und für das Zertifikat erforderlich.
- »C« Die Umsetzung dieser Maßnahme ist nur für das IT-Grundschutz-Zertifikat erforderlich.
- »Z« Die Umsetzung dieser zusätzlichen IT-Sicherheitsmaßnahmen sollte zur Steigerung der IT-Sicherheit erfolgen, ist jedoch zur Qualifizierung nach IT-Grundschutz nicht erforderlich.

Die im GSHB genannten Prioritäten (1-3) sind hierbei nicht mit der o.g. Einstufung zu verwechseln. Die Prioritäten geben der Institution lediglich

einen Hinweis auf die Umsetzungsreihenfolge der umzusetzenden Standardsicherheitsmaßnahmen.

Die Maßnahme M2.191 (Etablierung des IT-Sicherheitsprozesses) und M2.198 (Sensibilisierung der Mitarbeiter für IT-Sicherheit) sind beide bereits für die Einstiegsstufe erforderlich. Aufgrund der unterschiedlich definierten Prioritäten der beiden Maßnahmen ergibt sich, dass zunächst M2.191 und anschließend M2.198 umgesetzt werden sollte.

Das GSTOOL unterstützt die Institution dabei zu ermitteln, welche Stufe der Qualifizierung erreicht ist, indem zu jeder Maßnahme (siehe Abbildung 36) angegeben wird, in welcher Qualifizierungsstufe eine Umsetzung erforderlich ist.

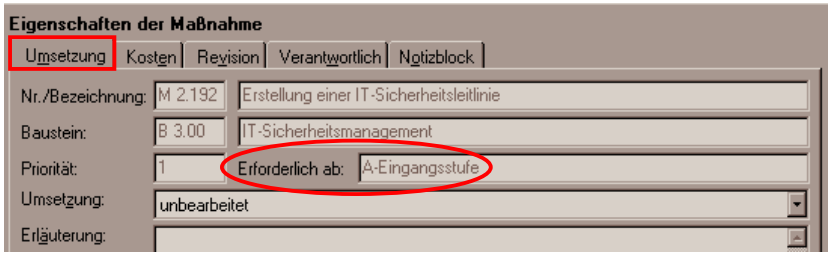


Abbildung 36: Eigenschaften einer Maßnahme

Die Informationen werden für jede Schicht zusammengefasst, so dass in den einzelnen Schichten ersichtlich wird, wo Defizite bestehen und welche Qualifizierungsstufe mit den umgesetzten Maßnahmen erreicht werden kann. In Abbildung 37 ist exemplarisch die Schicht „übergreifende Aspekte“ dargestellt und es wird angezeigt (durch C✓), dass mit den umgesetzten Maßnahmen in dieser Schicht die Anforderungen an die Stufe 3 erfüllt wurden.

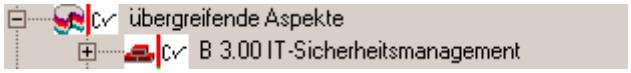


Abbildung 37: Erreichte Siegelstufe innerhalb des Bausteins B 3.00

Zertifizierung

Als Vorarbeit für eine Zertifizierung werden durch die Institution die Phasen 1-6 (wie in den Kapiteln 4 bis 9 erläutert) durchlaufen und die relevanten Dokumente erstellt. Anschließend werden durch einen von der Institution zu beauftragenden und durch das BSI lizenzierten IT-Grundschutz-Auditor die folgenden Punkte geprüft:

1. **Plausibilitätsprüfung**

   Der Auditor prüft, ob der IT-Verbund eine sinnvolle Mindestgröße aufweist, sowie die Plausibilität der IT-Strukturanalyse. Weiterhin prüft der Auditor die durchgeführte Modellierung auf Korrektheit sowie die Vollständigkeit und Plausibilität des Basis-Sicherheitschecks.

2. **Realisierungsprüfung**

   In diesem Punkt überprüft der Auditor stichprobenartig den im Basis-Sicherheitscheck ermittelten Umsetzungsstatus. Hierzu überprüft der Auditor, ob die Maßnahmen aus den Bausteinen „IT-Sicherheitsmanagement“ sowie die aus jeweils einem Baustein der fünf Schichten und aus vier weiteren Bausteinen umgesetzt sind.

