Bundesamt
für Sicherheit in der
Informationstechnik

Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise

ISi-E

Version 1.0

Vervielfältigung und Verbreitung

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände finden Sie auf den Internet-Seiten des BSI.

http://www.bsi.bund.de oder http://www.isi-reihe.de

Bundesamt für Sicherheit in der Informationstechnik
ISi-Projektgruppe
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsübersicht

Inhaltsverzeichnis

1 Management Summary

Ziel der BSI-Standards zur Internet-Sicherheit (ISi-Reihe) ist es, Behörden und Unternehmen umfassende und aktuelle Informationen zur Verfügung zu stellen, damit diese ihre Internet-Aktivitäten möglichst eigenständig neu aufbauen, erweitern oder umbauen können. Im Fokus aller Betrachtungen steht dabei die IT-Sicherheit.

Bestandteile der ISi-Reihe sind die hier vorliegende Einführung ISi-E, Leitlinien ISi-L mit kurzen Abrissen aller relevanten Fachthemen, individuelle Studien ISi-S zu diesen Fachthemen sowie zugehörige Checklisten ISi-Check. Die Leitlinien ISi-L richtet sich primär an Führungskräfte und IT-Koordinatoren, die Studien ISi-S an alle IT-Fachleute, die Checklisten ISi-Check speziell an die Administratoren, Programmierer und Web-Entwickler sowie an die Revisoren.

Das Besondere an der ISi-Reihe ist, dass sie dem Leser einerseits einen konkreten Vorschlag macht, wie Dienste über das Internet sicher genutzt und angeboten werden können, andererseits aber dem Leser durch das Aufzeigen von Varianten große Flexibilität bei der Anpassung an individuelle Begebenheiten lässt. Durch diesen Ansatz wird sowohl normaler als auch hoher Schutzbedarf umfassend adressiert.

Die ISi-Reihe ergänzt die IT-Grundschutz-Kataloge des BSI um eine vertiefte und detailliertere Sicht rund um das Thema Internet-Sicherheit. Alle in der ISi-Reihe beschriebenen grundsätzlichen Empfehlungen werden zudem auch in die IT-Grundschutz-Kataloge aufgenommen, sodass eine Zertifizierung nach IT-Grundschutz auch die Erfüllung der Basis-Anforderungen aus der ISi-Reihe attestiert.

Anwendung finden können die BSI-Standards zur Internet-Sicherheit in allen Phasen eines Internet-Projekts: von der Analyse, über die Konzeption, die Realisierung bis hin zur Administration und zum Betrieb. Auch für die Revision können die Dokumente gewinnbringend eingesetzt werden. Detaillierte Schritt-für-Schritt-Anleitungen für die verschiedenen Projekt-Phasen werden in dem vorliegenden Dokument im sogenannten Ablaufplan gegeben.

Warum ist IT-Sicherheit überhaupt ein so wichtiges Thema? Einerseits hängen die heutigen Prozesse immer mehr von funktionierender Informations- und Kommunikationstechnik ab, andererseits wachsen die Risiken kontinuierlich. Ziel eines IT-Betriebs muss es sein, diese Risiken zu vermindern. Hierzu müssen zahlreiche IT-Sicherheitsmaßnahmen umgesetzt werden. Unter der Kernformel „Schwachstelle plus Bedrohung ergibt Gefährdung/Risiko“ werden die Begriffe „Schwachstelle“, „Bedrohung“, „Gefährdung“, „Risiko“ und „Maßnahme“ in dem vorliegenden Text erläutert und an Beispielen verständlich gemacht.

Der Kerngedanke ist, dass eine Bedrohung erst dann zum Risiko wird, wenn sie eine Schwachstelle ausnutzen kann. Da aber ständig neue Schwachstellen und Bedrohungen bekannt werden, empfiehlt es sich, von Anfang an Maßnahmen im Hinblick auf beide Aspekte zu ergreifen.

Die ISi-Reihe gibt in ihren verschiedenen Modulen detailliert Auskunft, welche Maßnahmen im Einzelfall notwendig oder sinnvoll sind und wie diese am besten umgesetzt werden. Wird der in diesem Dokument enthaltene Ablaufplan befolgt und werden alle Empfehlungen sorgfältig umgesetzt, so kann das auf der Behörde oder dem Unternehmen lastende, durch den massiven IT-Einsatz verursachte Risiko drastisch reduziert werden.

2 Einführung in die ISi-Reihe

Das Internet ist aus dem alltäglichen Handeln nicht mehr wegzudenken. Sehr viele Privatanwender und fast alle Firmen und Behörden nutzen die durch das weltumspannende Netz bereitgestellten Kommunikations- und Informationsmöglichkeiten. Das Internet hat im Zuge der Kommerzialisierung heute eine Nutzungsbreite und -intensität erreicht, die bei seiner Entwicklung nicht ansatzweise erahnt wurde. Dies ist einer der Gründe, weshalb in den 70er Jahren bei der ursprünglichen Konzeption – als es sich noch um ein mehr oder weniger geschlossenes Netz mit allseitigem Vertrauen handelte – Sicherheitsaspekte keine bzw. nur eine untergeordnete Rolle gespielt haben. Die grundlegenden Konzepte sind bis heute unverändert. Die Bedrohungslage ist jedoch eine andere.

Wie sehen wir das Internet heute? Einerseits besteht inzwischen, zumindest in den Industrienationen, eine fast flächendeckende IT-Vernetzung mit Internet-Anbindung. Parallel hierzu steigt die Abhängigkeit von einer reibungslos funktionierenden IT stetig: Immer mehr klassische Verfahren werden durch IT-gestützte, vernetzte Verfahren ersetzt. Immer mehr kritische Daten werden in Computer-Netzen wie dem Internet übertragen, verarbeitet und gespeichert.

Andererseits sind inzwischen wirkungsvolle internet-basierte Angriffsmethoden entwickelt und publiziert worden sowie passende Sabotage- und Spionagewerkzeuge nachweislich verfügbar. Die Häufigkeit von gestreuten wie auch von gezielten Angriffen aus dem Internet und auf das Internet als Infrastruktur steigt kontinuierlich an. Eine der Ursachen hierfür ist, dass immer wieder neue Schwachstellen in Standard-Produkten bekannt werden und ein Beheben dieser Schwachstellen oft nicht hinreichend schnell möglich ist.

Es ist daher die Aufgabe eines jeden Einzelnen, seinen Privat- oder Arbeitsplatz-PC, seine mobilen Endgeräte, seine Server und Hintergrundsysteme sowie sein lokales Netz vor Angriffen aus dem Internet zu schützen.

Um den offenkundigen Bedrohungen entgegenzuwirken, hat das BSI unterschiedliche Aktivitäten eingeleitet. Dazu gehört die Entwicklung und Veröffentlichung der BSI-Standards zum Thema Internet-Sicherheit, der sogenannten ISi-Reihe. Der Fokus dieser Reihe liegt auf der Sicherheit bei der Anbindung an das Internet. Dazu zählen wir auch die Nutzung des Internets sowie das Anbieten von Diensten über das Internet.

Das BSI stellt die Empfehlungen im Rahmen der ISi-Reihe in verschiedenen Sichtweisen und Detaillierungsgraden für unterschiedliche Primär-Zielgruppen zur Verfügung. Hierbei liegt der Schwerpunkt auf technischen Aspekten; organisatorische und rechtliche Aspekte werden nur insoweit betrachtet, wie sie internet-spezifisch sind.

In den folgenden Abschnitten finden Sie Informationen zu Zielsetzung und Zielgruppen sowie Aufbau und Anwendung der ISi-Reihe. Neben dieser allgemeinen Einführung enthält dieses Dokument eine Einführung in die Grundlagen der Internet-Sicherheit sowie einen detaillierten Ablaufplan für die Phasen „Planung“, „Konzeption“, „Realisierung“ sowie „Administration und Betrieb“ einer sicheren Internet-Anbindung.

Bei Fragen und Anregungen können Sie sich über die E-Mail-Adressen isi@bsi.bund.de bzw. internetsicherheit@bsi.bund.de jederzeit an uns wenden. Wir freuen uns auf Ihr Feedback.

Vorab noch zwei Hinweise:

Die Veröffentlichung der ISi-Reihe erfolgt im Internet auf den Webseiten des BSI unter dem Stichwort „Internet-Sicherheit“. Die Seiten sind auch unmittelbar über die Web-Adresse http://www.isi-reihe.de erreichbar.

Die Gültigkeit der einzelnen Texte ist aufgrund technischer Weiterentwicklungen zeitlich begrenzt. Jedes Dokument wird daher in regelmäßigen Abständen auf Aktualität geprüft und gegebenenfalls aktualisiert. Die veröffentlichten Stände werden durch Versionsnummern gekennzeichnet, sodass sie jederzeit eindeutig referenzierbar sind.

2.1 Zielsetzung, Zielgruppen und formaler Aufbau

Das BSI verfolgt mit den BSI-Standards zur Internet-Sicherheit (ISi-Reihe) drei Kernziele.

1. Die ISi-Reihe dient als Wissensbasis und Hilfe zur Selbsthilfe für Behörden und Unternehmen, damit diese die notwendige, definierte Standard-Internet-Sicherheit in allen im Ablaufplan beschriebenen Projekt-Phasen („Planung“, „Konzeption“, „Realisierung“ sowie „Administration und Betrieb“) selbst umsetzen können. Sie bildet die Grundlage für die Beratung zum Thema Internet-Sicherheit durch das BSI und seine Vertragspartner.
2. Die ISi-Reihe dokumentiert den aktuellen Stand der Technik und schafft darüber hinaus durch die Formulierung von allgemeinen wie auch konkreten Anforderungen einen Quasi-Standard für den Bereich Internet-Sicherheit, der referenzierbar zur Verfügung steht.
3. Die ISi-Reihe macht Internet-Sicherheit prüfbar und stellt somit insbesondere eine Arbeitshilfe für Administratoren sowie eine Grundlage für die Revision von Internet-Anbindungen zur Verfügung.

Die ISi-Reihe besteht aus

- der vorliegenden Einführung in die ISi-Reihe (ISi-E),
- Leitlinien zur Internet-Sicherheit (ISi-L),
- Studien zur Internet-Sicherheit (ISi-S) sowie
- Checklisten zur Internet-Sicherheit (ISi-Check).

In Abbildung 2.1 ist der zuvor beschriebene Aufbau der ISi-Reihe grafisch dargestellt. Eine Studie wird zusammen mit der zugehörigen Leitlinie und Checklisten als Modul der ISi-Reihe bezeichnet. Eine genauere Beschreibung der einzelnen Teile erfolgt im nachfolgenden Abschnitt 2.2.

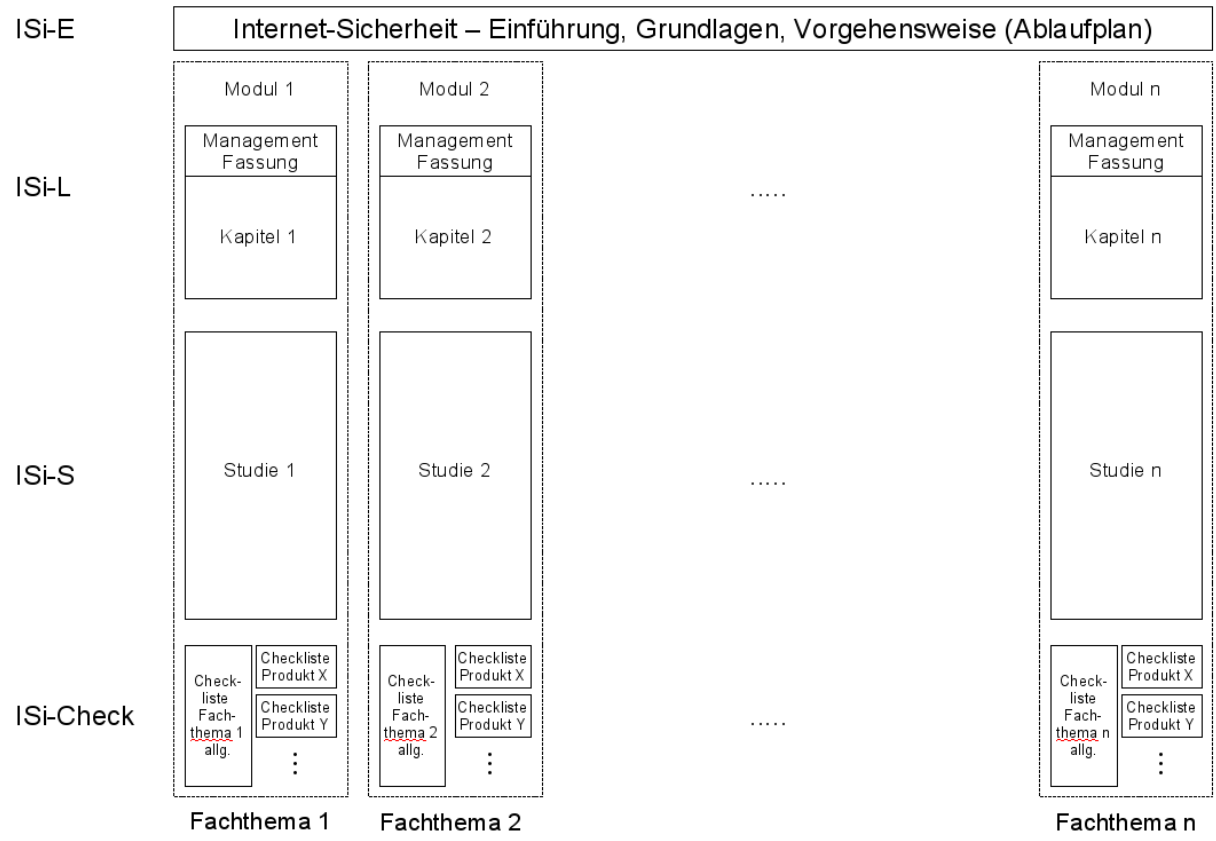

Abbildung 2.1: Aufbau der ISi-Reihe

Die zuvor beschriebenen Publikationen richten sich in erster Linie an folgende Primärzielgruppen:

- IT-Führungskräfte (z. B. CIO, IT-Leiter, IT-Direktoren, ...) in Behörden und Unternehmen,
- IT-Fachleute, -Experten, -Berater in Behörden und Unternehmen, insbesondere IT-Sicherheitsbeauftragte, sowie
- Administratoren, Programmierer und Web-Entwickler in Behörden und Unternehmen,

die sich mit der Internet-Anbindung beschäftigen, dazu zählen in diesem Kontext auch das Anbieten von Diensten über das Internet und die Nutzung des Internets. Darüber hinaus hält sich das BSI im Rahmen der ISi-Reihe die Option offen, auch die Betreiber der Internet-Infrastruktur anzusprechen.

Allerdings sind nicht alle Dokumente gleichermaßen für alle Zielgruppen bestimmt. Die Leitlinien ISi-L richten sich primär an Führungskräfte und IT-Koordinatoren, die Studien ISi-S an alle IT-Fachleute, die Checklisten ISi-Check speziell an die Administratoren, Programmierer und Web-Entwickler sowie an die IT-Revisoren.

Die Publikationen sind darüber hinaus für weitere Zielgruppen von Interesse. Hierzu zählen insbesondere

- Hersteller von IT, die die getroffenen Aussagen bei der Produktentwicklung und -weiterentwicklung berücksichtigen sollen, sowie

- Lehrende und Dozenten, insbesondere an Universitäten und Fachhochschulen, die die Inhalte der ISi-Reihe als umfassendes Basismaterial für die Aus- und Fortbildung im Bereich Internet-Sicherheit nutzen können.

2.2 Elemente der ISi-Reihe

Wie in Abbildung 2.1 gesehen, besteht die ISi-Reihe aus ISi-E, ISi-L, ISi-S und ISi-Check. Was verbirgt sich hinter diesen einzelnen Elementen?

2.2.1 ISi-E

Als Einführung und Wegweiser durch die ISi-Reihe dient der vorliegende Text ISi-E unter dem Titel „Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise“. Nach einer allgemeinen Sensibilisierung für das Thema Internet-Sicherheit wird eine umfassende Einführung in Zielsetzung, Aufbau und Anwendung der ISi-Reihe gegeben. Durch einen detaillierten Ablaufplan wird die Anwendung der ISi-Reihe in allen Projekt-Phasen der Internet-Anbindung konkret erläutert. Darüber hinaus wird im ISi-E ein Überblick zur Thematik Bedrohungen, Schwachstellen, Gefährdungen und IT-Sicherheitsmaßnahmen gegeben: Begriffe, die bei der Erarbeitung der in der ISi-Reihe formulierten Empfehlungen eine entscheidende Rolle spielen und somit auch für das Verständnis und die Anwendung der ISi-Reihe hilfreich sind.

2.2.2 ISi-L

Die „Leitlinie zur Internet-Sicherheit“ (ISi-L) gibt einen fachlichen Überblick über das spezielle Fachthema (zur Themenauswahl siehe Abschnitt 2.3). Hierin werden die Leser für die konkreten Frage- und Problemstellungen des jeweiligen Fachthemas sensibilisiert. Eine Kurzdarstellung der bestehenden Gefährdungen sowie der Möglichkeiten zur Absicherung rundet den ISi-L ab.

Jede Leitlinie ISi-L enthält zudem eine Management-Fassung, die über die wesentlichen Thesen zu dem behandelten Fachthema informiert und die Hauptaussagen zusammenfasst. Die gesamte Darstellung ist für technisch geprägte Leser allgemein verständlich; das Abstraktionsniveau ist hoch. Auf technische Details wird im ISi-L weitestgehend verzichtet.

2.2.3 ISi-S

Kernelement der ISi-Reihe sind die „Studien zur Internet-Sicherheit“ (ISi-S). Zu jedem Fachthema, wird eine Studie erstellt, die alle hierfür relevanten Aspekte detailliert ausführt.

In einer konkreten Studie werden die Grundlagen des behandelten Fachthemas ausführlich erläutert sowie Wechselwirkungen und Zusammenhänge mit anderen Fachthemen beleuchtet. Ebenso wird auf die relevanten Standards und Protokolle eingegangen.

Der Fokus einer konkreten Studie liegt auf der Darstellung einer Grundarchitektur und grundlegender Vorgaben für Beschaffung, Konfiguration und Betrieb sowie auf der Beschreibung der spezifischen Gefährdungen (Schwachstellen und Bedrohungen) und der sich darauf beziehenden Varianten für das betrachtete Fachthema. Unter Varianten fallen hier Maßnahmen, Musterlösungen/Beispiele und Lösungsansätze, die sich von der Grundarchitektur unterscheiden. Dabei werden, wo sinnvoll,

mehrere unterschiedliche Lösungen vorgestellt und diskutiert, sodass in allen Situationen ein angemessenes Sicherheitsniveau erreicht werden kann.

2.2.4 ISi-Check

Als praxisnahe Anwendungshilfe werden die „Checklisten zur Internet-Sicherheit“ (ISi-Check) erstellt und veröffentlicht. Zu jeder Studie gibt es eine produktübergreifende Checkliste, in der die relevanten Sicherheitsmaßnahmen zusammengefasst sind und anhand derer die Umsetzung der im ISi-S gegebenen Empfehlungen zum jeweiligen Fachthema im Detail überprüft werden kann.

Ferner kann es in Ergänzung zu der produktübergreifenden Checkliste, wenn nötig und sinnvoll, auch produktbezogene Checklisten geben, die gezielt auf die speziellen Aspekte einzelner Produkte bzw. Produktklassen im Kontext Internet-Sicherheit eingehen. Die Aufnahme von Produkt-Checklisten ist allerdings nur dann sinnvoll und möglich, wenn der Markt durch wenige Produkte beherrscht wird.

