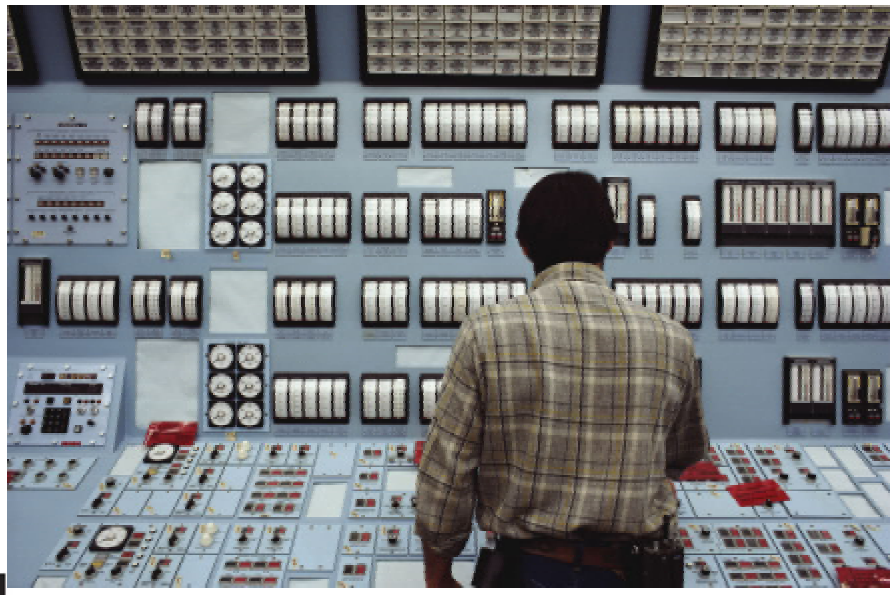
Bundesamt
für Sicherheit in der
Informationstechnik

Ein IT-Grundschutzprofil für eine große Institution



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 114 IT-Sicherheitsmanagement und IT-Grundschutz
Postfach 200363
53133 Bonn
Tel: +49 228 99 9582-0
E-Mail: gshb@bsi.bund.de
Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit der im IT-Grundschutzhandbuch [GSHB] beschriebenen Methode eine wirkungsvolle Möglichkeit zur Erstellung eines IT-Sicherheitskonzepts zur Verfügung. Das GSHB hat sich in den letzten Jahren als ein Standardwerk etabliert und 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 nach der Methodik des GSHB sehr effizient durchgeführt werden.

Die Umsetzung des GSHB in einer großen Institution ist mit verschiedenen Problemen in allen Phasen der Umsetzung verbunden. Insbesondere die meistens große Anzahl von zu betrachtenden Komponenten erschwert die Umsetzung und erfordert einen hohen zeitlichen und personellen Aufwand. Aufgrund knapper Budgets muss sowohl bei der Erstellung des Sicherheitskonzepts als auch bei der Umsetzung der resultierenden einzelnen IT-Sicherheitsmaßnahmen die wirtschaftliche Angemessenheit berücksichtigt werden. Dies erfordert vorab eine genaue Planung und ein striktes Projektmanagement bei der Durchführung.

Das vorliegende Dokument behandelt Probleme, die bei der Umsetzung des GSHB in einer großen Institution auftreten können und zeigt Lösungsansätze, wie diese Probleme gelöst werden können. Zusätzlich wird an einem beispielhaft dargestellten IT-Verbund eines Rechenzentrums (vgl. Kapitel 3) gezeigt, wie diese Probleme konkret gelöst wurden. Vielfach wird daher auf die Situation innerhalb eines Rechenzentrums verwiesen.

Gerichtet ist dieses Dokument an IT-Sicherheitsverantwortliche, die bereits mit dem Umgang des GSHB vertraut sind, dessen Vorgehensweise kennen und gegebenenfalls aktuell das GSHB in ihrer Institution anwenden.

Beispiele innerhalb des Dokuments sind durch einen doppelten Rahmen und das links dargestellte Symbol im Text hervorgehoben.

Tipps sind durch einen einfachen Rahmen, kursive Schrift und dem links dargestellten Symbol hervorgehoben.

2 Rahmenbedingung des Profils

In den nachfolgenden Kapiteln werden die Rahmenbedingungen beschrieben, unter denen das in diesem Dokument verwendete Profil des IT-Verbundes einer großen Institution anwendbar ist. Da durch den Einsatz des GSTOOL die Umsetzung des GSHB erheblich vereinfacht und unterstützt wird, ist die Nutzung empfehlenswert aber nicht verpflichtend. Es können vorhandene Tools wie z. B. Systems-Management Systeme, PC-gestützte Tabellen oder Formulare genutzt werden, auch andere Hersteller bieten Tools die ähnliche Funktionalität wie das GSTOOL bieten an.

2.1 Erläuterung zum Schutzbedarf

„Sicherheit“ ist eine Eigenschaft, die einem Rechenzentrum per se zugeschrieben wird. Insbesondere die Kunden gehen von „100%iger Sicherheit“ aus, wenn Sie die Dienstleistungen eines Rechenzentrums in Anspruch nehmen. Daher müssen für ein Rechenzentrum Sicherheit und die Gewährleistung von Sicherheit eine Selbstverständlichkeit sein und große Anstrengungen unternommen werden, diese dauerhaft zu gewährleisten.

Neben seinen eigenen Daten und Systemen ist der Betreiber eines Rechenzentrums (kurz: RZ) insbesondere für die Daten und Systeme verantwortlich, die er für seine Kunden verwaltet und betreibt. Durch vertragliche Zusicherungen – z. B. Zusicherungen zur Verfügbarkeit der Systeme – ist er angehalten, die für die Kunden betriebenen Systeme vor der Bedrohung der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit zu schützen. Können vertraglich zugesicherte Eigenschaften nicht eingehalten werden, drohen dem RZ-Betreiber Regressforderungen, die sich direkt finanziell auswirken.

Neben diesen direkten wirtschaftlichen Konsequenzen, welche im Allgemeinen durch Haftungsausschlüsse beschränkt werden können, sind insbesonde-

re die indirekten Schäden durch z. B. Imageverlust für ein Rechenzentrum relevant.

Für einen RZ-Betreiber steht somit insbesondere die Bewertung des Schutzbedarfs der Daten und Systeme seiner Kunden im Mittelpunkt, bzw. muss das vertraglich zugesicherte „Sicherheitsniveau" als Grundlage für die umzusetzenden Sicherheitsmaßnahmen dienen.

2.2 Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen hinsichtlich der Informationssicherheit in einer großen Institution sind sehr kompliziert. In einem RZ müssen beispielsweise auch die Anforderungen der Kunden mit berücksichtigt und vertraglich vereinbart werden.

Ein Kreditinstitut unterliegt verschiedenen gesetzlichen Bestimmungen und Richtlinien. Sind an ein RZ Bereiche ausgelagert, die für das Kreditinstitut von wesentlicher Bedeutung für die Durchführung der Bankgeschäfte sind, ist das Kreditinstitut verpflichtet, den §25a des KWG (Kreditwesengesetz) zu beachten. Hierin wird zusammenfassend gefordert, dass das Kreditinstitut auch bei den durch sie beauftragten Unterauftragnehmen dafür Sorge tragen muss, dass gesetzliche Bestimmungen, denen die Bank unterliegt, eingehalten werden. In dessen Konsequenz muss das Kreditinstitut dafür sorgen, dass das beauftragte RZ letztendlich alle rechtlichen Anforderungen erfüllt.

Für ein RZ sind daher insbesondere die Anforderungen der Kunden hinsichtlich der Sicherheit relevant und müssen vertraglich fixiert werden.

Der Verlust der Vertraulichkeit, aber auch eine Verletzung der Integrität oder der Verfügbarkeit können daher für ein RZ sowohl Verstöße gegen Gesetze, Vorschriften oder Verträge zur Folge haben. Insbesondere das Nichteinhalten bestehender Verträge (z.B. aufgrund nicht erreichter, aber vertraglich zugesicherter Verfügbarkeit von Daten und Systemen) und daraus resultierender Konventionalstrafen sind für ein RZ zu berücksichtigen.

Die Bewertung eines Schadens ist demnach abhängig von den rechtlichen und den direkten finanziellen Konsequenzen (z.B. Regressforderungen der Kunden) für das RZ. Neben diesen Schäden können ferner solche Schäden, die zwar beim Kunden entstehen, ihre Ursache jedoch in Defiziten innerhalb des RZ-Betriebs haben, negative Auswirkungen auf das Rechenzentrum selbst haben.

In einem RZ gibt es somit genug Gründe, sich dem Thema „Sicherheit“ zu stellen und nach außen hin die Bedeutung der Sicherheit transparent zu machen. Sicherheit ist als ein integraler Bestandteil der Dienstleistungen zu betrachten, die ein RZ seinen Kunden erbringt. Sicherheit wird vom Rechenzentrum erwartet und der Verlust von Sicherheit kann gravierende Imageschäden zur Folge haben oder sich finanziell auswirken.

Das IT-Grundschutzhandbuch bietet einem Rechenzentrum eine Möglichkeit, Sicherheit zu gewährleisten und dies durch ein IT-Grundschutz-Zertifikat nach außen zu dokumentieren.

2.3 Verantwortlichkeiten und Vorgehensweise

Gemäß der Methodik des GSHB ist der IT-Sicherheitsbeauftragte für die Umsetzung der Methodik und in dieser Eigenschaft für die Abstimmung der Sicherheits-Leitlinie mit dem Leitung und der 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 und Leiter des IT-Sicherheitsmanagement-Teams.

Innerhalb eines Rechenzentrums treten die Mitarbeiter grundsätzlich als IT-Verantwortliche in Erscheinung, da die IT-Systeme für den Kunden des RZ betrieben werden. Die RZ-Mitarbeiter übernehmen die Pflege und Wartung der IT-Systeme und IT-Anwendungen und sorgen für die Umsetzung der festzulegenden technischen Sicherheitsmaßnahmen.

Die IT-Benutzer sind die Anwender beim Kunden, welche die vom RZ betriebenen IT-Systeme und IT-Anwendungen für die Ausübung Ihrer Tätigkeiten nutzen.

Die bei der Erstellung eines IT-Sicherheitskonzepts nach GSHB durchzuführenden Tätigkeiten sind in Kapitel 2 [GSHB] definiert und umfassen die Phasen:

1. Initiierung des IT-Sicherheitsprozesses (vgl. Kapitel 2.0 [GSHB])
2. Durchführung einer Strukturanalyse (vgl. Kapitel 2.1 [GSHB])
3. Durchführung einer Schutzbedarfsfeststellung (vgl. Kapitel 2.2 [GSHB])
4. Modellierung nach IT-Grundschutz (vgl. Kapitel 2.3 [GSHB])
5. Durchführung des Basis-Sicherheitsscheck (vgl. Kapitel 2.4 [GSHB]) und der ergänzenden Sicherheitsanalyse (vgl. Kapitel 2.5 [GSHB])
6. Realisierung von IT-Sicherheitsmaßnahmen (vgl. Kapitel 2.6 [GSHB])

Die Durchführung aller Phasen sowie deren zeitlicher Aufwand ist stark von der Komplexität des individuellen IT-Verbundes abhängig. Phase 6 nimmt hierbei den überwiegenden Teil der Zeit in Anspruch, da gegebenenfalls sowohl technische, als auch organisatorische und bauliche Maßnahmen umzusetzen sind. Für diese Phase bietet sich daher die Erstellung eines separaten Projektplans an, der die Basis für die Umsetzung der Maßnahmen darstellt.

Gerade bei der Anwendung des GSHB innerhalb einer großen Institution treten verschiedene Probleme auf, die es bei der Umsetzung zu lösen gilt. So ist die IT-Infrastruktur üblicherweise sehr komplex und die Strukturanalyse damit sehr aufwändig. Innerhalb eines Rechenzentrums – als Beispiel einer großen Institution – wird bei der Schutzbedarfsfeststellung oft ausschließlich ein hoher Schutzbedarf zugrunde gelegt, um den Anforderungen der Kunden gerecht zu werden. Dies macht in vielen Fällen eine ergänzende Sicherheitsanalyse erforderlich und dadurch die Durchführung der Phase 5 aufwändig.

Im folgenden Kapitel 3 wird ein exemplarischer IT-Verbund eines Rechenzentrums beschrieben. Dieses Beispiel wird in den darauf folgenden Kapiteln verwendet, um die in den einzelnen Phasen auftretenden Probleme darzustellen und Lösungsansätze aufzuzeigen.

3 Definition und Abgrenzung des IT-Verbundes

In diesem Abschnitt wird der IT-Verbund des Rechenzentrums beschrieben. Die Beschreibung des IT-Verbundes aus der Sicht des GSHB wird in Kapitel 5 (Strukturanalyse) vorgenommen.

Netzplan

In Abbildung 1 ist der durch Gruppenbildung bereits stark bereinigte Netzplan des Rechenzentrums dargestellt. Hinter den gruppierten Windows und Unix Servern verbergen sich üblicherweise komplette Server-Farmen aus identischen oder ähnlichen Systemen. Die einzelnen Server dieser Server-Farmen können in der Regel aufgrund der Einstufung in gleiche Schutzbedarfskategorien – wie dargestellt – sehr gut zu Gruppen zusammengefasst werden. Der IT-Verbund soll im Beispiel lediglich die grau hinterlegten Bereiche umfassen, also die Büroumgebung des RZ-Personals und die des Operating nicht mit einschließen.

Das dargestellte Rechenzentrum betreibt neben Windows und UNIX Servern auch einen Mainframe.

Das Operating wird von einer zentralen Stelle aus übernommen, von der aus eine 24/7 Überwachung gewährleistet wird.

Zur Datensicherung ist eine zentrale Backup-Lösung vorhanden.

Die Notstromversorgung wird durch unterbrechungsfreie Stromversorgungen (USV) für kurzzeitige Stromausfälle und einem zentralen Notstromaggregat für mittelfristige Stromausfälle sichergestellt.

Aus dem Internet sind Dienste des WWW- und Mail-Servers erreichbar. Die Anbindung an das Internet ist über ein 3-stufiges Firewallsystem abgesichert (externer und interner Paketfilter sowie Internet Firewall). Zusätzlich ist das Rechenzentrum über eine RZ-Firewall von den Büro- und Operating-Netzen logisch getrennt.

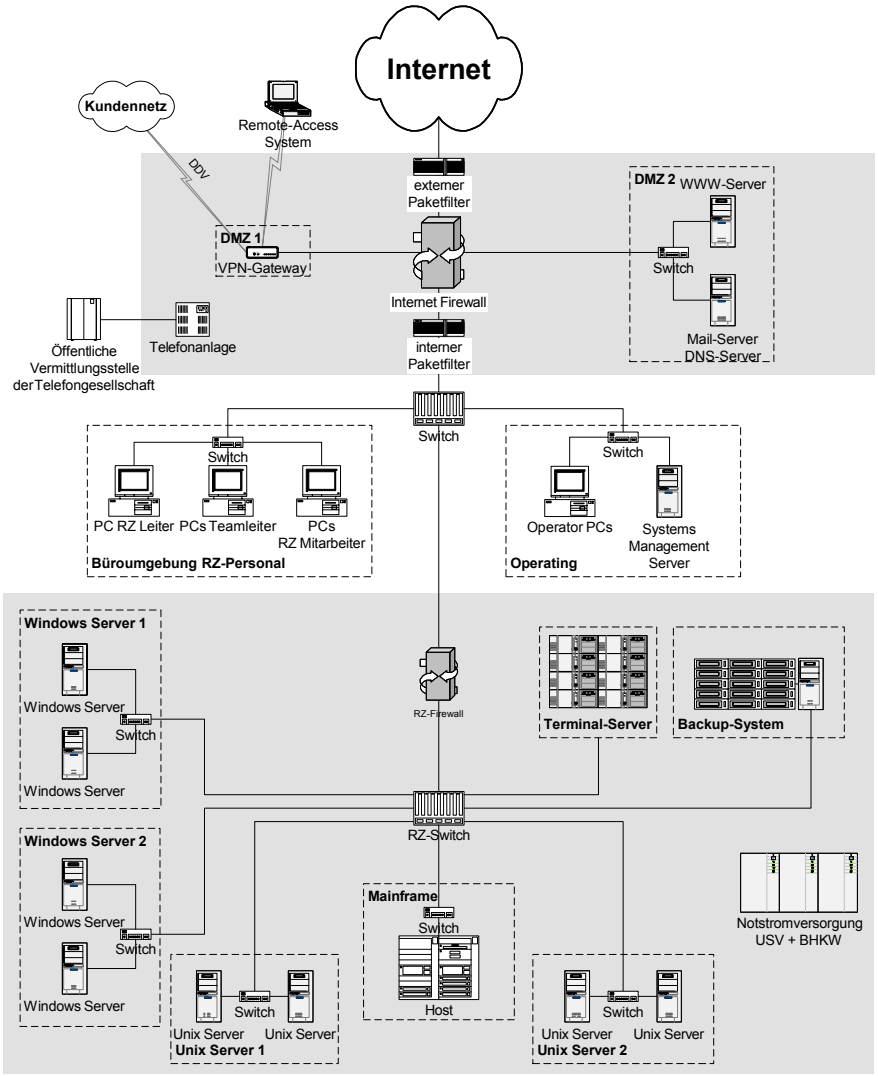


Abbildung 1: Bereinigter Netzplan

Ein gesicherter externer Zugang zum Rechenzentrum erfolgt über ein per Internet und Dial-In erreichbares VPN-Gateway. Ein Zugang von Kunden zu deren im RZ aufgestellten Systemen ist hierüber ebenfalls realisiert und erfolgt über eine DDV oder per ISDN als Backup.

Über einen Terminalserver ist ein Konsolenzugang zu allen Serversystemen möglich.

Das RZ-Personal hat eigene Arbeitsplatz-PCs, von denen aus zu Wartungs- und Administrationszwecken auf die Server zugegriffen werden kann. Für den Remote-Access stehen den Bereitschaften der einzelnen Teams identisch konfigurierte Remote-Access Notebooks zur Verfügung.

Organigramm / Personal

Abbildung 2 stellt das Organigramm des Rechenzentrums dar. Einzelne Teams sind für die Wartung und Pflege der unterschiedlichen Serverplattformen verantwortlich. Zusätzlich existieren Teams für das Operating und die Technik (Telekommunikation, Netzwerktechnik, Klima, Stromversorgung und USV, etc.). Sicherheit und Datenschutz sind als Stabsstelle definiert. Übergeordnet zeichnet der RZ-Leiter für das Rechenzentrum verantwortlich. Die Stelle der Verwaltung ist u.a. für die Beschaffung und Organisation der Mitarbeiter zuständig. Auch das Gebäudemanagement ist hier angesiedelt.

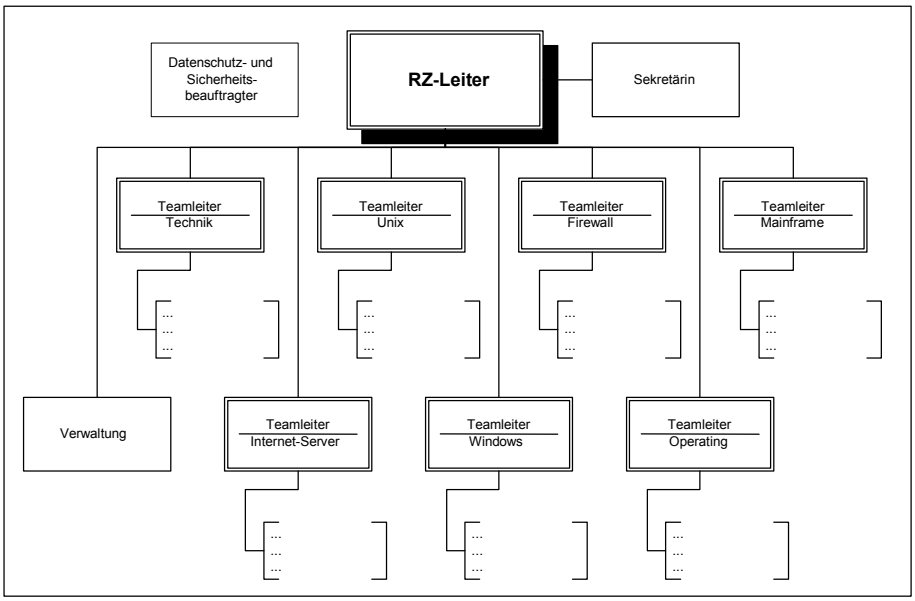


Abbildung 2: Organigramm der exemplarischen großen Institution

4 Sicherheits-Leitlinie und Sicherheitskonzept

Bild 1: Kompass

Die erste Aufgabe bei der Initiierung des Sicherheitsprozesses besteht in der Ernennung eines IT-Sicherheitsbeauftragten, der Definition des IT-Verbundes (also der Festlegung des Geltungsbereiches) und der Erstellung einer Sicherheits-Leitlinie. Der IT-Sicherheitsbeauftragte hat die Aufgabe, die Erstellung eines IT-Sicherheitskonzepts zu koordinieren und im Anschluss daran für die dauerhafte Einhaltung des erreichten Sicherheitsniveaus in der Institution Sorge zu tragen. Er ist in diesem Sinne der Projektleiter für die Umsetzung des GSHB.

Innerhalb großer Institutionen existieren üblicherweise bereits Grundlagen eines Sicherheitsmanagements. Dies können Dokumente, Prozesse und auch Verantwortlichkeiten mit Sicherheitsbezug sein. Eine Änderung vorhandener Prozesse und Verantwortlichkeiten führt in der Regel zu einem erhöhten Aufwand. Aus diesem Grund ist es für den zuständigen IT-Sicherheitsbeauftragten vorteilhaft, die vorhandenen Teile eines Sicherheitsmanagements aufzunehmen und bei der weiteren Vorgehensweise zu berücksichtigen.

4.1 Generelle Vorgehensweise bei der Erstellung der Sicherheits-Leitlinie

Die Sicherheits-Leitlinie definiert das innerhalb des Geltungsbereiches (IT-Verbundes) angestrebte Sicherheitsniveau. In ihr werden daher der Geltungsbereich, in dem die Sicherheits-Leitlinie gültig ist und die von der Institution angestrebten Sicherheitsziele sowie die verfolgte Sicherheitsstrategie festgehalten. Die Sicherheits-Leitlinie ist somit Anspruch und Aussage

zugleich. Über die Sicherheits-Leitlinie wird das zu erreichende „Ziel“ (Sicherheitsniveau) der Institution festgelegt. Die Leitung der Institution unterrichtet alle Mitarbeiter über diese Sicherheits-Leitlinie und weist auf die verpflichtende Einhaltung und Verbindlichkeit innerhalb der Institution hin.