Anschließend erstellt der Auditor einen Audit-Bericht für die Vorlage beim BSI. Das BSI erteilt der Institution ein Zertifikat, sofern ein positives Untersuchungsergebnis vorliegt.

11 Beispiel Sicherheits-Leitlinie

Die nachfolgend aufgeführte Sicherheits-Leitlinie ist aus [MURI] abgeleitet und auf eine mittlere Institution (orientiert am in Kapitel 3 dargestellten IT-Verbund) angepasst. Die *[kursiv]* dargestellten Textpassagen müssen den individuellen Gegebenheiten angepasst werden.

IT-Sicherheits-Leitlinie

Die *[Institutsleitung]* verabschiedet hiermit folgende IT-Sicherheits-Leitlinie als Bestandteil ihrer Strategie:

Stellenwert der Informationsverarbeitung

Informationsverarbeitung unterstützt unsere Aufgabenerfüllung und spielt eine *[wesentliche]* Rolle. Alle wesentlichen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt *[kurzfristig]* kompensiert werden können. Insbesondere im Bereich der *[Produktion]* darf unser Geschäft nicht zusammenbrechen. Da unsere Kernkompetenz in der *[Beratung unserer Kunden]* liegt, Ver- und Bearbeiten wir vielfach sensible Daten unserer Kunden. Der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung ist von *[existenzieller]* Bedeutung.

Übergreifende Ziele

Unsere Daten sowie die Daten unserer Kunden und unsere IT-Systeme in allen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten *[toleriert]* werden können und keine wesentlichen Auswirkungen auf den Geschäftsbetrieb haben. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind *[nur in geringem Umfang]* und *[nur in Ausnahmefällen]* akzeptabel, die Gewährleistung der Integrität ist ein *[wichtiges]* Ziel. Die Anforderungen an Vertraulichkeit haben ein *[normales]*, an Gesetzeskonformität orientiertes Niveau.

IT-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit *[existenzbedrohenden]* finanziellen Auswirkungen (d.h. Auswirkungen von über *[10%]* des monatlichen Umsatzes) müssen verhindert werden.

Alle Mitarbeiter des Unternehmens halten die einschlägigen Gesetze (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen sowie internen Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter und die Institutsleitung sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die IT-Sicherheitsstrategie nach besten Kräften.

Detailziele

Die Datenschutzgesetze und die Interessen unserer Mitarbeiter verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. Die Daten und die IT-Anwendungen der Personalabteilung werden daher einem *[normalen]* Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Kunden und Geschäftspartner.

Die Geschäftsabwicklung darf nicht verzögert oder gar gefährdet werden. Wenn vertraglich festgelegte Lieferfristen nicht eingehalten werden können, kann dies weitreichende negative Folgen haben. Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu *[Erlösminderungen]* führen und *[Vertragsstrafen]* nach sich ziehen.

Innerhalb der Produktionsabteilung wird die Verfügbarkeit und die Fehlerfreiheit der Systeme sichergestellt. Ausfallzeiten von IT-Systemen innerhalb der Produktion sind nur in einem *[geringen]* Maße akzeptabel, da diese direkt, aber auch indirekt – durch negative Auswirkungen auf nachfol-

gende Prozesse – zu *[Erlösminderungen]* und *[Vertragsstrafen]* führen können.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns *[selbstverständlich]* und für die Kommunikation mit Kunden und Geschäftspartnern *[wesentlich]*. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

IT-Sicherheitsmanagement

Zur Erreichung der IT-Sicherheitsziele wurde ein IT-Sicherheitsbeauftragter benannt. Der IT-Sicherheitsbeauftragte ist für die Erstellung und Fortschreibung des Sicherheitskonzepts sowie die Aufrechterhaltung des Sicherheitsniveaus verantwortlich. Er berichtet in seiner Funktion direkt an den *[Institutsleiter]*.

Dem IT-Sicherheitsbeauftragten werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen für die Ausübung seiner Tätigkeit zur Verfügung gestellt. Er ist durch die IT-Verantwortlichen und IT-Benutzer ausreichend zu unterstützen und frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Gleiches gilt, sofern personenbezogene Daten betroffen sind.

Die IT-Verantwortlichen und IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des IT-Sicherheitsbeauftragten zu halten.

Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein angemessenes Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten den IT-Sicherheitsbeauftragten.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine Datensicherung wird daher gewährleistet, dass kurzfristig verlorene oder fehlerhafte Teile des operativen Datenbestandes wiederhergestellt werden können. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

IT-Benutzer nehmen mindestens jährlich an einer internen Sicherheitsunterweisung durch den IT-Sicherheitsbeauftragten teil.

Verbesserung der Sicherheit

Das IT-Sicherheitskonzept wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft.

Die Institutsleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an den IT-Sicherheitsbeauftragten weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt.

Abweichungen werden mit dem Ziel analysiert, die IT-Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

Datum / Unterschrift

Anhang A Systeme des beispielhaften IT-Verbundes

In der nachfolgenden Tabelle sind zunächst die Serversysteme und anschließend die Arbeitsplatzsysteme des beispielhaften IT-Verbunds aus Kapitel 3 aufgeführt. Die in den Klammern angegebenen Bezeichnungen sind hierbei interne Inventarnummern:

IT-System	Beschreibung
Firewall (FIREWALL01)	Firewallsystem der Institution auf der Basis einer kommerziellen Linux Lösung sowie eines zusätzlichen Paketfilters (Paketfilter). Betriebssystem: speziell angepasstes Linux Anwendungen: speziell angepasstes Linux
Telefonanlage (TK01)	Telefonanlage der Institution. Die Anlage wird durch die Telefongesellschaft administriert. Betriebssystem: herstellerspezifisch Anwendungen: herstellerspezifisch
Switch (SWITCH01)	Interner Switch zur Verkabelung des Netzwerkes. Betriebssystem: herstellerspezifisch Anwendungen: herstellerspezifisch
FW-Intern (FW-INT)	Interne Firewallkomponente, die die Abteilung Organisation/Finanzen vom übrigen Hausnetzt abkoppelt. Betriebssystem: herstellerspezifisch Anwendungen: herstellerspezifisch

IT-System	Beschreibung
Server Zeiterfassung (SRV-ZE01)	Server, auf dem die integrierte Anwendung zur Personal- und Zeiterfassung installiert ist. Betriebssystem: Linux Anwendungen: ZEITERFASS V2.0
Server File/Print (SRV-FILE01)	File-/Printserver der Institution. Betriebssystem: Windows 2000 Server Anwendungen: Windows Standard
Server Mail (SRV-MAIL01)	Mailserver und Groupware-Server der Institution. Die Groupware-Lösung wird als zentrale Adress- und Termindatenbank eingesetzt. Betriebssystem: Linux Anwendungen: Linux Groupware Solution
PC Institutsleiter (PC001)	Arbeitsplatz-PC (Laptop) des Institutsleiters. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung
PC Sek (PC002,PC502)	Arbeitsplatz-PC der Sekretärinnen. Diese PCs sind identisch konfiguriert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung

IT-System	Beschreibung
PC QM / Sicherheit (PC101)	Arbeitsplatz-PC des QM und Sicherheitsbeauftragten. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, GSTOOL, QM-Tool
PC AL[2] Org./Finanz (PC201)	Arbeitsplatz-PC des Abteilungsleiters der Abteilung Organisation/Finanzen. Zusätzlich zu den Standardanwendungen ist auf diesem PC eine Rechnungswesensoftware installiert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Rechnungswesen-Software
PC MA Rechnungswesen (PC21x)	Arbeitsplatz-PC der Mitarbeiter des Teams Rechnungswesen. Zusätzlich zu den Standardanwendungen ist auf diesem PC eine Rechnungswesensoftware installiert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Rechnungswesen-Software, Arbeitszeitauswertung
PC MA Organisation (PC221)	Arbeitsplatz-PC der Mitarbeiter des Teams Organisation. Zusätzlich zu den Standardanwendungen ist auf diesem PC eine Software zur Arbeitszeitauswertung installiert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Arbeitszeitauswertung, Rechnungswesen-Software