2.3 Überblick über die fachlichen Inhalte

Die ISi-Reihe richtet sich im weitesten Sinne an IT-Fachleute, die sich mit der Nutzung des Internets und dem Anbieten von Diensten über das Internet beschäftigen.

Die ISi-Reihe enthält daher im Themenbereich „Dienste und Anwendungen im Internet“ als zentralem Teil eine Reihe von Modulen, die sich mit der sicheren Nutzung bzw. dem sicheren Betrieb dieser Dienste und Anwendungen beschäftigen. In diesen Modulen wird insbesondere auf die dienst- bzw. anwendungsspezifischen Gefährdungen (Schwachstellen und Bedrohungen) und sich darauf beziehende Empfehlungen eingegangen. Die Ausführungen in diesem Teil der ISi-Reihe betreffen im Wesentlichen die Anwendungsschicht des TCP/IP-Referenzmodells.

Eine Absicherung der Anwendungen kann jedoch nur erfolgreich sein, wenn sie nicht durch Angriffe auf darunter liegenden Schichten umgangen werden kann. Folglich beschäftigt sich die ISi-Reihe im Themenbereich „Aufbau des Netzes“ auch umfassend mit den zugrunde liegenden Techniken auf den unteren Schichten des TCP/IP-Referenzmodells. Daneben darf der Schutz der im Netz eingesetzten Komponenten nicht vernachlässigt werden. Im Themenbereich „Komponenten im Netz“ werden daher die Absicherung von Servern und PC-Clients im Allgemeinen beschrieben.

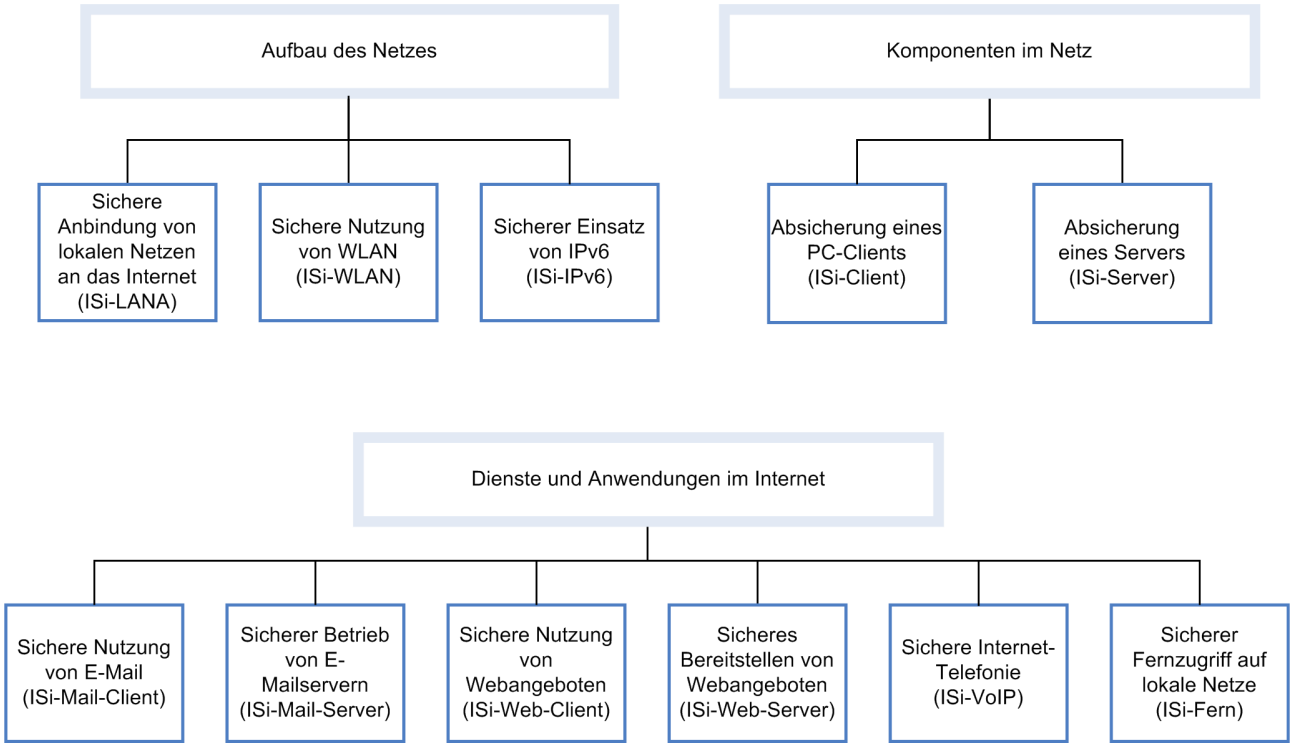

Abbildung 2.2: Themenstruktur der ISi-Reihe

Auswahl und Strukturierung der Inhalte werden durch das BSI laufend überprüft und bei Bedarf aktualisiert.

Um an die jeweilige Situation vor Ort angepasste, d. h. für verschiedene Szenarien angemessene Empfehlungen geben zu können, wird in den Modulen der ISi-Reihe nach verschiedenen Sicherheitsniveaus (Schutzbedarfsklassen) unterschieden. Verwendet wird hierbei grundsätzlich die Einteilung in die Klassen „normaler Schutzbedarf“, „hoher Schutzbedarf“ und „sehr hoher Schutzbedarf“, wie sie im BSI-Standard 100-2 (vormals IT-Grundschutzhandbuch) definiert ist.

2.4 Was ist das Besondere an der ISi-Reihe?

Die flächendeckende Vernetzung von informationstechnischen Komponenten führt dazu, dass das Internet zu einem vorrangig genutzten Ort für Computerkriminalität geworden ist. Die individuelle Absicherung der in einem Informationsverbund bestehenden IT-Systeme reicht nicht mehr aus, um Systeme und Daten hinreichend zu schützen. Durch die Verbindung mit dem Internet entsteht eine Vielzahl neuer Gefährdungen. Die ISi-Reihe zeigt daher wie IP-Netze und -Dienste sicher gestaltet werden können.

Die ISi-Reihe verfolgt dabei einen ganzheitlichen Ansatz und legt ganz bewusst einen Schwerpunkt auf die Phase der Konzeption. Hierunter fällt sowohl die Konzeption einer neuen oder die Überarbeitung einer bestehenden Internet-Anbindung, die Integration eines neuen Dienstes in ein bestehendes Netz als auch die Aktualisierung des Sicherheitskonzepts aufgrund geänderter Rahmenbedingungen. In der ISi-Reihe wird durch die konkrete Beschreibung einer sicheren, modular erweiterbaren Grundarchitektur die Basis für ein ganzheitliches Sicherheitskonzept gelegt, die alle Aspekte der Internetsicherheit berücksichtigt.

Die in den Modulen vorgestellte Grundarchitektur sowie die grundsätzlichen Empfehlungen für die Beschaffung, für die sichere Konfiguration und für den sicheren Betrieb der einzelnen Komponenten bilden eine Art Quasi-Standard für Institutionen, die ihr lokales Netz mit normalem Schutzbedarf sicher an das Internet anbinden und die Dienste und Anwendungen im Internet sicher nutzen und anbieten wollen.

Klar ist, dass nicht jedes Netz und nicht jede Internet-Anbindung gleich aussieht. Um dies zu berücksichtigen, werden in der ISi-Reihe neben den Grundempfehlungen alternative Möglichkeiten vorgestellt, die geeignet sind, den bestehenden Gefährdungen zu begegnen. Dabei wird auch erläutert, worin das jeweilige Restrisiko besteht, wenn man sich für die eine oder andere Lösung entscheidet.

Darüber hinaus bietet die ISi-Reihe ausdrücklich zusätzliche Empfehlungen für Bereiche mit hohem Schutzbedarf, also z. B. für den Schutz der Vertraulichkeit von sensiblen, personenbezogenen Daten. Empfehlungen für „sehr hohen Schutzbedarf“ werden nicht gegeben; das BSI geht davon aus, dass Anwendungen und Daten mit „sehr hohem Schutzbedarf” nicht an das Internet angeschlossen werden.

Dieser Aufbau der ISi-Reihe gewährleistet, dass sich der Leser für seine individuelle Situation angemessene und wirtschaftliche Lösungen modular zusammenstellen kann.

Die geschlossene Darstellung eines jeden Fachthemas zur Internetsicherheit in einem Modul bietet zudem eine attraktive Möglichkeit, sich intensiv mit einzelnen Themen zu beschäftigen oder auch sein Wissen nach und nach um weitere Bereiche zu erweitern. Dabei werden bestehende Wechselwirkungen gezielt beschrieben, sodass der ganzheitliche Ansatz trotz des modularen Aufbaus konsequent bestehen bleibt.

2.4.1 Zusammenspiel mit anderen Veröffentlichungen des BSI

Mit den IT-Grundschutz-Katalogen und den BSI-Standards 100-1ff verfügt das BSI über eine zentrale Veröffentlichung, die in vielen Bereichen großen Einfluss auf die Absicherung bestehender IT-Landschaften hat. Es ist auch möglich, einen Informationsverbund nach ISO 27001 auf der Basis von IT-Grundschutz zu zertifizieren.

In den vergangenen Jahren wurden zudem einige Studien durch das BSI erstellt, die sich dem Bereich Internet-Sicherheit zuordnen lassen. Aufgrund des umfassenden – alle Bereiche der IT betrachtenden – Ansatzes von IT-Grundschutz, werden die Bedrohungen und Maßnahmen in den IT-Grundschutz-Katalogen zumeist in einer kompakten Form dargestellt.

Die ISi-Reihe ergänzt die IT-Grundschutz-Kataloge in Bezug auf das Teilgebiet Internet-Sicherheit in dreierlei Hinsicht:

1. Die ISi-Reihe beschreibt die gegebenen Empfehlungen detailliert und ergänzt sie durch Checklisten.
2. Die ISi-Reihe präsentiert in Bezug auf bestehende Gefährdungen alternative Empfehlungen, aus denen der Anwender für seine individuelle Situation die am besten geeignete auswählen kann.
3. Die ISi-Reihe gibt in allen Bereichen auch Empfehlungen für hohen Schutzbedarf.

Alle Standard-Gefährdungen und Standard-Maßnahmen aus den Modulen der ISi-Reihe werden – in komprimierter Form – auch in die IT-Grundschutz-Kataloge übernommen. Aspekte, in erster Linie organisatorischer Art, die für die gesamte IT gelten, werden hingegen in der Regel ausschließlich in den IT-Grundschutz-Katalogen betrachtet.

3 Anwendung der ISi-Reihe

Fast alle Unternehmen und Behörden haben inzwischen Schritte unternommen, um Dienste über das Internet zu nutzen, Dienste selbst anzubieten oder sogar ihr lokales Netz teilweise oder vollständig an das Internet anzubinden. Um sich vor den zwangsläufig vorhandenen Gefahren bei der physikalischen Verbindung von Rechnern oder lokalen Netzen mit dem Internet zu schützen, werden bereits viele IT-Sicherheits-Maßnahmen umgesetzt. In der Regel dürfte die Absicherung jedoch lückenhaft sein. Dies liegt zum einen an dem rasanten technischen Fortschritt verbunden mit immer neuen Bedrohungen und Schwachstellen sowie immer neuen Schutzmechanismen, zum anderen an den zumeist sukzessive gewachsenen Strukturen in den Institutionen, die Sicherheit erst nach und nach berücksichtigt haben.

Mithilfe der ISi-Reihe soll es Ihnen gelingen, diese Lücken in der Absicherung zu schließen und/oder neue Dienste sicher in einen bestehenden Aufbau zu integrieren. Allerdings müssen Sie sich darauf einlassen, ihre bestehende Architektur für eine gewisse Zeit zu vergessen und in einem ersten Schritt nochmal ganz von vorne anzufangen (zumindest im Kopf oder auf Papier). So wie es auch diejenigen tun, die ihre Institution erstmalig mit dem Internet verbinden wollen. Es lohnt den Aufwand. Wie also nutzen Sie konkret die ISi-Reihe?

Ablaufplan

Der in Abschnitt 5 dieses Textes beschriebene Ablaufplan erläutert Ihnen Schritt für Schritt, wie Sie die ISi-Reihe in den Phasen „Analyse“, „Konzeption“, „Realisierung“ sowie „Administration und Betrieb“ anwenden. Um Ihnen aber schon hier einen ersten Eindruck zu vermitteln, gehen wir genauer auf das zentrale Element der ISi-Reihe ein, die Studien ISi-S.

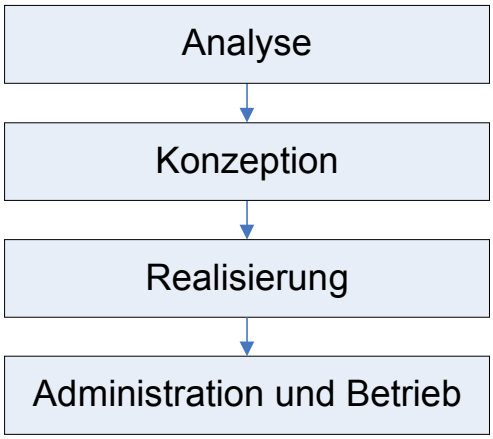

Abbildung 3.1.: Die Phasen im Ablaufplan.

Jede Studie ISi-S besteht im Wesentlichen aus den Abschnitten Grundlagen, Grundarchitektur, Grundanforderungen an Auswahl, Konfiguration und Betrieb, Gefährdungen und Empfehlungen mit Varianten für den normalen und hohen Schutzbedarf sowie einer Abdeckungsmatrix zwischen Gefährdungen und Empfehlungen (siehe Abbildung 3.2). Beispiele für verschiedene Szenarien sind im Anhang jeder Studie zu finden.

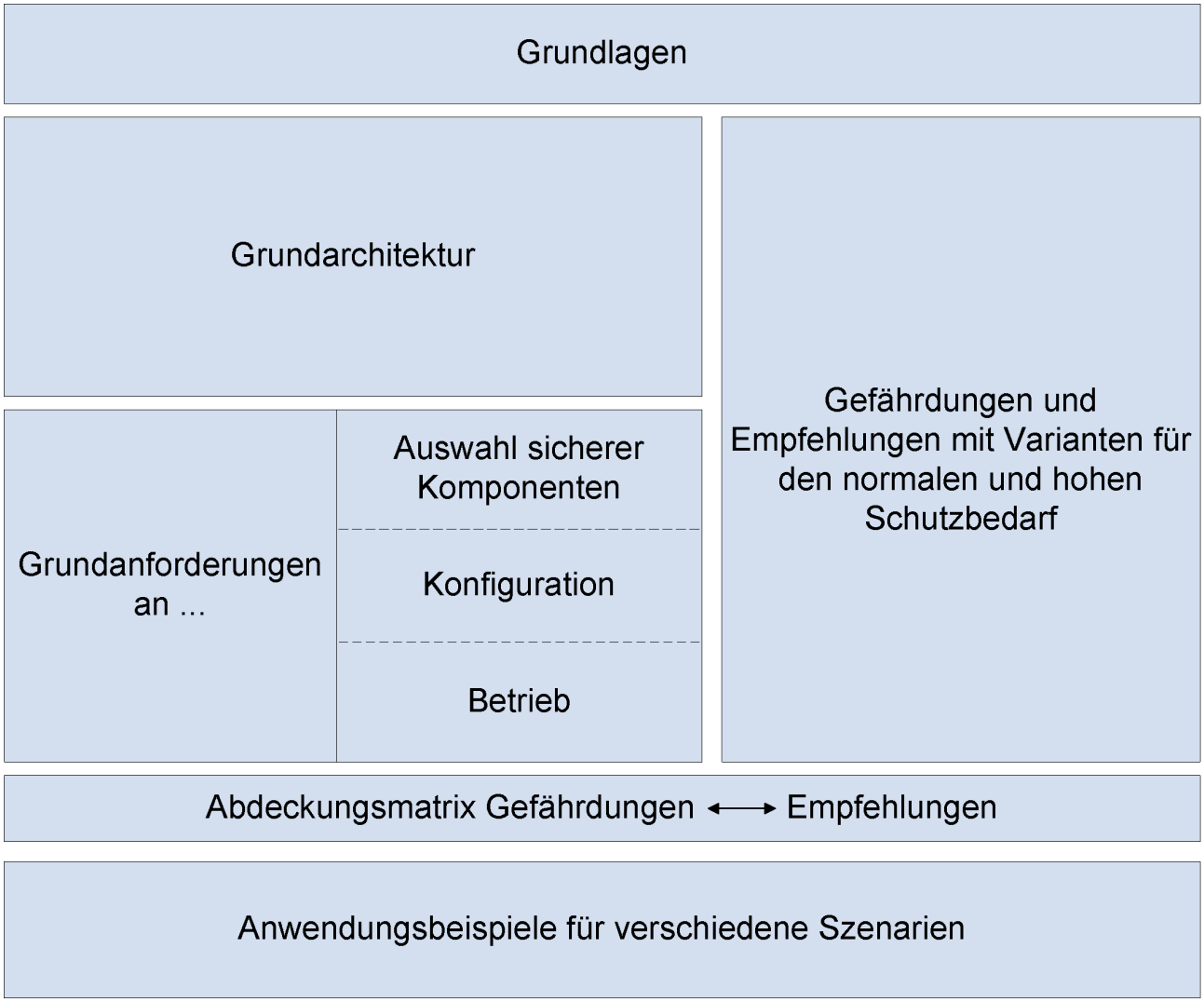

Abbildung 3.2: Bestandteile jeder Studie ISi-S

Die ISi-Reihe unterstützt durch ihre umfassenden Empfehlungen insbesondere die Phase der Konzeption; denn ein gutes und sicheres Konzept ist die Grundvoraussetzung für das sichere Umsetzen aller nachfolgenden Schritte.

3.1 Konzeption

Der Aufbau der Studien ISi-S spiegelt direkt die im Rahmen der Konzeption aufeinander folgenden Schritte wider. Dabei werden einige Schritte mehrfach durchlaufen (siehe hierzu Phase 2 im Ablaufplan (siehe Abschnitt 5), zunächst für das interne Netz und den Übergang zum Internet, anschließend für die benötigten Komponenten im Netz sowie für Dienste und Anwendungen. Die Anwendung der ISi-Reihe wird im Folgenden beschrieben (Abbildung 3.3).