Die Sicherheits-Leitlinie kann auf unterschiedliche Arten erstellt werden. Ausgehend von den oben genannten Aspekten bietet es sich an, einen Workshop zu den einzelnen Themen zu veranstalten und mit den Verantwortlichen die Formulierung eines Entwurfs der Sicherheits-Leitlinie zu erarbeiten. Als Grundlage für die Sicherheits-Leitlinie bietet es sich an, die durch das BSI veröffentlichte Dokumente [MURI] zu nutzen.

4.2 Häufige Probleme bei der Erstellung der Sicherheits-Leitlinie

Insbesondere mangelnde Ressourcen, die Nutzung bereits vorhandener Ansätze einer Sicherheits-Leitlinie und die Berücksichtigung von Kundenanforderungen sind häufige Probleme bei der Erstellung einer Sicherheitspolitik.

4.2.1 Personelle Probleme

Die Erstellung einer Sicherheits-Leitlinie ist ein aufwändiger Prozess, der personelle Ressourcen bindet. Insbesondere stellt sich daher als Problem heraus, dass die für die Erstellung der Sicherheits-Leitlinie benötigten Ressourcen nicht zur Verfügung stehen.

4.2.1.1 Benennung des IT-Sicherheitsbeauftragten

Aufgrund der Anforderungen des GSHB muss ein IT-Sicherheitsbeauftragter benannt werden. Kann hierbei auf vorhandenes Personal zurückgegriffen werden?

Aufgrund eines häufig herrschenden Personalmangels wird das Thema IT-Sicherheit oft vernachlässigt. Insbesondere bei der Benennung eines IT-Sicherheitsbeauftragten wird auf bereits vorhandenes Personal zurückgegriffen, ohne diesem zusätzliche Ressourcen zur Verfügung zu stellen. Hierdurch können Interessenkonflikte entstehen, wenn z.B. der für die IT-Sicherheit zuständige Mitarbeiter gleichzeitig Aufgaben innerhalb des IT-Betriebs wahrnimmt. Der IT-Sicherheitsbeauftragte hat innerhalb der Organisation die Aufgabe

- im gesamten IT-Sicherheitsprozess mitzuwirken,
- die Erstellung der IT-System-Sicherheitleitlinie(n) zu koordinieren,
- die Erstellung des IT-Sicherheitskonzepts zu koordinieren,
- die Erstellung des Notfallvorsorgekonzepts und anderer Teil-Konzepte zu koordinieren,
- die Erstellung des Realisierungsplanes für IT-Sicherheitsmaßnahmen und die Initiierung und Überprüfung der Realisierung,
- dem IT-Sicherheitsmanagement-Team und der Leitungsebene zu berichten,
- den Informationsfluss innerhalb des Sicherheitsmanagement-Teams sicherzustellen sowie
- evtl. auftretende sicherheitsrelevante Zwischenfälle festzustellen und zu untersuchen.

Bei der Benennung eines Mitarbeiters zum IT-Sicherheitsbeauftragten ist darauf zu achten, dass diesem auf der einen Seite ausreichend Ressourcen zur Verfügung gestellt werden, um seinen Tätigkeiten nachzukommen, und auf der anderen Seite die Unabhängigkeit vom IT-Betrieb sichergestellt ist.

In größeren Institutionen hat der IT-Sicherheitsbeauftragte hauptsächlich koordinierende Funktionen und ist nicht zwangsläufig für die Formulierung technischer Sicherheitsmaßnahmen verantwortlich. Es bietet sich daher an,

einem bereits vorhandenen QM- oder Datenschutzbeauftragten zusätzlich die Funktion des IT-Sicherheitsbeauftragten zuzuweisen. Hierfür müssen ihm jedoch zusätzliche Ressourcen zur Verfügung gestellt werden. Weiterhin ist auf ausreichende Qualifikation zu achten und falls erforderlich, sind entsprechende Schulungsmaßnahmen durchzuführen.

4.2.1.2 Fehlende personelle Ressourcen

In der Institution soll eine Sicherheits-Leitlinie erstellt werden. Wie kann am effizientesten vorgegangen werden?

Die Festlegung der Eckpunkte einer Sicherheits-Leitlinie erfolgt sehr effizient im Rahmen von Workshops mit Vertretern der Institutsleitung und der Teamleiter. Hierbei ist es die Aufgabe des IT-Sicherheitsbeauftragten die Workshops zu moderieren, um die relevanten Aspekte (Geltungsbereich/IT-Verbund, Sicherheitsziele, Sicherheitsstrategie) zu erarbeiten, diese anschließend schriftlich niederzulegen und mit der Institutsleitung abzustimmen. Die abschließende Verabschiedung der Sicherheits-Leitlinie obliegt der Institutsleitung.

Das Rechenzentrum hat eigene Verantwortliche für das Gebäudemanagement, denen auch der Betrieb der Zutrittskontrollsysteme, des Brandschutzsystems und der USV obliegt. Die Sicherheits-Leitlinie betrachtet Gebäudesicherheit als eigenen Aspekt. Um diesen zu bearbeiten, veranstaltet der IT-Sicherheitsbeauftragte mit den Verantwortlichen des Gebäudemanagement einen Workshop und erarbeitet mit diesen gemeinsam ein eigenes Kapitel zum Thema physische Sicherheit.

4.2.1.3 Fehlendes Sicherehtitsbewusststein des Managements

Die Institutsleitung sieht die Erstellung einer Sicherheits-Leitlinie als nebensächlich an. Wie kann die Institutsleitung von der Notwendigkeit überzeugt werden?

Teilweise ist sich das Managent nicht ihrer Verantwortung hinsichtlich der Einführung und Aufrechterhaltung von Sicherheitsmaßnahmen bewusst. Dies ist insbesondere dann der Fall, wenn die Institutsleitung stark kaufmännisch ausgerichtet ist. In einem solchen Fall ist es die Aufgabe des IT-Sicherheitsbeauftragten, die Leitung hinsichtlich ihrer Verantwortung zu überzeugen. Die Überzeugungsarbeit muss hierbei sowohl fachlicher Natur sein, als auch die rechtlichen Aspekte berücksichtigen.

Muss die Institutsleitung hinsichtlich ihrer Verantwortung überzeugt werden, bietet sich als Einstieg für Argumentationen sowohl das Kapitel 2.2 aus diesem Dokument, als auch die Ausführungen im Dokument „Leitfaden IT-Sicherheit“ [LEITF] an.

4.2.2 Inhaltliche Probleme

Neben Problemen, die aufgrund mangelnder Ressourcen entstehen, sind inhaltliche Fragestellungen ein weiteres Problem. Hierbei ist zu entscheiden, in welchem Detaillierungsgrad die Sicherheits-Leitlinie zu formulieren ist und wie die vielfältigen Kundenanforderungen mit berücksichtigt werden.

4.2.2.1 Detaillierungsgrad der Sicherheits-Leitlinie

Wie detailliert müssen die Formulierungen in der Sicherheits-Leitlinie gewählt werden?

Eine zu detailliert formulierte Sicherheits-Leitlinie birgt die Gefahr, häufig angepasst werden zu müssen. Eine zu ungenau formulierte Sicherheits-Leitlinie kann hingegen missverstanden werden, so dass wesentliche Aspek-

te keine Berücksichtigung finden. Der Detaillierungsgrad ist abhängig vom Geschäftsfeld der Institution. Grundsätzlich kann davon ausgegangen werden, dass die Sicherheits-Leitlinie ein „lebendes" Dokument ist und im Laufe der Zeit an Stabilität zunimmt.

Sowohl die Aussage „*Es werden geeignete Maßnahmen gegen das Auftreten von schadhafter Software (z.B. Viren) ergriffen.*" als auch die Aussage „*Risiken, die Auswirkungen auf die Institution haben, werden ermittelt und geeignete Gegenmaßnahmen definiert.*" sind in einer Sicherheits-Leitlinie möglich. Jedoch ist es abhängig von den Schwerpunkten der Geschäftstätigkeit der Institution, ob die detaillierte Aussage oder eher die allgemeiner gefasste Aussage in die Sicherheits-Leitlinie aufgenommen wird.

Die Sicherheits-Leitlinie sollte nicht zu ausführlich auf einzelne Aspekte eingehen. Es bietet sich daher an, die für den Geschäftszweck wesentlichen Aspekte detailliert aufzunehmen, und die anderen Aspekte eher allgemein zu behandeln.

Eine Formulierung, die den obigen Hinweis beachtet ist z.B.:

„*Risiken, die Auswirkungen auf die Institution haben, werden ermittelt und geeignete Gegenmaßnahmen definiert. Besondere Beachtung finden hierbei u.a. Risiken, die aus dem Auftreten maliziöse Software (z.B. Viren und Würmer) oder dem Ausfall von Kundensystemen entstehen.*"

4.2.2.2 Nutzung vorhandener Dokumente

In der Institution sind bereits verschiedene Dokumente vorhanden, in denen Sicherheitsaspekte und Sicherheitsziele definiert werden. Kann die bereits geleistete Arbeit weiterverwendet werden?

Innerhalb einer großen Institutionen existieren in der Regel verschiedene Dokumente, die – zumindest in Teilen – den Charakter einer Sicherheits-Leitlinie besitzen oder Aspekte einer Sicherheits-Leitlinie behandeln. Es

muss daher davon ausgegangen werden, dass die Sicherheits-Leitlinie nicht als „grüne Wiese-Konzept“ von Grund auf neu erstellt werden kann, sondern dass vielmehr bereits existierende Aspekte konsolidiert und zusammengefasst werden müssen. Dies ist insbesondere auch deshalb notwendig, da große Veränderungen den Mitarbeitern schwer vermittelt werden können.

Die Sichtung vorhandener Dokumente und Konsolidierung relevanter Aspekte ist einer der ersten Schritte, die der IT-Sicherheitsbeauftragte durchzuführen hat. Das Ergebnis kann als Grundlage für den weiter oben genannten Workshop und damit als Ausgangspunkt für die Sicherheits-Leitlinie dienen.

Häufig sind in Rechenzentren interne Richtlinien vorhanden und Hausmitteilungen erlassen worden. Derartige Dokumente spiegeln das Sicherheitsempfinden sehr gut wieder und enthalten teilweise Aussagen, die Bestandteil einer Sicherheits-Leitlinie sein müssen. Derartige Dokumente sollten daher in die Erstellung der Sicherheits-Leitlinie mit einbezogen werden. Dies ist vorteilhaft, da hierdurch bereits etablierte und bekannte Aspekte in die Sicherheits-Leitlinie einfließen.

Im Laufe der Jahre hat die Institutsleitung verschiedene verbindliche Hausmitteilungen veröffentlicht. Hierunter fällt auch eine Hausmitteilung zur generellen Nutzung von Passworten und zum Virenschutz. Der IT-Sicherheitsbeauftragte nutzt Aussagen dieser Hausmitteilungen um einen ersten Entwurf für die Sicherheits-Leitlinie zu erstellen.

4.2.2.3 Berücksichtigung von Kundenanforderungen

Im Rahmen der angebotenen Dienstleistungen müssen den Kunden verschiedene Zusicherungen, die auch Auswirkungen auf Sicherheitsaspekte haben, gemacht werden. Müssen diese mit in der Sicherheits-Leitlinie genommen werden?

Wie bereits oben ausgeführt, sind für große Institutionen die Kundenbelange und -anforderungen sehr relevant. Ein Problem ergibt sich häufig daraus,

wenn die Anforderungen der einzelnen Kunden stark voneinander abweichen. Besonders problematisch ist es, wenn Anforderungen von Kunden sich gegenseitig ausschließen. Kundenbelange sollten daher indirekt in der Sicherheits-Leitlinie Berücksichtigung finden.

Da die Sicherheits-Leitlinie ein möglichst stabiles Dokument sein soll und daher wenig geändert werden sollte, darf nicht jede konkrete Kundenanforderung in die Sicherheits-Leitlinie einfließen. Eine übergeordnete Aussage, dass Kundenbelange bei der Auswahl von Sicherheitsmaßnahmen berücksichtigt werden, ist meistens ausreichend.

Die Kunden des Rechenzentrums stellen unterschiedliche Anforderungen bezüglich Verfügbarkeiten der von ihnen genutzten Serversysteme. In der Sicherheits-Leitlinie des Rechenzentrums ist daher folgender Satz enthalten:

Für unsere Kunden ist die Verfügbarkeit der durch uns betriebenen Serversysteme wichtig, da interne Prozesse des Kunden von der Verfügbarkeit abhängen. Durch die Umsetzung technischer und organisatorischer Maßnahmen gewährleisten wir, dass die Verfügbarkeitsanforderungen unserer Kunden eingehalten werden.

4.2.2.4 Definition des IT-Sicherheitsmanagement-Teams

Der IT-Sicherheitsbeauftragte soll auch infrastrukturelle und personelle Themen behandeln. Es sind jedoch eigene Abteilungen für das Gebäudemanagement und eine Personalabteilung vorhanden. Kann der IT-Sicherheitsbeauftragte auf Unterstützung durch diese Abteilungen zurückgreifen?

Bei großen Institutionen ist die Einrichtung eines IT-Sicherheitsmanagement-Teams unter Leitung des IT-Sicherheitsbeauftragten sinnvoll. Das IT-Sicherheitsmanagement-Team

- entwickelt IT-Sicherheitsziele und -strategien sowie die IT-Sicherheitsleitlinie,
- überprüft die Umsetzung der IT-Sicherheitsleitlinie,
- initiiert, steuert und kontrolliert den IT-Sicherheitsprozess,
- wirkt an der Erstellung des IT-Sicherheitskonzepts mit,
- prüft, ob die im IT-Sicherheitskonzept geplanten IT-Sicherheitsmaßnahmen wie geplant funktionieren, sowie ob diese geeignet und wirksam sind,
- erstellt einen Realisierungsplan für die IT-Sicherheitsmaßnahmen und stellt die erforderlichen Ressourcen zur Verfügung,
- erstellt die Schulungs- und Sensibilisierungsprogramme für IT-Sicherheit und
- berät die Leitungsebene in IT-Sicherheitsfragen.

Das IT-Sicherheitsmanagement-Team ist somit für die Erstellung und Fortschreibung der IT-Sicherheits-Leitlinie und des IT-Sicherheitskonzepts zuständig. Weiterhin initiiert und koordiniert es im Falle von auftretenden Sicherheitsproblemen (z.B. Teilausfälle der Infrastruktur) geeignete Gegenmaßnahmen.

Abhängig von der organisatorischen Größe der Institution können Funktionen, die für die Umsetzung des GSHB relevant sind, auf verschiedene Personen verteilt sein. Oft ist es üblich, eine verantwortliche Person für die infrastrukturellen Themen (Strom-/Wasser-/Klimaversorgung, bauliche Themen) und einen Verantwortlichen für personelle Themen (Einstellung, Ausscheiden) zu benennen. Da auch solche Themen bei der Umsetzung des GSHB relevant sind, bietet es sich an, diese bei der Erstellung des IT-Sicherheitskonzepts mit einzubeziehen.

Die Institution definiert in der Sicherheits-Leitlinie ein IT-Sicherheitsmanagement-Team (vgl. Abbildung 3), dessen Leitung dem IT-Sicherheitsbeauftragten obliegt. Neben dem IT-Sicherheitsbeauftragten besteht das IT-Sicherheitsmanagement-Team aus verschiedenen Sicherheitsverantwortlichen für Technik, Internet-Server, Firewall, Windows, Unix, für das Operating und die Hostsysteme. Der IT-Sicherheitsbeauftragte nimmt in diesem Team eine koordinierende Funktion und vertritt die Institutsleitung in Fragen der IT-Sicherheit.

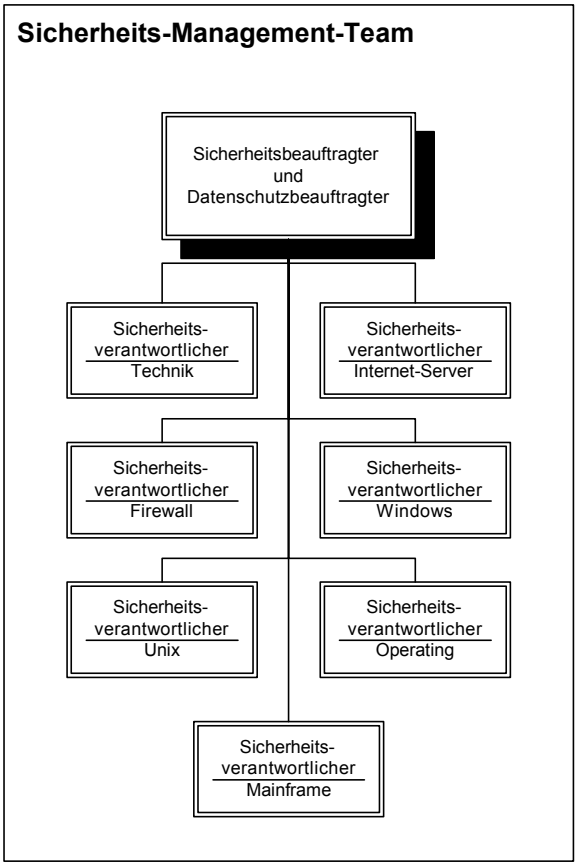


Abbildung 3: Struktur eines Sicherheitsmanagement-Teams

4.3 Generelle Vorgehensweise bei der Erstellung eines IT-Sicherheitskonzepts

Die IT-Sicherheitskonzeption besteht aus den in Abbildung 4 dargestellten Phasen IT-Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, Basis-Sicherheitscheck und Realisierung. Die während der einzelnen Phasen erstellte Dokumentation bildet das IT-Sicherheitskonzept im Sinne des GSHB.

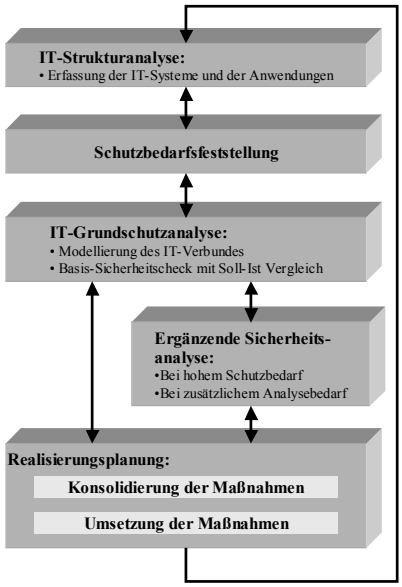


Abbildung 4: Phasen der IT-Sicherheitskonzeption

Der IT-Verbund (und damit das IT-Sicherheitskonzept) muss nicht die gesamte Institution umfassen, sondern kann auch sinnvolle Teilbereiche betreffen (vgl. Kapitel 3). Ein IT-Sicherheitskonzept für den Teilbereich der Institution ist somit möglich und sinnvoll, wenn es als Ausgangspunkt für ein umfassendes IT-Sicherheitskonzept einer komplexen IT-Infrastruktur dient.

Das IT-Sicherheitskonzept nach GSHB besteht aus den dokumentierten Phasen „Strukturanalyse“ bis „Realisierungsplanung“. Für die Erstellung ist der IT-Sicherheitsbeauftragte verantwortlich. Ihm obliegt die Koordinierung der in den einzelnen Phasen erforderlichen Tätigkeiten. Da in einer großen Institution davon auszugehen ist, dass bereits Ansätze eines IT-Sicherheitskonzepts vorhanden sind, besteht die erste Aufgabe des IT-Sicherheitsbeauftragten in der Sichtung vorhandener und der Identifikation verwendbarer Dokumente.

4.4 Häufige Probleme bei der Erstellung des IT-Sicherheitskonzepts

Die bei der Erstellung des IT-Sicherheitskonzepts meist auftretenden Probleme ähneln denjenigen, die sich bei der Erstellung der Sicherheits-Leitlinie ergeben. Hierzu zählen insbesondere die Berücksichtigung bereits vorhandener Dokumente und deren Sichtung sowie Zeitmangel aufgrund herrschenden Kostendrucks und Ressourcenmangels.

4.4.1 Inhaltliche Probleme – Nutzung vorhandener Dokumentationen

In der Institution sind viele Sicherheitskonzepte für unterschiedliche Systeme erstellt worden. Wie können die bereits existierenden Dokumente genutzt werden?

Wie auch bei der Erstellung der Sicherheits-Leitlinie gehört es zur erste Aufgabe des IT-Sicherheitsbeauftragten, bereits vorhandene Dokumente zu sichten und gegebenenfalls wiederzuverwenden.

Ausgehend von vertraglichen Zusicherungen hat ein Rechenzentrum fünf Schutzbedarfsklassen für die Verfügbarkeit definiert (*unbedeutend*, *niedrig*, *mittel*, *hoch* und *existenzbedrohend*). Eine Änderung dieser Schutzbedarfsklassen ist nicht ohne weiteres möglich, da diese Bestandteil verschiedener Verträge sind.

Die Vorgehensweise nach GSHB sieht explizit die Nutzung von mehr als drei Schutzbedarfsklassen vor, daher verwendet das Rechenzentrum die bereits etablierten Definitionen und nutzt diese während der Schutzbedarfsfeststellung. In der weiteren Vorgehensweise werden die Schadensszenarien für die bereits existierenden Schutzbedarfsklassen konkretisiert.

4.4.2 Einschränkungen aufgrund von Wirtschaftlichkeitsüberlegungen

Meist wird durch die Institutsleitung der Wunsch nach einer möglichst kosteneinsparenden Umsetzung von Sicherheitsmaßnahmen gewünscht. Dies wird meist damit begründet, dass kein direkter „Return of Investment“ durch die zu ergreifenden Maßnahmen zu erwarten ist. Für die Umsetzung werden dann oft nur eingeschränkt Ressourcen für die Umsetzung des GSHB zur Verfügung gestellt.

4.4.2.1 Reduzierung des Aufwands

Wie lässt sich der Aufwand für die Durchführung der einzelnen Phasen reduzieren?

Wirtschaftlichkeitsüberlegungen spielen in jeder Institution eine wesentliche Rolle. Da versucht wird, die Kosten in allen Bereichen auf ein Minimum zu reduzieren, müssen auch bei der Erstellung eines IT-Sicherheitskonzepts Wirtschaftlichkeitsbetrachtungen berücksichtigt werden.

Die Aspekte der Wirtschaftlichkeitsbetrachtung kommen bei der IT-Sicherheitskonzeption nach GSHB vor allem in der Phase der Realisierungsplanung zum Tragen. Bei der Festlegung der Umsetzungsreihenfolge muss neben der angestrebten Siegelstufe auch das verfügbare Budget festgelegt werden.

Abhängig hiervon müssen bestimmte Standard-Sicherheitsmaßnahmen umgesetzt werden, um die gewünschte Siegelstufe zu erreichen. Eine Minimierung der dadurch entstehenden Kosten ist damit lediglich durch Optimierung der Kosten für die Umsetzung der notwendigen Einzelmaßnahmen für die jeweilige Siegelstufe möglich. Durch eine Dokumentation der Abläufe und Zuständigkeiten erreicht man eine Fortentwicklung und Straffung der Prozesse, dies spart langfristig Zeit und Ressourcen.