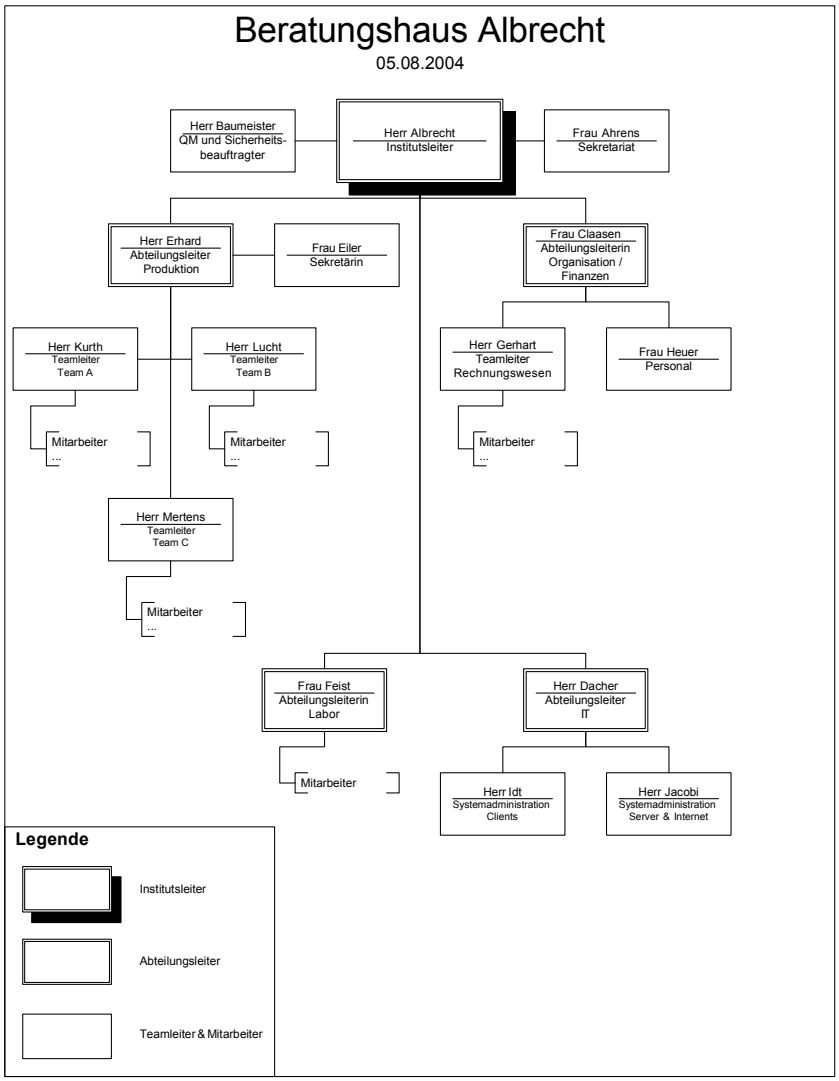
[2] AL = Abteilungsleiter

IT -System	Beschreibung
PC AL IT (PC301)	Arbeitsplatz-PC des Abteilungsleiters der Abteilung IT. Zusätzlich zu den Standardanwendungen ist auf diesem PC eine Software zum Systemmanagement installiert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Systemmanagement
PC MA IT (PC311,PC312)	Arbeitsplatz-PC der Mitarbeiter der Abteilung IT. Die Systeme unterscheiden sich von den üblichen Standard-PC, das Betriebssystem ist Linux und neben einer Office Lösung ist eine Software zum Systemmanagement installiert. Betriebssystem: Linux Anwendungen: Office-Lösung, Systemmanagement
PC AL Produktion (PC401)	Arbeitsplatz-PC (Laptop) des Abteilungsleiters der Abteilung IT. Zusätzlich zu den Standardanwendungen ist auf diesem PC eine Software zum Projektmanagement installiert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Projektmanagement
PC MA Produktion (PC41x, PC42x, PC43x)	Arbeitsplatz-PC der Teamleiter und Mitarbeiter der Abteilung Produktion. Zusätzlich zu den Standardanwendungen ist auf diesen PCs eine Projektmanagement- Software installiert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Projektmanagement

IT-System	Beschreibung
PC AL Labor (PC501)	Arbeitsplatz-PC des Abteilungsleiters der Abteilung Labor. Zusätzlich zu den Standardanwendungen ist auf diesem PC eine Software zur Softwareentwicklung installiert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Softwareentwicklung
PC MA Labor (PC51x)	Arbeitsplatz-PC der Mitarbeiter der Abteilung Produktion. Zusätzlich zu den Standardanwendungen ist auf diesen PCs eine Software zur Softwareentwicklung installiert. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Softwareentwicklung
PC Gast (PC999)	Arbeitsplatz-PC, der auch von Gästen genutzt werden kann. An dem PC ist ein Scanner angeschlossen. Betriebssystem: Windows 2000 Anwendungen: Office-Lösung, Scanner-Software