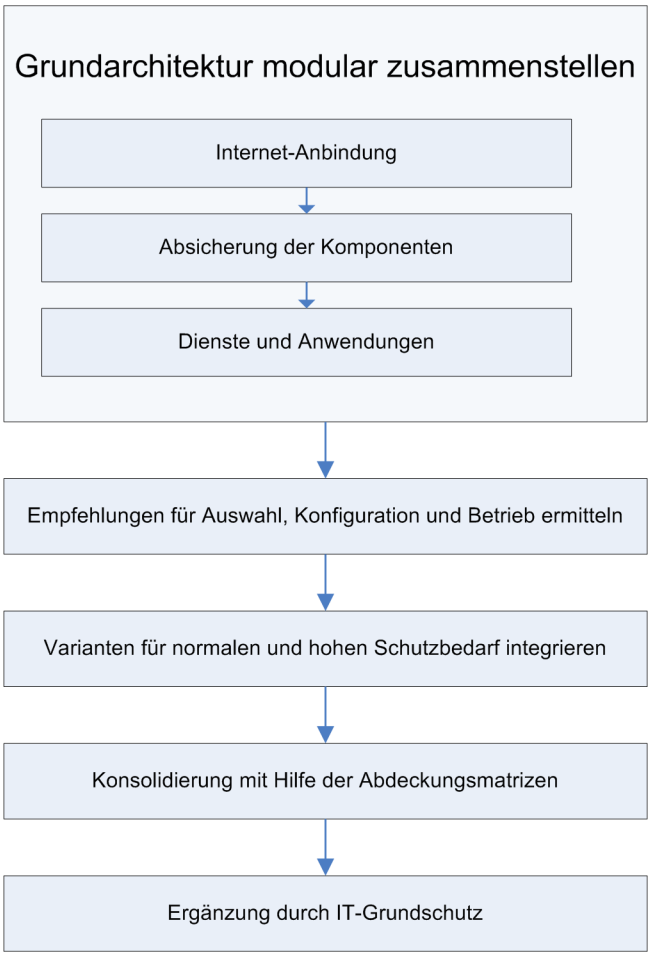

Abbildung 3.3: Ablaufschema der Konzeption

Grundarchitektur und Grundanforderungen für Auswahl, Konfiguration und Betrieb

Um eine Internet-Anbindung oder einen neuen Dienst von Grund auf zu konzipieren, beginnen Sie mit der Grundarchitektur. Dieses Vorgehen empfehlen wir Ihnen, auch wenn Sie bereits eine komplexe Anbindung im Einsatz haben. Die für Sie passende Architektur finden Sie im ISI-S der jeweiligen Module der ISi-Reihe (vgl. Abschnitt 2.3). Beginnend mit den Modulen zum Aufbau des Netzes, ergänzt durch die Empfehlungen zu den Komponenten im Netz und den Diensten, die Sie einsetzen möchten, stellen Sie Ihre Grundarchitektur modular zusammen. Zu allen Komponenten der Grundarchitektur finden Sie im ISi-S zudem Grundanforderungen für die Auswahl, die Konfiguration und den Betrieb.

Gefährdungen und Empfehlungen mit Varianten für den normalen und hohen Schutzbedarf

Zu diesem Zeitpunkt haben Sie bereits ein für normalen Schutzbedarf sicheres Netz mit einer sicheren Anbindung an das Internet vollständig entworfen. Nun haben Sie aber eventuell Teilbereiche in Ihrem internen Netz, die einen hohen Schutzbedarf in Bezug auf Vertraulichkeit und/oder Verfügbarkeit haben. Oder die auf dem Papier erstellte Architektur ist noch sehr weit entfernt von der bereits umgesetzten Architektur. Oder Sie schätzen gewisse Anforderungen als übertrieben bzw. als nicht ausreichend ein.

Nutzen Sie daher im Anschluss die Varianten, die im jeweiligen ISi-S den Gefährdungen zugeordnet dargestellt sind, um Ihre Grundarchitektur anzupassen. Hier werden ganz bewusst andere Lösungsmöglichkeiten dargestellt, unter Abwägung der damit verbundenen Restrisiken. Sie können also Ihre entworfene Architektur ganz individuell an Ihre Bedürfnisse anpassen und verändern. Die ISi-Reihe gibt Ihnen ausreichend Informationen, um in eigener Verantwortung eine gute Entscheidung treffen zu können.

Die Beispiele im Anhang der Studie unterstützen Sie bei Ihrer Auswahl. Anhand verschiedener Szenarien wird gezeigt, wie Institutionen unterschiedlicher Größe (klein, mittel, groß) sowohl eine Lösung für den normalen als auch den hohem Schutzbedarf finden können. Exemplarisch wird dargestellt, welchen Einfluss die Auswahl verschiedener Varianten auf das verbleibende Risiko hat.

Auf diese Weise konzipieren Sie auf Basis der ISi-Reihe eine Architektur und Anforderungen an die darin enthaltenen Komponenten, die Ihren Erfordernissen entsprechen und zugleich die Eigenheiten des bei Ihnen bereits realisierten Netzaufbaus – soweit diese sicher sind – bestmöglich berücksichtigen. Bei verbleibenden Unterschieden zwischen Soll und Ist sollten Sie dann sehr genau überlegen, ob Sie an diesen Punkten den Ist-Zustand unverändert beibehalten können.

Konsolidierung und Überprüfung anhand der Abdeckungsmatrix

In einem letzten Schritt sollten Sie zu Ihrer eigenen Sicherheit die Abdeckungsmatrizen nutzen. Mit deren Hilfe können Sie feststellen, ob Sie durch die ausgewählten Empfehlungen alle Gefährdungen hinreichend abdecken. In diesem Zuge können Sie auch erkennen, ob Sie auf die Umsetzung einzelner Empfehlungen verzichten können, weil der abzusicherten Gefährdung eventuell schon durch andere Empfehlungen ausreichend begegnet wurde. So können Sie Ihren Aufwand ohne Sicherheitseinbußen reduzieren.

Allgemeine IT-Grundschutz-Maßnahmen

Nachdem Sie nun wissen, welche Komponenten Sie einsetzen werden, empfiehlt sich eine abschließende Modellierung nach IT-Grundschutz. Viele der dabei identifizierten Maßnahmen können Sie ignorieren, da Sie diese bereits im Rahmen der ISi-Konzeption berücksichtigt haben. Allerdings erhalten Sie darüber hinaus eine Reihe von IT-Grundschutz-Maßnahmen, die sich allgemeinen Aspekten zuwenden (Gebäudesicherheit, allgemeine personelle und organisatorische Regelungen), die nicht internet-typisch sind und daher in der ISi-Reihe nicht erneut aufgegriffen werden. Ergänzen Sie daher Ihre Konzepte um diese Maßnahmen, sofern Sie solch allgemeine Maßnahmen nicht auch in übergeordnete Konzepte ausgelagert haben.

3.2 Realisierung

Die Phase 3 im Ablaufplan beschreibt die Realisierung der zuvor konzipierten Architektur. Hierunter fallen insbesondere auch die Auswahl und Beschaffung sowie die Konfiguration der benötigten Komponenten, also der Hardware und der Software. Sollte in Einzelfällen z. B. keine geeignete Software existieren, so können aus den im ISi-S enthaltenen Anforderungen Anforderungen an die Erstellung dieser Software abgeleitet werden.

Im Rahmen der Konzeption wurden mithilfe des ISi-S bereits die relevanten Anforderungen an die Komponenten zusammengestellt, die es nun zu berücksichtigen gilt. Um diesen Schritt besonders einfach zu gestalten, enthält die ISi-Reihe Checklisten, die bei der Realisierung angewendet werden können, und zwar sowohl für die Auswahl als auch für die Konfiguration der Komponenten.

3.3 Administration und Betrieb

Im Ablaufplan werden in Phase 4 der Betrieb der Internet-Anbindung mit ihren Diensten und Anwendungen sowie die zugehörige Administration betrachtet. Hier kommen die aus den Studien ISi-S zusammengestellten Empfehlungen für einen sicheren Betrieb zur Anwendung. Und wie schon in der Phase 3 „Realisierung“ unterstützt eine Checkliste ISi-Check die Administratoren bei diesem Vorgehen.

3.4 IT-Revision

Die Checklisten ISi-Check sind so erstellt, dass sie sich auch gut für den Einsatz im Zuge einer IT-Revision eignen. Um darzustellen, wie eine IT-Revision sinnvoll durchgeführt werden kann, soll zu einem späteren Zeitpunkt im Ablaufplan eine eigene Phase mit dem Titel „IT-Revision“ aufgenommen werden. Detaillierte Informationen finden sich schon heute in dem vom BSI veröffentlichten Leitfaden „Integration und IT-Revision von Netzübergängen“[1].

1 https://www.bsi.bund.de/cae/servlet/contentblob/478312/publicationFile/30909/Teil_I_LeitfadenRevision_pdf.pdf

4 Grundlagen der Internet-Sicherheit

Bevor in den einzelnen Modulen der ISi-Reihe ins Detail gegangen wird, sollen in den nachfolgenden Abschnitten die Grundbegriffe Bedrohung, Schwachstelle, Gefährdung und Maßnahme eingeführt und erläutert werden. Ein grundlegendes Verständnis dieser Begriffe ist wichtig, um ein IT-System sicher zu konzipieren, zu realisieren und zu betreiben.

Wichtig ist zudem, dass man sich dauerhaft mit dem Thema IT-Sicherheit beschäftigt. Eine wertvolle Quelle für aktuelle Informationen sind hier die Computer Emergency Response Teams (CERTs), wie z. B. CERT-Bund[2].

Beim Konzipieren und Administrieren von sicheren IT-Systemen gibt es ein grundlegendes Problem: aus Sicherheitssicht müssen sehr strenge Forderungen aufgestellt werden, die den Nutzer zum Teil bei seiner Arbeit einschränken oder belasten. Will man die Anforderungen der Nutzer bestmöglich umsetzen, so lassen sich die in der Sicherheitsleitlinie formulierten Sicherheitsanforderungen nicht mehr vollständig umsetzen.

Es geht hier also um ein Abwägen: Es muss ein Kompromiss gefunden werden zwischen Sicherheit, Funktionalität und Benutzerfreundlichkeit. Klar ist auch, dass es 100%ige Sicherheit nicht gibt. Die erreichte Sicherheit muss angemessen sein, der Umfang der Absicherung hängt also in erster Linie von dem Schutzbedarf der betrachteten Daten und Systeme ab. Die verbleibende Unsicherheit nennt man Restrisiko. Dieses muss man selbst tragen oder über Versicherungen auf Dritte übertragen.

4.1 Einführung der Begriffe

Bedrohung plus Schwachstelle ergibt Gefährdung; dies ist die Kernformel für die Betrachtung von Gefährdungen und Gegenmaßnahmen. Dabei richtet sich die Bedrohung stets gegen einen Grundwert der Informationssicherheit, also gegen die Vertraulichkeit, die Verfügbarkeit oder die Integrität von Informationen. Eine Schwachstelle besteht z. B. in einem IT-System oder in organisatorischen Regelungen.

Eine Bedrohung allein, wie sie durch einen Hacker, einen Spion, jegliche Form von Schadprogrammen (Viren, Würmer, Trojanische Pferde …) oder aber auch durch höhere Gewalt besteht, wäre für ein perfektes IT-System (sofern es so etwas gäbe) nicht gefährlich. Erst dadurch, dass das System oder die das System umgebenden Personen, Räumlichkeiten oder Regelungen eine Schwachstelle aufweisen, die durch eine Bedrohung ausgenutzt werden kann, entsteht eine Gefährdung und damit verbunden ein Risiko.

Gibt es ein IT-System ohne Schwachstellen? Nein. Die perfekte Software gibt es genauso wenig wie den perfekten Menschen oder die perfekte Organisation. Schwachstellen sind allgegenwärtig. Angreifer sind stets auf der Suche nach bisher unentdeckten Schwachstellen. Finden sie eine solche, bevor es der Hersteller weiß, können sie mit entsprechenden Exploits[3] besonders große Schäden anrichten. Aber auch bekannte Schwachstellen können noch lange Zeit missbräuchlich ausgenutzt werden.

Welcher Handlungsbedarf besteht bei den IT-Verantwortlichen? Sie müssen Maßnahmen ergreifen, einerseits, um bekannte Schwachstellen schnellstmöglich zu schließen, und andererseits, um prophylaktisch Bedrohungen erst gar nicht zu ihren Systemen gelangen zu lassen. Lässt ein Sicherheits-Gateway beispielsweise eine von Viren befallene E-Mail erst gar nicht in das Hausnetz, so können eventuelle Schwachstellen durch diese Bedrohung auch nicht ausgenutzt werden; eine Ge-

2 https://www.bsi.bund.de/DE/Themen/CERTBund/certbund_node.html
3 Routine zum Ausnutzen einer Schwachstelle

fährdung besteht aufgrund der ergriffenen Maßnahme „Sicherheits-Gateway korrekt konfiguriert“ nicht.

In der dreigeteilten Abbildung 4.1 werden die Begriffe „Bedrohung“, „Schwachstelle“, „Gefährdung“, „Risiko“ und „Maßnahme“ grafisch in Zusammenhang gebracht.

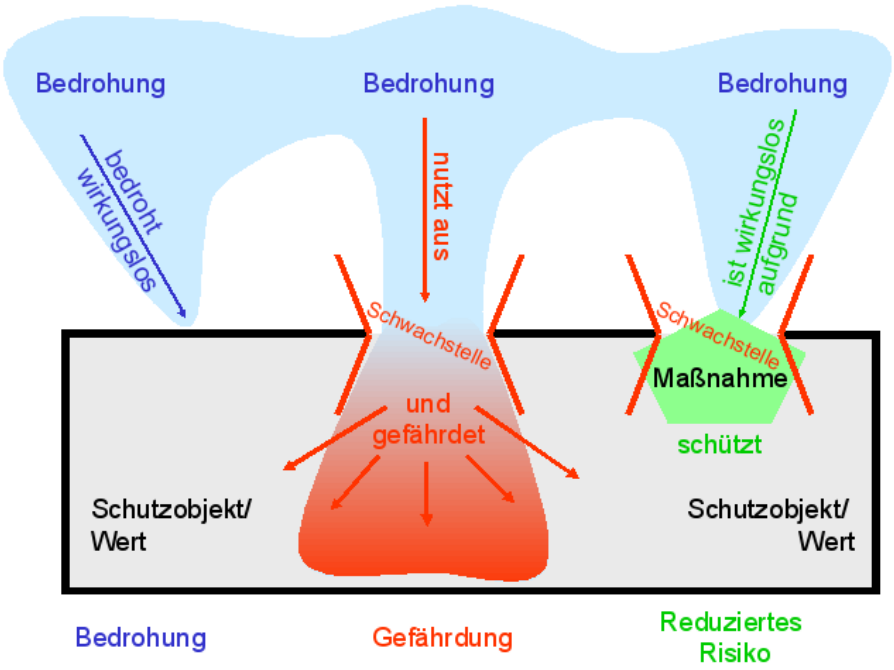

Abbildung 4.1: Grafische Veranschaulichung der Begriffe „Bedrohung“, „Schwachstelle“, „Gefährdung“, „Risiko“ und „Maßnahme“. Erläuterung siehe im Text.

Was ist im Einzelnen dargestellt?

- Linker Teil: Eine Bedrohung, die auf ein sicheres Schutzobjekt trifft, hat keine (schädigende) Wirkung.
- Mittlerer Teil: Eine Bedrohung wird erst durch die Ausnutzung einer vorhandenen Schwachstelle zur Gefährdung des Schutzobjekts.
- Rechter Teil: Eine korrekt eingesetzte (IT-Sicherheits-)Maßnahme kann dafür sorgen, dass die Schwachstelle „gestopft“ wird, d. h. dass die Bedrohung nicht zur Gefährdung wird. Das mit der Bedrohung verbundene Risiko wird durch die Maßnahme – im Idealfall auf Null – reduziert.

In den nachfolgenden Abschnitten werden Kategorien für Schwachstellen und Bedrohungen vorgestellt und an Beispielen erläutert. Abschließend werden einige grundlegende Maßnahmen bzw. Kategorien von Maßnahmen erläutert, die zur Abwehr bestehender Gefährdungen in der Regel zum Einsatz kommen.

Die vorgestellte Klassifizierung dient in erster Linie den Autoren der ISi-Reihe, um die bestehenden Gefährdungen möglichst vollständig zu erfassen. Insbesondere die zahlreichen Beispiele sind aber zur Sensibilisierung und zum Verständnis auch für alle anderen Leser gewinnbringend.

4.2 Schwachstellen (Verwundbarkeiten, Fehler)

Täglich werden neue Schwachstellen bekannt. Fast ebenso häufig gibt es für irgendein Produkt ein neues Sicherheits-Update, um gefundene Schwachstellen zu beseitigen. Dabei bezieht sich die Berichterstattung in den meisten Fällen auf Standard-Software oder Firmware zu verbreiteten Hardware-Komponenten. Zumeist werden Schwachstellen daher auch nach den betroffenen Systemen klassifiziert.

Schwachstellen können jedoch an vielen Stellen auftreten: nicht nur in Software und Hardware, sondern auch in der Netztopologie, in der Infrastruktur oder im Verhalten des Anwenders selbst.

Eine in Bezug auf Internet-Sicherheit wichtige Unterscheidungsmöglichkeit ist die Frage, ob eine Schwachstelle nur lokal (bei physischem Zugang zu dem System) oder auch aus der Ferne (remote), insbesondere über das Internet, ausnutzbar ist. Gegen lokal ausnutzbare Schwachstellen reichen oft Standard-Maßnahmen wie Zugangskontrollen zu Server-Räumen u. Ä. Die ISi-Reihe hingegen zeigt insbesondere solche Maßnahmen auf, die gegen Schwachstellen, die aus der Ferne, nämlich über das Internet, ausnutzbar sind, wirken.

Aufgrund der immer neuen Schwachstellen ist es in der ISi-Reihe jedoch zumeist nicht möglich, einzelne Schwachstellen konkret zu benennen. Viele Schwachstellen haben aber gemeinsame Eigenschaften, sie werden daher im Folgenden in Kategorien zusammengefasst.

Diese Kategorien orientieren sich an den Phasen der Internet-Anbindung. Bei der Erstellung der Module der ISi-Reihe werden diese Kategorien dann herangezogen, um herauszufinden, welche Arten von Schwachstellen für das jeweilige Fachthema relevant sind. Die sich daraus ergebenden Gefährdungen und Maßnahmen werden in den einzelnen ISi-Modulen umfassend erläutert.

4.2.1 Konzeptionelle Schwachstellen (Konzeptionsfehler)

Am Anfang jeder Entwicklung steht die Konzeption, sei es die Konzeption eines Algorithmus, eines Computerprogramms (Software), einer Hardware-Komponente, der Netzarchitektur oder auch der organisatorischen Regelungen. Wird bei der Konzeption nicht sorgfältig vorgegangen, können Fehler passieren. Werden – vielleicht später einmal wichtig werdende – Aspekte nicht betrachtet, können weitere Schwachstellen entstehen. Solche Fehler oder Schwachstellen in der Konzeption können grundsätzlich in keinem nachfolgenden Schritt, also weder in der Realisierung, noch durch geschickte Administration ausgeglichen werden.

Unter die Rubrik Konzeptionsfehler fallen auch viele Verstöße gegen rechtliche Regelungen (Gesetze, Verordnungen, Verträge). Insbesondere das BDSG (Bundes-Datenschutzgesetz) hat – weil in aller Regel personenbezogene Daten verarbeitet werden – große Auswirkungen auf die Konzeption einer Internet-Anbindung.

Beispiel 1: Bei der Verwendung des Protokolls FTP werden die Passwörter im Klartext übertragen (*konzeptionelle Schwäche des Protokolls*). Mit einfachen Mitteln kann ein per FTP übertragenes Passwort mitgelesen und anschließend zum unberechtigten Anmelden missbraucht werden.

Beispiel 2: Die Kontrolle der Eingabewerte in einem Webformular wird – um maximalen Komfort bereitzustellen – schon per JavaScript im Browser des Nutzers durchgeführt. Eine neuerliche Kontrolle auf Server-Seite im internen Netz findet nicht statt (*konzeptioneller Fehler der Software*). Es ist nun auf Client-Seite möglich, – am Browser vorbei – beliebige Daten an den Server zu übertragen und so z. B. per SQL-Injection vertrauliche Inhalte aus internen Datenbanken auszulesen.

Beispiel 3: Herr M. ist der Experte für Server und der einzige, der die Server z. B. nach einem Stromausfall wieder hochfährt. Ein Vertreter ist nicht vorgesehen (*Konzeptionsfehler bei den organisatorischen Regelungen*). Während seines Urlaubs muss der Strom aufgrund Straßenbauarbeiten zweimal für kurze Zeit abgestellt werden. Die verbliebenen Mitarbeiter wollen die Server wieder hochfahren, stellen dabei jedoch fest, dass Herr M. der einzige ist, der das benötigte Passwort kennt. Die Server stehen still, bis sich Herr M. aus dem Urlaub meldet.