4.4.2.2 Folgeaufwände und Fortschreibung

Welche Aufwände entstehen durch die Fortschreibung und regelmäßige Aktualisierung des IT-Sicherheitskonzepts?

Die Erstellung des IT-Sicherheitskonzepts ist kein einmaliger Arbeitsschritt, sondern ein kontinuierlicher Prozess der permanent fortgeführt werden muss. Die Erstellung eines IT-Sicherheitskonzepts für eine große Institution nimmt in der Regel etwa ein Zeitjahr in Anspruch. Bei kontinuierlicher Fortschreibung muss bei einer großen Institution davon ausgegangen werden, dass ein Mitarbeiter für die Koordinierung der Fortschreibung des IT-Sicherheitskonzepts benötigt wird.

5 Strukturanalyse

Erster Schritt bei der Erstellung eines IT-Sicherheitskonzepts ist die Durchführung der Strukturanalyse des betrachteten IT-Verbundes. In den nachfolgenden Abschnitten wird zunächst die generelle Vorgehensweise zur Durchführung einer Strukturanalyse erläutert. Im Anschluss werden häufig auftretende Probleme im Zusammenhang mit der Strukturanalyse innerhalb einer großen Institution dargestellt und Ansätze zur Lösung dieser Probleme erläutert.

5.1 Generelle Vorgehensweise bei der Strukturanalyse

Ziel der Strukturanalyse[1] (vgl. Kapitel 2.1 [GSHB]) ist die vollständige Erfassung aller IT-Anwendungen, IT-Systeme, der Kommunikationsverbindungen und der IT-Räume des in Kapitel 3 beispielhaft betrachteten IT-Verbundes. Mit Abschluss der Strukturanalyse liegt eine vollständige Beschreibung des Ist-Zustands dieser Komponenten vor. Für den konkreten IT-Verbund ist der bereinigte Netzplan in Abbildung 3 dargestellt.

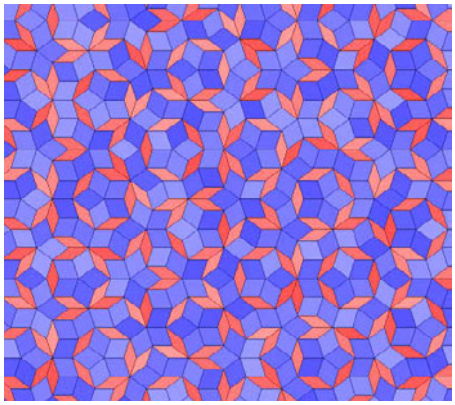


Bild 2: Penrose-Parkett

[1] Das Bild zeigt als Struktur ein nach dem britischen Mathematiker Roger Penrose benanntes Parkett. Aus zwei verschiedenen Formen wird eine vollständige Überdeckung einer Fläche erreicht. Die entstehenden Strukturen scheinen, oberflächlich betrachtet, periodisch zu sein. Tatsächlich handelt es sich jedoch um eine nichtperiodische Struktur. Das Ergebnis einer Strukturanalyse liefert im Gegensatz dazu eine „flächendeckende“ Übersicht aller IT-Komponenten des Rechenzentrums, die eine sehr viel einfachere Interpretation erlaubt.

Die Strukturanalyse wird vom IT-Sicherheitsbeauftragten mit Unterstützung durch die jeweiligen IT-Verantwortlichen erstellt, wobei der IT-Sicherheitsbeauftragte die Rolle des Projektleiters und somit die Koordination der Aufgaben übernimmt.

Eine Strukturanalyse besteht aus den folgenden drei Schritten:

Schritt 1 Auswertung eines Netzplans

Ein bereits bestehender Netzplan (beispielsweise in Form eines Netztopologieplans) mit den eingesetzten Komponenten und deren Vernetzung wird zur Vorbereitung der Strukturanalyse auf Vollständigkeit und Aktualität geprüft. Bei einer großen Institution der betrachteten Größe kann aufgrund der vorhandenen Systems Management Systeme davon ausgegangen werden, dass jederzeit ein aktueller und vollständiger Netzplan (in Form eines Netztopologieplans) vorhanden ist.

Es ist in diesem Schritt wichtig darauf zu achten, dass zusätzlich zu den Kommunikationsverbindungen zwischen den IT-Systemen auch alle Außenverbindungen erfasst und aufgeführt werden. Als Außenverbindungen sind hierbei sämtliche Verbindungen anzusehen, die über die Grenze des IT-Verbundes gehen.

An das Rechenzentrum sind verschiedene Abteilungen angebunden. Da diese Abteilung außerhalb des Rechenzentrums liegen, welcher einen IT-Verbund bildet, sind die Netzübergänge zu diesen Abteilungen als Außenverbindungen anzusehen.

Das Rechenzentrum identifiziert die über das VPN-Gateway realisierten Verbindungen DDV und Remote-Access System sowie die Verbindungen in die Büroumgebung RZ-Personal und Operating als Außenverbindungen des IT-Verbundes.

Bedingt durch die komplexe Infrastruktur eines Rechenzentrums bietet es sich für die Durchführung dieses Schritts an, diesen nochmals in folgende kleinere Arbeitspakete zu unterteilen.

1. *Bestimmung von Teilnetzen*

   Um die Aktualisierung eines Netzplans übersichtlicher zu gestalten, sollten zunächst Teilnetze definiert werden, durch die die gesamte Infrastruktur erfasst wird.

Im beispielhaft betrachteten IT-Verbund (Kapitel 3) bietet es sich beispielsweise an, die Gruppen der *Windows Server* zu einem separaten Teilnetz zusammenzufassen und zu aktualisieren.

2. *Erstellung eines Netzplans für die einzelnen Teilnetze*

   Für jedes dieser Teilnetze wird der Teilnetzplan auf den neuesten Stand gebracht, indem er mit der tatsächlich vorhandenen IT-Struktur abgeglichen wird.

3. *Konsolidierung der einzelnen Teilnetzpläne*

   Während der Konsolidierung werden die Teilnetzpläne bereinigt, d. h. hier werden gleichartige Komponenten mit gleichem Schutzbedarf zu einer Gruppe zusammengefasst und durch ein einzelnes Objekt dargestellt (vgl. Kapitel 2.1 [GSHB]). Durch diese Gruppenbildung erfolgt eine Komplexitätsreduktion, welche zusätzlich eine Erhöhung der Übersichtlichkeit bewirkt. Wichtig ist hierbei, dass die Information, welches System zu welcher Gruppe gehört und der Schutzbedarf, dokumentiert werden (z.B. direkt im Systems Management System).

Mehrere identisch aufgebaute und identisch installierte IT-Systeme innerhalb des Teilnetzes, können zu einer Gruppe zusammengefasst werden, wenn sie denselben Schutzbedarf besitzen.

Das Rechenzentrum setzt ein Systems-Management System für die Verwaltung der vorhandenen IT-Anwendungen und IT-Systeme ein. Die Information, welcher Gruppe die Systeme zugeordnet werden, wird direkt im Systems Management System hinterlegt, so dass die Gruppenbildung jederzeit nachvollziehbar ist.

Daher dokumentiert das Rechenzentrum für alle in der DMZ 2 vorhandenen Webserver die Information, dass diese der Gruppe WWW-Server zugeordnet sind und einen normalen Schutzbedarf besitzen direkt im vorhandenen Systems-Management System.

4. Zusammenfassung der Ergebnisse der Teilnetze

Die Ergebnisse der einzelnen Teilnetze werden zu einem Gesamtnetzplan zusammengefasst und erneut in der o. g. Form bereinigt.

Dieser Gesamtnetzplan wird in einer gemeinsamen Sitzung mit den IT-Verantwortlichen abgestimmt, um sicherzustellen, dass die Einordnung "ihrer" IT-Komponenten in den Gesamtverbund korrekt wiedergegeben wird.

Schritt 2 Erhebung der IT-Systeme

Zur Vorbereitung der Schutzbedarfsfeststellung und Modellierung des IT-Verbundes werden alle Komponenten aus dem bereinigten Netzplan im GSTOOL erfasst. Die Erfassung muss sämtliche, also auch nicht im Netzplan aufgeführte IT-Systeme, enthalten. Hierbei ist für jedes IT-System

- eine eindeutige Bezeichnung (z.B. eine Inventarnummer),
- Typ und Funktion des Systems (z.B. Webserver des Kunden X),
- die Hard- und Softwareplattform (d.h. Hardware und Betriebssystem),
- der Standort (z.B. Raumnummer, Koordinaten im RZ),

- der zuständige Administrator sowie
- die Art der Netzanbindung und die Netzadresse(n)

festzuhalten.

Besonders zu beachten ist, dass nicht-vernetzte – daher insbesondere nicht im Netzplan aufgeführte – IT-Systeme (z.B. Telefonanlagen) ebenfalls vollständig erfasst werden müssen!

Ist eine Gruppierung von nicht-vernetzten Systemen möglich, können diese als ein Objekt dargestellt werden.

Sofern diese eindeutig identifizierbar sind, werden mit der Erfassung der IT-Systeme gleichzeitig auch die IT-Benutzer und IT-Verantwortlichen des jeweiligen IT-Systems festgehalten. Diese erbrachte Vorleistung kann später bei der Personalerfassung eingespart werden.

Zu den nicht-vernetzten Systemen gehören beispielsweise Telefonanlagen, die im Rahmen der Strukturanalyse erfasst werden müssen aber nicht zwangsläufig eine Netzanbindung besitzen.

Das Rechenzentrum nimmt die mit der öffentlichen Vermittlunsstelle verbundene Telefonanlage mit in die Erfassung der IT-Systeme auf.

Schritt 3 Erfassung der IT-Anwendungen

In einem Rechenzentrum kann zur Durchführung dieser Aufgabe auf bestehende *Systems Management Systeme* zurückgegriffen werden. Es muss jedoch kritisch hinterfragt werden, ob die dort hinterlegten Informationen vollständig und auf dem neuesten Stand sind. Wesentlich bei der Erfassung der IT-Anwendungen sind die mit den Anwendungen verarbeiteten Daten, da diese entscheidend die Bestimmung des Schutzbedarfs der Anwendung beeinflussen.

Bei der Erfassung der IT-Anwendungen muss bereits eine mögliche Gruppierung berücksichtigt werden. Hierbei werden einzelne Anwendungen im Sinne des GSHB zusammengefasst. Darüber hinaus muss eine Zuordnung von den IT-Anwendungen zu den IT-Systemen – also welche IT-Anwendungen auf welchen IT-Systemen laufen – dokumentiert werden. Hierzu bietet sich eine tabellarische Übersicht der Abhängigkeiten an.

In der Institution werden IT-Anwendungen zur Textverarbeitung, Adressverwaltung sowie E-Mail und WWW-Browser eingesetzt als Standardsoftware auf allen Systemen eingesetzt. Diese Anwendungen werden nicht einzeln erfasst, sondern zu einer Gruppe „Office-Paket“ zusammengefasst.Das Rechenzentrum betreibt fünf verschiedene Datenbanksysteme unterschiedlicher Hersteller. Die Daten werden hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität als Hoch-Schutzbedürftig angesehen und daher zu einer Gruppe zusammengefasst.

Zur Bestimmung von Sicherheitsmaßnahmen für neu einzuführende IT-Anwendungen wird die im GSHB dargelegte Vorgehensweise genutzt. Es wird jedoch bereits an dieser Stelle darauf hingewiesen, dass eine Zertifizierung nur für vorhandene IT-Systeme und IT-Anwendungen durchgeführt werden kann.

Die im Rahmen der Strukturanalyse erforderlichen Schritte sollten mit Hilfe des GSTOOL nachvollzogen und durchgeführt werden. Vorteile aus der konsequenten Nutzung des GSTOOL entstehen dadurch, dass beispielsweise mit Hilfe der Import-Funktionalitäten Daten über Zielobjekte aus bereits vorhandenen Verwaltungssystemen (Systems Management Systeme) übernommen werden können (vgl. Kapitel 9 in [GSTHB]).

5.2 Häufig auftretende Probleme bei der Strukturanalyse für einen großen IT-Verbund

In einem Rechenzentrum werden – anders als in homogenen Client-Umgebungen – viele verschiedene IT-Systeme mit unterschiedlichen IT-Anwendungen und unterschiedlichen Schutzbedürftigkeiten betrieben. Die Durchführung einer Strukturanalyse ist vor diesem Hintergrund komplizierter als bei kleineren IT-Verbänden.

In den nachfolgenden Abschnitten wird auf Probleme und Fragen im Zusammenhang mit der Erstellung einer Strukturanalyse für ein Rechenzentrum eingegangen. Dabei werden die Themenbereiche

- Informationserhebung,
- Netz- und Topologiepläne,
- Gruppenbildung,
- Erfassung von IT-Anwendungen und
- Erfassung von Kommunikationsverbindungen

besonders betrachtet.

5.2.1 Probleme bei der Informationserhebung

Die Erfassung der relevanten Komponenten ist alleine aufgrund der umfangreichen Infrastruktur in einem Rechenzentrum sehr aufwändig, sowie arbeits- und zeitintensiv.

Die nachfolgenden Unterabschnitte zeigen Probleme bei der Informationserhebung im Rahmen der Strukturanalyse auf, die typisch für eine große Institution sind und geben Hilfestellungen für eine effiziente Umsetzung.

5.2.1.1 Nutzungsmöglichkeiten vorhandener Informationen

Woher können die Informationen zur Strukturanalyse bezogen werden?

Im Gegensatz zu IT-Verbänden von kleineren oder mittleren Institutionen sind Rechenzentren meist gut organisiert und strukturiert. Die Verwaltung und Dokumentation der vorhandenen Infrastruktur wird in einem Rechenzentrum z.B. unterstützt durch

- Systems-Management Systems[2],
- Cable Management Software / Software für Kabelmanagement[3] und
- Facility Management Software / Gebäudemanagement Software[4].

Eine Dokumentation der vorhandenen Infrastruktur sollte damit bereits gegeben und jederzeit aktuell sein.

Durch den Einsatz von Dokumentations-Software (z.B. Systems-Management Systeme, Inventory Software, etc.) werden die wesentlichen Informationen automatisiert vorgehalten und verwaltet. Neben den IT-Systemen lassen sich auch die Systemkonfigurationen und – was für die Vorgehensweise nach GSHB relevant ist – die auf den Systemen installierten IT-Anwendungen einfach verwalten. Wird die Umsetzung des GSHB sorgfältig geplant, können zusätzliche Informationen (z.B. zum Schutzbedarf der IT-Anwendungen und IT-Systeme) mitverwaltet werden, was den Aufwand der nachfolgenden Schritte erheblich reduziert, da auf bereits vorhandene Informationen zugegriffen werden kann.

---

[2] www.ins.com/solutions/netsysmanage.asp oder
www3.ca.com/solutions/product.asp?id=2869

[3] www.crimp.com/SolutionsSec/Sol_main.html oder
www.access-networking.com/cablespec_pro.htm

[4] www.graphisoft.com/products/archifm/ oder www.fame-online.de/default_d.htm

Das GSTOOL bietet verschiedene Importfunktionen an. Man sollte daher prüfen, ob die vorhandene Dokumentations-Software eine Schnittstelle zum GSTOOL zur Verfügung stellt[5].

In einem RZ sind wahrscheinlich Zertifizierungen wie z.B. ISO 900x, BS 7799-2, schon durchgeführt worden. Die hierfür erstellte Dokumentation eignet sich sehr gut zur erweiterten Unterstützung.

5.2.1.2 Technik ändert sich schneller als Dokumentation

Bei der Installation neuer IT-Systeme und IT-Anwendungen sind die Mitarbeiter oft ausschließlich mit der Inbetriebnahme und Umsetzung beschäftigt und haben keine Zeit für die Pflege der Dokumentation, da meist das nächste Projekt wieder ansteht. Wie kann man dieses Problem entschärfen?

Aus diesen oder ähnlichen Gründen ist Dokumentation häufig ein vernachlässigter Punkt, da sie als lästig und unproduktiv empfunden wird.

Die Verpflichtung Dokumentation aktuell zu halten und den Mitarbeitern ausreichende Ressourcen für die Pflege der Dokumentation zu geben, sollte in der IT-Sicherheits-Leitlinie aufgenommen werden!

Die Dokumentation entspricht dann nicht den tatsächlichen Gegebenheiten, da sich die Technik schneller ändert, als die zugehörige Dokumentation. Die Aktualisierung der Dokumentation wird – wenn überhaupt – erst im nachhinein mit einer erheblichen zeitlichen Differenz durchgeführt. Es muss jedoch berücksichtigt werden, dass Dokumentation ein kontinuierlicher Prozess ist und Aufwände für die Erstellung von Dokumentation bereits in der Kalkulation von Projekten (z.B. Projektplänen) berücksichtigt werden müssen.

[5] Zielobjekt-Import aus Textdatei: Dieser Import übernimmt in Tabellenform bereitgestellte Zielobjekte aus TXT- und CSV-Dateien in die GSTOOL-Datenbank. Weitere Details hierzu finden sich im **Kapitel 9 (Export / Import)** im GSTOOL-Handbuch.

Je aktueller die Dokumentation ist, desto geringer ist der Aufwand, der während der Strukturanalyse für die Konsolidierung und Aktualisierung aufgebracht werden muss. Die Umsetzung des GSHB bietet eine gute Gelegenheit, um die vorhandene Dokumentation zu aktualisieren und einen permanenten Aktualisierungsprozess zu etablieren. Daher sollte eine Aktualisierung bereits frühzeitig initiiert werden!

5.2.1.3 Umgang mit im Aufbau befindlichen Systemen

Kann die Vorgehensweise des GSHB auch genutzt werden, wenn die Installation neuer IT-Systeme und IT-Anwendungen geplant werden?

Abhängig von Anforderungen durch Kunden, reguläre Produktzyklen und ständigen Weiterentwicklungen ist die Infrastruktur in einem Rechenzentrum einem ständigen Wandel unterzogen. Es stellt sich damit die Frage, was während der Strukturanalyse mit Komponenten geschehen soll, die gerade

- im Aufbau befindlich sind,
- im Abbau befindlich sind oder
- migriert werden.

Wesentlich ist, dass diejenigen Komponenten erfasst werden, die bei erstmaliger Fertigstellung des IT-Sicherheitskonzepts in Betrieb sind. Wichtig ist, dass das IT-Sicherheitskonzept in sich konsistent ist und die aktuelle Situation wiederspiegelt. Dies bedeutet insbesondere, dass auch IT-Systeme und IT-Anwendungen mit berücksichtigt werden, deren Außerbetriebnahme absehbar ist. Bleiben solche Systeme unberücksichtigt und werden im IT-Sicherheitskonzept nicht aufgenommen, sind Inkonsistenzen des IT-Sicherheitskonzepts absehbar.

Die Aktualität ist insbesondere für eine beabsichtigte Zertifizierung relevant, da im Rahmen der Zertifizierung auch die Konsistenz des IT-Sicherheitskonzepts mit dem IT-Verbund geprüft wird.

Bei derzeit in Planung befindlichen IT-Systemen dient das GSHB als Entwicklungshilfe (vgl. Kapitel 2.3 [GSHB]). Die auf den IT-Systemen umzusetzenden Standard-Sicherheitsmaßnahmen werden dann bereits in der Entwicklungsphase berücksichtigt. Nach Inbetriebnahme eines IT-Systems kann dieses nahtlos in das bestehende IT-Sicherheitskonzept integriert werden.

Die Institution setzt erstmals einen Webserver ein. Da bisher kein Mitarbeiter Erfahrungen über die Sicherheitsfunktionen der eingesetzten Anwendung besitzt, wird der entsprechende Baustein aus dem GSHB genutzt, um die umzusetzenden Sicherheitsfunktionen festzulegen.

5.2.1.4 Umfangreiche und komplexe Kommunikationsinfrastruktur

Die Kommunikations- und Netzwerkinfrastruktur ist sehr komplex. Welche Möglichkeiten gibt es, bei der Erfassung der Kommunikationsinfrastruktur die Komplexität zu reduzieren?

Bei der Erfassung der Kommunikationsverbindungen macht die große Anzahl der einzelnen Netzverbindungen auch hier die Vorgehensweise kompliziert und aufwändig.

Bei der Erfassung der Kommunikationsverbindungen bietet es sich wie in Kapitel 5.1 ausgeführt an, schrittweise zunächst die einzelnen Teilnetze und die dort befindlichen Kommunikationsverbindungen zu betrachten. Anschließend können die in den Teilnetzen erfassten Kommunikationsverbindungen konsolidiert werden.

Einen guten Ausgangspunkt für die Erfassung stellen in der Regel die Netzwerktopologiepläne dar, auf denen die physikalischen Netze dargestellt werden. Aufgrund der in Kapitel 5.2.5.1 erläuterten Problematik bezüglich der virtuellen Netze dürfen die Topologiepläne jedoch nicht als einzige Informationsquelle genutzt werden.

5.2.1.5 Daten lassen sich nicht in das GSTOOL importieren

Es wird bereits ein Systems Management Werkzeug zur Verwaltung der Systeme eingesetzt. Wie lassen sich die vorhandenen Daten importieren?

Rechenzentren besitzen – abhängig von ihrer Größe – bereits Informationssysteme, in denen für die GSHB-Vorgehensweise relevante Informationen hinterlegt sind. Hierzu gehören z.B. Informationen, die in Systems-Management Systemen hinterlegt sind. Eine direkte Anbindung dieser Systeme an das GSTOOL existiert derzeit nicht, so dass die Informationen aus Systems-Management Systemen per Dateiimport-Funktion übernommen werden müssen.

Werden Systems Management Systeme für die Verwaltung von Systemen eingesetzt, bietet es sich an, diese als zentrale Stelle für die Datenhaltung zu nutzen und die Daten anschließend in das GSTOOL zu importieren (vgl. Kapitel 9 [GSTHB]).

Für die Verwaltung der IT-Systeme und der IT-Anwendungen wird eine Systems- und Network-Management Lösung eingesetzt. Hierin sind alle Informationen bezüglich Betriebssystem, Netzwerkkonfiguration und installierter Anwendungen hinterlegt. Bereits im Rahmen der Strukturanalyse wurde auf die Informationen aus der Systems-Management Lösung zurückgegriffen.

Im Rahmen der Modellierung werden im Systems-Management System zusätzlich Informationen über die Modellierung vorgehalten. Hierbei wird beispielsweise festgehalten, dass der vorhandene IBM-Host mit dem IBM-Baustein des GSHB modelliert wird. Somit ist diese Information dokumentiert, obwohl dieser Baustein noch nicht im GSTOOL vorhanden ist.