Tabelle 2: Übersicht über IT-Systeme

Anhang B Organigramm



Anhang C Glossar

BSI	Bundesamt für Sicherheit in der Informationstechnik
GF	Geschäftsführer / Institutsleiter
AL	Abteilungsleiter
MA	Mitarbeiter
QMH	Qualitäts-Management-Handbuch
QM-Beauftragter	Qualitäts- Management-Beauftragter
GSHB	IT-Grundschutzhandbuch
Maximum-Prinzip	Der Schaden mit den schwerwiegendsten Auswirkungen bestimmt den Schutzbedarf einer IT-Komponente.
Gruppenbildung	Ähnliche Komponenten des IT-Verbundes werden zu einer Gruppe zusammengefasst. *Beispiel:* Mitarbeiter derselben Abteilung, die ein ähnliches Tätigkeitsfeld haben, mit identischen Anwendungen und vergleichbaren PCs arbeiten lassen sich zu einer Gruppe zusammenfassen. Ebenso lassen sich deren PCs zu einer Gruppe zusammenfassen.

Pflichtbausteine	Bausteine des GSHB, die unabhängig vom betrachteten Verbund immer anzuwenden sind (z.B. IT-Sicherheitsmanagement aus Schicht 1).
Sicherheitsprozess	Organisatorischer Prozess, der die Umsetzung und Kontrolle von IT-Sicherheitsmaßnahmen zum Ziel hat.
IT-Sicherheitskonzeption	Prozess, der die Erstellung des IT-Sicherheitskonzepts zum Ziel hat. Er besteht aus den Schritten: IT-Strukturanalyse, Schutzbedarfsfeststellung, IT-Grundschutzanalyse und Realisierungsplanung.
Grundwerte der IT-Sicherheit	Vertraulichkeit, Verfügbarkeit und Integrität

Netzplan	Ein Netzplan ist eine graphische Übersicht über die eingesetzten Komponenten und deren Vernetzung. Üblicherweise unterscheidet man drei Arten von Netzplänen: **Roher Netzplan:** Welcher auf der Basis vorhandener Dokumentationen (z.B. Topologiepläne) erstellt wird. **Aktualisierter Netzplan:** Der rohe Netzplan spiegelt in der Regel nicht die aktuelle Situation wieder, da zwischenzeitlich Systeme neu hinzugekommen oder entfernt werden. Der aktualisierte Netzplan spiegelt die aktuelle Situation wieder. **Bereinigter Netzplan:** Hierbei handelt es sich um den aktualisierten Netzplan, dessen Komplexität durch Gruppenbildung reduziert wurde.
Vertraulichkeit	Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
Verfügbarkeit	Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Integrität	Die Daten sind vollständig und unverändert. Der Begriff „Information“ wird in der Informationstechnik für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass - diese unerlaubt verändert wurden oder - Angaben zum Autor verfälscht wurden oder - der Zeitpunkt der Erstellung manipuliert wurde.

Anhang D Referenzen

[GSHB] IT-Grundschutzhandbuch, http://www.bsi.de/gshb/deutsch/menue.htm

[GSHILF] Hilfsmittel zum IT-Grundschutzhandbuch, http://www.bsi.de/gshb/deutsch/hilfmi/hilfmi.htm

[GSFORM] Formblätter für die IT-Grundschutzerhebung, http://www.bsi.de/gshb/deutsch/download/formgshb2003.zip

[GSTOOL] IT-Grundschutz-Tool, http://www.bsi.de/gstool/index.htm

[GSTHB] Das GSTOOL-Handbuch, http://www.bsi.de/gstool/handbuch.htm

[GSZERT] Allgemeine Informationen zum IT-Grundschutz-Zertifikat, http://www.bsi.de/gshb/zert

[GSRISK] Risikoanalyse auf der Basis von IT-Grundschutz, http://www.bsi.de/gshb/risikoanalyse

[LEITF] Leitfaden IT-Sicherheit, http://www.bsi.de/gshb/Leitfaden

[SCHUBE1] http://www.mittelstand-sicher-im-internet.de/content-details.php?53

[MURI] Musterrichtlinien und Beispielkonzepte http://www.bsi.de/gshb/deutsch/musterrichtlinien