4.2.2 Schwachstellen in der technischen Realisierung (Implementierungs- bzw. Umsetzungsfehler)

Viele Fehler entstehen bei der Umsetzung der Konzepte, also bei der Implementierung oder der technischen Realisierung. Insbesondere Software enthält heutzutage sehr viele Fehler. Dies hat verschiedene Ursachen, wie z. B.

- dass die Programme aus sehr vielen Code-Zeilen bestehen, sodass selbst bei geringer Fehlerquote hohe absolute Fehlerzahlen vorliegen,
- dass neue Programmversionen nicht ausreichend getestet, sondern statt dessen frühzeitig auf den Markt gebracht werden, z. B. um schneller zu sein als die Konkurrenz, sowie
- dass ein Bewusstsein für sichere Software erst langsam entsteht und Sicherheit für viele Programmierer und Software-Firmen eine untergeordnete Rolle spielt.

Neben Implementierungsfehlern in Software gehören zu dieser Kategorie aber auch Fehler bei der Umsetzung aller anderen Konzepte, wie z. B. der Netzarchitektur. Hier einige Beispiele:

Beispiel 1: Zu Testzwecken ist im Code einer Datenbankschnittstelle der Benutzer „test“ mit dem Passwort „test“ als Benutzer mit allen Rechten fest eingebaut (*Implementierungsfehler*). Die öffentlichen Webseiten greifen auf diese Schnittstelle zu. Gibt ein Nutzer in der Anmelde-Webseite statt seiner eigenen Zugangsdaten die o. g. „test“-Benutzerdaten ein (die er zuvor erraten hat), so hat er freien Zugriff auf alle ggf. vertraulichen Daten.

Beispiel 2: In einem Eingabefeld wird die Länge des übergebenen Textes nicht überprüft (*häufiger Implementierungsfehler*). Ein Angreifer kann durch einen überlangen Text einen Pufferüberlauf (buffer overflow) erzeugen und das Programm zum Absturz bringen oder – wenn der Text geschickt aufgebaut ist – beliebigen Code auf dem fremden Rechner zur Ausführung bringen.

Beispiel 3: In der Konzeption wurden zwei physikalisch getrennte Netze geplant, das eine für die Personalabteilung ohne Internet-Zugang, das andere für den Vertrieb mit freiem Internet-Zugang. Beide sollten nur über Router mit ACLs verbunden werden. In der Realisierung werden die beiden Netze stattdessen nur logisch getrennt, nämlich über durch Switches verbundene VLANs (*Fehler in der technischen Realisierung*). Ein Angreifer kann nun die bekannten Schwächen von VLANs ausnutzen, um die Netzgrenzen zu überwinden.

4.2.3 Konfigurationsfehler

Moderne Software bietet eine Vielzahl von Möglichkeiten zur Konfiguration. Durch diese Komplexität kommt es sehr häufig zu Fehlern bei der Konfiguration der Systeme.

Wünschenswert wäre auch, wenn die eingesetzten Produkte bei Auslieferung eine sichere Standardkonfiguration mit sich brächten. Aufgrund der Konkurrenz zwischen Komfort und Sicherheit ist dies aber oft nicht der Fall.

Beispiel 1: Die Terminal-Server-Software wird im Rahmen des Netzaufbaus installiert. Im weiteren Verlauf wird vergessen, die nach Konzept vorgesehenen Konfigurationsschritte durchzuführen, es bleibt bei der unsicheren Standard-Konfiguration (*Konfigurationsfehler*). Folglich ist z. B. ein Zugriff mit vollen Rechten über den produktseitig eingerichteten Test-Nutzer möglich.

Beispiel 2: Die lokalen Arbeitsplatz-PCs sind mit einem Browser in der aktuellen Version ausgestattet. Der Browser ist so eingestellt, dass er (Sicherheits-)Updates automatisch nachlädt und lokal installiert. Folglich ist es nicht Aufgabe der Administratoren, Patches für den Browser einzuspielen. Die Benutzer haben jedoch – gemäß bestehender Konfiguration des Betriebssystems – kein Schreibrecht in dem Dateiordner, in dem der Browser installiert ist (*Konfigurationsfehler*). Folglich erscheint bei jedem Installationsversuch eine Fehlermeldung; die Browser sind dauerhaft nicht aktuell. Bekannte, aufgrund des Konfigurationsfehlers nicht gepatchte Sicherheitslücken können gezielt durch Angreifer ausgenutzt werden.

4.2.4 Verhaltensfehler im Betrieb (Bedienungs- und Administrationsfehler)

Eine große, nie zu vernachlässigende Gefahr für die Sicherheit eines IT-Systems ist der Mensch, der das System bedient, sei es als Anwender oder als Administrator. Fehler in der Bedienung eines Systems oder allgemein im (Benutzer-)Verhalten im Umfeld des Systems können Löcher für Angriffe aufreißen.

Erschwerend kommt hinzu, dass viele Einstellungen, die von den Anwendern gewünscht werden, z. B. weil sie den Bedienkomfort steigern, gleichzeitig die Sicherheit des Systems beeinträchtigen. Die Administratoren befinden sich somit dauerhaft in einer Konfliktsituation, die sie nicht zu allseitiger Zufriedenheit lösen können.

Ideal ist es, wenn bereits bei der Konzeption entschieden wurde, welche Konfigurationsmöglichkeiten einen so wesentlichen Einfluss auf die Sicherheit des Gesamtsystems haben, dass sie auf keinen Fall im Betrieb gegenüber der im Konzept vorgegebenen Einstellung verändert werden dürfen. Nur so kann sichergestellt werden, dass die konzeptionell geplante Sicherheit später auch vorhanden ist.

Vor diesem Hintergrund werden Bedienungs- bzw. Administrationsfehler im Betrieb hier als weitere Kategorie für Schwachstellen aufgenommen.

Beispiel 1: Der Browser wird gemäß Konzept mit abgeschaltetem JavaScript als Schutz vor bösartigen Aktiven Inhalten ausgeliefert, da eine zentrale Filterung aus Kostengründen im Konzept nicht vorgesehen ist. In den ersten Tagen häufen sich die Beschwerden über nicht mehr funktionierende Webseiten. Im Eifer des Geschäfts schaltet der Administrator JavaScript in den Browsern frei (*Administrationsfehler, da Abweichung von der im Konzept vorgegebenen Konfiguration*). Ein Angreifer kann nun ohne große Probleme ein Trojanisches Pferd zum Ausspähen interner Daten in das interne Netz einschleusen. Korrekt wäre es gewesen, die Nutzer auf die gemäß Konzept neu eingerichteten Internet-PC zu verweisen und die Konfiguration unverändert zu belassen.

Beispiel 2: Ein Mitarbeiter surft entgegen der Regelung zum Verbot der privaten Internet-Nutzung aus privatem Interesse auf Seiten zwielichtigen Inhalts (*Verhaltensfeh-*

ler) und lädt sich von dort unbemerkt Spyware herunter. Die Spyware registriert alle Eingaben auf der Tastatur und sendet diese an einen Angreifer, der so in Kenntnis der verwendeten Benutzerkennungen und Passwörter gelangt, die er anschließend missbräuchlich nutzen kann.

Beispiel 3: Das Webmail-Postfach, in dem auch eingehende Aufträge gesammelt werden, ist voll, sodass keine neuen E-Mails mehr angenommen werden. Der Administrator klickt beim Versuch, die E-Mails in ein anderes Postfach zu kopieren, auf die falsche Schaltfläche, sodass alle E-Mails unwiederbringlich gelöscht sind (*Bedienungsfehler*). Der Firma gehen Aufträge verloren, ihr Ansehen sinkt bei den nicht bedienten Kunden.

Bedienungsfehler, die dadurch entstehen, dass z. B. Wertebereiche in Web-Formularen nicht geprüft werden, sollten hingegen der Kategorie Implementierungsfehler zugeordnet werden. Es ist Aufgabe des Programmierers für einen sicheren Umgang mit Fehleingaben zu sorgen.

4.3 Bedrohungen

Wie im vorhergehenden Abschnitt 4.2 dargelegt, gibt es zahlreiche Schwachstellen. Werden die fehlerhaften (mit Schwachstellen versehenen) Systeme nun auch noch bedroht, sprechen wir von einer Gefährdung oder einem Risiko. Doch wodurch werden die Systeme bedroht?

Grundsätzlich unterschieden werden kann zwischen Bedrohungen, die von Menschen ausgehen (im Fall von Vorsatz auch „Angriff“ genannt) und Bedrohungen aus der Natur oder der Umgebung, wie z. B. Hochwasser, Sturm, Erdbeben, Feuer, globaler Stromausfall usw. Die zweite Form der Bedrohungen sind nicht spezifisch für das Internet und durch die allgemeinen Maßnahmen zur IT-Sicherheit aus den IT-Grundschutz-Katalogen hinreichend abgedeckt.

In der ISi-Reihe betrachten wir daher in der Regel nur die von Menschen ausgehenden Bedrohungen. Unterschieden werden kann hier zwischen Fahrlässigkeit und Vorsatz. Eine fahrlässige (unabsichtliche) Bedrohung für die Daten und Systeme besteht dann, wenn IT-Anwender oder Mitarbeiter im IT-Bereich Fehler bei ihrer Arbeit machen. Demgegenüber geht es bei Vorsatz um eine absichtliche Bedrohung der Daten und Systeme. Hier unterscheidet man in der Regel zwischen Außentätern und – den zumeist an Bedeutung unterschätzten – Innentätern. Oft ist es zudem interessant zu unterscheiden, ob es sich um eine (gegen ein bestimmtes Ziel) gerichtete oder eine ungerichtete Bedrohung handelt.

Die Bedrohungen menschlichen Ursprungs lassen sich sehr übersichtlich danach kategorisieren, was potenzielle Angreifer zu erreichen versuchen. Auch wenn sich diese und viele folgende Formulierungen rein auf vorsätzliche Bedrohungen beziehen, so sind sie doch eins zu eins auf fahrlässige Bedrohungen übertragbar. Die in den nachfolgenden Unterabschnitten vorgestellten Kategorien orientieren sich an den Sicherheitsgrundwerten, die durch einen eventuellen Angriff bzw. durch eine fahrlässige Handlung beeinträchtigt werden können.

4.3.1 Eindringen/Übernehmen

Die erste Kategorie von Bedrohungen besteht darin, dass ein Angreifer versucht, in Systeme einzudringen oder Systeme zu übernehmen. Dieses sogenannte Hacking erfolgt zumeist, um anschließend Sicherheitsgrundwerte zu beeinträchtigen, also Angriffe auszuüben, die in die im Folgenden beschriebenen Kategorien fallen.

4.3.2 Ausspähen/Entwenden (Vertraulichkeit)

Das Ausspähen oder Entwenden von u.U.vertraulichen Daten stellt die zweite Bedrohungs-Kategorie dar. Bedroht ist hierbei die Vertraulichkeit von Daten.

Beispiel 1: Ein Angreifer zeichnet die per WLAN empfangene Kommunikation eines Firmenstandorts auf (*Bedrohung der Vertraulichkeit der übertragenen Daten*). Da die Kommunikation unverschlüsselt erfolgt (*Schwachstelle, Konfigurationsfehler*), kann er vertrauliche Daten ausspähen (*Gefährdung*).

Beispiel 2: Ein Mitarbeiter möchte den Entwurf für ein Angebot per E-Mail an seinen Vorgesetzten, Herrn Rolf Meyer, schicken. Versehentlich wählt er nach Eingabe von „Meyer“ als Empfänger den im Alphabet weiter oben stehenden Herrn Alfons Meyer (*Schwachstelle, Bedienungsfehler*).

Variante 1: Herr Alfons Meyer kann mit der Mail nichts anfangen und löscht sie ungelesen (*keine Bedrohung, keine Gefährdung*).

Variante 2: Herr Alfons Meyer arbeitet bei einem Konkurrenz-Unternehmen (*Bedrohung der Vertraulichkeit des Angebots*). Er liest die E-Mail. Folglich ist die Vertraulichkeit des Angebots beeinträchtigt (*Gefährdung*).

Beispiel 3: Per E-Mail wird einem an australischen Weinen interessierten Behördenmitarbeiter ein Angebot zugeschickt, das genau seinen Interessen entspricht. Beim Betrachten des Angebots im Browser wird im Hintergrund mithilfe Aktiver Inhalte (*Schwachstelle in der Konzeption: Aktive Inhalte aus unbekannter Quelle werden auf dem PC ausgeführt*) ein Trojanisches Pferd installiert, das Spyware nachlädt (*Bedrohung der Vertraulichkeit*) und fortan alle Eingaben auf der Tastatur mitschneidet und an den Angreifer sendet (*Gefährdung*).

4.3.3 Verhindern/Zerstören (Verfügbarkeit)

Eine weitere Kategorie von Bedrohungen besteht darin, die Verfügbarkeit eines Systems oder von Daten zu beeinträchtigen. Ein potenzieller Angreifer versucht hierbei, den Zugriff auf Daten oder Systeme zu verhindern oder relevante Daten oder Hardware-Komponenten zu zerstören.

Beispiel 1: Ein Angreifer mietet ein Bot-Netz an und verschickt von mehreren Tausend Rechnern Anfragen auf den Webserver eines Unternehmens (*Bedrohung der Verfügbarkeit eines Servers*), um von dem Unternehmen Geld zu erpressen. Es handelt sich hier um einen verteilten Denial-of-Service-Angriff (DDoS). Ist der Webserver nicht ausreichend leistungsstark ausgelegt (*konzeptionelle Schwachstelle*), so kann es zu einem Ausfall kommen (*Gefährdung*).

Beispiel 2: Ein Angreifer versendet in großem Umfang Spam-E-Mails an ein Unternehmen (*Bedrohung der Verfügbarkeit der E-Mail-Server*). Ist der empfangene E-Mail-Server durch diese Flut überlastet, sodass er die Annahme weiterer E-Mails komplett verweigert (*konzeptionelle Schwachstelle: keine ausreichende Auslegung für Lastspitzen*), so ist das Unternehmen vom E-Mail-Verkehr abgeschnitten (*Gefährdung*).

Beispiel 3: Durch eine Gasexplosion im Nachbargebäude wird die Glasfaser-Anbindung des Firmennetzes an das Internet zerstört (*Bedrohung der Verfügbarkeit der Internet-Anbindung*). Steht keine redundante Anbindung an das Internet zur Verfügung

(*konzeptionelle Schwachstelle*), so ist das Firmennetz vom Internet aus nicht mehr zu erreichen (*Gefährdung*).

4.3.4 Verändern/Täuschen/Betrügen/Fälschen (Integrität/Authentizität)

In der vierten Kategorie von Bedrohungen fassen wir alle Aspekte zusammen, die im weitesten Sinne eine Beeinträchtigung der Integrität oder auch der Authentizität bedeuten können. Potenzielle Angreifer versuchen dabei, Daten oder Systeme zu verändern oder zu fälschen, Anwender oder Systeme zu täuschen oder zu betrügen. Hierunter fällt insbesondere das Vortäuschen falscher Identitätsmerkmale (auch Maskerade oder Spoofing genannt) sowie die missbräuchliche Nutzung von Funktionen, die zwar keine Authentisierung verlangen, aber eigentlich nur für andere Nutzer vorgesehen sind. Häufig ist das Ziel der Angreifer, sich einen finanziellen Vorteil zu verschaffen (Computer-Betrug).

Hierunter fällt auch die Computer-Sabotage. Für das Opfer ist die Veränderung von Daten nicht immer offensichtlich, es arbeitet ggf. lange Zeit mit den veränderten Daten weiter. Wenn dann der Angriff bzw. die Fehlbedienung bemerkt wird, haben die Veränderungen evtl. schon weitreichende Folgen gehabt.

Beispiel 1: Ein Angreifer versucht, die Preise in einem Online-Shop so zu verändern, dass sie auf Preisvergleichs-Websites nicht mehr in die Top 5 gelangen (*Bedrohung der Integrität*). Da die Datenbank auf dem Webserver liegt und nur mit einem Standardpasswort geschützt ist (*Schwachstelle: Konzeptions- und Konfigurationsfehler*), kann dies dem Angreifer leicht gelingen (*Gefährdung*).

Beispiel 2: Ein Angreifer sendet eine E-Mail mit einem virenbefallenen Anhang an eine Behörde (*Bedrohung der Integrität*). Der Mitarbeiter öffnet den Anhang (*Schwachstelle im Betrieb: Nichterkennen des manipulierten Anhangs, Nichtaktualität der Virensignaturen*), der Virus nistet sich auf dem Rechner ein und er verändert die Daten auf der Festplatte (*Gefährdung*). Er wird fortan bei jedem Neustart des Rechners mit ausgeführt.

Beispiel 3: Ein Angreifer kopiert die Seite einer deutschen Bank auf seinen Server, um PIN und TAN von Benutzern zu erbeuten (*Bedrohung: Vortäuschen einer Web-Präsenz*). Er fordert per Spam-Mail mit Absenderangabe `sicherheit@bank.de` (*Bedrohung: Vortäuschen einer E-Mail-Adresse*) zum Besuch dieser Webseite auf (*Schwachstelle: Mensch, Fehlbedienung (erkennt nicht Phishing-Absicht)*). Nach Aufruf der Seite gibt der Anwender PIN und TAN ein, die der Angreifer dann zu seinen Gunsten verwenden kann (*Gefährdung*).

Beispiel 4: Ein Angreifer versucht, die Einträge auf einem DNS-Server zu manipulieren (*Bedrohung der Integrität*) mit dem Ziel, Anwender auf seine Webseite umzulenken (*Bedrohung der Authentizität*). Aufgrund des Designs des DNS-Protokolls ist es möglich, dem DNS-Server Einträge unterzuschieben (*Schwachstelle: Konzeptionsfehler im DNS-Protokoll*). Nach erfolgreicher Manipulation werden DNS-Anfragen nach der manipulierten Web-Adresse in die falsche IP-Adresse übersetzt (*Gefährdung*).

4.4 Gefährdungen

Die bestehenden Gefährdungen lassen sich nun als Kombination aus Schwachstellen und Bedrohungen ermitteln[4]. Bei der Erstellung eines Moduls der ISi-Reihe wird die Tabelle 1 angewendet, um die bestehenden Gefährdungen möglichst vollständig zu identifizieren. Nichtsdestotrotz kann nicht ausgeschlossen werden, dass neue Gefährdungen relevant werden, die zum Zeitpunkt der Erstellung eines ISi-Moduls nicht absehbar waren.

Anzumerken ist jedoch, dass die inzwischen verbreiteten, komplexen Gefährdungen wie z. B. Phishing sich nicht einem einzigen Feld zuordnen lassen. Sie bestehen aus vielen Schritten und nutzen dabei mit verschiedenen Bedrohungen unterschiedliche Schwachstellen aus, um das Opfer letztlich zu schädigen.

Gefährdung = Bedrohung + Schwachstelle		***Schwachstelle***			
		… bei der Konzeption	***… bei der Realisierung***	***… bei der Konfiguration***	***... im Betrieb***
Bedrohung	***… der System-Hoheit (Eindringen/ Übernehmen)***				
	… der Vertraulichkeit (Ausspähen/ Entwenden)				
	… der Verfügbarkeit (Verhindern/ Zerstören)				
	… der Integrität/ Authentizität (Verändern/ Täuschen/ …)				

Tabelle 1: Matrix zur Ermittlung der Gefährdungen als Kombination von Schwachstellen und Bedrohungen.