5.2.2 Probleme mit Netz- und Topologieplänen

Eine vollständige Erfassung aller im definierten IT-Verbund vorkommenden Komponenten erfordert eine strukturierte Vorgehensweise auf der Basis von bereits vorhandener Dokumentation.

Diese kann in einem Rechenzentrum in Form von Topologieplänen bestehen, aus denen der im IT-Verbund betrachtete Netzplan generiert wird. Nachfolgend werden mögliche Probleme in diesem Zusammenhang benannt und evtl. vorhandene Lösungsansätze aufgezeigt.

5.2.2.1 Erstellung des Netzplans aus den Topologieplänen

Es existieren umfangreiche Topologiepläne. Wie können diese aufbereitet werden, ohne den Überblick zu verlieren?

Für die Erstellung eines Netzplans in einem Rechenzentrum muss häufig auf mehrere Topologiepläne zurückgegriffen werden, die konsolidiert und zusammengefasst werden müssen.

Um den Topologieplänen die Komplexität zu nehmen, kann z. B. der Bereich *Unix Server* als eigenes Teilnetz betrachtet werden. Dieses kann dann für sich geordnet, aktualisiert und konsolidiert werden. Anschließend werden dieses und alle anderen Teilnetze wieder zu einem großen Netzplan zusammengeführt.

Da die Erstellung eines Netzplans für die gesamte Infrastruktur in einem Schritt erfahrungsgemäß zu aufwändig ist, sollten zunächst Teilnetze definiert werden.

In komplexen Umgebungen bietet sich daher die Vorgehensweise an, zunächst Netzpläne für solche Teilnetze zu erstellen und diese später wieder zusammenzuführen.

Auch wenn sich hierdurch nicht der Gesamtaufwand reduzieren lässt, vereinfacht diese strukturierte Vorgehensweise die Erstellung eines Netzplans für eine komplexe Umgebung erheblich.

Häufig existieren bereits unterschiedliche „Sichten" auf die vorhandene Netzinfrastruktur, die z.B. das Gesamtnetz aus der Sicht verschiedener Kunden zeigt. In diesem Fall bietet sich die Definition einer zusätzlichen Grundschutz-Sicht an, mit der der Netzplan verwaltet werden kann. Dies hat den Vorteil, dass bestehende Werkzeuge genutzt werden können, um den für die Umsetzung des GSHB erforderlichen Netzplan zu erstellen.

5.2.3 Probleme bei der Gruppenbildung

Bei der Bildung von Gruppen ist die Kreativität, die Erfahrung und das Know-how des IT-Sicherheitsbeauftragten erforderlich und eine technische Unterstützung ist nur begrenzt möglich. Ein genaues Verständnis über die Methodik bleibt unabdingbar.

Lösungen für die nachfolgend genannten Probleme gibt es nur mittelbar und nur dort, wo eine Erhebung von Daten durchgeführt wird und eine technische Unterstützung möglich ist (z.B. durch Systems Management Systeme). Die sich hierdurch ergebenden Möglichkeiten sind jedoch stark davon abhängig, wie konsequent diese Werkzeuge im Vorfeld eingesetzt wurden und wie exakt die hinterlegten Informationen sind.

Je genauer und aktueller die bereits bestehende Dokumentation der Infrastruktur ist, desto einfacher sind die einzelnen Schritte!

5.2.3.1 Vom GSHB abweichende bereits vorhandene Gruppenbildung

Es bestehen bereits eigene Gruppierungen, können diese bestehen bleiben?

Aufgrund der komplexen Infrastruktur und der großen Anzahl einzelner IT-Systeme ist die Gruppenbildung in großen Institutionen besonders wichtig, um die Modellierung des IT-Verbundes handhabbar zu machen.

Oftmals sind IT-Systeme und Netzwerkkomponenten in der bereits bestehenden Dokumentation, den Netztopologieplänen und in der Verwaltungssoftware bereits in Gruppen gegliedert. Diese Gruppierung wird jedoch oftmals nach Typisierung oder räumlicher Zuordnung vorgenommen und ist daher für die Vorgehensweise nach GSHB nicht nutzbar. Eine Neugruppierung muss vorgenommen werden, die den Schutzbedarf berücksichtigt.

In einem Rechenzentrum ist es z.B. durchaus üblich, alle Backupserver in einer Gruppe *Backup-Systeme* aufzuführen. Werden hierbei aber auf einigen Servern Daten mit einem hohen Schutzbedarf gesichert, so müssen diese in einer eigenen Gruppe erfasst werden. Ebenso ist zu verfahren, wenn für Systeme eine identische Modellierung und Schutzbedarfsfeststellung durchgeführt wurde. In diesem Fall sind diese Gruppen zusammenzufassen (z.B. Windows 2000 Clients und Windows NT Clients, die als Arbeitsplatzsysteme genutzt werden, können in einer Gruppe zusammengefasst werden)

Da die Gruppenbildung des GSHB bei komplexen Infrastrukturen besonders aufwändig aber gleichzeitig sehr wichtig ist, ist es empfehlenswert, der Gruppenbildung und Neustrukturierung ausreichend Ressourcen zuzumessen.

Bei der Gruppenbildung sollte Schritt für Schritt vorgegangen werden, so dass im ersten Zug identische Systeme zusammen gefasst werden. Daraufhin werden diese einfachen Gruppen wiederum auf Gemeinsamkeiten geprüft. Weitere Zusammenfassungen sind möglich, wenn aus Sicht des GSHB keine relevanten Unterschiede existieren, wie z.B. unterschiedliche Schutzbedarfseinstufungen.

Sind die vorhandenen Systeme bereits zu Gruppen zusammengefasst, kann diese Gruppenbildung meist nicht für die Umsetzung des GSHB verwendet werden. Da meistens für die existierenden Gruppen umfangreiche Dokumen-

tationen existieren, bietet es sich an den GS-Gruppen die existierenden Gruppen zuzuordnen. So kann die bestehende Dokumentation weiterverwendet werden.

5.2.3.2 Komponenten dürfen nicht in verschiedenen Gruppen vorhanden sein

Manche Komponenten lassen sich mehreren Gruppen zuordnen. Sollen diese dann auch mehrfach angegeben werden?

Lassen sich IT-Anwendungen oder IT-Systeme zunächst nicht eindeutig einer Gruppe zuordnen, werden sie fälschlicherweise oft unterschiedlichen Gruppen zugewiesen und tauchen somit mehrfach (in verschiedenen Gruppen) auf.

Die *externe Firewall* wird als Router und Firewall eingesetzt. Aufgrund dieser doppelten Verwendung könnte bei einer schlecht gewählten Gruppierung (Gruppe aller *Router* und Gruppe aller *Firewalls*) das System mehrfach aufgelistet werden. In diesem Fall ist es besser, das System separat aufzulisten.

Komponenten dürfen nur in genau einer Gruppe vorkommen! Sind Komponenten in verschiedenen Gruppen vertreten, deutet dies auf eine fehlerhafte Gruppenbildung / -definition hin.

Sind identische Komponenten mit gleichem Schutzbedarf in verschiedenen Gruppen vertreten, muss die Gruppierung derart angepasst werden, dass jede Komponente nur in genau einer Gruppe vertreten ist.

Aus Redundanz- oder Performancegründen werden in Rechenzentren häufig mehrere Server – die dieselbe Aufgabe wahrnehmen – zu Clustern zusammengeschaltet. Derartige Cluster lassen sich sehr gut und einfach zu Gruppen zusammenfassen.

5.2.3.3 Fehlende Zuordnung der Verantwortlichkeit

Für einige Komponenten ist kein direkter Verantwortlicher definiert. Dies ist damit begründet, dass diese Komponente „schon lange“ in der Institution vorhanden ist und jeder darauf aufpasst. Reicht das nicht?

Sicherheit setzt ein gewisses Maß an Ordnung voraus. Undurchsichtige Infrastrukturen, nicht dokumentierte oder nicht auffindbare, aber aktive Systeme, sowie auch unklare Verantwortlichkeiten wirken sich negativ auf das Sicherheitsniveau eines IT-Verbundes aus. Wenn nicht klar ist, was zu schützen ist und wer es schützen soll, kann es nicht geschützt werden!

Oft bestehen auch in Rechenzentren historisch gewachsene unklare Strukturen, die aufgrund sich ändernder Kundenanforderungen oder kurzfristigen Entscheidungsumsetzungen entstehen. Dabei wird die Zuweisung der Verantwortlichkeit vernachlässigt und nicht weiter verfolgt.

Die Vorgehensweise des GSHB erfordert jedoch eine strukturierte Vorgehensweise und eine klar erkennbare Struktur in der Dokumentation der Infrastruktur. So wird ein dauerhaft angemessenes Sicherheitsniveau erreicht.

Bei richtiger Anwendung des GSHB kann dies nicht vorkommen, da ein IT-Verantwortlicher in der Dokumentation aufgeführt und eine Vertretungsregelung bestehen muss.

Dieser Fall kann jedoch auftauchen, wenn das GSHB zum ersten Mal angewendet wird, oder eine in den Hintergrund geratene Komponente auftaucht, bzw. eine übersehene Komponente aufgefunden wird. In diesem Fall muss unverzüglich ein IT-Verantwortlicher bestimmt und diesem die notwendigen Ressourcen zur ordentlichen Betreuung der Komponente zur Verfügung gestellt werden (Schulung, Dokumentation etc.).

Wird das GSHB nicht „gelebt“, d.h. z.B. die vorhandene Dokumentation nicht regelmäßig aktualisiert, kann dies zu dem oben genannten Problem führen.

5.2.3.4 Verteilte Informationen/Verantwortlichkeiten

Die für die Gruppenbildung erforderlichen Informationen sind nicht von einem einzelnen Ansprechpartner erhältlich, da sie auf verschiedene Ansprechpartner verteilt sind. Wie sollen die Informationen eingeholt werden, wenn keine klaren Verantwortlichkeiten definiert sind?

Die Informationsbeschaffung ist der wesentliche Schritt der Strukturanalyse. Bereits in der IT-Sicherheitsleitlinie sollte daher eine Informationspflicht verankert werden, die eine Unterstützung des IT-Sicherheitsbeauftragten bei der Erstellung des IT-Sicherheitskonzepts gewährleistet. Die Einholung der Informationen im Rahmen eines Workshops ist dann eine geeignete Möglichkeit, effektiv alle Ansprechpartner präsent zu haben.

Die Systembetreuung in der Institution ist kundenorientiert organisiert, d.h. ein Team betreut die Systeme eines Kunden. Dies hat zur Folge, dass identische Systeme unterschiedlicher Kunden, von unterschiedlichen Teams betreut werden. Ein eindeutiger Ansprechpartner lässt sich nicht finden, der IT-Sicherheitsbeauftragte wird von einem Ansprechpartner zum nächsten verwiesen.

In der IT-Sicherheitsleitlinie ist die Unterstützungspflicht verankert. Mit Verweis auf diese Unterstützungspflicht koordiniert der IT-Sicherheitsbeauftragte Workshops an denen Vertreter der einzelnen „Kundenteams“ teilnehmen, die identische Systeme unterschiedlicher Kunden verwalten.

Durch eine in der IT-Sicherheitsleitlinie verankerte Informations- und Unterstützungspflicht lassen sich die Möglichkeiten des IT-Sicherheitsbeauftragten ausweiten und die Mitarbeiter zur Unterstützung verpflichten.

5.2.3.5 Zu feine Gruppenbildung

Der IT-Verbund weist viele Gruppen mit wenigen Komponenten auf, welche negativen Auswirkungen kann dies haben?

Durch eine zu feine Gruppenbildung kann es vorkommen, dass Bausteine zu oft auf ähnliche Gruppen angewandt werden müssen. Damit steigt der Aufwand während der nachfolgenden Phasen erheblich. Beim Basis-Sicherheitscheck kann es so vorkommen, dass identische Antworten in verschiedenen Bausteinen gegeben werden,

Das Rechenzentrum betreibt verschiedene Windows-Server Farmen für unterschiedliche Kunden. Die Server-Farmen der einzelnen Kunden werden jeweils zu Gruppen zusammengefasst. Als Ergebnis sind mehrere Gruppen vorhanden, in denen Windows-Datenbankserver zusammengefasst sind.

Im Rahmen der Modellierung wird festgestellt, dass die einzelnen Gruppen identisch modelliert werden. Die Schutzbedarfsfeststellung hat ergeben, dass auch ein identischer Schutzbedarf gefordert wird. Die Gruppen werden daraufhin zusammengefasst.

5.2.4 Probleme bei der Erfassung von IT-Anwendungen

Die Probleme bei der Erfassung der IT-Anwendungen entsprechen im wesentlichen den Problemen bei der Erfassung der IT-Systeme und ergeben sich aus der großen Anzahl der vorhandenen Systeme und darauf vorhandenen IT-Anwendungen. Auch hier ist eine technische Unterstützung (z.B. durch Systems-Management Systeme) möglich, jedoch unterliegt sie denselben Einschränkungen wie bei den IT-Systemen.

5.2.4.1 Müssen alle Anwendungen eines IT-Systems erfasst werden?

Was macht man mit all den kleinen Tools*, die für den RZ-Betrieb benutzt werden. Sind das alles einzelne IT-Anwendungen im Sinne des GSHB?*

Werden alle „kleinen“ IT-Anwendungen einzeln erfasst, führt dies schnell zu einer unübersichtlichen Strukturanalyse. Um hier Abhilfe zu schaffen, werden „kleine“ IT-Anwendungen, die einen identischen Schutzbedarf aufweisen, einer Anwendungsgruppe zugeordnet.

Im Rechenzentrum werden verschiedene Scripte eingesetzt, die die Erreichbarkeit der Datenbanken, Web- und Mailserver überprüfen. Im Fehlerfall wird das Operating informiert. Der Schutzbedarf dieser Scripte wird hinsichtlich der drei Grundwerte als normal eingestuft.

Das Rechenzentrum gruppiert diese Scripte in eine Gruppe „Verfügbarkeits-Script“.

5.2.4.2 Unterschiedliche Klassifizierung der IT-Anwendung auf verschiedenen Plattformen

Wie geht man mit einer IT-Anwendung um, die auf verschiedenen Plattformen unterschiedlich klassifiziert wird?

In einem Rechenzentrum wird eine IT-Anwendung oft auf unterschiedlichen Plattformen betrieben. Bei der Gruppierung ist nicht die Anwendung an sich relevant, sondern die mit ihr verarbeiteten Daten. Nur wenn unterschiedlich schutzbedürftige Daten verarbeitet werden, muss dies bei der Erstellung der Strukturanalyse entsprechend berücksichtigt werden.

Apache Webserver werden sowohl unter Windows als auch unter Linux betrieben. Dabei enthalten z. B. die Webserver unter Linux höher schutzbedürftige Daten als die unter Windows betriebenen. Dies muss bei der Zuordnung in unterschiedliche Gruppen (*Windows Webserver* und *Linux Webserver*) unbedingt beachtet werden.

Die IT-Anwendung bestimmt nicht die endgültige Gruppierung, sondern dient nur einer ersten Zuordnung. Eine abschließende Gruppierung muss

immer anhand der Schutzbedürftigkeit der mit ihr verarbeiteten Daten stattfinden.

5.2.4.3 „Sich in Details verlieren“

Es existieren so viele IT-Anwendungen, und bei jeder einzelnen muss man erneut überlegen, wie diese zusammengefasst werden. Ist jede Anwendung relevant?

Um sich bei der Erfassung der IT-Anwendungen auf die Wesentlichen zu konzentrieren, ist die Beantwortung der nachfolgend genannten Fragen hilfreich. Sie bieten eine Hilfestellung bei der Bestimmung der Relevanz einer Anwendung:

- Welche Aufgabe hat die Anwendung?
- Wer nutzt die Anwendung?
- Welche Auswirkungen hat der Ausfall der Anwendung?
- Welche Daten werden mit der Anwendung verarbeitet?
- Welche Auswirkungen hat der Verlust dieser Daten?
- Welche Auswirkungen hat es, wenn die Anwendung fehlerhafte Daten liefert?

IT-Anwendungen, die für die Funktionalität eines Systems und die Erfüllung der primären Aufgabe nicht relevant sind, sollten nicht erfasst werden.

5.2.5 Probleme bei der Erfassung von Kommunikationsverbindungen

Die Erfassung der Kommunikationsverbindungen ist üblicherweise kein besonders problematischer Schritt. Er ist jedoch mit verschiedenen „Fallen“ versehen.

Insbesondere stellen die umfangreiche Netztopologie und die nicht-physikalischen (virtuellen) Kommunikationsverbindungen häufig ein Problem dar, welches manchmal erst bei einer Überprüfung des IT-Sicherheitskonzepts (z.B. im Rahmen einer Zertifizierung) erkannt wird.

Durch die vorhandenen elektronischen Dokumentationswerkzeuge (z.B. Cable Management Systeme) wird dem IT-Sicherheitsbeauftragten ein Grossteil der Arbeit abgenommen. Voraussetzung hierbei ist jedoch auch in diesem Fall, dass die vorhandene Dokumentation aktuell ist und ständig an die Gegebenheiten angepasst wurde.

5.2.5.1 Unbekannte und nicht dokumentierte Kabelverbindungen

Es existieren temporär gezogene Verbindungen, die für diese kurze Zeit gar nicht erst im Cable Management System erfasst werden, wie geht man mit diesen um?

Oft werden in Rechenzentren temporäre Verbindungen für einen beschränkten Zeitraum aufgebaut, um Funktionalitäten zu testen oder ein Problem durch Umstecken der Datenverbindung zu umgehen. Der Mitarbeiter „*erinnert*“ sich daran und „*kümmert sich darum*“ sobald das Problem korrigiert wurde. Dies wird oft versäumt und daher nicht dokumentiert oder erfasst. Daher geben Dokumentationen zu Kommunikationsverbindungen oftmals nicht den aktuellen Stand der Verkabelungen wieder.

Wird ein defekter Port an einem Core-Router festgestellt, an den ein wichtiger Kunde angeschlossen ist, wird dieses Kundensystem kurzfristig auf einen anderen Port umgesteckt. Dies wird anschließend nicht dokumentiert und es besteht die Gefahr, dass dies schnell in Vergessenheit gerät.

Auch temporäre Kabelverbindungen sollten immer dokumentiert werden. Hierbei hilft ein vereinfachtes Formblatt, in dem die temporäre Kabelverbindung dokumentiert und erst nach entfernen des Kabels ausgetragen werden darf.

5.2.5.2 Probleme durch virtuelle Verbindungen

Stellen virtuelle Verbindungen auch zu erfassende Kommunikationsverbindungen nach dem GSHB dar?

Neben den physikalisch existierenden Verbindungen müssen auch virtuelle Verbindungen erfasst werden. Dies kann z.B. tabellarisch erfolgen oder durch eine besondere Kennzeichnung der virtuellen Verbindungen innerhalb des Netzplans.

Aufgrund der ohnehin sehr komplexen Netzinfrastruktur in Rechenzentren werden virtuelle Verbindungen häufig übersehen, obwohl gerade sie aufgrund hoher Schutzbedürftigkeit (z.B. hohe erforderliche Vertraulichkeit) eingerichtet wurden.

Sie sind damit als kritische Kommunikationsverbindungen einzustufen und im Rahmen der Schutzbedarfsfeststellung von besonderer Bedeutung!

Beispiele für virtuelle Verbindungen sind *Virtual Private Networks (VPNs)*, welche zur Anbindung von Kundennetzen eingerichtet und betrieben werden.

Einen Hinweis auf existierende virtuelle Verbindungen geben häufig die Filterlisten von Firewall-Systemen oder vorhandene VPN-Gateways, die für die Einrichtung verschlüsselter Kommunikationsverbindungen eingesetzt werden. Bei der Erfassung der Kommunikationsverbindungen sollten daher die Konfigurationen dieser Systeme berücksichtigt werden.

Zusätzlich bietet es sich an, bei jeder IT-Anwendung (und damit bei jedem IT-System) zu überlegen, mit welchen anderen Anwendungen bzw. Systemen Kommunikationsbeziehungen bestehen, wie diese realisiert sind und ob diese im Netzplan erfasst wurden.

6 Schutzbedarfsfeststellung

Das Ziel der Schutzbedarfsfeststellung (vgl. Kapitel 2.2 [GSHB]) ist die Bestimmung des Schutzbedarfs für alle Komponenten des IT-Verbundes einschließlich ihrer Daten. Dieser Schutzbedarf wird bezüglich der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit der Daten ermittelt.

Bild 3: Goldbarren

Bei der Schutzbedarfsfeststellung treten insbesondere dadurch Probleme auf, dass die Auffassung zum Schutzbedarf des Kunden vom Schutzbedarf aus der Sicht der Institution getrennt werden muss. Wichtig ist, dass lediglich der Schutzbedarf aus der Sicht der Institution betrachtet werden darf.

Grosse Institutionen müssen verschiedenen Sicherheitsanforderungen genügen. Neben den eigenen Sicherheitsanforderungen müssen insbesondere auch die Anforderungen der Kunden berücksichtigt werden. Diese gehen üblicherweise in die mit den Kunden geschlossenen Verträge (z.B. Service-Level-Agreements) mit ein.

Rechenzentren sollten für alle Bereiche ein grundsätzlich hohes Sicherheitsniveau anstreben und damit einen hohen Schutzbedarf bei allen Systemen wählen. Nur so kann sichergestellt werden, dass alle Sicherheitsanforderungen abgedeckt sind.

6.1 Generelle Vorgehensweise bei der Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung für die im IT-Verbund vorhandenen Komponenten orientiert sich an denkbaren möglichen Schäden, die zu Beeinträchtigungen führen können.

Die Schutzbedarfsfeststellung besteht hauptsächlich aus einer Vorbereitungsphase, bei der die Schutzbedarfskategorien definiert, mögliche Schadensszenarien betrachtet und die Ergebnisse dokumentiert werden, sowie der Durchführung der Schutzbedarfsfeststellung bei allen Komponenten des IT-Verbundes.

Die Schutzbedarfsfeststellung besteht aus den folgenden fünf Schritten:

Schritt 1 Vorbereitungen

Zunächst werden die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ definiert. Hierzu werden verschiedene Schadensszenarien betrachtet, die zu einem Schaden beim Verlust der Verfügbarkeit, Vertraulichkeit oder Integrität einer IT-Anwendung einschließlich ihrer Daten entstehen können. Betrachtet werden hierbei üblicherweise die Schadensszenarien

- Verstoß gegen Gesetze/Vorschriften/Verträge,

Ein Verstoß gegen einen Vertrag kann bereits dann eintreten, wenn zugesagte Verfügbarkeiten nicht erreicht werden. In der Regel sind in den Verträgen auch die Konsequenzen festgehalten.

- Beeinträchtigung des informationellen Selbstbestimmungsrechts,

Das informationelle Selbstbestimmungsrecht ist bereits beeinträchtigt, wenn Daten eines Kunden durch einen Fehler an einen anderen Kunden oder an die Öffentlichkeit gelangen.