4 Die Zuordnung einer Gefährdung zu einer Schwachstelle und einer Bedrohung ist meist problemlos möglich. Schwierig kann es in der Regel nur werden, wenn der „Faktor Mensch“ eine maßgebliche Rolle spielt.
Denn der Mensch kann einerseits Bedrohung sein, z. B. wenn er vorsätzlich versucht eine Schwachstelle auszunutzen, er fahrlässig Daten oder Systeme zerstört oder er zufällig auf geheime Unterlagen stößt. Eine Schwachstelle kann dann z. B. darin liegen, dass Zugriffsrechte nicht beschränkt sind, dass nach außen verschickte E-Mails nicht inhaltlich kontrolliert werden, dass keine redundanten Systeme vorhanden sind oder dass geheime Unterlagen ungeschützt auf dem Webserver liegen.
Ein Mensch bzw. sein Verhalten kann andererseits auch Schwachstelle sein, so z. B. wenn er versehentlich geheime Daten an Dritte verschickt.

4.5 IT-Sicherheits-Maßnahmen

Trifft eine Bedrohung auf eine Schwachstelle, so liegt eine Gefährdung vor. Wenn der gefährdete Teil der Daten oder des IT-Systems auch noch vertraulich oder kritisch ist, d. h. einen nicht zu vernachlässigenden Schutzbedarf hat, so besteht ein relevantes Risiko. Dieses Risiko führt umgehend zu einem Schaden, sobald der Bedrohende einen Angriff auch wirklich ausführt.

Der Betreiber der IT hat zu diesem Zeitpunkt keine Möglichkeit mehr, den Angriff abzuwehren; er muss früher handeln. Was kann er tun? Betrachten wir die drei Elemente, die zu einem Risiko gehören: den Schutzbedarf, die Bedrohung und die Schwachstelle.

1. Den **Schutzbedarf** der Daten und Systeme kann der IT-Betreiber nur bewerten, nicht aber reduzieren. Es besteht also keine Handlungsmöglichkeit. Dies wird in der Praxis leider häufig anders gesehen. Durch die Korrektur des im Sicherheitskonzept bewerteten Schutzbedarfs, z. B. von „hoch“ auf „normal“, entledigt man sich auf dem Papier einiger Probleme. Auf die tatsächliche Gefährdung haben solche „Manipulationen“ allerdings keine Auswirkung! Wir können nur dringend davon abraten, sich bei der Bewertung des Schutzbedarfs von etwas anderem als der Schutzwürdigkeit der betrachteten Daten leiten zu lassen.

   Lassen sich gewisse Maßnahmen aus Kostengründen nicht umsetzen, so sollte dies unter dem Stichpunkt „Restrisiko“ im Sicherheitskonzept aufgenommen werden und auf keinen Fall der Schutzbedarf so geändert werden, dass es so scheint, als würde die Maßnahme erst gar nicht benötigt.

2. Einen direkten Einfluss hat der IT-Betreiber jedoch auf die Schwachstellen, die von einem potenziellen Angreifer ausgenutzt werden können. Als wichtigste Vorkehrung muss er daher versuchen, **Schwachstellen** von vornherein zu vermeiden oder bestehende Schwachstellen zu beseitigen. Hierzu wendet er sogenannte IT-Sicherheitsmaßnahmen oder kurz Maßnahmen an.

3. Das Absichern bestehender Schwachstellen wird dem IT-Betreiber dennoch nicht zu 100% gelingen. Er sollte sein Netz daher zusätzlich direkt vor den bestehenden **Bedrohungen** schützen. Der Betreiber kann zwar eine Bedrohung nicht abschalten, er kann aber etwas dafür tun, dass die Bedrohung nicht zu einem realen Angriff wird. Viele IT-Sicherheits-Maßnahmen, wie beispielsweise der Einsatz von Paketfiltern, zielen genau darauf ab, Hürden für Angriffe aufzubauen oder Angriffe vollständig abzuwehren, unabhängig davon, ob ausnutzbare Schwachstellen vorliegen oder nicht. Es liegt also in der Verantwortung des IT-Betreibers, über die Beseitigung der Schwachstellen hinaus geeignete Maßnahmen gegen die stets vorhandenen Bedrohungen umzusetzen.

Konkrete Empfehlungen für umzusetzende Maßnahmen werden in den einzelnen Modulen der ISi-Reihe gegeben. Im Folgenden werden aber bereits die wesentlichen Grundprinzipien vorgestellt, an denen sich alle Maßnahmen orientieren. Dabei greifen wir die zuvor eingeführten Kategorien für Schwachstellen und Bedrohungen erneut auf.

- Einerseits werden Maßnahmen vorgestellt, die in den einzelnen Phasen, in denen Schwachstellen entstehen können, relevant sind. Diese können gegen alle Arten von Bedrohungen wirken.
- Andererseits werden Maßnahmen vorgestellt, die speziell gegen eine Bedrohungs-Kategorie wirken. Diese müssen aber in allen Phasen, in denen Schwachstellen entstehen können, berücksichtigt werden.

4.5.1 Maßnahmen, um Schwachstellen zu vermeiden/zu beseitigen

Schwachstellen, auch Verwundbarkeiten (engl. vulnerabilities) genannt, bieten Angreifern das Einfallstor, um die Sicherheitsgrundwerte zu verletzen. Sie zu vermeiden oder zu beseitigen ist eine wesentliche Aufgabe bei allen Betrachtungen zur IT-Sicherheit. Durch welche Maßnahmen kann dies erreicht werden?

Bevor wir uns den einzelnen Phasen zuwenden, nach denen wir die Schwachstellen klassifiziert haben, seien zwei allgemein gültige „Regeln“ aufgeführt:

1. Jeder Schritt sollte mit großer Sorgfalt und Genauigkeit erledigt werden und dabei die in den vorhergehenden Phasen getroffenen Entscheidungen ohne Abweichung umsetzen.
2. Nach jedem Schritt sollte genau überprüft werden, dass alles richtig gemacht wurde (Qualitätssicherung, Testen).

Diese „Regeln“ klingen banal, treffen aber den Kern des Problems. Die meisten Schwachstellen entstehen, weil jemand *mal schnell* dies oder das machen will, weil dies oder das *doch gar kein Problem* ist, weil jemand es *viel besser* kann, *als im Konzept* geschrieben, oder weil *der Chef das so will*. Gehen wir etwas mehr ins Detail.

4.5.1.1 Konzeption

Das A und O in einem IT-Projekt[5] ist die Konzeption. Die Konzeption muss alle Informationen enthalten, die für die anschließende Realisierung notwendig sind. Selbst vermeintliche Selbstverständlichkeiten sollte man im Konzept oder in allgemeinen Richtlinien (z. B. Programmierrichtlinie) festhalten. Denn gerade diese Dinge werden gerne vergessen. Beispiel: Ist es selbstverständlich, beim Programmieren darauf zu achten, dass keine Pufferüberläufe (buffer overflows) entstehen können?

Anders gesagt: Das **Konzept** muss so **sorgfältig durchdacht und vollständig erarbeitet** sein, dass im Zuge der Realisierung keine konzeptionellen Fragen mehr offen sind. Ist doch noch eine solche Frage offen, so muss sie beantwortet und die Antwort unter Berücksichtigung eventueller Nebeneffekte in das Konzept eingearbeitet werden.

Wie im Ablaufplan (siehe Abschnitt 5) für den Fall der Internet-Anbindung im Detail dargestellt, gehört zur Konzeption sowohl die funktionale als auch die IT-Sicherheits-Konzeption, also z. B. der Netzplan (die Netzarchitektur), das Konzept für neu zu erstellende Software, die Auswahl der zu ergreifenden technischen Maßnahmen sowie der zu treffenden organisatorischen Regelungen.

Voraussetzung für ein vollständiges Konzept ist eine **umfassende Recherche zu Bedrohungen und Schwachstellen**, d. h. dass sich der Verantwortliche zuvor umfassend über bestehende Schwachstellen in den im Konzept enthaltenen Elementen (Protokollen, Hardware-Komponenten, Standard-Software, …) sowie über die relevanten Bedrohungen informiert. Diese Arbeit haben Ihnen die Autoren der ISi-Reihe soweit möglich bereits abgenommen. In den einzelnen Studien der ISi-Reihe sind alle relevanten Gefährdungen aufgeführt, es werden für alle Gefährdungen Empfehlungen gegeben, wie das damit verbundene Risiko gemindert werden kann.

5 Die Ausführungen können auf alle Arten von IT-Projekten angewendet werden: auf eine Internet-Anbindung einer Behörde, das Erstellen von Webseiten, das Programmieren einer Anwendung oder eines Betriebssystems, die Entwicklung einer neuen Hardware-Komponente oder das Entwickeln eines neuen Protokolls. Folglich richten sich die Ausführungen – im jeweiligen Zuständigkeitsbereich – sowohl an die IT-Abteilungen in Firmen und Behörden als auch an die Entwickler in Software- und Hardware-Unternehmen sowie an die IT-Berater.

Bereits vor der Konzeption wird laut Ablaufplan (siehe Abschnitt 5.1.4) die Schutzbedarfsfeststellung gemäß IT-Grundschutz durchgeführt, sodass zu diesem Zeitpunkt bereits bekannt ist, für welche Daten Sicherheit in welchem Umfang benötigt wird.

4.5.1.2 Realisierung (Implementierung)

Nach der Konzeption folgt die Realisierung, in Bezug auf Software auch Implementierung genannt. Auch hier gelten wieder die beiden allgemeinen Regeln.

Wichtigste Voraussetzung für eine fehlerarme Realisierung ist das **strenge Einhalten der Vorgaben aus der Konzeption einschließlich der** allgemeinen **Programmierrichtlinien**[6].

Zu den in den Programmierrichtlinien enthaltenen allgemeinen Vorgaben sollten dabei Maßnahmen zur sicheren Programmierung (**Secure Programming**) gehören. Wichtig ist auch, dass Unnötiges abgeschaltet wird (beim Installieren von Standard-Software wird in aller Regel mehr installiert, als das Konzept als notwendig erachtet). Lassen sich gewisse, eigentlich nicht benötigte und im Konzept nicht vorgesehene Programme, Funktionen o. Ä. nicht abschalten oder entfernen, so muss das Konzept entsprechend angepasst werden. Hier muss insbesondere überlegt werden, ob weitere IT-Sicherheits-Maßnahmen notwendig sind, um das durch die zusätzlichen Funktionen erhöhte Risiko wieder zu reduzieren.

Zum Abschluss der Realisierung ist es dann wichtig, **umfangreiche Tests** durchzuführen, um mögliche Schwachstellen bzw. Fehler aufzuspüren und zu prüfen, ob die Realisierung auch wirklich mit dem Konzept übereinstimmt.

Im Zuge der Realisierung sollte zudem ein **Feinkonzept** erstellt werden, in dem die allgemeinen Vorgaben aus dem Konzept für die konkreten Anwendungen und Systeme spezifiziert werden.

Beispiel: Im Konzept steht, dass der Paketfilter so eingerichtet werden muss, dass alles verboten ist, was nicht ausdrücklich erlaubt ist. Im Feinkonzept muss diese allgemeine Vorgabe dann verfeinert werden in die konkrete Regel, die bei der Konfiguration in der Paketfilter-Software hinterlegt werden muss.

Für die Bereiche, die man über Outsourcing an Dritte vergibt, müssen die Vorgaben aus dem Konzept vollständig und unverändert an diese weitergegeben werden. Das Stichwort in diesem Zusammenhang ist **Service Level Agreement**.

4.5.1.3 Konfiguration

Bevor ein System in Betrieb gehen kann, muss es konfiguriert werden. Auch hier können viele Fehler gemacht werden (Schwachstellen entstehen). Besonders wichtig ist hierbei, dass die **Vorgaben des Feinkonzepts streng eingehalten werden**. Das Feinkonzept war schließlich im Zuge der Realisierung erstellt worden, um eine korrekte Konfiguration zu ermöglichen. Stellt sich heraus, dass Vorgaben im Feinkonzept falsch oder nicht umsetzbar sind, so muss zur Realisierung zurückgekehrt werden und das Feinkonzept überarbeitet werden.

6 In Programmierrichtlinien werden Aspekte geregelt, die sich auf alle Software-Projekte beziehen und somit nicht in jedem individuellen Konzept erneut aufgeschrieben werden sollen.

4.5.1.4 Betrieb (Nutzung und Administration)

Nicht alles kann im Feinkonzept geregelt werden. So wird dort z. B. nur von Rollen und Gruppen die Rede sein, die Festlegung, wer genau zu welcher Gruppe gehört, ist aber Aufgabe der Administration. Um Fehler zu vermeiden oder zumindest nachvollziehbar zu machen, ist hier eine **lückenlose Dokumentation** der Administrationstätigkeit die wesentliche Maßnahme. Stichwort in diesem Zusammenhang ist die **Revisionssicherheit**. Auch das Einspielen von Patches gehört zur vordringlichen Aufgabe der Administratoren.

Maßnahmen müssen aber nicht nur auf Betreiberseite, sondern auch beim Anwender umgesetzt werden. Wie lassen sich hier Bedienungs- oder Verhaltensfehler vermeiden?

Wichtigste Maßnahme in diesem Zusammenhang ist das **Schaffen von Bewusstsein** bei den Anwendern (awareness raising), das Informieren und das Schulen der Anwender. In einer normalen Behörde oder einem normalen Unternehmen muss davon ausgegangen werden, dass das Gros der Mitarbeiter keine überdurchschnittlichen IT-Kenntnisse hat. Ein Anwender wird daher zwangsläufig Fehler machen, wenn ihm die grundlegenden Bedrohungen nicht bekannt sind, die kombiniert mit seinen Verhaltens- oder Bedienungsfehlern zu einer Gefährdung und in Folge zu einem Schaden für seinen Arbeitgeber führen.

Neben dieser Sensibilisierung ist es ratsam wichtige Regelungen, z. B. in Form von globalen **Benutzerrichtlinien**, als verbindlich vorzugeben und die strenge Einhaltung auf Führungsebene vorzuleben und auch zu kontrollieren. Beide Aspekte sind entscheidend, um zu verhindern, dass Regeln im Kopf der Mitarbeiter in die Schublade „macht ja eh keiner“ einsortiert werden. Solch ignorierte Regeln sind ein großes Problem für die IT-Sicherheit, da diese Schwachstellen im Betrieb nicht ohne Weiteres gefunden werden, schließlich sieht auf dem Papier alles korrekt aus. Welche Punkte dabei für das jeweilige Fachthema besonders wichtig sind, wird in der entsprechenden Studie aufgeführt.

Um Sicherheitsverstöße kurzfristig aufzuspüren, ist es zudem wichtig, an sicherheitsrelevanten Punkten im zulässigen Rahmen alle Aktivitäten **umfassend** zu **protokollieren** (logging) und die **Protokolldaten** auch **schnellstmöglich auszuwerten**. Gleichfalls wichtig ist es, alle im Betrieb vorgenommenen **Änderungen** nachvollziehbar zu **dokumentieren**.

4.5.2 Maßnahmen zur Absicherung gegen Bedrohungen

Neben der gezielten Beseitigung bzw. Vermeidung von Schwachstellen, die in den einzelnen Phasen auftreten können, ist es notwendig, gezielt Maßnahmen gegen bekannte Bedrohungen umzusetzen. Die IT-Sicherheits-Firmen bieten hierfür ein breites Portfolio an spezieller Sicherheits-Software an. Ein solches Produkt wirkt häufig genau gegen eine Bedrohungs-Kategorie; der Einsatz des Produkts muss dabei in allen Phasen sicher ausgestaltet werden, d. h. ohne neue Schwachstellen zu erzeugen. Diese Art der Maßnahmen lässt sich also den Bedrohungs-Kategorien zuordnen.

Zu allen vorgestellten Kategorien werden in den Modulen der ISi-Reihe detaillierte Maßnahmen vorgeschlagen. Hierzu zählen sowohl

- Maßnahmen, die die Wahrscheinlichkeit reduzieren, dass ein Angriff Erfolg hat (Beispiel: Sicherheits-Gateway, Verschlüsselung), als auch
- Maßnahmen, die helfen, einen eventuellen Angriff schnellstmöglich zu erkennen und somit den daraus folgenden Schaden zu reduzieren (Beispiel: Intrusion-Detection-Systeme, Signaturen).

Auch bei bestmöglicher Absicherung – durch präventive Maßnahmen – verbleibt ein gewisses Restrisiko, Opfer eines erfolgreichen Angriffs zu werden. Für diesen Fall gilt es reaktive Maßnahmen zu

planen, die umgesetzt werden, sobald ein Angriff erfolgt ist *und* erkannt wurde (Beispiele: Alarmierung, Trennen des angegriffenen Systems vom Internet, forensische Untersuchungen). Diese Maßnahmen können unter dem Titel Notfallvorsorge zusammengefasst werden. Sie sind in aller Regel nicht Internet-typisch und werden daher in der ISi-Reihe nicht besonders betrachtet. Die dazu notwendigen Schritte werden im BSI-Standard 100-4 erläutert.

4.5.2.1 Eindringen/Übernehmen

Die ISi-Reihe behandelt im Themenbereich 4 „**Komponenten zum Schutz lokaler Netze**“ Komponenten, die in einem ersten Schritt gegen das Eindringen und Übernehmen schützen und somit Bedrohungen gegen die Sicherheitsgrundwerte von vornherein verhindern (sollen) oder die ein Eindringen und Übernehmen zumindest feststellen lassen. Hierzu zählen sowohl Sicherheits-Gateways als auch Intrusion-Detection-Systeme. Komponenten zur Netzüberwachung oder Frühwarnung können ebenso eingesetzt werden.

Außerdem müssen Maßnahmen unter der Überschrift **Zugangs- bzw. Zugriffsschutz** umgesetzt werden. Hierzu gehören das Rechte-Management auf Servern genauso wie das Abschließen der Tür zum Server-Raum. Im weitesten Sinne fällt hierunter auch die Segmentierung der internen Netze, die im Idealfall bewirkt, dass ein erfolgreicher Angriff sich nur auf ein einziges Segment auswirkt.

Eine umfassende **Protokollierung** und zügige Auswertung der Protokolldaten ermöglicht zudem das schnelle Erkennen eines Angriffs.

4.5.2.2 Ausspähen/Entwenden (Vertraulichkeit)

Die wirksamste Maßnahme gegen das Ausspähen von vertraulichen Daten ist die **Verschlüsselung**. E-Mails und Webseiten können verschlüsselt werden, aber auch ganze Festplatten. Auch bei Standard-Kommunikations-Protokollen können sichere Varianten eingesetzt werden, die die relevanten Daten bei der Übertragung verschlüsseln (SSH statt TELNET, SFTP statt FTP oder HTTPS statt HTTP).

Wenn Daten erfolgreich ausgespäht wurden, kann man diesen Schaden nicht mehr begrenzen. Es ist jedoch wichtig, die Schwachstelle schnell zu identifizieren und so weitere Angriffe auf die Vertraulichkeit zu verhindern.

4.5.2.3 Verhindern/Zerstören (Verfügbarkeit)

Welche Arten von Maßnahmen wirken gegen Bedrohungen der Art Verhindern oder Zerstören? Hier geht es im weitesten Sinne darum, **Redundanz** zu **schaffen**, um auch bei außergewöhnlichen Lastspitzen – wie z. B. bei einem DoS-Angriff – die Verfügbarkeit des Systems zu erhalten.

Im Falle eines erfolgreichen Angriffs muss die Schwachstelle schnell identifiziert und isoliert werden, um zumindest die nicht anfälligen Systeme schnellstmöglich wieder in Betrieb nehmen zu können.

Beispiele für konkrete Maßnahmen sind redundante Anbindung von Servern, zusätzliche Server (Hot Standby oder Cold Standby), unternehmenskritische Daten auf verschiedene, räumlich getrennte Server replizieren und regelmäßige Datensicherung.