- Beeinträchtigung der persönlichen Unversehrtheit,

Dieser Fall tritt z.B. durch Fehlfunktionen in IT-gestützten Narkosesystemen oder Bestrahlungsapparaten auf, bei denen ein Menschenleben gefährdet ist.

- Beeinträchtigung der Aufgabenerfüllung,

Der Ausfall eines Trouble-Ticket Systems kann bereits die Aufgabenerfüllung eines Kundendienstes beeinträchtigen.

- negative Außenwirkung

Für ein Rechenzentrum sind prinzipiell alle Sicherheitsprobleme mit negativen Außenwirkungen verbunden.

- und finanzielle Auswirkungen.

Für eine Bank wäre der Ausfall eines Zahlungsverkehrssystem ein Vorfall mit direkten finanziellen Auswirkungen.

Die Schadensszenarien werden genutzt, um die einzelnen Schutzbedarfsklassen voneinander abzugrenzen. Hierbei werden die Schadensszenarien für jede Schutzbedarfsklasse konkretisiert.

Komponenten mit niedrigem Schutzbedarf dürfen maximal geringfügige Konsequenzen bei Verstößen gegen Vorschriften oder Gesetzte zur Folge haben. Vertragsverletzungen verursachen höchstens geringfügige Konventionalstrafen.

Die Definition der Schutzbedarfskategorien sowie der betrachteten Schadensszenarien sind Bestandteil des IT-Sicherheitskonzepts.

Schritt 2 IT-Anwendungen

Bei der Schutzbedarfsfeststellung von IT-Anwendungen wird anhand der durch sie verarbeiteten Daten entschieden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Der Schutzbedarf der IT-Anwendung leitet sich somit direkt aus dem Schutzbedarf der verarbeiteten Daten ab. Für jede IT-Anwendung wird festgehalten, welche möglichen Schäden bei einer Beeinträchtigung der IT-Anwendung bzw. der verarbeite-

ten Daten entstehen können. Der Schutzbedarf orientiert sich direkt an diesen Schadensausmaßen.

Für die Mailserver-Anwendung des IT-Verbundes wird folgende Kategorisierung vorgenommen:

- **Vertraulichkeit**: *hoch*, da im Rahmen des Trouble-Ticket-Systems vertrauliche Daten behandelt werden und eine Kompromittierung einen großen Imageschaden verursacht, der mit Kosten von bis zu 2,3 % des Jahresumsatzes geschätzt wird.
- **Verfügbarkeit**: *hoch*, da der gesamte Kundensupport incl. Trouble-Ticket-System insbesondere über Email abgewickelt wird und ein längerer Ausfall kritisch ist, da Supportverträge mit hohen Vertragsstrafen existieren, wenn die vertraglich vereinbarte Reaktionszeit von meist 30 Minuten überschritten wird.
- **Integrität**: *hoch*, da aufgrund der per Email eingereichten Störungen Handlungen wie z. B. eine Neuinstallation durchgeführt werden. Werden diese Daten unbemerkt verfälscht, kann eine solche Neuinstallation unberechtigt angewiesen werden. Die Kosten hierfür können bis zu 4,2 % des Jahresumsatzes betragen.

Schritt 3 IT-Systeme

Bei der Ermittlung des Schutzbedarfs der IT-Systeme wird der Schutzbedarf der auf dem IT-System laufenden Anwendungen auf das System übertragen. Ausgehend von den 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 Vorgehensweisen Maximum-Prinzip, Beachtung von Abhängigkeiten, Kumulationseffekt und Verteilungseffekt unterschieden.

Beim *Maximum-Prinzip* bestimmt sich der Schutzbedarf eines IT-Systems aus dem möglichen Schaden mit den schwerwiegendsten Auswirkungen.

Die *Betrachtung von Abhängigkeiten* kommt zum Tragen, wenn die Funktionsfähigkeit eines IT-Systems oder einer IT-Anwendung von anderen IT-Systemen/IT-Anwendungen abhängig ist. In diesem Fall wird der Schutzbedarf von der einen Komponente auf die andere übertragen (z. B. wenn eine Anwendung eine Datenbank eines anderen IT-Systems nutzt).

Der *Kumulationseffekt* besagt, dass sich der Schutzbedarf des IT-Systems erhöht, 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.

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

Schritt 4 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-Raums festzustellen, müssen die im jeweiligen IT-Raum aufgestellten IT-Systeme betrachtet werden. Der Schutzbedarf dieser IT-Systeme wird auf den Raum übertragen, er „vererbt“ sich somit von den IT-Systemen auf den IT-Raum. Eine

Übersicht, für welche IT-Räume eine Schutzbedarfsfeststellung durchzuführen ist, wurde bei der Strukturanalyse erfasst.

Schritt 5 Kommunikationsverbindungen

Die Schutzbedarfsfeststellung von Kommunikationsverbindungen unterscheidet sich von der Schutzbedarfsfeststellung der IT-Anwendungen, IT-Systeme und IT-Räume, da sie lediglich der Identifikation kritischer Verbindungen dient. 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 eines hohen Integritätsschutzes bedürfen,
- ob die übertragenen Informationen einer hohen Verfügbarkeit bedürfen

und

- ob hochschutzbedürftige Informationen nicht übertragen werden dürfen.

Es bietet sich an die kritischen Verbindungen direkt im Netzplan hervorzuheben und im GSTOOL als solche zu markieren.

Nach erfolgreich durchgeführter Schutzbedarfsfeststellung steht fest, welche Daten und dadurch abgeleitet auch welche IT-Anwendungen, IT-Systeme und IT-Räume eine normale, hohe bzw. sehr hohe Schutzbedürftigkeit aufweisen. Zusätzlich wurden kritische Kommunikationsverbindungen ermittelt.

6.2 Häufig auftretende Probleme bei der Schutzbedarfsfeststellung für einen großen IT-Verbund

Mit der zunehmenden Größe eines IT-Verbundes nimmt die Homogenität der IT-Landschaft ab. Es werden viele verschiedene IT-Systeme mit unterschiedlichen IT-Anwendungen und unterschiedlichen Schutzbedürftigkeiten betrieben. Bei der Durchführung einer Schutzbedarfsfeststellung sind daher verschiedene Problematiken zu beachten.

In den nachfolgenden Abschnitten wird auf Probleme und Fragen im Zusammenhang mit der Durchführung einer Schutzbedarfsfeststellung in einer großen Institution eingegangen. Hierbei werden die im vorangegangen Abschnitt genannten Themenbereiche betrachtet.

6.2.1 Probleme bei der Definition der Schutzbedarfsklassen

In gewachsenen Strukturen hat sich oft ein Sicherheitsempfinden entwickelt, welches sich nicht in jedem Fall mit der formalen Vorgehensweise des GSHB in Einklang bringen lässt. Unterschiedliche Sicherheitsempfindungen oder die Frage, wie der Schutzbedarf von Kunden berücksichtigt werden soll, sind nur zwei Beispiele der auftretenden Probleme.

6.2.1.1 Kein unternehmensweiter Konsens über die Definition der Schutzbedarfsklassen

Es gelingt nicht, ein einheitliches Verständnis über die drei Schutzbedarfsklassen festzulegen. Wie geht man mit unterschiedlichen Vorstellungen von Schutzbedarf um?

Je größer der IT-Verbund ist, desto schwieriger ist es, ein einheitliches Schutzbedarfsempfinden zu erhalten. Die Auffassung darüber, wie ein Schaden einzuschätzen und eine Schutzbedarfsklasse zu definieren ist, variiert mit der Anzahl der befragten Personen und deren subjektiven Einschätzungen. Zwei Personen können grundsätzlich stark unterschiedliche Aussagen

über die Einstufung eines Schadens vertreten. Ziel der Definition von Schutzbedarfsklassen ist es jedoch, ein einheitliches Verständnis über Schutzbedarfsklassen zu erhalten.

Die Auffassung über einen „normalen“ Schutzbedarf hinsichtlich der Verfügbarkeit einer Komponente gehen in der Institution stark auseinander. Das für die Windows-Server zuständige Team sieht einen Ausfall von zwei Stunden als überschaubar an. Das ist für das für die Unix-Server zuständige Team nicht nachvollziehbar, hier wird ein Ausfall von zwei Stunden als beträchtlich angesehen. Eine einheitliche Definition der Schutzbedarfsklassen würde nicht zustande kommen.

Der IT-Sicherheitsbeauftragte hält mit den Sicherheitsverantwortlichen einen Workshop ab und erarbeitet für die Leitung eine Entscheidungsvorlage mit definierten Schutzbedarfsklassen. Die oberste Leitung muss abschließend diese Schutzbedarfsklassen prüfen und verabschieden.

Die Schutzbedarfsklassen werden grundsätzlich durch die oberste Leitung vorgegeben. Das IT-Sicherheitsmanagement-Team erarbeitet hierfür eine Entscheidungsvorlage, die anschließend von der Leitung geprüft und verabschiedet wird.

Ursache für das dargestellte Problem ist z.B. ein historisch gewachsenes Sicherheitsbewusstsein.

Langfristig muss das intern vorhandene Sicherheitsempfinden mit den definierten Schutzbedarfsklassen harmonisiert werden. Dies bedeutet insbesondere, dass den Mitarbeitern die Schutzbedarfsklassen erläutert werden müssen, so dass sich das Verständnis vom Schutzbedarf den definierten Schutzbedarfsklassen angleicht.

Hierzu ist es hilfreich, alle Begründungen nachvollziehbar zu dokumentieren.

6.2.1.2 Trennung des eigenen Schutzbedarfs von dem des Kunden

Für Kunden werden IT-Systeme betrieben. Was ist, wenn für den Kunden die Verfügbarkeit des Systems unverzichtbar ist?

Die Kundenanforderungen bezüglich des Schutzbedarfs gehen nur mittelbar in die Schutzbedarfsfeststellung des Rechenzentrums ein.

*Im Rahmen der Schutzbedarfsfeststellung muss primär die Frage geklärt werden: „*Welche Auswirkung hat der Schaden auf die Institution?*“. Die Frage „*Welche Auswirkung hat der Schaden auf den Kunden?*“ geht hierbei nur dann mit ein, wenn dieser Schaden direkte Auswirkungen auf die Institution hat (z. B. wenn hieraus Regressforderungen abgeleitet werden können).*

Einem Kunden des Rechenzentrums entsteht durch den eintägigen Ausfall eines beim Rechenzentrum betriebenen WWW-Servers ein finanzieller Schaden von 15.000 EUR. Das Rechenzentrum ist für den Schaden verantwortlich, eine grobe Fahrlässigkeit liegt jedoch nicht vor. Der Schaden wird vom Kunden als „sehr hoch“ angesehen.

Aufgrund der vertraglichen Gegebenheiten gewährleistet das Rechenzentrum eine Verfügbarkeit von 99,7% pro Jahr. Erst bei geringerer Verfügbarkeit ist das Rechenzentrum beim Ausfall von Servern haftbar. Somit liegt der eintägige Ausfall des Systems innerhalb der zugesicherten Verfügbarkeit und der Ausfall hat keine Auswirkungen auf das Rechenzentrum.

6.2.1.3 Schutzbedarfsklassen des GSHB nicht ausreichend fein gegliedert

Es sind in der Institution feinere Schutzbedarfsklassen etabliert als die drei durch das GSHB vorgegebenen, müssen die etablierten Klassen nun auf die Schutzbedarfsklassen des GSHB umgestellt werden?

Häufig reichen die drei Schutzbedarfsklassen des GSHB nicht für die Zwecke einer großen Institution aus (z.B. innerhalb von Banken), da hier eine

feinere Unterscheidung benötigt wird und gegebenenfalls bereits in existierenden Vertragswerken eingeflossen ist. Eine Änderung der etablierten Schutzbedarfsklassen ist damit nicht ohne weiteres möglich.

Sind bereits Schutzbedarfsklassen in der Institution etabliert, lassen sich diese selten durch die Schutzbedarfsklassen des GSHB ersetzen. Das GSHB sieht jedoch nicht zwingend drei Schutzbedarfsklassen vor. Alternative Schutzbedarfsklassen sind möglich, nur lässt sich dann das GSTOOL nicht ohne Probleme anwenden.

Lösung 1: Beibehaltung etablierter Schutzbedarfsklassen

Die etablierten Schutzbedarfsklassen der Institution können beibehalten werden, beachtet werden muss hierbei jedoch, dass die im GSHB genannte Vorgehensweise für die Definition der Schutzbedarfsklassen (insbesondere die Betrachtung von Schadensszenarien) gegebenenfalls nachträglich erfolgen muss. Werden die etablierten Schutzbedarfsklassen weitergenutzt, kann das GSTOOL nicht verwendet werden, da hierin fest drei Schutzbedarfsklassen vorgesehen sind.

Lösung 2: Abbildung der etablierten auf die durch das GSHB vorgegebenen Schutzbedarfsklassen

Die zweite Möglichkeit besteht in der Abbildung (auch Mapping genannt) der etablierten Schutzbedarfsklassen auf die drei im GSHB erwähnten Schutzbedarfsklassen.

Die Methode des Mapping ist in der nachfolgenden Tabelle dargestellt, und wurde für den in Kapitel 3 definierten IT-Verbund verwendet. Etabliert sind hier bereits fünf Schutzklassen, die den drei Schutzklassen des GSHB gegenübergestellt werden müssen. Der Schutzbedarfsklasse „normal“ (dargestellt als GS-normal) wird hierbei z. B. die höherwertige maximale Ausfallzeit von 8 Stunden zugewiesen und umfasst damit die etablierten Schutzbedarfsklassen „unbedeutend“ und „niedrig“.

Schutzbedarfsklasse		Maximal tolerierte Ausfallzeit
Etabliert	nach GSHB	
Unbedeutend	G -normal	24 Stunden
Niedrig		8 Stunden
Mittel	G -hoch	1 Stunde
Hoch	G -sehr hoch	15 Minuten
existenzbedrohend		1 Minute

Werden die etablierten Schutzbedarfsklassen auf die des GSHB abgebildet, ist die Nutzung des GSTOOL möglich.

Diese Vorgehensweise ist insbesondere dann empfehlenswert, wenn das GSTOOL abgewandt werden soll aber Schutzbedarfsklassen z. B. in Verträgen mit Kunden fixiert sind.

6.2.2 Probleme bei den IT-Anwendungen

Bei der Schutzbedarfsfeststellung von IT-Anwendungen muss berücksichtigt werden, dass dieser immer ausgehend von den durch die Anwendung verarbeiteten Daten festzulegen ist. Problematisch wirken sich oft Fehler in der Gruppenbildung und einem falschen Verständnis der Schutzbedarfsfeststellung von IT-Anwendungen aus.

6.2.2.1 Zu grobe Gruppenbildung verhindert Kategorisierung der IT-Anwendungen

Die Art der IT-Anwendungen innerhalb der Gruppe ist ähnlich (z.B. ähnliche Datenbanken), aber die verarbeiteten Daten weisen unterschiedliche Schutzbedürftigkeiten aus, was nun?

Häufig wirkt sich eine zu grobe Gruppierung der einzelnen IT-Anwendungen, also die Zusammenfassung zu vieler unterschiedlicher Anwendungen zu einer Gruppe, negativ aus. Hieraus ergibt sich dann das Prob-

lem, dass eine einheitliche Schutzbedarfsfeststellung und Modellierung nicht möglich ist, da sich die Schutzbedürftigkeit der einzelnen Anwendungen der Gruppe zu stark unterscheidet. Eine neue Gruppierung ist in diesem Fall erforderlich.

Der IT-Sicherheitsbeauftragte definiert eine Gruppe „Datenbanken“, in die alle Datenbankanwendungen aufgenommen werden. Bei zwei der in der Gruppe enthaltenen Datenbanken werden personenbezogene Daten gespeichert, so dass sie hinsichtlich der Vertraulichkeit einen hohen Schutzbedarf erfordern. Mit den übrigen Datenbanken werden lediglich unkritische Daten verwaltet. Eine einheitliche Schutzbedarfsdefinition ist nicht möglich und sinnvoll.

Der IT-Sicherheitsbeauftragte gruppiert die zwei Datenbanken, mit denen personenbezogene Daten gespeichert werden, in einer separaten Gruppe, so dass zwei Gruppen von Datenbanken („Datenbanken“ und „Datenbanken hohe Vertraulichkeit“) bestehen.

Unterscheiden sich die Schutzbedürftigkeiten der zu einer Gruppe gehörenden Anwendungen zu stark, so dass keine eindeutige Schutzbedarfsfeststellung für diese Gruppe durchgeführt werden kann, muss die Gruppierung erneut durchgeführt werden. Die Gruppe muss dabei aufgeteilt und derart umgestaltet werden, dass eine Schutzbedarfsfeststellung dasselbe Ergebnis für alle Anwendungen der Gruppe ergibt.

6.2.2.2 Keine Trennung des Schutzbedarfs

Muss der Schutzbedarf hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität immer getrennt betrachtet werden oder reicht es aus nur einen gesamten Schutzbedarf zu betrachten?

Oft wird nur ein gesamter Schutzbedarf festgelegt und keine Trennung hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität vorgenommen. Dies entspricht nicht der Vorgehensweise des GSHB und führt spätestens bei der

Maßnahmenauswahl zu Problemen. Dann kann jedoch nicht mehr entschieden werden, ob eine spezielle Maßnahme ausreichend oder bereits überflüssig ist.

Eine Schutzbedarfsfeststellung muss immer hinsichtlich der drei Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität erfolgen.

6.2.2.3 Uneinheitliche Schutzbedarfsfeststellung

Bei der Bestimmung des Schutzbedarfs einer Komponente müssen verschiedene Personen innerhalb der Institution gefragt werden. Wie geht man vor, wenn die Aussagen über den Schutzbedarf der Komponente uneinheitlich sind?

Wie bereits erwähnt, ist hierzu die erschöpfende Antwort auf die Fragestellung „*Welche Auswirkung hat der Schaden auf die Institution?*“ relevant.

Häufig besteht jedoch das Problem, dass die technischen Ansprechpartner den Schutzbedarf zu hoch einschätzen, da ihnen z. B. vertragliche Hintergründe nicht bekannt sind.

Bei der Schutzbedarfsfeststellung innerhalb einer großen Institution müssen daher neben den üblichen – rein technischen – Aspekten auch die vertraglichen Aspekte mit berücksichtigt werden. Hierbei sind beispielsweise die für die Ausformulierung der Verträge und SLAs (Service Level Agreements) zuständigen Personen zu befragen.

Die Durchführung der Schutzbedarfsfeststellung muss vom IT-Sicherheitsbeauftragten koordiniert werden. Auf der technischen Seite sind die für den Betrieb der Komponente zuständigen Teams als Ansprechpartner zu wählen, und auf der rechtlichen Seite die für die Vertragsausarbeitung zuständigen Personen.

Die Aussagen beider Aspekte müssen vom IT-Sicherheitsbeauftragten abschließend bewertet und zusammengefasst werden.

Der Teamleiter eines für einen Kunden betriebenen Server stuft den Schutzbedarf hinsichtlich der Verfügbarkeit als „sehr hoch“ ein, da der Kunde „in keinem Fall auf die Daten verzichten kann“.

Nach Rücksprache mit der Rechtsabteilung stellt sich heraus, dass vertraglich nur eine Verfügbarkeit zwischen 8:00 Uhr und 18:00 Uhr von 99,5% zugesichert wird. Außerhalb dieser Zeit sind längere Ausfälle (z.B. Wartungen) hinnehmbar. Der IT-Sicherheitsbeauftragte stuft daher den Schutzbedarf hinsichtlich Verfügbarkeit auf „normal“ herunter. Er bespricht dies mit dem Teamleiter und begründet ihm diese Entscheidung.

6.2.3 Probleme bei den IT-Systemen

Der Schutzbedarf der IT-Systeme leitet sich direkt aus den auf ihnen laufenden IT-Anwendungen ab. Oftmals stellt sich die Frage, wie System-Cluster oder spezielle Sicherheitskomponenten zu betrachten sind.

6.2.3.1 System mit Anwendungen unterschiedlicher Schutzbedürftigkeiten

Wie bestimmt man den Schutzbedarf, wenn auf dem System verschiedene relevante Anwendungen laufen?

In den meisten Fällen laufen auf einem Server gleichzeitig verschiedene Anwendungen mit unterschiedlichen Schutzbedürftigkeiten. Der Schutzbedarf des Systems leitet sich dann nach dem Maximumsprinzip von den installierten Anwendungen ab.

Auf dem Windows-Server des Rechenzentrums sind zwei unterschiedliche Anwendungen installiert. Die erste Anwendung hat hinsichtlich der Vertraulichkeit einen normalen Schutzbedarf, die zweite Anwendung (eine Datenbank) hat diesbezüglich einen hohen Schutzbedarf.

Der IT-Sicherheitsbeauftragte wendet das Maximumsprinzip an. Der Schutzbedarf hinsichtlich Vertraulichkeit wird als „hoch“ bewertet.

6.2.3.2 Viele Anwendungen auf einem Server

Auf einem Server ist eine Vielzahl von Anwendungen installiert. Der Schaden einer Anwendung ist unerheblich. Wie ist der Fall zu betrachten, dass viele Anwendungen einen Schaden nehmen?

Wenn auf einem IT-System mehrere IT-Anwendungen bzw. Informationen verarbeitet, so kann durch Kumulation mehrerer (z.B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen. In diesem Fall muss der Schutzbedarf des IT-Systems entsprechend erhöht werden (Kumulationseffekt).

6.2.3.3 Verteilungseffekt bei Cluster-Systemen

Wie geht man mit implementierten Hochverfügbarkeitslösungen um, die eine Vererbung des Schutzbedarfs kompliziert machen?

In Rechenzentren werden häufig, zur Erhöhung bzw. Gewährleistung der Verfügbarkeit, IT-Systeme zu Clustern zusammengeschlossen. Problematisch ist hierbei die Bewertung des Schutzbedarfs, da sowohl der Schutzbedarf jedes einzelnen Systems des Clusters, wie auch des Clusters als Gesamtheit betrachtet werden muss.

Für das Rechenzentrum ist die Funktionsfähigkeit der Firewall unverzichtbar. Ein Ausfall würde zum Stillstand jeglicher Kommunikation führen, daher ist der Anwendung „Firewall“ ein hoher Schutzbedarf hinsichtlich Verfügbarkeit zugeordnet. Da die IT-Systeme, auf denen die Firewall-Anwendung läuft, redundant ausgelegt sind, kann der Schutzbedarf für diese Systeme auf „normal“ herabgesetzt werden, da der Ausfall eines einzelnen Systems dieser Gruppe keine Auswirkungen auf die Verfügbarkeit hat.

Bei der Bewertung von Systemen, die Teil einer Cluster- oder Hochverfügbarkeits-Lösung sind, muss bei der Betrachtung des Schutzbedarfs bezüglich der Verfügbarkeit der Verteilungseffekt berücksichtigt werden. Hierbei leitet sich der Schutzbedarf der Anwendung nicht direkt auf das System ab.

6.2.4 Probleme bei den Kommunikationsverbindungen

Im Rahmen der Schutzbedarfsfeststellung werden die kritischen Kommunikationsverbindungen identifiziert. Insbesondere stellt sich hierbei als problematisch heraus, dass Vorgaben von Kunden berücksichtigt oder Standleitungen als grundsätzlich „sicher“ angesehen werden.

6.2.4.1 Behandlung von Standleitungen

Müssen Standleitungen als kritisch angesehen werden?

Standleitungen zwischen Kommunikationspartner sind öffentliche Leitungen und müssen aus diesem Grund als kritisch bewertet werden. Eine Verschlüsselung bietet sich an, wenn sensible Daten übertragen werden.

Eine Standleitung ist häufig kein dediziertes „Kabel“ zwischen den beteiligten Kommunikationspartner. Die Telekommunikationsunternehmen legen Datenleitungen innerhalb ihrer internen Netze zusammen, um so kosteneffektiv Datenleitungen anbieten zu können. Weiterhin ist mit ausreichender technischer Kenntnis das Abhören von Standleitungen z.B. innerhalb von Verteilerstellen möglich.

Das Rechenzentrum besitzt Standleitungen zu verschiedenen Kunden. Über diese Standleitungen werden teilweise personenbezogene Daten übertragen und müssen somit als kritisch angesehen werden.

Auf den Kommunikationsverbindungen, die vom Rechenzentrum betrieben werden, werden die Daten bis zum Übergabepunkt zum Kunden durch eine Hardwarelösung verschlüsselt.

6.2.4.2 Kommunikationsverbindung unterliegt den Vorgaben des Kunden (z.B. keine Verschlüsselung möglich)

Was ist zu unternehmen, wenn die Kommunikationsverbindung den Vorgaben des Kunden entspricht und nicht denen des GSHB?

Insbesondere für Rechenzentren ist dies ein Problem, denn sie sind Dienstleister für ihre Kunden. Dies wirkt sich auch auf die Gestaltung von Kommunikationsverbindungen aus. Häufig unterliegen die Anbindungen an Kunden deren Anforderungen.

Bei der IT-Sicherheitskonzeption ist hierbei zunächst zu entscheiden, unter wessen Hoheit die Kommunikationsverbindung liegt.

Bei der Schutzbedarfsfeststellung von Kommunikationsverbindungen sind lediglich diejenigen Kommunikationsverbindungen relevant, die direkt der Institution zugeordnet werden können. Kommunikationsverbindungen, die der Kunde betreibt, gehören nicht zum IT-Verbund und müssen somit nicht berücksichtigt werden.

Für die direkt der Institution zugeordneten Kommunikationsverbindungen ist diese für die Sicherheit zuständig und muss entsprechende Sicherheitsmaßnahmen umsetzen.

Der Kunde des Rechenzentrums wünscht eine proprietäre Anbindung an das Rechenzentrum. Er organisiert die hierfür erforderliche Datenleitung und stellt im Rechenzentrum einen Router als Übergabepunkt auf.

Bei der durch Kunden betriebenen Kommunikationsverbindungen weist das Rechenzentrum diese auf die Erfordernis einer Verschlüsselung hin. Die Kommunikationsverbindung ist jedoch nicht Bestandteil des IT-Verbundes.

7 Modellierung

Nach durchgeführter Schutzbedarfsfeststellung wird der betrachtete IT-Verbund mit Hilfe der Bausteine des IT-Grundschutzhandbuchs nachgebildet (vgl. Kapitel 2.3 [GSHB]). Neben allgemeinen Bausteinen, die in jedem Fall anzuwenden sind (z.B. B3.0 IT-Sicherheitsmanagement), werden individuelle Bausteine in Abhängigkeit vom jeweiligen IT-Verbund genutzt.

Bild 4: Modellierte Figuren

Als Ergebnis dieser Phase erhält man ein IT-Grundschutzmodell des betrachteten IT-Verbundes, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen des GSHB besteht, und eine Abbildung zwischen den Bausteinen sowie den sicherheitsrelevanten Aspekten des IT-Verbundes darstellt. Die Modellierung des IT-Verbundes wird dabei anhand der im GSHB vorgesehenen Gruppierung der IT-Systeme, IT-Anwendungen und IT-Räume durchgeführt.

7.1 Generelle Vorgehensweise bei der Modellierung

Die Modellierung des IT-Verbundes mittels GSHB-Bausteinen erfolgt stufenweise anhand der fünf definierten Schichten des IT-Grundschutzmodells:

Schicht 1: Übergreifende Aspekte

Die Schicht 1 umfasst alle übergreifenden IT-Sicherheitsaspekte, die für den Großteil des IT-Verbundes in gleicher Weise gelten. Beispiele für Bausteine der Schicht 1 sind IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Computer-Virenschutzkonzept.

Schicht 2: Infrastruktur

Hier werden die baulich-technischen Bausteine zusammengefasst, die Aspekte der infrastrukturellen Sicherheit betreffen. Die Bausteine Gebäude, Räume, Schutzschränke und häuslicher Arbeitsplatz sind Beispiele für diese Schicht.

Schicht 3: IT-Systeme

Die 3. Schicht behandelt die IT-Systeme des IT-Verbundes. Die Bausteine Unix-System, Tragbarer PC, Windows NT Netz und TK-Anlage sind Beispiele für Bausteine dieser Schicht.

Schicht 4: Netze

Aspekte der Vernetzung werden in der Schicht 4 betrachtet. Hierzu gehören u.a. die Bausteine Heterogene Netze, Netz- und Systemmanagement und Firewall.

Schicht 5: IT-Anwendungen

IT-Anwendungen werden in der Schicht 5 behandelt. E-Mail, WWW-Server, Faxserver und Datenbanken sind Bausteine aus dieser Schicht.

Diese Schichteneinteilung führt zu einer Komplexitätsreduktion, da übergeordnete, technische und infrastrukturelle Aspekte voneinander getrennt betrachtet werden und so eine Aktualisierung einzelner Aspekte des IT-Sicherheitskonzepts einfach vorgenommen werden kann.

Im Rahmen der Modellierung wird für die Bausteine der einzelnen Schichten entschieden, wie und ob diese zur Abbildung des IT-Verbundes verwendet werden können.

In Kapitel 2.3 von [GSHB] wird ausführlich erläutert, unter welchen Voraussetzungen die Bausteine auf den IT-Verbund angewandt werden.

Die Dokumentation des IT-Grundschutzmodells, also die Zuordnung der Bausteine zu den Komponenten des IT-Verbundes, sollte

- die Nummer und der 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),
- einen Ansprechpartner und
- Notizen (z. B. als Begründung oder für weitere Informationen)

enthalten.

Nachdem die Modellierung anhand der einzelnen Schichten erfolgt ist, sollte überprüft werden, ob die Modellierung des IT-Verbundes vollständig und lückenlos ist. Hierzu prüft man,

- ob jedes Teilnetz vollständig abgebildet wurde und
- ob durch alle Teilnetze das Gesamtsystem vollständig abgebildet wird.

Wichtig ist hierbei, dass sowohl die technischen als auch die vorhandenen organisatorischen, personellen und infrastrukturellen Aspekte berücksichtigt wurden. Weiterhin ist zu prüfen, ob die Modelierungshinweise des GSHB der einzelnen Schichten angewandt wurden und ob in Abhängigkeit vom Schutzbedarf zusätzliche Bausteine erforderlich sind.

Pflichtbausteine sind z.B. die Bausteine *IT-Sicherheitsmanagement* (B3.00) und *Gebäude* (B4.01). Ein Baustein, der bei hohem Schutzbedarf hinsichtlich Vertraulichkeit bei einer Komponente angewandt werden muss, ist der Baustein *Kryptokonzept* (B3.07).

7.2 Häufig auftretende Probleme bei der Modellierung eines großen IT-Verbundes

Bei der Modellierung eines komplexen IT-Verbundes sind sowohl der Umfang der erforderlichen Arbeiten, als auch fehlende oder veraltete Bausteine oft auftretende Hindernisse. Die Modellierung und deren Dokumentation er-

fordert viel „Fleißarbeit“, die sich durch den Einsatz des GSTOOL reduzieren lässt.

7.2.1 Fehlende Bausteine

Ein häufiges Problem bei der Anwendung des GSHB in komplexeren IT-Verbünden wie einem Rechenzentrum ist, dass nicht für jede Komponente ein entsprechender Baustein aus dem GSHB vorhanden ist. Dies ist insbesondere damit zu begründen, dass häufig spezielle oder sehr aktuelle Komponenten eingesetzt werden.

7.2.1.1 Anwendung ähnlicher Bausteine

Es werden großflächig Anwendungen, für die es keine passenden Bausteine im GSHB gibt, verwendet. Es gibt jedoch einen Baustein einer älteren Version der Anwendung. Kann dieser angewendet werden?

Wenn zu einer Komponente kein passender Baustein vorhanden ist, kann der Baustein einer ähnlichen Komponente sinngemäß eingesetzt werden. Dies ist möglich, wenn ein oder mehrere Bausteine existieren, mit denen das gewünschte System sinngemäß nachgebildet werden kann. Die Maßnahmen der verwendeten Bausteine müssen hierbei ebenfalls sinngemäß angewandt werden, sofern eine Anwendung der jeweiligen Maßnahme möglich ist.

Für die in der Institution eingesetzten „Windows XP Professional“ Systeme existiert im GSHB kein eigener Baustein. Daher werden diese Systeme mit dem GSHB-Baustein B5.07 *Windows 2000 Client* modelliert. Hierbei werden die Maßnahmen auf die Windows XP Professional Systeme angewandt und gegebenenfalls angepasst und erweitert.

Sobald ein eigener Windows XP Professional Baustein verfügbar ist, wird die Modellierung entsprechend angepasst.

7.2.1.2 Erstellung individueller Bausteine

Es sind Komponenten im IT-Verbund vorhanden, für die es keine passenden oder ähnlichen Baustein im GSHB gibt. Wie geht man vor?

Ein IT-Verbund, der wesentliche Komponenten enthält, zu denen es keine Bausteine innerhalb des GSHB gibt, kann nicht zertifiziert werden!

Sind keine Bausteine im GSHB vorhanden, die in abgewandelter Form genutzt werden können, um eine vorhandene Komponente zu modellieren, gibt es die Möglichkeit, einen eigenen Baustein zu definieren (vgl. Kapitel 2.3.2 in [GSHB]). Hierbei bietet es sich an, sich an der Struktur der vorhandenen Bausteine zu orientieren.

Die Möglichkeit einen eigenen Baustein zu definieren ist sehr aufwändig, bietet jedoch den Vorteil, dass der Baustein auf die Anforderungen der Institution zugeschnitten werden kann.

Bei fehlenden Bausteinen sollte daher versucht werden, das System durch vorhandene Bausteine des GSHB nachzubilden. Nur so kann sichergestellt werden, dass eine GS-Zertifizierung möglich ist. Sollten selbstdefinierte Bausteine angewendet werden, wird die Umsetzung dieser bei der Zertifizierung nicht berücksichtigt.

Vgl. [GSHB] Kapitel 2.3: *„Für den Fall, dass die Modellierung nicht vollständig durchführbar ist, weil entsprechende Bausteine im IT-Grundschutzhandbuch fehlen, wird darum gebeten, den Bedarf an die IT-Grundschutz-Hotline des BSI weiterzuleiten."*

Vgl. [GSHB] Kapitel 2.3: *„Wenn die in dem neu erstellten Baustein betrachtete Komponente oder Vorgehensweise nicht zu speziell ist, bietet es sich an, die erarbeiteten Dokumente dem IT-Grundschutz-Team des BSI zur weiteren Verwendung zur Verfügung zu stellen. Das BSI wird prüfen, ob auch andere Anwender von den Inhalten profitieren können und den neuen Baustein gegebenenfalls über die üblichen Vertriebswege des IT-Grundschutzhandbuchs allen Anwendern zur Verfügung stellen."*

7.2.1.3 Entfernen entbehrlicher Maßnahmen im GSTOOL

Maßnahmen innerhalb der Bausteine, die als nicht erforderlich angesehen werden, werden aus der GSTOOL-Datenbank entfernt. Ist das ein Problem?

Wird eine Maßnahme als nicht erforderlich angesehen, ist sie im Sinne des GSHB als „entbehrlich“ zu kennzeichnen. Ein Entfernen von Maßnahmen aus der Datenbank des GSTOOL ist nicht empfehlenswert und widerspricht der Vorgehensweise des GSHB. Wenn entbehrliche Maßnahmen aus der Datenbank entfernt werden, kann auch dies zu Problemen führen. Bei einer Zertifizierung des IT-Verbundes zum Beispiel, ist der Auditor auf die Begründung, weshalb eine Maßnahme entbehrlich ist, angewiesen. Ist die Maßnahme aus der Datenbank entfernt, kann diese Begründung nicht einfach nachvollzogen werden.

Entbehrliche Maßnahmen sollten im GSTOOL als solche gekennzeichnet werden. Eine Begründung, durch welche höherwertige Maßnahme diese Entscheidung gerechtfertigt ist, kann dann direkt im GSTOOL hinterlegt werden.

7.2.1.4 Integration neuer Bausteine in das GSTOOL

Für eine Komponente des IT-Verbundes ist ein Baustein entwickelt worden, kann dieser in das GSTOOL integriert werden?

Das GSTOOL bietet die Möglichkeit individuelle Bausteine zur Datenbank hinzu zu fügen (vgl. Kapitel 7.3.4 [GSTHB]). Hierzu ist im GSTOOL die Sicht *GSHB benutzerdefiniert* vorhanden (vgl. Kapitel 7 [GSTHB]). In dieser Sicht des GSTOOL können vorhandene Bausteine angepasst (konkretisiert) oder neue Bausteine zur Datenbank hinzugefügt werden. Hierbei ist wieder zu beachten, dass ein IT-Verbund mit einem individuellen Baustein nicht zertifiziert werden kann. Das GSTOOL setzt daher die Auditrelevanz der individuellen Bausteine auf „nein“.

8 Basis-Sicherheitscheck / Ergänzende Sicherheitsanalyse

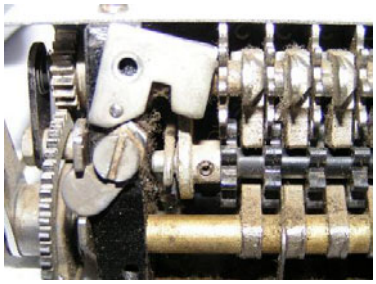


Bild 5: Zahnräder

Nachdem die Modellierung des IT-Verbundes durchgeführt wurde, muss ermittelt werden, ob die durch das GSHB geforderten Standard-Sicherheitsmaßnahmen umgesetzt und für den Schutzbedarf der einzelnen Komponenten ausreichend sind. Hierbei wird

- der Umsetzungsstatus der durch die Bausteine vorgegebenen Standard-Sicherheitsmaßnahmen ermittelt und
- bei Komponenten mit hohem Schutzbedarf, geprüft, ob die umgesetzten Standard-Sicherheitsmaßnahmen ausreichend sind, um dem hohen Schutzbedarf gerecht zu werden.

Ziel dieser Phase ist es fehlende Standard-Sicherheitsmaßnahmen – bei Komponenten mit mindestens hohen Schutzbedarf zusätzliche Sicherheitsmaßnahmen – zu ermitteln und damit die Grundlage für die nächste Phase (Erstellung eines Realisierungsplans umzusetzender Maßnahmen) zu legen.

8.1 Generelle Vorgehensweise beim Basis-Sicherheitscheck

Für den Modellierten IT-Verbund müssen die umzusetzenden Sicherheitsmaßnahmen ermittelt werden. Dies erfolgt im Rahmen des Basis-Sicherheitscheck (vgl. Kapitel 2.4 [GSHB]) und ab einem hohen Schutzbedarf anhand einer ergänzenden Sicherheitsanalyse (vgl. Kapitel 8.3 und Kapitel 2.5 [GSHB]).

Bei einem Basis-Sicherheitscheck wird die durchgeführte Modellierung als Prüfplan für einen Soll-Ist-Vergleich genutzt. Die Durchführung des Basis-Sicherheitscheck besteht hierbei aus den drei Schritten:

Schritt 1 Organisatorische Vorbereitungen

Während der organisatorischen Vorarbeiten werden die für die einzelnen Bausteine verantwortlichen Ansprechpartner ermittelt und festgelegt. Weiterhin werden vorhandene Dokumente als Vorbereitung auf den anschließenden Soll-Ist-Vergleich gesichtet.

Schritt 2 Durchführung des Soll-Ist-Vergleichs

Mit den zuvor festgelegten Ansprechpartnern werden die Soll-Ist-Vergleiche durchgeführt. Hierbei wird für jeden Baustein ermittelt, ob die durch den Baustein vorgegebenen Standard-Sicherheitsmaßnahmen „entbehrlich“ sind, „umgesetzt“, „teilweise umgesetzt“ oder „nicht umgesetzt“ sind.

Eine Maßnahme

- wird als „*umgesetzt*“ angesehen, wenn alle Empfehlungen in der Maßnahme vollständig und wirksam umgesetzt wurden.
- ist „*teilweise umgesetzt*“, wenn einige der Empfehlungen sind umgesetzt, andere noch nicht oder nur teilweise umgesetzt sind.
- ist als „*nicht umgesetzt*“ anzusehen, wenn die Empfehlungen der Maßnahme größtenteils noch nicht umgesetzt sind.
- wird als „*entbehrlich*“ angesehen, wenn den entsprechenden Gefährdungen mit höherwertigen 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.

Schritt 3 Dokumentation der Ergebnisse

Bereits während der Interviews werden die Ergebnisse dokumentiert. Hierbei bietet es sich an, den Umsetzungsstand direkt im GSTOOL zu dokumentieren.

Das Ergebnis dieser Schritte ist eine Übersicht über den Umsetzungsstand der durch die einzelnen Bausteine vorgegebenen Standard-Sicherheitsmaßnahmen.

8.2 Häufig auftretende Probleme beim Basis-Sicherheitscheck

Die auftretenden Probleme sind abhängig von dem jeweiligen Schritt des Basis-Sicherheitschecks. Bei den organisatorischen Vorarbeiten stellt sich häufig als Problem heraus, dass eine Vielzahl von Dokumenten Informationen über umgesetzte Maßnahmen enthält und dass Ansprechpartner nur schwer festgelegt werden können. Die meisten Probleme treten jedoch bei der Durchführung des Soll-Ist-Vergleichs auf. Hier stehen insbesondere die Interpretation der Maßnahme im Vordergrund und die Frage, wie wörtlich eine Maßnahme umzusetzen ist oder was zwingende Anforderungen einer Maßnahme sind.

8.2.1 Organisatorische Vorarbeiten

Dem Basis-Sicherheitscheck gehen organisatorische Vorarbeiten voraus. Ziel dieser Vorarbeiten ist es, einen Hinweis auf den Umsetzungsgrad der Maßnahmen zu erhalten und geeignete Ansprechpartner zu identifizieren. Insbesondere die Sichtung aller hausinternen Papiere (z.B. Verfahrensanweisungen, Prozessbeschreibungen, Systemdokumentationen) gehört zu diesen organisatorischen Vorarbeiten. Diese Dokumente geben einen Hinweis auf den Umsetzungsgrad der einzelnen Maßnahmen und auf mögliche Ansprechpartner.

Anschließend sollten Termine mit den einzelnen Ansprechpartnern koordiniert werden. Gegebenenfalls bietet es sich an, die Interviews im Rahmen von Workshops durchzuführen. Dies ist besonders dann empfehlenswert, wenn mehrere Ansprechpartner zu einem Thema existieren.

8.2.1.1 Auswahl von Ansprechpartnern

Wie wird der richtige Ansprechpartner ermittelt?

Das GSHB sieht die Festlegung von Verantwortlichen für Anwendungen und IT-Systeme vor. Im Rahmen einer erstmaligen Umsetzung des GSHB kann es vorkommen, dass diese Verantwortlichkeiten nicht klar fixiert und Ansprechpartner nur schwer auszumachen sind. Systemdokumentationen oder –konzepte können einen ersten Hinweis auf Verantwortliche liefern. Ausgangspunkt für die Suche nach Verantwortlichen können die für die Systeme zuständigen Administratoren sein. Sollte kein Verantwortlicher gefunden werden, muss notfalls jemand bestimmt werden.

Als „richtige Ansprechpartner" können die Personen angesehen werden, die für die Initiierung oder Umsetzung einer Maßnahme verantwortlich zeichnen. Das GSHB gibt am Anfang jeder Maßnahmenbeschreibung Hinweise darauf, in welchem Personenkreis geeignete Ansprechpartner zu finden sind (Im GSHB sind mögliche Ansprechpartner hinter den Punkten „Verantwortlich für Initiierung" und „Verantwortlich für Umsetzung" innerhalb der einzelnen Bausteine genannt).

Für ein von der Buchhaltung genutztes System ist kein direkter Ansprechpartner definiert, das System läuft „wartungsfrei". Probleme gab es seit der Installation nicht, ist die Aussage. In dem für den Betrieb für die Bürosysteme zuständigen Team fühlt sich kein Administrator für das System verantwortlich.

Der IT-Sicherheitsbeauftragte wendet sich direkt an den Teamleiter und teilt ihm mit, dass es erforderlich ist, einen Verantwortlichen für dieses System

zu definieren. Der ursprünglich für die Installation des Systems zuständige Administrator wird daraufhin als verantwortlich für das System festgelegt.

Lassen sich keine Verantwortlichen für eine Komponente finden oder sind keine Verantwortlichen definiert, muss dieses Problem eskaliert werden.

8.2.1.2 Verteilte Verantwortlichkeiten

Die IT-Infrastruktur in der Institution ist sehr umfangreich. Für ähnliche Systeme sind verschiedene Verantwortliche benannt. Wie wird vorgegangen?

Es kann vorkommen, dass ähnliche Systeme von unterschiedlichen Verantwortlichen betreut werden. Dies ist z.B. der Fall, wenn ein Server-Park für einen Kunden von einem einzelnen Team verwaltet wird.

Das Rechenzentrum betreibt für unterschiedliche Kunden Unix-Serversysteme, die Serversysteme eines Kunden werden dabei jeweils von einem Team betrieben. So kommt es vor, dass Unix-Server von zwei verschiedenen Teams betreut werden.

Bei der Feststellung des Umsetzungsgrades der Maßnahmen des Bausteins „B6.2 Unix-Server“ lädt der IT-Sicherheitsverantwortliche Vertreter beider Teams zu einem Workshop ein. Ist eine Maßnahme nur in einem Team umgesetzt, definiert der IT-Sicherheitsverantwortliche den Umsetzungsgrad als „teilweise umgesetzt“.