4.5.2.4 Verändern/Täuschen/Betrügen/Fälschen (Integrität/Authentizität)

Als letzten Fall betrachten wir Maßnahmen gegen Bedrohungen der Art Verändern, Täuschen, Betrügen oder Fälschen, insbesondere bei der Übertragung über das Internet. Dort, wo man selbst Einfluss hat, sollte man angemessene **Authentisierungs-Mechanismen** umsetzen. Allerdings hat man nicht auf alles Einfluss. Insbesondere in den Fällen, wo Standard-Protokolle keine Authentisierung verlangen, wird es schwierig. Hier ist es ggf. nur möglich, die Anwender auf die bestehenden Bedrohungen hinzuweisen und Ihnen Hilfestellungen zu geben, Täuschungs- und Betrugsfälle zu erkennen.

Zum Erkennen von Integritäts-Verletzungen eignet sich zudem die Nutzung von **Signaturen**. Wichtig ist jedoch, dass die erzeugten Signaturen auch überprüft werden, um Integritätsverletzungen festzustellen.

Hat man die in den vorhergehenden Unterabschnitten besprochenen Maßnahmen zum Schutz vor einem Eindringen sowie zum Schutz der Verfügbarkeit gut konzipiert und umgesetzt, so kann der Schaden aufgrund einer zeitnah erkannten Verletzung der Integrität in aller Regel gering gehalten werden.

4.5.3 Auswahl angemessener Maßnahmen

Bei der Konzeption einer Internet-Anbindung gilt es, aus den zuvor beschriebenen Kategorien die notwendigen Maßnahmen zusammenstellen. Was aber heißt „notwendig" konkret? Im Idealfall würden Maßnahmen so ausgewählt, dass alle Schwachstellen vollständig beseitigt werden und dass Bedrohungen durch umgesetzte Maßnahmen vollständig daran gehindert werden, wirksame Angriffe umsetzen zu können. Dann hätten wir 100%ige Sicherheit. Theoretisch.

Praktisch ist das nicht möglich. Es wird immer ein gewisses Restrisiko verbleiben, das der IT-Betreiber bewusst in Kauf nimmt. Zur Erläuterung: Rein mathematisch bestimmt sich das Risiko als Produkt der möglichen Schadenshöhe und der Eintrittswahrscheinlichkeit für einen Schaden (auch wenn wir im Rahmen der ISi-Reihe keine solchen Berechnungen durchführen und ohnehin nicht jeder Schaden ohne Weiteres in Zahlen zu bemessen ist).

Dabei hängt die Eintrittswahrscheinlichkeit von den Bedrohungen und den Schwachstellen ab. Je besser die bestehenden Gefährdungen durch Maßnahmen abgedeckt sind, desto geringer ist die Eintrittswahrscheinlichkeit und somit auch das Restrisiko, das auf ein sinnvolles Maß reduziert werden sollte. Nach dem – mehr oder weniger allgemeingültigen – Pareto-Prinzip (80-20-Verteilung) ist es offensichtlich, dass man das Risiko zunächst mit wenig Aufwand deutlich reduzieren kann, anschließend aber viel Aufwand benötigt wird, um durch weitere Maßnahmen auch nur geringe Erfolge zu erzielen. Es geht also um die Angemessenheit.

Woran orientiert sich nun die Auswahl „angemessener" Maßnahmen?

- Höhe des Schutzbedarfs

  Zentrales Auswahlkriterium ist der Schutzbedarf: Je höher der Schutzbedarf, d. h. je höher der mögliche Schaden, desto wirksamere Maßnahmen müssen umgesetzt werden. Nur so kann das zu akzeptierende Restrisiko angemessen gering gehalten werden.

  Beispiel: Daten mit hohem Schutzbedarf in Bezug auf die Vertraulichkeit müssen bei der Kommunikation über das Internet verschlüsselt werden. Bei Daten mit normalem Schutzbedarf ist dies nicht immer erforderlich.

- Grad der Bedrohung

Je wahrscheinlicher es ist, dass eine Bedrohung auf den konkreten Informationsverbund einwirkt, desto wirksamere Maßnahmen müssen umgesetzt werden. Nur so kann das zu akzeptierende Restrisiko angemessen gering gehalten werden.

Beispiel: Es ist in der Regel wahrscheinlicher, dass Kriminelle versuchen, Daten bei einem großen Konzern auszuspähen als beim örtlichen 3-Mann-Handwerksbetrieb. Der Konzern muss gegen die Bedrohung durch Wirtschaftsspionage daher zusätzliche Maßnahmen umsetzen, auch wenn es sich von der Art her bei beiden Unternehmen um Daten gleichen Schutzbedarfs handelt.

- Zahl der (potenziellen) Schwachstellen

  Je mehr Schwachstellen in einem Informationsverbund ausnutzbar sind, desto mehr Maßnahmen müssen umgesetzt werden. Nur so kann das insgesamt zu akzeptierende Restrisiko angemessen gering gehalten werden.

  Beispiel: Es ist wahrscheinlicher, einen Webserver zu übernehmen, auf dem sehr viele Zusatzprogramme installiert (und womöglich nie aktualisiert) wurden, als einen Webserver, der nur die absolut notwendigen Komponenten auf einem immer aktuellen Stand enthält.

- Wirtschaftlichkeit / Restrisiko-Akzeptanz

  Ein zusätzlicher, nicht zu vernachlässigender Aspekt bei der Auswahl von Maßnahmen ist die Wirtschaftlichkeit. Im Vergleich zum Restrisiko sehr teure oder sehr arbeitsintensive Maßnahmen sind häufig nicht angemessen, um das Restrisiko noch weiter zu senken.

  Beispiel: Die Umsetzung einer Maßnahme kostet 10.000 €. Diese Maßnahme wirkt gegen eine Bedrohung, die sehr, sehr unwahrscheinlich ist und im Schadensfall einen Schaden in Höhe von 20.000 € erzeugen würde. Auch ohne konkrete Berechnungen anzustellen, wird man i.d.R. Zu dem Schluss kommen, dass sich eine solche Investition nicht lohnt.

- Größe des Informationsverbunds

  Dabei hängt die Frage, ob eine Maßnahme wirtschaftlich realisiert werden kann, stark davon ab, wie groß der betrachtete Informationsverbund und die betrachtete Organisation sind.

  Beispiel: Ist ein komplexer Aufbau des Sicherheits-Gateways für große Netze eine Selbstverständlichkeit, so dürfte bei einem aus nur fünf PCs bestehenden Netz in einem kleinen Unternehmen der Paketfilter die wirtschaftlichere Lösung sein. Das in diesem Fall höhere verbleibende Restrisiko muss dann jedoch bewusst getragen und im Sicherheitskonzept angegeben werden.

Die ISi-Reihe unterstützt die Leser bewusst bei der Auswahl angemessener Maßnahmen, indem zu jeder vorgeschlagenen Maßnahme bestmöglich angegeben wird,

- für welchen Schutzbedarf („normal” oder/und „hoch”) sie empfohlen wird,
- gegen welche Bedrohung sie wirkt bzw. welcher Schwachstelle sie entgegenwirkt und
- wie gut ihre Wirkung ist (Hinweis auf ein dennoch verbleibendes Restrisiko) sowie
- wie hoch der mit der Umsetzung verbundene Aufwand ist.

Als Vorgehensweise bei der Anwendung empfiehlt es sich, zunächst alle (nicht redundanten) in der ISi-Reihe beschriebenen Maßnahmen für den vorliegenden Schutzbedarf auszuwählen. Hiervon können anschließend diejenigen Maßnahmen gestrichen werden, die gegen nicht vorhandene Schwachstellen oder gegen nicht relevante Bedrohungen wirken. In einem letzten Schritt sollte dann die Wirtschaftlichkeit der ausgewählten Maßnahmen überprüft werden. Wichtig ist beim Streichen von Maßnahmen jedoch, dass dies begründet und unter der Überschrift „Restrisiko” im Sicherheitskonzept dokumentiert wird.

Auf diese Weise sollte es dem Leser möglich sein, für jede Internet-Anbindung angemessene Maßnahmen zusammenzustellen und das verbleibende Restrisiko explizit zu benennen. Beides fließt in das zu erstellende Sicherheitskonzept ein.

5 Ablaufplan

Der vorliegende Ablaufplan soll Behörden und Unternehmen bei der Anbindung einer Institution an das Internet sowie bei der Einführung neuer Dienste, sei es als Nutzer oder als Anbieter, unterstützen. Er beschreibt die notwendigen Schritte in den einzelnen Phasen der Internet-Anbindung: Dabei wird zwischen Analyse, Konzeption, Realisierung sowie Administration und Betrieb unterschieden (Abbildung 5.1). Für jede Phase werden die Aktivitäten beschrieben, die bei der Anbindung an das Internet oder bei deren Erweiterung durchgeführt werden sollten.

Die erste Phase, die Analyse, erfolgt auf Basis der im BSI-Standard 100-2 beschriebenen IT-Grundschutz-Vorgehensweise. Für die übrigen Phasen liefern die innerhalb der ISi-Reihe erstellten Module das notwendige Fachwissen für die Durchführung. Zusammen mit den ISi-Modulen zu dem jeweiligen Fachthema und verschiedenen weiteren Publikationen des BSI, auf die an den entsprechenden Stellen verwiesen wird, kann so eine Internet-Anbindung sicher geplant, beschafft, konfiguriert und betrieben werden.

Der Ablaufplan sollte nicht als starre Vorgabe angesehen werden. Er sollte vielmehr als Rahmen in allen Projekt-Phasen der Internet-Anbindung dienen. Obwohl nur an einigen Stellen explizite Sprünge zwischen den Phasen vorgesehen sind, sind Rücksprünge, wenn immer sinnvoll oder notwendig, auch an anderen Stellen möglich, um Korrekturen vorzunehmen. Zumindest am Ende einer jeden Phase sollte eine Entscheidung darüber getroffen werden, ob das Projekt mit dem derzeitigen Stand fortgeführt, abgebrochen oder anders geplant wird.

Die in den Aktivitäten angegebenen Beispiele sollen bereits eine Vorstellung vermitteln, welche Punkte im Einzelnen beachtet werden müssen. Für alle fachlichen Details sei jedoch auf die weiteren Dokumente der ISi-Reihe verwiesen, die bedarfsorientiert herangezogen werden sollen.

Abbildung 5.1 zeigt eine Übersicht der Phasen des Ablaufplans. Parallel zur vierten Phase „Administration und Betrieb“ soll in regelmäßigen Abständen eine Revision durchgeführt werden. Diese Phase wird im Ablaufplan derzeit noch nicht beschrieben. Stattdessen wird auf die gängige Literatur oder den vom BSI veröffentlichten Leitfaden „Integration und IT-Revision von Netzübergängen“ verwiesen. Neben den Revisionen sollten ebenfalls regelmäßig Notfallvorsorgeübungen gemäß dem Notfallvorsorgekonzept durchgeführt werden. Umfangreiche Informationen zum Notfallmanagement gibt der BSI-Standard 100-4.

Die Phasen im ISi-Ablaufplan sind konsistent mit den im BSI-Standard 100-1 beschriebenen Phasen für den IT-Grundschutz, den ebenfalls dort beschriebenen Phasen im Lebenszyklus nach Deming (PDCA-Modell) sowie den im V-Modell beschriebenen Phasen.

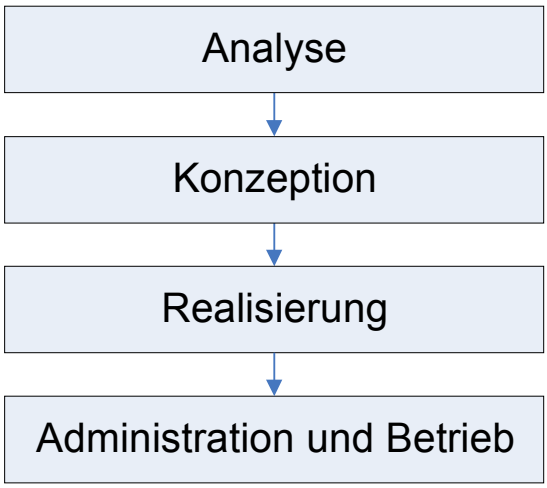

Abbildung 5.1: Phasen des Ablaufplans

5.1 Phase 1: Analyse

Beim Neuaufbau einer Internet-Anbindung oder der Einführung eines neuen Dienstes, der in die vorhandene Umgebung integriert werden soll, sollte zunächst eine gründliche Analyse der Anforderungen an den neuen Dienst und des aktuellen Zustands erfolgen. Die dabei durchgeführten Schritte sind Voraussetzung für das Vorgehen in den späteren Phasen.

Zunächst müssen der aktuelle Zustand der IT-Strukturen und die existierenden Datenbestände erfasst werden. Im Weiteren muss natürlich definiert werden, welche Anforderungen der neue Dienst erfüllen soll. Dabei sollten auch die rechtlichen Rahmenbedingungen berücksichtigt werden. Außerdem muss ermittelt werden, welche IT-Sicherheitsmaßnahmen bereits umgesetzt wurden. Diese Dokumentation hilft im späteren Verlauf des Projekts, die neuen Maßnahmen sorgfältig planen und Wechselwirkungen erkennen zu können.

Parallel dazu muss eine Sicherheitsleitlinie erstellt werden bzw. die bestehende muss auf ihre Aktualität hin überprüft werden. Diese Aktivität schließt auch die Festlegung eines Maßstabs für die Schutzbedarfsklassen mit ein. Anhand dessen wird allen betrachteten (bereits vorhandenen und geplanten) Komponenten des IT-Systems ein Schutzbedarf zugeordnet.

Im Idealfall existieren die meisten der zuvor genannten Dokumente bereits. Lediglich die Analyse des Bedarfs und des Schutzbedarfs muss immer neu durchgeführt werden. Am Ende der ersten Phase kann eine Entscheidung über das weitere Vorgehen getroffen werden. Darüber sollten alle Beteiligten informiert werden.

Wie Abbildung 5.2 zeigt, ist die Reihenfolge, in der die Aktivitäten durchgeführt werden sollen, nicht für alle Aktivitäten fest vorgegeben. Aktivitäten, die keine Ergebnisse vorangegangener Aktivitäten benötigen, können gleichzeitig oder in beliebiger Reihenfolge ausgeführt werden. Die Aktivitäten „Bedarf analysieren“, „Sicherheitsleitlinie und Maßstab für Schutzbedarfsklassen erstellen“ und „Ist-Zustand analysieren“ können daher parallel bzw. in beliebiger Abfolge durchgeführt werden. Die Ergebnisse dieser einzelnen Aktivitäten müssen jedoch als Voraussetzung für die beiden verbleibenden Aktivitäten vorliegen, die dann in der angegebenen Reihenfolge sequenziell abgearbeitet werden müssen.

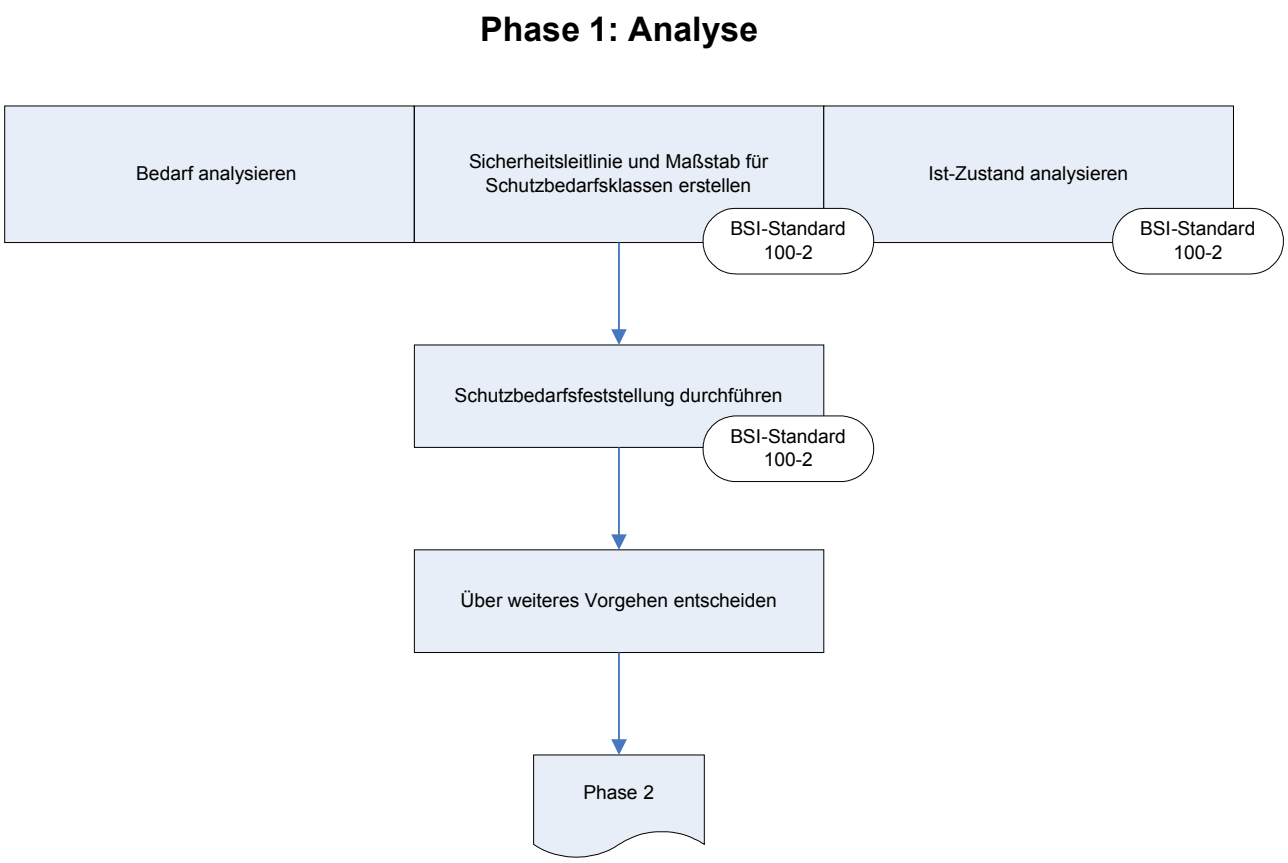

Abbildung 5.2: Aktivitäten der Phase 1: Analyse

5.1.1 Aktivität „Bedarf analysieren“

Voraussetzungen:	keine
Hilfsmittel:	keine
Ergebnisse:	Auflistung der benötigten Dienste und Kommunikationsverbindungen
	Auflistung der rechtlichen Rahmenbedingungen

Der Einführung eines neuen Dienstes oder der erstmaligen Anbindung an das Internet sollte eine gründliche Planung vorausgehen. Ein wesentlicher Aspekt ist dabei die Bedarfsanalyse. Hier steht die Ermittlung der benötigten Dienste im Vordergrund. Diese Dienste müssen noch nicht im Detail spezifiziert werden und können anhand der gewünschten Ziele beschrieben werden. Eine Befragung der Nutzer über ihre bisherigen Vorgehensweisen und aufgetretenen Schwierigkeiten kann Aufschluss darüber geben, welche Dienste benötigt oder verbessert werden sollten. Auch die Nutzungsart spielt dabei eine Rolle. So kann zum Beispiel unterschieden werden, ob das Internet zur Recherche eingesetzt, über das Internet kommuniziert werden soll oder ob eigene Dienste nach außen angeboten werden sollen.

Wenn zum Beispiel als neue Funktionen das Herunterladen von Prospekten angeboten werden soll, so muss zu diesem Zeitpunkt spezifiziert werden, um welche Art von Prospekten es sich handelt. Eine Abschätzung über die Größe dieser Daten und die Häufigkeit der Anfragen sollte ebenfalls erfolgen. Die Anzahl der nachgefragten Prospekte kann dabei aus den bisherigen Erfahrungen gewonnen werden, wenn diese über andere Bezugswege verfügbar waren. Es sollte jedoch beachtet werden, dass dieser Wert nicht direkt übernommen werden kann. Wurden die Prospekte bisher nur über den Postweg versandt und sollen sie nun über einen Webauftritt beziehbar sein, so sinkt der Aufwand für den Kunden. Damit ist es auch wahrscheinlich, dass sich die Anzahl der Anfragen erhöhen wird.