Sind verschiedene Verantwortliche für ähnliche oder identische Systeme zuständig, bietet es sich an, einen Workshop mit allen in Frage kommenden Verantwortlichen abzuhalten und so die erforderlichen Informationen zu sammeln.

8.2.2 Durchführung des Soll-Ist Vergleichs

Die Durchführung des Soll-Ist Vergleichs ist verhältnismäßig einfach. Zu jeder erforderlichen Maßnahme muss entschieden werden, wie der Umsetzungsgrad ist. Maßnahmen die als entbehrlich angesehen werden, müssen gesondert begründet werden.

Als Vorbereitung auf die Interviews ist die inhaltliche Kenntnis der Maßnahmen erforderlich.

Für die Dokumentation der Ergebnisse bietet sich die Nutzung des GSTOOL an. Alternativ können die in den Hilfsmitteln des GSHB enthaltenen Formulare zur Dokumentation des Umsetzungsgrads genutzt werden.

8.2.2.1 Wie viel technisches Know-how ist für die Befragung nötig?

Der IT-Sicherheitsbeauftragter muss entscheiden, ob die einzelnen Standard-Sicherheitsmaßnahmen umgesetzt sind. Teilweise sind die Empfehlungen sehr speziell, so dass dieser aufgrund des fehlenden Fachwissens nicht entscheiden kann, ob diese komplett umgesetzt wurden. Wie löst man das Problem?

Während des Basis-Sicherheitschecks muss durch den IT-Sicherheitsbeauftragten entschieden werden, ob die Maßnahme umgesetzt ist. Abhängig von der jeweiligen Maßnahme bedeutet dies, zu entscheiden, ob die umgesetzten Maßnahmen ausreichen, um die in der Standardsicherheitsmaßnahme angegebenen Gefährdungen abzuwenden. Problematisch wird dies, wenn die Empfehlungen sehr tief in technische Details gehen und dem IT-Sicherheitsbeauftragten das erforderliche Know-how fehlt. Neben den in den Maßnahmen genannten ergänzenden Kontrollfragen kann es erforderlich sein, dass der IT-Sicherheitsbeauftragte im Einzelfall auf Expertenwissen von Dritten zurückgreift.

Der IT-Sicherheitsbeauftragte muss prüfen, ob die Maßnahme M 4.26 (Regelmäßiger Sicherheitscheck des Unix-Systems) ausreichend umgesetzt ist

und orientiert sich an den in der Maßnahme gemachten Angaben. Der zuständige Ansprechpartner erläutert, dass für Sicherheitsüberprüfungen von Unix-Systemen das Public-Domain-Programm Nessus und ein kommerzielles Programm eingesetzt werden, welches nicht in der Maßnahme erwähnt wird. Die Sicherheitsüberprüfungen werden dokumentiert. Der IT-Sicherheitsbeauftragte kennt diese Programme nicht.

Um beurteilen zu können, ob die Maßnahme ausreichend umgesetzt ist, nutzt er die Unterstützung des Service-Technikers eines Herstellers, welcher ein eigenes Büro in der Institution hat und für die Institution einen Vor-Ort-Support gewährleistet. Da dieser als Unix-Administrator weitreichende Kenntnisse besitzt, kann er den IT-Sicherheitsbeauftragten bei der Beurteilung unterstützen.

Beim Basis-Sicherheitscheck muss der IT-Sicherheitsbeauftragte gegebenenfalls auf technisches Know-how zurückgreifen, um zu entscheiden, ob eine Standardsicherheitsmaßnahme ihrem Wesen nach umgesetzt wurde.

8.2.2.2 Wie genau müssen die Empfehlungen einer Maßnahme umgesetzt werden?

Die Maßnahme eines Bausteins empfiehlt die Änderung eines Konfigurationsparameters. Dieser Parameter wurde bewusst auf einen anderen Wert gesetzt. Müssen die Empfehlung umgesetzt werden?

Die Empfehlungen in den definierten Maßnahmen eines Bausteins sind häufig sehr detailliert beschrieben. In der Einleitung einer jeden Maßnahme ist häufig die Gefährdungssituation und damit der Grund für die Empfehlungen enthalten. Die anschließenden Empfehlungen sollen einen Hinweis darauf geben, durch welche konkreten Maßnahmen die Gefährdung eingedämmt bzw. verhindert werden kann. Eine Umsetzung aller Empfehlungen ist nicht in jedem Fall möglich. Wesentlich ist, dass durch die in der Institution umgesetzten Maßnahmen den dort genannten Gefährdungen effektiv begegnet wird.

Die Maßnahme M 4.98 fordert dazu auf, die Kommunikation durch Paketfilter auf ein Minimum zu beschränken. In der Maßnahme sind für Dienste genannt, die für einzelnen Serversysteme zulässig sind.

Werden die Hinweise wortgetreu umgesetzt, kann dies dazu führen, dass das System nicht mehr administrierbar ist. Bei der Anwendung der Maßnahme ist insbesondere auf die sinngemäße Anwendung zu achten.

Beim Basis-Sicherheitscheck muss geprüft werden, ob die Maßnahme in ihrem Wesen umgesetzt wurde. Eine wortgetreue Einhaltung aller Punkte der Maßnahme ist nicht erforderlich.

8.2.2.3 Detailtiefe des Basis-Sicherheitschecks

In welcher Detailtiefe sollte der Basis-Sicherheitscheck erfolgen?

Der Basis-Sicherheitscheck hat das Ziel zu ermitteln, ob die zur Erreichung eines normalen Schutzbedarfs erforderlichen Standard-Sicherheitsmaßnahmen umgesetzt sind. An diesem Ziel orientiert sich auch die Detailtiefe der Betrachtung des Basis-Sicherheitschecks. Sicherheitsaspekte von Anwendungen mit hohem Schutzbedarf werden erst anschließend im Rahmen der ergänzenden Sicherheitsanalyse betrachtet.

Die Detailtiefe des Basis-Sicherheitschecks orientiert sich am den Standard-Sicherheitsmaßnahmen. Zusätzliche Aspekte von hochschutzbedürftigen Anwendungen werden erst nach Abschluss des Basis-Sicherheitschecks betrachtet.

Das Rechenzentrum betreibt einen Server, dessen Verfügbarkeitsanforderungen mit „hoch“ angesehen werden. Zunächst wird im Rahmen des Basis-Sicherheitscheck der Umsetzungsgrad der Standard-Sicherheitsmaßnahmen geprüft. Im Anschluss daran werden zusätzliche Maßnahmen definiert, um eine hohe Verfügbarkeit zu gewährleisten.

8.3 Generelle Vorgehensweise bei der ergänzenden Sicherheitsanalyse

Die Vorgehensweise der ergänzenden Sicherheitsanalyse (vgl. Kapitel 2.5 [GSHB]) ist im BSI Dokument „Risikoanalyse auf der Basis von IT-Grundschutz“ [GSRISK] ausführlich beschrieben, Abbildung 4 zeigt schematisch die einzelnen Phasen.

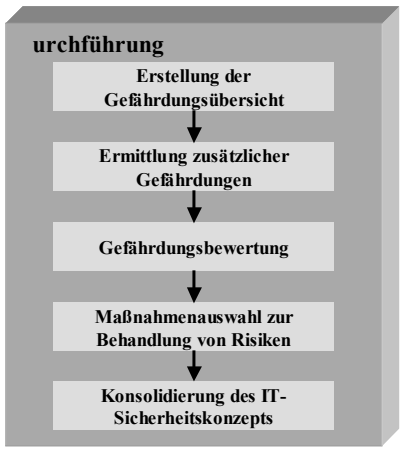


Abbildung 4: Phasen der ergänzenden Sicherheitsanalyse

Zunächst werden diejenigen im GSHB aufgeführten Gefährdungen ermittelt, die auf die hochschutzbedürftigen Komponenten wirken.

Anschließend werden zusätzliche – über die im GSHB aufgeführten hinausgehenden – Gefährdungen ermittelt. Diese müssen in der weiteren Vorgehensweise ebenfalls betrachtet werden.

Nachdem die auf die Komponente wirkenden Gefährdungen ermittelt wurden, muss für jede Gefährdung bestimmt werden, ob die bereits umgesetzten Standard-Sicherheitsmaßnahmen des GSHB einen ausreichenden Schutz bieten.

Aus den Risiken, für die keine ausreichenden Maßnahmen definiert sind, resultiert Handlungsbedarf. Es muss in der nächsten Phase entschieden werden, wie mit den verbleibenden Gefährdungen umgegangen wird. Es ist üblich, in dieser Phase die Leitungsebene mit in die Entscheidungsfindung einzubeziehen, da sich erhebliche Risiken ergeben oder erhebliche Kosten entstehen können.

Abschließend wird das IT-Sicherheitskonzept konsolidiert. Werden zusätzlich zu den Standard-Sicherheitsmaßnahmen weitere Maßnahmen als notwendig angesehen, müssen diese entsprechend in der Dokumentation vermerkt werden.

8.4 Häufig auftretende Probleme der ergänzenden Sicherheitsanalyse

Die bei der ergänzenden Sicherheitsanalyse auftretenden Gefährdungen lassen sich in die Probleme der einzelnen Phasen einteilen. Hierbei lassen sich die fünf Phasen in „Gefährdungsfindung und -bewertung“ sowie „Maßnahmenauswahl“ zusammenfassen.

Problematisch ist auch hier die große Anzahl zu berücksichtigender Informationen. Weitere Probleme ergeben sich durch die bei der Maßnahmendefinition einzubeziehende Leitungsebene und dadurch bedingte längere Entscheidungswege.

8.4.1 Probleme bei der Gefährdungsfindung

Wenn festgestellt werden soll, ob weitere Gefährdungen für die betrachtete Komponente relevant sind, stellt sich zunächst die Frage, welche Bereiche für die ergänzende Sicherheitsanalyse betrachtet werden sollen. Ist dies festgelegt, sieht man sich oft mit einer Flut zusätzlich zu betrachtender Gefährdungen konfrontiert.

8.4.1.1 Zu betrachtende Bereiche

Welche Bereiche sollten zuerst einer Risikoanalyse unterzogen werden? Alle Bereiche gleichzeitig zu betrachten, ist unrealistisch.

Abhängig von der Anzahl hochschutzbedürftiger Komponenten muss eine Reihenfolge für die Betrachtung festgelegt werden. Hierbei ist zu entschei-

den, welche Bereiche „weniger hochschutzbedürftig“ sind und welche „stärker hochschutzbedürftig“. Ein Hinweis auf die Reihenfolge kann eine Einschätzung eines aus einem Verlust an Vertraulichkeit, Integrität oder Verfügbarkeit resultierenden Schadens geben. Die Schadenshöhe kann als Maßstab für die Reihenfolge gewählt werden. Hierbei können sowohl finanzielle Schäden als auch ein zu erwartender Imageverlust als Kriterium herangezogen werden.

Ein Rechenzentrum betreibt für zwei Kunden Systeme, die beide als hochschutzbedürftig hinsichtlich der Verfügbarkeit angesehen werden. Eine ergänzende Sicherheitsanalyse ist damit für beide Systeme erforderlich. Die Vertragswerke sehen unterschiedliche Entschädigungen bei Nichtverfügbarkeit vor. Die ergänzende Sicherheitsanalyse wird daher zuerst bei dem System durchgeführt, dessen Ausfall den höheren Schaden für das Rechenzentrum verursacht.

Der zu erwartende Schaden bei Eintreten eines Verlustes der Verfügbarkeit, Vertraulichkeit oder Integrität legt die Reihenfolge fest, in der die ergänzende Sicherheitsanalyse durchgeführt wird.

8.4.1.2 Ermitteln neuer Gefährdungen

Auf welche Art lassen sich neue Gefährdungen am effektivsten ermitteln?

Für die Ermittlung neuer Gefährdungen hat sich in der Praxis die Durchführung von Workshops bewährt. Hieran nehmen verschiedene Mitarbeiter teil, die mit der zu betrachtenden Komponente in Verbindung stehen (als Administrator, Verantwortlicher oder Benutzer). Die Moderation des Workshops sollte durch den IT-Sicherheitsbeauftragten übernommen werden.

8.4.1.3 Flut an Gefährdungen

Im Rahmen eines Workshop sind eine Vielzahl zusätzlicher Gefährdungen ermittelt worden. Wie wird man mit der Flut an Gefährdungen fertig?

Bereits bei der Festlegung neuer Gefährdungen sollte versucht werden jede Gefährdung in eine der fünf vom GSHB definierten Gefährdungskataloge (G 1 Höhere Gewalt, G 2 Organisatorische Mängel, G 3 Menschliche Fehlhandlungen, G 4 Technisches Versagen und G 5 Vorsätzliche Handlungen) einzusortieren. Um die Komplexität der nachfolgenden Schritte zu reduzieren, sollte versucht werden die neuen Gefährdungen zu Gruppen zusammenzufassen und somit die Anzahl der neuen Gefährdungen zu reduzieren.

Während des Workshops bemängelt ein Mitarbeiter, dass das Gebäude einfach durch die Belüftungsanlage unberechtigt betreten werden kann. Ein anderer Mitarbeiter ergänzt, dies sei auch durch verschiedene Fenster und Türen möglich.

Der IT-Sicherheitsbeauftragte stellt fest, dass die Gefährdung *G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen* hierfür angewandt werden kann. Es ist nicht nötig die Definition einer neuen Gefährdung vorzunehmen.

Werden für eine Komponente neue Gefährdungen festgestellt, sollte zunächst geprüft werden, ob eine Gefährdung des GSHB anwendbar ist. Ist dies nicht der Fall, sollte versucht werden, die neuen Gefährdungen zu verallgemeinern und anschließend zu Gruppen zusammenzufassen.

8.4.2 Probleme bei der Maßnahmenauswahl

Bei der Maßnahmenauswahl müssen Maßnahmen gefunden werden, die geeignet sind, die neuen Gefährdungen einzudämmen bzw. die Schadensauswirkungen zu reduzieren. Oftmals sind die erforderlichen Maßnahmen kostenintensiv, so dass die Leitung darüber entscheiden muss, welche Maßnahmen umzusetzen sind.

8.4.2.1 Maßnahmenauswahl

Es wurde festgestellt, dass die Standard-Sicherheitsmaßnahmen des GSHB nicht ausreichen. Welche Zusatzmaßnahmen kommen in Frage?

Geeignet sind alle Maßnahmen, die das Ausmaß einer Gefährdung wirkungsvoll reduzieren. Hierzu können sowohl technische als auch organisatorische Maßnahmen gehören.

Für ein System mit hoher Verfügbarkeitsanforderung wurde festgestellt, dass die Standard-Sicherheitsmaßnahmen nicht ausreichen. Als zusätzliche Maßnahme wurde das bereithalten eines gleichwertigen Ersatzsystems (Cold-Standby) definiert.

Bei der Definition zusätzlicher Maßnahmen ist die Kreativität gefragt. Es hat sich in der Praxis herausgestellt, dass die Zuhilfenahme eines externen Sicherheitsexperten hilfreich ist.

8.4.2.2 Wer trifft die Entscheidungen?

Die ergänzende Sicherheitsanalyse wurde für alle relevanten Bereiche durchgeführt, geeignete Maßnahmen sind identifiziert und eine Kostenschätzung ist durchgeführt worden. Viele Maßnahmen übersteigen ein mögliches Budget, wie wird weiter verfahren?

Es bietet sich an die Leitung bereits nach der Phase 3 (Gefährdungsbewertung) über das Gefährdungspotenzial zu informieren. Bereits an dieser Stelle kann die Leitung entscheiden, welche der verbleibenden Restrisiken getragen werden können und gegen welche Maßnahmen zu welchen Kosten ergriffen werden sollen. Meist sind auch Migrationsstrategien möglich, so dass man eine schrittweise Umsetzung vornehmen kann.

Das Rechenzentrum befindet sich innerhalb eines einzelnen Gebäudes in der Nähe eines Flughafens. Auch wenn ein Flugzeugabsturz unwahrscheinlich

ist, wird dies als Gefahr angesehen. Als mögliche Maßnahme wurde ein zweiter Standort angesehen, der einen Neubau und hohe Investitionen zur Folge hätte.

Der Leitung wurden die Gefährdungen vorgelegt. Insbesondere die Gefährdung durch einen Flugzeugabsturz wird von der Leitung als „tragbar“ eingestuft und nicht weiter betrachtet. Die Entscheidung der Leitung wird im Rahmen der ergänzenden Sicherheitsanalyse dokumentiert.

9 Realisierungsplan

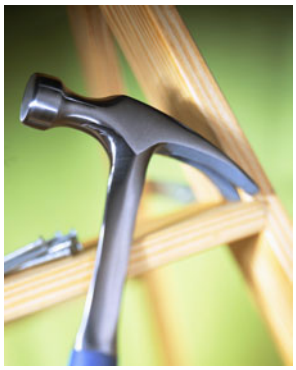


Bild 6: Werkzeug

Vor der Realisierung von IT-Sicherheitsmaßnahmen müssen für den IT-Verbund die IT-Strukturanalyse, die Schutzbedarfsfeststellung und die Modellierung durchgeführt worden sein. Weiterhin werden die Ergebnisse des Basis-Sicherheitschecks benötigt. Wurde eine ergänzende Sicherheitsanalyse durchgeführt, so sollten die hierbei definierten Maßnahmenvorschläge ebenfalls vorliegen und bei der Realisierung berücksichtigt werden.

9.1 Generelle Vorgehensweise bei der Realisierung

Wenn nur wenige fehlende Maßnahmen identifiziert wurden und wenn deren Umsetzung wenig finanzielle oder personelle Ressourcen bindet, kann oft ad hoc entschieden werden, wer diese Maßnahmen bis wann umzusetzen hat.

Die Regel ist jedoch, dass eine Vielzahl von Maßnahmen umgesetzt werden muss. Der IT-Sicherheitsbeauftragte erstellt einen Projektplan, der die folgenden Schritte beinhaltet:

Schritt 1 Sichtung der Untersuchungsergebnisse

Alle nicht umgesetzten bzw. nur teilweise umgesetzten Maßnahmen (Ergebnis des Basis-Sicherheitschecks und der ergänzenden Sicherheitsanalyse) einschließlich ihrer Prioritäten werden extrahiert und in einer Tabelle zusammengefasst.

Schritt 2 Konsolidierung der Maßnahmen

Eventuell ist eine weitere Konkretisierung der ausgewählten Maßnahmen oder Anpassung an organisatorischen und technischen Gegebenhei-

ten erforderlich. Die IT-Sicherheitsmaßnahmen müssen 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

Für jede zu realisierende Maßnahme muss festgehalten werden, welche Investitionskosten und welcher Personalaufwand erforderlich ist. 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. Das GSTOOL unterstützt hier die Vorgehensweise, da zu erwartende Kosten direkt umzusetzenden Maßnahmen mit aufgenommen werden können.

Schritt 4 Festlegung der Umsetzungsreihenfolge der Maßnahmen

Oft fehlen Ressourcen (finanziell und personell) für die sofortige Umsetzung sämtlicher Maßnahmen, daher muss die Reihenfolge der Maßnahmenumsetzung festgelegt werden.

Die Umsetzungsreihenfolge kann durch eine angestrebte Zertifizierung bestimmt werden. 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. Abschließend werden die für das IT-Grundschutz-Zertifikat erforderlichen Maßnahmen realisiert.

Schritt 5 Festlegung der Verantwortlichkeit

Nach der Festlegung der Umsetzungsreihenfolge für die Umsetzung der Maßnahmen wird festgelegt, wer bis wann welche Maßnahmen zu realisieren hat. Hierbei ist auf ausreichende Kompetenz und Fähigkeit, aus-

reichende personelle und finanzielle Ressourcen sowie auf eine regelmäßige Berichtung des Umsetzungsstands an den IT-Sicherheitsbeauftragten zu achten.

Schritt 6 Realisierungsbegleitende Maßnahmen

Schon während der Umsetzung der IT-Sicherheitsmaßnahmen sollten die Mitarbeiter informiert werden. Die betroffenen Mitarbeiter sollten

- für die Belange der IT-Sicherheit sensibilisiert,
- über die Notwendigkeit und die Konsequenzen der Maßnahmen unterrichtet und
- dahingehend geschult werden, so dass diese die neuen IT-Sicherheitsmaßnahmen korrekt um- und einsetzen.

Die Mitarbeiter sollten möglichst frühzeitig in die Planungen mit einbezogen werden.

Nachdem die neuen IT-Sicherheitsmaßnahmen umgesetzt wurden, sollte der IT-Sicherheitsbeauftragte prüfen, ob die notwendige Akzeptanz der Mitarbeiter vorhanden ist. Ist dies nicht gegeben, ist ein Misserfolg absehbar. In diesem Fall müssen die Ursachen ermittelt werden und gegebenenfalls ist eine zusätzliche Aufklärung erforderlich.

9.2 Häufig auftretende Probleme bei der Realisierung

Bei der Umsetzung von IT-Sicherheitsmaßnahmen treten insbesondere Probleme aufgrund mangelnder finanzieller und personeller Ressourcen auf. Sind beispielsweise bauliche Maßnahmen umzusetzen, stellt sich unter Umständen zusätzlich das Problem, dass hier gegebenenfalls Genehmigungen (z.B. vom Vermieter, Eigentümer, Bauamt) eingeholt werden müssen. Dies kann dazu führen, dass sich diese Maßnahmen nicht oder nur schwer umsetzen lassen. Grundsätzlich lassen sich die Probleme in zwei Gruppen unterteilen:

einerseits entstehen Probleme in der Realisierungsplanung und auf der anderen Seite bei der Umsetzung der Maßnahmen.

9.2.1 Probleme bei der Realisierungsplanung

Insbesondere die Planung der Maßnahmenumsetzung und die damit erforderliche Koordinierung zwischen unterschiedlichen Stellen der Institution und gegebenenfalls Kunden und Dienstleistern stellt sich hier als problematisch dar.

9.2.1.1 Komplexer Projektplan

Es müssen eine Vielzahl an einzelnen Maßnahmen umgesetzt werden. Wie koordiniert man die einzelnen Aktivitäten?

Es bietet sich an die Umsetzung der Maßnahmen als Projekt zu organisieren. Bei einer Vielzahl an umzusetzenden Maßnahmen ist es ratsam Teilprojekte zu definieren und einen Teilprojektleiter für einzelne Aspekte zu benennen.

Die Überwachung der Umsetzung und als Hauptprojektleiter muss der IT-Sicherheitsbeauftragte fungieren.