Parallel zur Betrachtung der benötigten Dienste sollten auch die neu entstehenden Kommunikationsverbindungen erfasst werden. Im Besonderen betrifft dies die Verbindungen zwischen dem internen und dem Internet, die durch die neuen Dienste entstehen.

Die Analyse bringt weitreichende Vorteile mit sich. Die Vorstellungen über die gewünschten Dienste und Verbindungen werden konkretisiert. Ideen können so genauer beschrieben werden, ohne sofort die technischen Details erfassen zu müssen. Damit bildet die Analyse eine Grundlage für das weitere Vorgehen. Dienste und Verbindungen, die nicht benötigt werden, können von Beginn an ausgeschlossen werden und stellen damit keinen unnötigen Angriffspunkt dar. Durch die konsequente Umsetzung der getroffenen Entscheidungen wird daher direkt die Sicherheit erhöht.

Im letzten Analyseschritt sollte überlegt werden, welche rechtlichen Rahmenbedingungen für das geplante Einsatzgebiet relevant sind. Für die meisten Dienste dürften zumindest das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG) und das Bundesdatenschutzgesetz (BDSG) relevant sein. Für einige Dienste kann das Gesetz über den Datenschutz bei Telediensten (TDDSG) oder das Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) bedeutsam sein. Die Ermittlung der zu beachtenden rechtlichen Rahmenbedingungen muss für jeden Dienst durchgeführt werden. Dazu sollte der Justiziar der Institution mit einbezogen werden. Da die ISi-Reihe lediglich Empfehlungen zur Internet-Sicherheit ausspricht, können in diesem Rahmen keine rechtsverbindlichen Aussagen getroffen werden.

5.1.2 Aktivität „Sicherheitsleitlinie und Maßstab für Schutzbedarfsklassen erstellen“

Voraussetzungen:	keine
Hilfsmittel:	BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“, Abschnitte 3.3 und 4.3.1
Ergebnisse:	Sicherheitsleitlinie
	Maßstab für Schutzbedarfsklassen

Neben der Bedarfsanalyse müssen die wichtigsten sicherheitstechnischen Parameter festgelegt werden. Dazu gehören die Erstellung einer Sicherheitsleitlinie für die Internet-Anbindung und die Festlegung des Maßstabs für die Schutzbedarfsklassen. Diese Vorgaben betreffen häufig nicht nur einen einzelnen Dienst, sondern werden institutionsweit benötigt.

Sicherheitsleitlinie

Ein erster Schritt ist die Erstellung beziehungsweise Aktualisierung der Sicherheitsleitlinie im besonderen Hinblick auf die Internet-Anbindung. Die Grundlage dafür bildet die bereits existierende, organisationsweite Sicherheitsleitlinie, in der die Leitaussagen zur IT-Sicherheit zusammengefasst werden.

Die Sicherheitsleitlinie dokumentiert die Sicherheitsziele und das zu erreichende Sicherheitsniveau der Institution. Aus den Aufgaben sowie den allgemeinen Zielen der Institution lassen sich unter Berücksichtigung der gesetzlichen Rahmenbedingungen die Sicherheitsziele ableiten.

Die Sicherheitsleitlinie sollte den Stellenwert der Informationssicherheit festlegen. Durch deren Veröffentlichung werden die definierten Sicherheitsziele allen Mitarbeitern bekannt. Daher ist es wichtig, dass die Sicherheitsleitlinie nachvollziehbar ist. So muss z. B. der Geltungsbereich klar definiert sein. Sie sollte kurz, prägnant und für den Anwenderkreis verständlich formuliert sein. Auf technische oder herstellerspezifische Details sollte verzichtet werden. Die Gesamtverantwortung für die Sicherheitsleitlinie liegt i. d. R. bei der Behörden- bzw. Unternehmensleitung.

Ausgehend von der allgemeinen Sicherheitsleitlinie sollte eine konkretisierte und auf den Anwendungsbereich angepasste Sicherheitsleitlinie für die Internet-Anbindung erstellt werden. Existieren in der Behörde oder dem Unternehmen weitere Richtlinien, die dieses Themengebiet betreffen, so sollten diese ebenfalls mit einfließen. Dabei kann die Sicherheitsleitlinie für die Internet-Anbindung Teil der allgemeinen Sicherheitsleitlinie werden oder als eigenständiges Dokument erstellt werden.

Die Sicherheitsleitlinie gibt eine Strategie für die weiteren Phasen, die in dem vorliegenden Ablaufplan beschrieben werden, vor und bildet eine Grundlage für die Erstellung von Konzepten für die einzelnen Teilbereiche. So kann beispielsweise festgelegt werden, dass der Übergang zwischen internem und externem Netz durch ein Sicherheits-Gateway gesichert werden muss. Regelungen für die dienstliche und private Nutzung der neuen Dienste können auch enthalten sein. Die Vorgabe, dass die eingesetzte Software so konfiguriert werden soll, dass nur die benötigten Funktionen aktiviert sind, sollte ebenfalls Bestandteil der Sicherheitsleitlinie sein.

Maßstab für Schutzbedarfsklassen

Ein weiterer Punkt ist die Festlegung eines Maßstabs für die Schutzbedarfsklassen. In der Sicherheitsleitlinie getroffene Aussagen haben Einfluss auf diese Definition. Anhand der definierten Klas-

sen werden alle Komponenten in einem späteren Schritt, der in Abschnitt 5.1.4 beschrieben wird, bezüglich ihres Schutzbedarfs untersucht, um so zu ermitteln, welche Schutzmaßnahmen für sie getroffen werden müssen.

Als Ausgangspunkt sollten die Definitionen für Schutzbedarfsklassen des BSI-Standards 100-2 „IT-Grundschutz-Vorgehensweise“ herangezogen werden. Bei dieser Vorgehensweise werden die drei Schutzbedarfsklassen „normal“, „hoch“ und „sehr hoch“ verwendet. Die Einteilung erfolgt anhand der in Tabelle 2 angegebenen qualitativen Aussagen, da eine quantitative Aussage häufig schwierig und mit großem Aufwand verbunden ist.

Schutzbedarfsklasse	***Beschreibung***
Normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
Hoch	Die Schadensauswirkungen können beträchtlich sein.
Sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 2: Definition der Schutzbedarfsklassen

Diese Definition der Schutzbedarfsklassen kann in den meisten Fällen übernommen werden. Sie muss jedoch in eine in der Praxis einsetzbare Definition überführt werden, indem konkrete, nachprüfbare Werte definiert werden. Dazu werden die individuellen Gegebenheiten der Institution im Hinblick auf die folgenden typischen Schadensszenarien betrachtet:

- Verstoß gegen Gesetze/Verträge/Vorschriften
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- negative Innen- oder Außenwirkung
- finanzielle Auswirkungen

So kann zum Beispiel festgelegt werden, dass ein finanzieller Schaden bis 10.000 Euro begrenzt und überschaubar ist, Schäden bis 100.000 Euro beträchtlich und alle darüber hinausgehenden die Existenz bedrohen. Daraus ergeben sich unter Berücksichtigung von Tabelle 2 die Grenzen für die Schutzbedarfsklassen, die für dieses Beispiel in Tabelle 3 angegeben werden.

Schutzbedarfsklasse	***Schaden in Bezug auf finanzielle Auswirkungen***
Normal	Schäden bis zu einer Höhe von 10.000 Euro
Hoch	Schäden zwischen 10.000 und 100.000 Euro
Sehr hoch	Schäden über 100.000 Euro

Tabelle 3: Beispiel für die Grenzen der Schutzbedarfsklassen anhand der finanziellen Auswirkungen

Diese konkreten Zahlen können nicht auf jede Institution übertragen werden. Die Grenzen der Schutzbedarfsklassen müssen vielmehr nach den individuellen Gegebenheiten festgelegt werden. Gleiches gilt für die übrigen Schadensszenarien. Der dabei entstandene Maßstab ist die Grundlage für die in Abschnitt 5.1.4 beschriebene Schutzbedarfsfeststellung.

5.1.3 Aktivität „Ist-Zustand analysieren“

Voraussetzungen:	keine
Hilfsmittel:	BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“, Abschnitt 4.2
Ergebnisse:	Dokumentation der vorhandenen IT-Struktur
	Dokumentation der erfassten Datenbestände
	Dokumentation der umgesetzten Sicherheitsmaßnahmen

Als weiterer wichtiger Punkt in Phase 1 steht die Erhebung der vorhandenen IT-Struktur, der vorhandenen Datenbestände und der bereits getroffenen Sicherheitsmaßnahmen an.

Zur Ermittlung der IT-Struktur bietet sich die IT-Strukturanalyse nach IT-Grundschutz an, die im BSI-Standard 100-2 in Kapitel 4.1 „IT-Strukturanalyse“ detailliert beschrieben wird. Daher soll an dieser Stelle nur kurz darauf eingegangen werden. Die in den folgenden Abschnitten beschriebenen Dokumente müssen nicht immer neu erstellt werden. Vielfach kann auf bereits bestehende Dokumentation zurückgegriffen werden, die gegebenenfalls aktualisiert werden muss.

Die in den nachfolgenden Schritten erarbeiteten Dokumente sind nicht nur für die Analyse und die Einführung neuer Dienste sinnvoll. Sie unterstützen auch den späteren Betrieb, die Wartung und die Fehlersuche.

IT-Strukturanalyse

Die IT-Strukturanalyse verfolgt den Zweck, den gesamten betrachteten Informationsverbund zu erfassen. Diese Dokumentation muss alle vorhandenen Komponenten enthalten, da jede Komponente für die einzuführenden neuen Dienste relevant sein könnte. Diese Bestandsaufnahme bringt weitere positive Nebeneffekte mit sich. Durch die mögliche Wieder- bzw. Weiterverwendung vorhandener Komponenten können Ressourcen eingespart werden. Dadurch kann sowohl eine Zeit- als auch Kostenersparnis eintreten. Außerdem können so neue Komponenten optimal in den vorhandenen Informationsverbund integriert werden.

Netzplan: Die Erstellung eines Netzplans ist Bestandteil der IT-Strukturanalyse. Dieser enthält zum Beispiel als Netztopologieplan alle Netzkomponenten (Clients, Server, aktive Netzkomponenten) sowie die Netzverbindungen. Dabei werden sowohl die Verbindungen zwischen diesen Systemen als auch die Verbindungen nach außen betrachtet. Zu jeder dieser Komponenten des Netzplans sollte ein Minimalsatz an Informationen mit erfasst werden. Dazu zählen:

- ein Identifikator,
- die Plattform,
- der Standort,
- ein Verantwortlicher und
- Informationen über die Netzanbindung (wie zum Beispiel der DNS-Name und die IP-Adresse).

Die Informationen über die Netzanbindung sind für die Schutzbedarfsfeststellung nicht dringend erforderlich. Die erfassten Daten sind jedoch wichtige Hilfsmittel für den Betrieb und die Administration.

Gruppenbildung: Um die Komplexität der gesammelten Informationen zu reduzieren, können Gruppen gebildet werden. Komponenten, die vom gleichen Typ sind, gleiche Aufgaben erfüllen

und den gleichen Rahmenbedingungen unterliegen, können zu einer Gruppe zusammengefasst werden. Diese Gruppe wird dann durch ein Element repräsentiert. Dadurch wird ein *bereinigter Netzplan* erzeugt, der (im Gegensatz zu dem zuvor beschriebenen Netzplan) anstatt der Einzelelemente die gebildeten Gruppen enthält. Zu jeder Gruppe wird zusätzlich angegeben, wie viele Elemente sie enthält. Abbildung 5.3 zeigt beispielhaft einen bereinigten Netzplan.

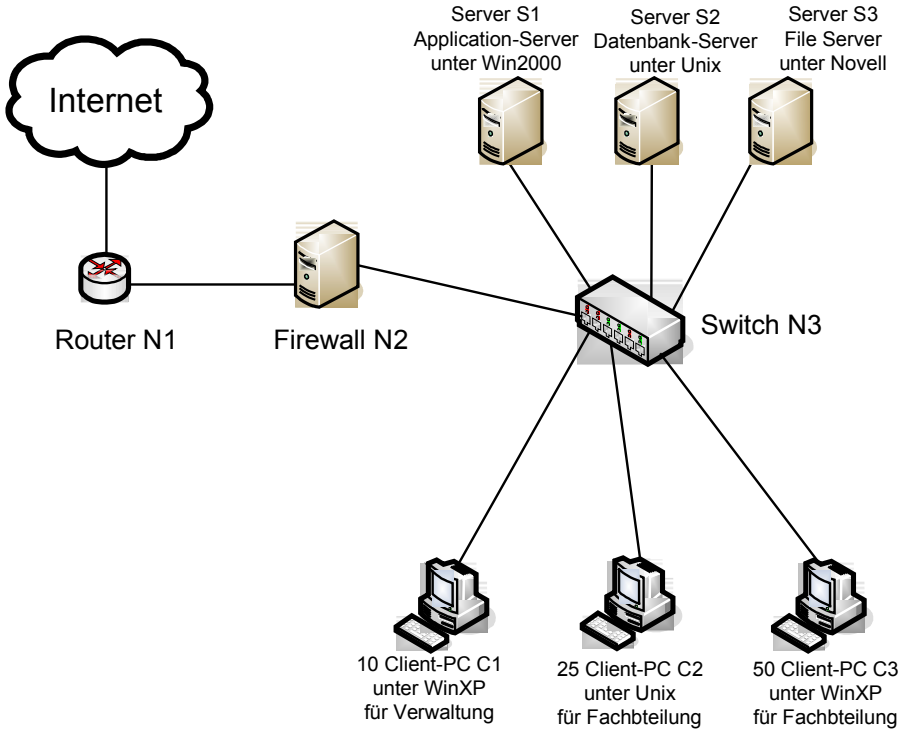

Abbildung 5.3: Beispiel eines bereinigten Netzplans

IT-Systeme und IT-Anwendungen: An die Erstellung des Netzplans schließt sich die Erhebung aller IT-Systeme und -Anwendungen an. Die Reihenfolge, in der diese beiden Gruppen erfasst werden, ist von der Organisationsstruktur abhängig. Für beide sollte eine Tabelle mit allen relevanten Daten erstellt werden.

Bei der Erfassung der IT-Systeme sollen nicht nur Computer im klassischen Sinne aufgelistet werden, sondern auch aktive Netzkomponenten, Netzdrucker, TK-Anlagen etc. Im Gegensatz zum Netzplan, der die vorgenannten Komponenten ebenfalls enthält, werden hier auch die nicht vernetzen IT-Systeme aufgeführt. Während beim Netzplan die grafische Übersicht über alle vernetzten Systeme und die zwischen ihnen bestehenden Netzverbindungen im Vordergrund stehen, sollen jetzt die Eigenschaften aller eingesetzten IT-Systeme dokumentiert werden.

Jedes IT-System sollte bezüglich seiner technischen Umsetzung erfasst werden. So kann zum Beispiel zwischen Client-PC, Server unter Unix oder TK-Anlage unterschieden werden. Die IT-Systeme werden nur als Ganzes erfasst, nicht durch ihre einzelnen Hardware-Bestandteile. Zu jedem erfassten IT-System sollte wiederum ein Minimalsatz an Informationen angegeben werden. Dazu zählen ein eindeutiger Bezeichner, eine kurze Beschreibung, die Plattform, die Anzahl der in der Gruppe vorhandenen Elemente, der Ort, der Status und der Verantwortliche für das System. Tabelle 4 zeigt beispielhaft einen Ausschnitt der Übersicht der IT-Systeme für den in Abbildung 5.3 dargestellten Netzplan.

Identifikator	*Beschreibung der IT-Systeme*	*Plattform*	*Anzahl*	*Ort*	*Status*	*Verant-wortlicher*
S1	Anwendungsserver	Win2000	1	Raum125	in Betrieb	
S2	Datenbank-Server	Unix	1	Raum 312	in Betrieb	
S3	Fileserver	Novell	1	Raum 013	in Betrieb	
C1	Gruppe von Client-PC für die Verwal-tung	WinXP	10	Raum 110-120	in Betrieb	
C2	Gruppe von Client-PC für die Fachab-teilung	Unix	25	Raum 210-235	in Betrieb	
C3	Gruppe von Client-PC für die Fachab-teilung	WinXP	50	Raum 315-340	in Betrieb	
N1	Router für den In-ternetzgang	Router	1	Raum 011	in Planung	
N2	Firewall	Application Gateway auf Unix	1	Raum 012	in Planung	
N3	Switch	Switch	1	Raum 101	in Betrieb	
TK1	TK-Anlage	ISDN-TK-Anlage	1	Raum 001	in Betrieb	

Tabelle 4: Beispiel für eine Auflistung der IT-Systeme

Analog zu dem Netzplan kann die Auflistung beispielsweise um IP-Adressen, DNS-Namen oder den Release-Stand erweitert werden. Auch wenn diese Daten für die Schutzbedarfsfeststellung nicht unbedingt notwendig sind, können sie bei der Administration hilfreich sein.

Als weiterer Schritt werden alle IT-Anwendungen erfasst. Dazu wird für jede IT-Anwendung ermittelt, von welchen IT-Systemen sie abhängig ist. Für jede IT-Anwendung erfolgt also eine Zuordnung zu einem oder mehreren IT-Systemen. Eine Anwendung kann z. B. auf *einem* IT-System ausgeführt werden, seine Daten jedoch von *einem anderen* System erhalten. Im Umfeld von verteilten Systemen oder Clustern ist eine solche Konstellation typischerweise anzutreffen.

Um zu einer solchen Auflistung der IT-Anwendungen zu kommen, kann ein Zwischenschritt eingefügt werden. Bei diesem werden für alle erfassten IT-Systeme die IT-Anwendungen ermittelt, die auf ihnen laufen.

Bei der Auflistung der IT-Anwendungen sollte parallel mit erfasst werden, ob von dieser IT-Anwendung personenbezogene Daten verarbeitet werden, da dies für die in Abschnitt 5.1.4 beschriebene Schutzbedarfsfeststellung eine wichtige Rolle spielt.

Tabelle 5 zeigt einen Auszug aus einer möglichen Zuordnung der IT-Systeme zu IT-Anwendungen.

Identifikator	*Beschreibung der IT-Anwendung*	*Personenbezogene Daten*	*S1*	*S2*	*S3*	*C1*	*C2*	*C3*
A1	Benutzer-Authentisierung	X		X		X	X	X
A2	Terminkalender	X	X			X		
A3	Systemmanagement				X		X	
A4	Dokumentenverwaltung		X	X		X		

Tabelle 5: Beispielhafter Auszug der Erfassung der IT-Anwendungen

Datenbestände

Die Erfassung der vorhandenen Datenbestände ist ein weiterer wichtiger Punkt. Aus der Zuordnung der IT-Anwendungen zu den IT-Systemen können Rückschlüsse darüber gezogen werden, über welche Systeme welche Daten fließen und auf welchen Systemen diese verarbeitet und gespeichert werden. Außerdem wird ermittelt, welche relevanten Daten vorliegen, die vor den neu entstehenden zusätzlichen Gefährdungen geschützt werden müssen.

Basissicherheit

Neben der IT-Strukturanalyse sind die im bestehenden System bereits getroffenen Sicherheitsmaßnahmen zu erfassen. Diese Informationen können durch die Sichtung der vorhandenen Dokumentation und die Befragung der Verantwortlichen gewonnen werden. Die Auflistung kann helfen, um bei der Planung der Absicherung des Netzes auf bereits getroffene Maßnahmen zurückzugreifen und die neuen Maßnahmen optimal in die bereits bestehenden zu integrieren. Später können so Maßnahmen erkannt werden, die in Beziehung zueinander stehen oder sich sogar gegenseitig aufheben.