Das Sicherheitsmanagement-Team des Rechenzentrums entscheidet sich, die Umsetzung der IT-Sicherheitsmaßnahmen als Projekt zu definieren. Die einzelnen Sicherheitsverantwortlichen übernehmen hierbei die Koordination von Teilaspekten. So ist der *Sicherheitsverantwortliche Technik* für die Koordinierung der Umsetzung aller Schicht 2-Maßnahmen (Infrastruktur) zuständig. Der IT-Sicherheitsbeauftragte übernimmt neben der Gesamtleitung die Koordinierung der aus der Schicht 1 (übergreifende Aspekte) ergebenden Maßnahmen.

So gelingt es, die einzelnen Aspekte aufzuteilen. Die einzelnen Teilprojektleiter erstellen jeweils unabhängige Projektpläne und Kostenschätzungen,

die der IT-Sicherheitsbeauftragte zusammenführt und mit der Leitung abstimmt.

9.2.1.2 Kostspielige Maßnahmen / Budgetgrenzen

Die Umsetzung aller erforderlicher Maßnahmen ist sehr kostspielig, es steht kein ausreichendes Budget zur Verfügung. Was kann man machen?

Meist sind viele Maßnahmen umzusetzen, die direkte Kosten verursachen oder Mitarbeiter lange Zeit binden. Dies wirkt sich direkt auf die Gesamtkosten bei der Umsetzung des GSHB aus. Eine Lösung dieses Problems gibt es nur indirekt, indem die umzusetzenden Maßnahmen priorisiert und die Reihenfolge der Maßnahmenumsetzung geändert wird. Die Gesamtkosten der Umsetzung aller identifizierten Maßnahmen lässt sich jedoch nur selten verringern.

Durch die Änderung der Umsetzungsreihenfolge können die anfallenden Kosten über die Gesamtlaufzeit des Projekts verteilt werden. Die Gesamtkosten werden hierdurch jedoch nicht beeinflusst.

Eine weitere Lösung ergibt sich, indem man sich an der zu erreichenden Siegelstufe der Zertifizierung orientiert.

Hierdurch lassen sich nicht die Gesamtkosten verringern, jedoch wird durch die definierten Ziele die Umsetzungsreihenfolge angepasst.

9.2.1.3 Bauliche Maßnahmen sind nicht umsetzbar

Die Institution befindet sich in einem angemieteten Gebäude, die geforderten Maßnahmen sind nicht umsetzbar. Wie löst man das Problem?

Insbesondere wenn bauliche Maßnahmen in angemieteten Räumen umgesetzt werden müssen, sind die Grenzen des Möglichen schnell erreicht. Prob-

lematisch wirkt sich dabei aus, dass gegebenenfalls für eine Zertifizierung erforderliche Maßnahmen nicht umgesetzt werden können.

Kann eine Maßnahme nicht wortgetreu umgesetzt werden, muss ermittelt werden, ob eine sinngemäße Umsetzung möglich ist (vgl. Kapitel 8.2.2.2).

Die Maßnahme M 1.24 (Vermeidung von wasserführenden Leitungen) kann in der Institution nicht umgesetzt werden, da die gegebene Infrastruktur genutzt werden muss und in einem Technikraum Wasserleitungen verlegt sind. Da auf keinen alternativen Raum ausgewichen werden kann, werden die Komponenten in einem Schrank platziert, der spritzwasserdicht nach IP52-Norm ist.

9.2.2 Probleme bei der Umsetzung von Maßnahmen

Bei der Umsetzung der IT-Sicherheitsmaßnahmen treten Probleme auf wenn Komponenten für einen Kunden betrieben werden. Insbesondere die Fragen nach der Einbeziehung der Kunden und der Motivation der Mitarbeiter stehen hierbei im Vordergrund.

9.2.2.1 Einbeziehung der Kunden bei der Maßnahmenumsetzung

Die Maßnahme hat Auswirkungen auf ein System welches für einen Kunden betrieben wird. Ist eine Einbeziehung des Kunden erforderlich?

Sind Maßnahmen umzusetzen, die Auswirkungen auf eine von einem Kunden genutzte Komponente haben, muss die Umsetzung der Maßnahme mit dem Kunden abgestimmt werden.

Bei umzusetzenden Maßnahmen sind negative Seiteneffekte zu vermeiden. Dies ist insbesondere dann der Fall, wenn Maßnahmen eine Komponente betreffen, die für einen Kunden betrieben werden. Durch die Maßnahmen dürfen die erbrachten Dienstleistungen nicht beeinträchtigt werden. Gegebe-

nenfalls muss die Umsetzung von Maßnahmen gemeinsam mit dem Kunden geplant werden.

Das Rechenzentrum betreibt Datenbanksysteme für verschiedene Kunden. Die Maßnahme M 4.69 fordert einen regelmäßigen Sicherheitscheck vorhandener Datenbanken. Für die Überprüfung wird ein eigenes Werkzeug eingesetzt, welches Auswirkungen auf die Antwortzeit der Datenbanken hat.

Der IT-Sicherheitsbeauftragte hat mit den Kunden Zeitfenster für die Durchführung dieser Analysen vereinbart. Es wurde festgestellt, das in der Nacht von Samstag auf Sonntag wenige Anfragen an die Datenbank gestellt werden und in dieser Zeit die Analysen am ehesten möglich sind.

9.2.2.2 Mangelnde Akzeptanz bei den Mitarbeitern

Die Maßnahmen wurden umgesetzt, jedoch werden sie von den Mitarbeitern nicht akzeptiert. Teilweise ignorieren sie die neuen Regelungen. Wie bezieht man die Mitarbeiter mit ein?

Die frühzeitige Einbeziehung der Mitarbeiter ist ein wesentlicher Erfolgsfaktor bei der wirksamen Umsetzung der IT-Sicherheitsmaßnahmen. Werden die Mitarbeiter nicht frühzeitig mit den neuen Maßnahmen vertraut gemacht, baut sich schnell eine ablehnende Haltung auf, die einen Misserfolg der Umsetzung des GSHB zur Folge haben kann.

Durch frühzeitige Schulungs- und Informationsveranstaltungen müssen die Mitarbeiter über die anstehenden Änderungen informiert werden. Wichtig ist hierbei die Notwendigkeit zu verdeutlichen und mitzuteilen, welchen Hintergrund die Änderungen haben.

Im Rechenzentrum sind neue interne Abläufe erforderlich, das Sicherheitsmanagement-Team wurde neu gegründet und damit stehen den Mitarbeitern neue Ansprechpartner für Sicherheitsfragen zur Verfügung.

Um die Mitarbeiter auf die neuen Prozesse vorzubereiten, werden interne Informationsveranstaltungen abgehalten, bei denen die Mitarbeiter über die einzelnen Änderungen informiert werden. Zuvor hat die Leitung im Rahmen einer Betriebsversammlung die neue Sicherheits-Leitlinie vorgestellt und die Notwendigkeit der Änderungen verdeutlicht. Die Abteilungs- und Teamleiter stehen den Mitarbeitern zusätzlich zu allen Fragen hinsichtlich der Änderungen zur Verfügung, so dass für eine ausreichende Information gesorgt ist und den Mitarbeitern die Hintergründe für die Änderungen vermittelt wurden.

10 Zertifizierung

Mit dem vom BSI ausgegebenen IT-Grundschutz-Zertifikat (vgl. [GSZERT]) kann die Umsetzung des GSHB nach außen transparent gemacht werden. Aufgrund der ständigen Aktualisierung und Erweiterung des IT-Grundschutzhandbuchs bleiben die aufgeführten Standardsicherheitsmaßnahmen praktisch auf der Höhe der Zeit.

Bild 7: IT-Grundschutz-Zertifikat

Derzeit sind drei verschiedene Ausprägungen der IT-Grundschutz-Qualifizierung definiert. Anhand dieser Ausprägungen kann eine Institution schrittweise ein IT-Grundschutz-Zertifikat erreichen. Die Gültigkeit einer Qualifizierungs 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

Stufe 2: Selbsterklärung „IT-Grundschutz Aufbaustufe“

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

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 Zertifizierungsstellen 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“.

10.1 Generelle Vorgehensweise bei der Zertifizierung

Als Vorarbeit für eine Zertifizierung wird durch die Institution ein IT-Sicherheitskonzept nach der Vorgehensweise des GSHB erstellt. Anschließend werden durch einen durch die Institution zu beauftragenden und durch das BSI lizensierten IT-Grundschutz-Auditor die folgenden Punkte geprüft:

1. **Plausibilitätsprüfung**

   Der Auditor prüft, ob der IT-Verbund eine sinnvolle Mindestgröße aufweist und die Plausibilität der IT-Strukturanalyse. Weiterhin wird durchgeführte Modellierung auf Korrektheit geprüft 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.

10.2 Häufig auftretende Probleme bei der Zertifizierung

Die Probleme bei der Zertifizierung ergeben sich im wesentlichen aus den durch die Institution durchzuführenden Vorarbeiten. Problematisch sind Entscheidungen, die während der IT-Sicherheitskonzeption getroffen wurden und sich negativ auf die Zertifizierung auswirken.

10.2.1 Probleme bei der Vorbereitung

Hierbei treten Probleme auf, wenn die Institution bewusst Maßnahmen nicht umsetzt sondern die entstehenden Risiken trägt oder wenn individuelle Bausteine zur Modellierung von Komponenten verwendet werden.

10.2.1.1 IT-Verbund mit individuellem Baustein nicht zertifizierbar

Während der Plausibilitätsprüfung fällt dem Auditor auf, dass ein nicht im GSHB enthaltener Baustein zur Modellierung einer wesentlichen Komponente des IT-Verbundes genutzt wird. Der Auditor stellt fest, dass der Verbund nicht zertifizierbar ist.

Ein IT-Verbund, der eine Komponente enthält, die durch einen individuellen Baustein modelliert wurde, ist grundsätzlich nicht zertifizierbar (vgl. 7.2.1.2).

Wurde ein individueller Baustein zur Modellierung einer Komponente verwendet, kann versucht werden den IT-Verbund anders zu definieren. In diesem Fall muss versucht werden die Komponente mit dem individuellen Baustein aus dem Verbund heraus zu nehmen, so dass der verbleibende Verbund weiterhin den Anforderungen des GSHB genügt.

10.2.1.2 Maßnahmen nicht umgesetzt, da das Risiko getragen wird

Die oberste Leitung hat entschieden Notfallübungen nicht durchzuführen, da mögliche negative Auswirkungen nicht abschätzbar sind. Das Risiko, die Notfallmaßnahmen sind nicht wirkungsvoll, wird getragen. Der Auditor bemängelt dies und teilt mit, dass daher maximal eine Selbsterklärung „IT-Grundschutz Aufbaustufe" mit Testat möglich ist.

Das GSHB sieht bei der Maßnahmenumsetzung keine Option für getragene Risiken vor. Die einzige Möglichkeit ist hierbei, eine Maßnahme durch eine höherwertige Maßnahme als „entbehrlich" (vgl. Kapitel 7.2.1.3) einzustufen.

11 Beispiel Sicherheitsleitlinie

Die nachfolgende IT-Sicherheitsleitlinie basiert auf den beispielhaften Richtlinien [MURI] und ist an die Belange eines Rechenzentrums angepasst. Die Leitlinie muss insbesondere bei den *[kursiv]* dargestellten Elementen des Textes an die individuellen Gegebenheiten der jeweiligen Institution angepasst werden.

IT-Sicherheitsleitlinie

Die Institutsleitung verabschiedet hiermit folgende IT-Sicherheitsleitlinie als Bestandteil ihrer Strategie:

Stellenwert der Informationsverarbeitung

Informationsverarbeitung spielt in unserer Institution eine Schlüsselrolle. Einerseits ist Informationsverarbeitung wesentlich für unsere eigene Aufgabenerfüllung*[, andererseits betreiben wir für unsere Kunden IT-Systeme, die für diese von wesentlicher Bedeutung sind]*.

Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können, *[die Verfügbarkeitsanforderungen unserer Kunden werden berücksichtigt]*. Auch in Teilbereichen darf unser Geschäft nicht erliegen. Da auf den von uns betriebenen Systemen auch sensible Informationen unserer Kunden abgelegt sind, ist der Schutz dieser Informationen vor unberechtigtem Zugriff, vor unerlaubter Änderung und vor Nichtverfügbarkeit von *[existenzieller]* Bedeutung.

Übergreifende Ziele

[Die durch uns betriebenen IT-Systeme und Daten unserer Kunden werden derart gesichert, dass die vertraglich mit den Kunden vereinbarten Zusagen

hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität eingehalten werden.]

Gespeicherte Daten und betriebene IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer *Verfügbarkeit* so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (*Integrität*). 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 hohen finanziellen Auswirkungen müssen verhindert werden.

Alle Mitarbeiter der Institution halten die einschlägigen Gesetze (insbesondere Gesetze und Regelungen zum Datenschutz) und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße oder Verstöße gegen vertragliche Regelungen sind zu vermeiden.

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

Detailziele

[Die mit den Kunden hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität der Daten und IT-Systeme vereinbarten Zusagen werden individuell vertraglich fixiert. Technische und organisatorische Maßnahmen stellen sicher, dass die vertraglichen Zusagen eingehalten werden.]

[Die Kommunikation mit unseren Kunden und eine funktionierende Netzanbindung an diese ist für unser Geschäft elementar. Die in unserer Hoheit

liegenden Kommunikationsanbindungen unterliegen daher einem hohen Integritäts-, Verfügbarkeits- und Vertraulichkeitsschutz.]

Die Datenschutzgesetze, die Interessen unserer Mitarbeiter *[und die unserer Kunden sowie Geschäftspartner]* verlangen eine Sicherstellung der Vertraulichkeit der *[Kunden- und]* Mitarbeiterdaten. Die Daten und die IT-Anwendungen der Personalabteilung *[sowie die für die Kunden betriebenen Systeme und Kundendaten]* werden daher einem *[hohen]* Vertraulichkeitsschutz unterzogen.

Für die Vertriebsabteilung ist die Aufrechterhaltung der Kommunikation nach außen zu den Kunden und Geschäftspartnern und der Zugriff auf die Kundendatenbank elementar. Die Geschäftsabwicklung darf nicht verzögert oder gar gefährdet werden. Wenn vertraglich festgelegte Lieferfristen nicht eingehalten werden können, kann dies weitreichende negative Folgen nach sich ziehen. Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu Erlösminderungen führen. Die Aufrechterhaltung der Kommunikation und der ständige Zugriff auf korrekte Daten für die Vertriebsmitarbeiter hat einen *[normalen]* Schutzbedarf.

Innerhalb des *[für den Systembetrieb zuständigen Bereichs]* wird die Verfügbarkeit und die Fehlerfreiheit der Systeme sichergestellt. Stillstandzeiten sind nur in einem sehr geringen Maße akzeptabel, da diese indirekt – durch negative Auswirkungen auf nachfolgende Prozesse – zu Erlösminderungen führen können.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich und fester Bestandteil der Kommunikationsinfrastruktur. 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 eine IT-Sicherheitsorganisation (ein IT-Sicherheitsmanagement-Team) eingerichtet. Es ist ein IT-Sicherheitsbeauftragter benannt worden. Der IT-Sicherheitsbeauftragte berichtet in seiner Funktion direkt an die Institutsleitung. *[Unterstützt wird der IT-Sicherheitsbeauftragte von Sicherheitsverantwortlichen aus den einzelnen Bereichen der Institution.]*

Dem IT-Sicherheitsbeauftragten, *[den Sicherheitsverantwortlichen der einzelnen Bereiche]* und den Administratoren werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vom Management festgelegten IT-Sicherheitsziele zu erreichen.

Die Administratoren, der IT-Sicherheitsbeauftragte *[und die Sicherheitsbeauftragten der einzelnen Bereiche]* sind durch die IT-Benutzer ausreichend in ihrer Arbeit zu unterstützen.

Das IT-Sicherheitsmanagement-Team ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Die IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des IT-Sicherheitsmanagement-Teams zu halten.

Es wurde ein Datenschutzbeauftragter bestellt. Der Datenschutzbeauftragte hat ein ausreichend bemessenes Zeitbudget für die Erfüllung seiner Pflichten zur Verfügung. Der Datenschutzbeauftragte ist angehalten, sich regelmäßig weiterzubilden.

[Der IT-Sicherheitsbeauftragte nimmt zusätzlich die Funktion des Datenschutzbeauftragten ein.]

[Der IT-Sicherheitsbeauftragte steht mit gegebenenfalls vorhandenen IT-Sicherheitsbeauftragten der Kunden in engem Kontakt und zieht diese bei

Problemen mit relevanten Systemen in die Entscheidungsfindung ein. Für die Kunden ist er der direkte Ansprechpartner zu sicherheitsrelevanten Fragestellungen.]

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 restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge *[und Netzkopplungen mit anderen Institutionen (z.B. Kunden)]* 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 das IT-Sicherheitsmanagement-Team.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar und vor unberechtigtem Zugriff geschützt sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall *[die für unsere Kunden kritischen]* Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb *[der vertraglich vereinbarten]* Zeitspanne wiederherzustellen.

IT-Benutzer nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Institutsleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Verbesserung der Sicherheit

Das Managementsystem der IT-Sicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Leitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an das IT-Sicherheitsmanagement-Team 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 Glossar

BSI	Bundesamt für Sicherheit in der Informationstechnik
GF	Geschäftsführer / Institutsleiter
DDV	Daten-Direktverbindung oder auch Standleitung für digitale Daten.
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.
SLA	Service Level Agreement – Die SLA regelt den Umfang und die Bedingungen für die Erbringung von Dienstleistungen zwischen dem Auftragnehmer und dem Auftraggeber.
Sicherheitsprozess	Organisatorischer Prozess, der die Umsetzung und Kontrolle von IT-Sicherheitsmaßnahmen zum Ziel hat.
Grundwerte der IT-Sicherheit	Vertraulichkeit, Verfügbarkeit und Integrität

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.
Notstromaggregat	Stromerzeuger, der beim Ausfall der festinstallierten Stromversorgung für eine gewisse Zeit den Strombedarf wichtiger technischen Einrichtungen einer Institution decken kann.
Sicherheit	Informationssicherheit ist ein Prozess zur kontinuierlichen Identifikation und Handhabung von Risiken, die eine Gefährdung von Informationen, Prozessen und Systemen innerhalb einer definier-

	ten Umgebung bedeuten.
IT-Sicherheitsmanagement-Team	Die zur Erreichung des angestrebten IT-Sicherheitsniveaus anfallenden Aufgaben müssen von einer Instanz innerhalb der Institution koordiniert und verantwortlich geregelt werden. Diese Instanz wird als „IT-Sicherheitsmanagement-Team“ bezeichnet.
USV	Unterbrechungsfreie Stromersorgung

Anhang B 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

[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

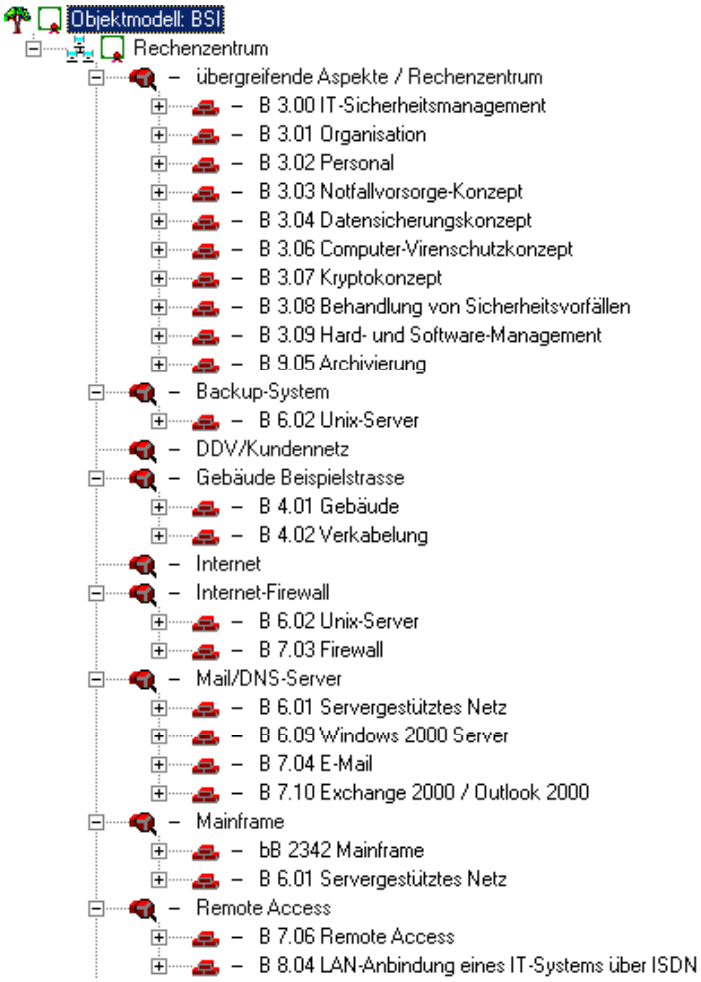
[RIABA] Risikoanalyse auf der Basis von IT-Grundschutz http://www.bsi.de/gshb/risikoanalyse/risiko.pdf

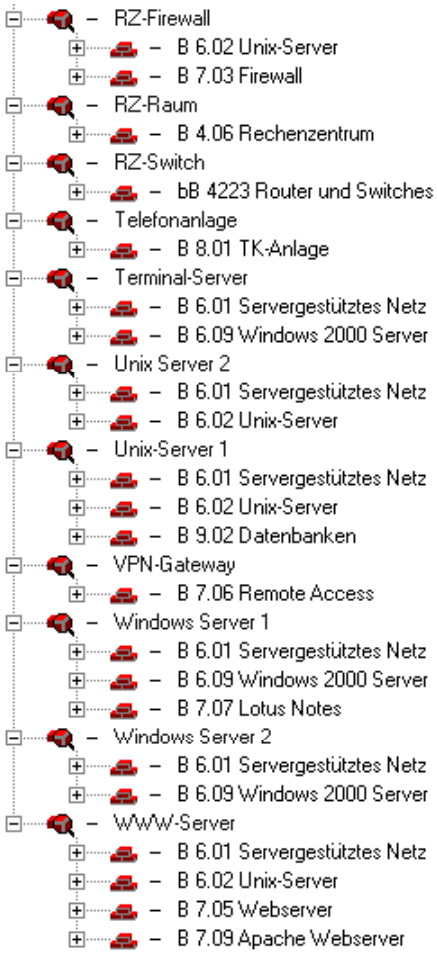
[WEBKURS] IT-Grundschutz-Schulung

http://www.bsi.bund.de/gshb/webkurs/index.htm

Anhang C Beispiele zur Strukturanalyse

In den nachfolgenden Bildern ist dargestellt, wie der in Kapitel 3 definierte IT-Verbund mit Hilfe des GSTOOL modelliert wurde.





Hierbei ist anzumerken, dass der IBM-Host (Mainframe) sowie der RZ-Switch durch individuelle Bausteine (bB2342 und bB4223) modelliert wurden.