5.1.4 Aktivität „Schutzbedarfsfeststellung durchführen“

Voraussetzungen:	Auflistung der benötigten Dienste und Kommunikationsverbindungen (Aktivität 5.1.1)
	Maßstab für Schutzbedarfsklassen (Aktivität 5.1.2)
	Erfassung aller IT-Systeme, IT-Anwendungen und Verbindungen (Aktivität 5.1.3)
Hilfsmittel:	BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“, Abschnitt 4.3
Ergebnisse:	Schutzbedarfsfeststellung

Die Ergebnisse der vorangegangenen Aktivitäten werden nun zusammen betrachtet. Für die IT-Systeme und -Anwendungen sowie die Kommunikationsverbindungen muss der Schutzbedarf bestimmt werden. Für den bereits bestehenden IT-Verbund wird eine solche Schutzbedarfsfeststellung vorausgesetzt, sodass in diesem Fall auf bereits existierende Dokumente zurückgegriffen werden kann. Für jeden Dienst muss der Schutzbedarf bezüglich der Sicherheitsgrundwerte Integrität, Vertraulichkeit und Verfügbarkeit ermittelt werden. Diese Untersuchung basiert auf den in Aktivität 5.1.2 bestimmten Kategorien für die einzelnen Schadensszenarien.

Bei der Feststellung des Schutzbedarfs sollen aus der Sicht der Anwender realistische Schadensszenarien entwickelt und die maximalen Schäden und Folgeschäden betrachtet werden. Bei der Einschätzung über die Höhe der möglichen Schäden, aus denen letztendlich der Schutzbedarf resultiert, ist es erforderlich, die Verantwortlichen und Benutzer nach ihrer persönlichen Einschätzung zu befragen.

Sollen zum Beispiel, wie bereits in Aktivität 5.1.1 beschrieben, Prospekte zum Herunterladen angeboten werden, so muss für diese Daten und die zugehörigen Kommunikationsverbindungen der Schutzbedarf anhand der Schadensszenarien und der definierten Schutzbedarfsklassen für alle Grundwerte bestimmt werden. Die Informationen wurden bisher auch herausgegeben und die Verteilung ist gerade das Ziel der Funktionalität. Daher liegt kein Schutzbedarf für die Vertraulichkeit vor. Für die Verfügbarkeit kann der Schutzbedarf „normal“ angenommen werden, da davon ausgegangen werden kann, dass die Informationen nicht zeitkritisch sind und andere Verbreitungswege existieren. Bezüglich der Integrität wird ein normaler Schutzbedarf angenommen. Dabei ist zu beachten, welche Zielgruppe von den Prospekten angesprochen wird und ob Entscheidungen allein auf der Grundlage der Prospekte getroffen werden. Bei reinen Werbeprospekten sind die Auswirkungen meist weniger ausgeprägt als bei technischen Spezifikationen. Integritätsverletzungen können beispielsweise zu einer negativen Außenwirkung oder zu finanziellen Schäden, z. B. Regressforderungen, führen.

5.1.5 Aktivität „Über weiteres Vorgehen entscheiden“

Voraussetzungen:	Ergebnisse der Aktivitäten 5.1.1 bis 5.1.4
Hilfsmittel:	keine
Ergebnisse:	Entscheidung über weiteres Vorgehen
	Präsentation der Ergebnisse

Zum Abschluss der Phase 1 sollten die Ergebnisse noch einmal im Zusammenhang betrachtet werden. Dabei wird auch geprüft, ob alle relevanten Dokumente dieser Phase vorliegen.

An dieser Stelle muss über das weitere Vorgehen entschieden werden. Haben sich während der einzelnen Aktivitäten dieser Phase Widersprüche ergeben, so müssen diese erst beseitigt werden, bevor das Projekt fortgesetzt werden kann. So kann zum Beispiel während der Schutzbedarfsfeststellung ein Schutzbedarf identifiziert worden sein, der nur durch eine Vielzahl von Maßnahmen gewährleistet werden kann. In diesem Fall muss entschieden werden, ob der Dienst ggf. in einer anderen Form oder gar nicht umgesetzt wird. Auf keinen Fall darf dieses Problem durch ein Anpassen des Schutzbedarfs gelöst werden.

Das Ergebnis dieser Aktivität kann also die Überarbeitung der in den vorangegangenen Schritten erstellten Dokumente zur Folge haben. Diese Rücksprünge innerhalb der Phase sind in Abbildung 5.2 aus Gründen der Übersichtlichkeit nicht dargestellt, sind jedoch möglich.

Zum Abschluss dieser Phase kann es sinnvoll sein, die gewonnenen Ergebnisse allen Beteiligten zu präsentieren, sodass alle relevanten Informationen für die nächsten Phasen weitergegeben werden.

5.2 Phase 2: Konzeption

Nach der in Phase 1 durchgeführten Analyse, bei der u. a. die benötigten Dienste einschließlich des Schutzbedarfs der internen Daten und Kommunikationsverbindungen ermittelt wurden, kann mit der Konzeption begonnen werden. Dabei wird auf die in der vorangegangenen Phase erstellten Dokumente zurückgegriffen. Im Rahmen der Konzeption kommt es zu Änderungen oder Konkretisierungen, die beispielsweise die Art der Kommunikationsverbindungen betreffen. Da sich dadurch auch die Anforderungen an die Sicherheit ändern können, erfordert dies eine Aktualisierung der Schutzbedarfsfeststellung und damit einen Rücksprung zu Aktivität 5.1.4.

Die Konzeption gliedert sich in zwei Blöcke, die jeweils mehrere Aktivitäten beinhalten. Zunächst werden das interne Netz und die Auswirkungen der Internet-Anbindung auf dieses betrachtet und dessen Architektur überarbeitet. Hauptbestandteil dieser Phase ist die Hauptschleife (grauer Kasten in der Abbildung 5.4 auf der folgenden Seite), die zunächst allgemein für den Netzübergang zum Internet und anschließend für jeden zu integrierenden Dienst zu durchlaufen ist. In dieser Hauptschleife werden die Architektur angepasst und Konzepte für Beschaffung, Konfiguration und Betrieb erstellt. Alle diese Aktivitäten können auf der Grundlage des zum jeweiligen Fachthema gehörigen ISi-S durchgeführt werden, der zu jeder Aktivität Empfehlungen gibt.

Nach der Zusammenstellung der umzusetzenden Maßnahmen aus den in der ISi-Reihe gegebenen Empfehlungen ist eine Modellierung nach IT-Grundschutz vorgesehen, um die fehlenden IT-Grundschutz-Maßnahmen, die sich im Wesentlichen auf übergeordnete, organisatorische und personelle Maßnahmen beschränken, zu berücksichtigen. Im Anschluss kann die Umsetzungsentscheidung getroffen und das technische Feinkonzept erstellt werden.

Durch die Einführung neuer Dienste oder die Schaffung der Internet-Anbindung treten eine Vielzahl neuer Gefährdungen auf, die die Daten und Anwendungen bedrohen können. Gegen diese müssen geeignete Schutzmaßnahmen ergriffen werden. Bei der Konzeptionsphase werden allerdings nicht nur funktionelle Aspekte betrachtet. Vielmehr soll die Planung von Anfang an unter dem Aspekt der IT-Sicherheit erfolgen, um sicherheitstechnischen Problemen beim späteren Betrieb schon von vornherein entgegenzuwirken. Auch wenn in dieser Phase noch keine Produktentscheidungen getroffen werden, sollten wirtschaftliche Aspekte mit in die Entscheidung einbezogen werden. Die Konzeption sollte im Normalfall marktübliche Maßnahmen und Lösungen enthalten. Sollen andere Maßnahmen ausgewählt werden, so muss bei dieser Entscheidung der zusätzlich entstehende Aufwand mit berücksichtigt werden.

Abbildung 5.4 verdeutlicht das Vorgehen in Phase 2.

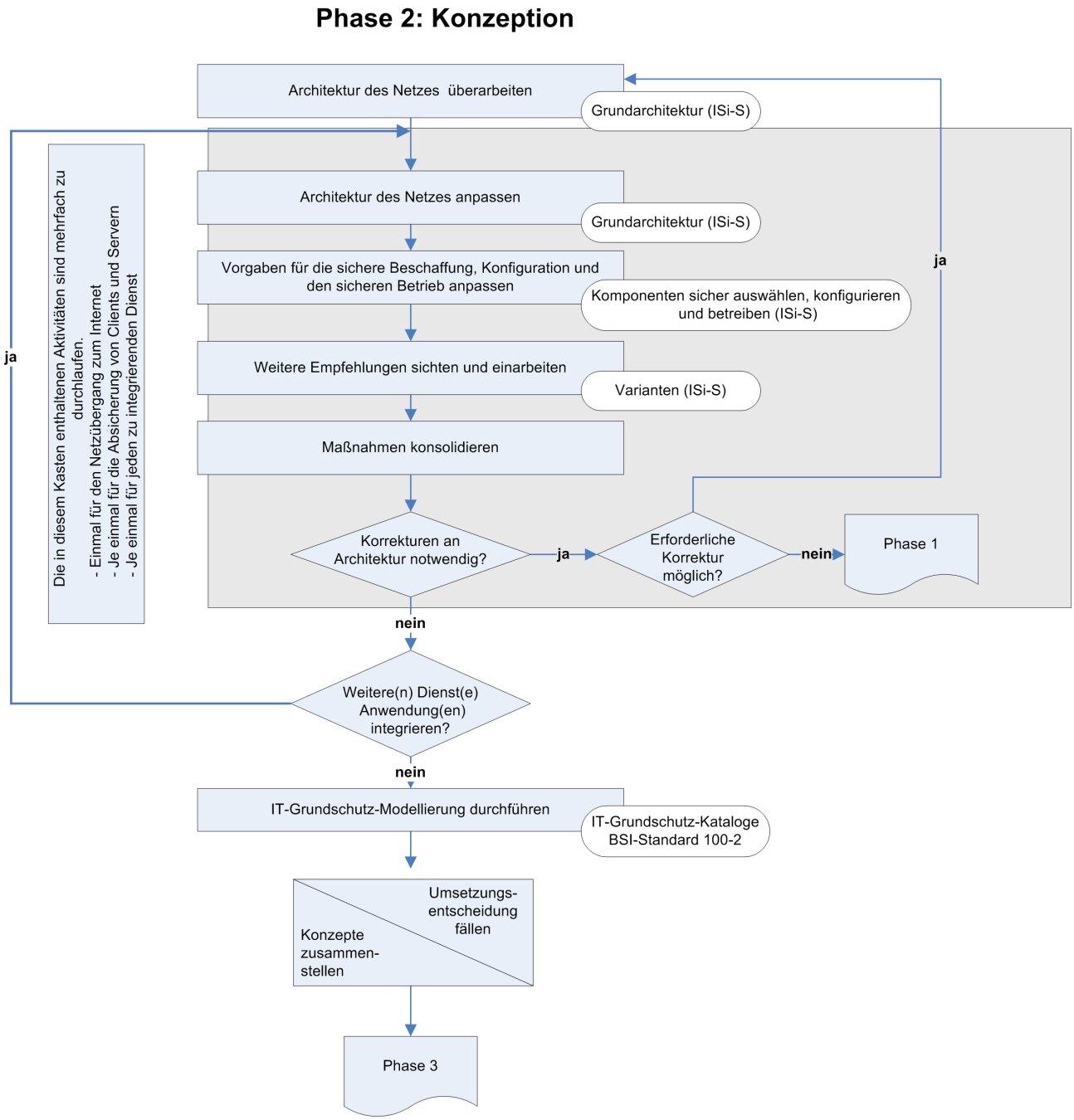

Abbildung 5.4: Aktivitäten der Phase 2: Konzeption

5.2.1 Aktivität „Architektur des Netzes überarbeiten“

Voraussetzungen:	Auflistung der benötigten Dienste und Kommunikationsverbindungen (Aktivität 5.1.1)
	Dokumentation der vorhandenen IT-Struktur (Aktivität 5.1.3)
	Schutzbedarfsfeststellung (Aktivität 5.1.4)
Hilfsmittel:	Modul 1.1/1.2 „Sichere Anbindung von Servern und lokalen Netzen an das Internet (ISi-LANA)“, ISi-S, Abschnitt 4 „Sichere Grundarchitektur für normalen Schutzbedarf“
Ergebnisse:	Grundarchitektur des Netzes

Um einen neuen Dienst in das bestehende Netz zu integrieren oder erstmalig eine Verbindung zum Internet herzustellen, muss zunächst überprüft werden, ob die Architektur des Netzes im derzeitigen Zustand dafür geeignet ist. Andernfalls muss das Netz angepasst werden, um die Anforderungen zu erfüllen und damit den späteren Einsatz der Dienste gewährleisten zu können.

Ein weiterer Punkt ist der Netzaufbau. Ist die Internet-Anbindung bereits vorhanden, so sind an dieser Stelle i. d. R. weniger Anpassungen notwendig, als wenn die Anbindung an das Internet neu geschaffen wird. Wenn die Internet-Anbindung neu geschaffen wird, kann es notwendig sein, den Netzaufbau vollkommen neu zu strukturieren. Netze, die aus Zonen mit verschiedenen Anforderungen an die Sicherheit bestehen, sind aus sicherheitstechnischer Sicht hierarchielosen Netzen vorzuziehen. Gibt es Zonen mit besonders schutzwürdigen Daten, so sollte auch in Betracht gezogen werden, diese ganz vom übrigen Netz abzukoppeln.

Dabei sollte darauf geachtet werden, dass die Architektur zukunftsträchtig ausgelegt wird und skaliert werden kann. Selbst wenn die vorhandene Architektur zum heutigen Zeitpunkt für die geplanten Dienste noch als ausreichend angesehen wird, sollte die Möglichkeit zur Anpassung in der Zukunft offen gehalten werden. Es kann davon ausgegangen werden, dass die heute notwendigen Anforderungen in der Zukunft korrigiert werden müssen. Eine Architektur, die dies unterstützt, wird sich als vorteilhaft erweisen.

Eine umfassende Betrachtung aller Aspekte, die bei der Überarbeitung der Netzarchitektur beachtet werden müssen, findet sich im Modul 1.1/1.2 „Sichere Anbindung von Servern und lokalen Netzen an das Internet (ISi-LANA)“. Der Abschnitt 4 „Sichere Grundarchitektur für normalen Schutzbedarf“ im ISi-S dieses Moduls liefert Empfehlungen, die als Grundlage für das weitere Vorgehen dienen. Die dortigen Empfehlungen werden für Rechnernetze mit normalem Schutzbedarf als ausreichend angesehen. Die ergänzenden Maßnahmen für Rechnernetze mit hohem Schutzbedarf werden beim ersten Durchlauf der Hauptschleife in Aktivität 5.2.4 betrachtet.

5.2.2 Aktivität „Architektur des Netzes anpassen“

Voraussetzungen:	Auflistung der benötigten Dienste und Kommunikationsverbindungen (Aktivität 5.1.1)
	Dokumentation der vorhandenen IT-Struktur (Aktivität 5.1.3)
	Schutzbedarfsfeststellung (Aktivität 5.1.4)
	Architektur des Netzes (Aktivität 5.2.1)
Hilfsmittel:	Grundarchitektur und Varianten im ISi-S der Module der ISi-Reihe
Ergebnisse:	Architektur des Netzes

Nach der ersten Anpassung der Netzarchitektur beginnt die Hauptschleife der Phase zwei, die in den Aktivitäten 5.2.2 bis 5.2.5 beschrieben wird. Diese wird einmal für jeden zu integrierenden Dienst durchlaufen (siehe Abbildung 5.4).
Bei der Anpassung der Architektur wird sowohl der Netzübergang zum Internet als auch das interne Netz betrachtet. Dabei müssen nicht zwangsläufig Änderungen durchgeführt werden. Es muss allerdings geklärt werden, ob die Architektur grundsätzlich für die geplanten Dienste geeignet ist. Bei dieser Aktivität kann es auch vorkommen, dass die bestehende Architektur um eine weitere Zone erweitert werden muss. Detaillierte Architekturvorschläge werden in den zum jeweiligen Dienst gehörenden Studien ISi-S herangezogen, die auf der Grundarchitektur von ISi-LANA aufbauen.

Ein wesentlicher Punkt bei der Integration eines neuen Dienstes ist das Sicherheits-Gateway. Dieses ist eine Kombination aus Hardware- und Software und trägt zum geregelten Datenaustausch zwischen verschiedenen Netzen bei. Komponenten eines Sicherheits-Gateways können beispielsweise Paketfilter, Application Level Gateways und Anwendungen zur Abwehr von Viren und Angriffen und zur Netzüberwachung sein.

Es sollte auch über die Einrichtung einer Demilitarisierten Zone (DMZ) nachgedacht werden, falls dies nicht bereits in Aktivität 5.2.1 im Zusammenhang mit den einzurichtenden Sicherheitszonen geschehen ist. In einer solchen DMZ können Systeme aufgestellt werden, die von anderen Netzen, d. h. sowohl dem internen Netz als auch dem Internet, durch Filtersysteme abgetrennt sind. So können Dienste sicher integriert werden, die sowohl von außen als auch von innen erreichbar sein müssen.

Es muss auch überlegt werden, ob die Anbindung an das Internet redundant ausgelegt werden soll. Dazu sollte der Schutzbedarf für die Verfügbarkeit der Anwendungen (Aktivität 5.1.4), die auf eine Netzanbindung angewiesen sind, herangezogen werden.

Ein weiterer Aspekt ist die zur Verfügung stehende Bandbreite am Übergang zum Internet. Zur Ermittlung geeigneter Werte muss berücksichtigt werden, welche Datenmengen die entsprechenden Dienste und Anwendungen erzeugen und welcher Durchsatz dabei benötigt wird. Eine solche Abschätzung sollte mit Erfahrungswerten kombiniert werden. Sollen lediglich einzelne neue Dienste eingeführt werden, so muss geprüft werden, ob die zur Verfügung stehende Bandbreite ausreicht oder vergrößert werden muss, um den neuen Dienst problemlos bereitzustellen.

Es muss überlegt werden, in welchem Bereich der Netztopologie die Hardware, auf der der Dienst läuft, platziert werden soll. Wurden verschiedene Sicherheitszonen geschaffen, so muss in Abhängigkeit vom Schutzbedarf der Dienst einer solchen Sicherheitszone zugeordnet werden. Dabei muss sichergestellt werden, dass alle Komponenten, die den Dienst nutzen sollen, auf ihn zugreifen können. Parallel dazu sollte aber auch der Zugriff, soweit technisch möglich, auf diese Komponenten

beschränkt werden. Außerdem sollten bei dieser Betrachtung nicht nur diejenigen bedacht werden, die den Dienst nutzen wollen. Es muss auch geprüft werden, dass die Ressourcen, die der Dienst selbst nutzt, erreichbar sind. Es kann beispielsweise der Fall sein, dass ein Webserver auf Daten auf einem Datenbank-Server zugreifen muss.

Dazu gehören nicht nur die Zugriffe auf das interne Netz, sondern auch am Netzübergang zum Internet. Soll der Dienst auch vom externen Netz aus erreichbar sein, so muss geprüft werden, ob dazu Anpassungen an Filtern etc. notwendig sind. Soll der Dienst sowohl vom internen als auch vom externen Netz aus erreichbar sein, wie es beispielsweise bei einem E-Mail-Server erforderlich ist, kann der Server in der DMZ platziert werden. Damit kann der Zugriff aus den beiden Netzen realisiert werden, gleichzeitig aber auch der Schutz des internen Netzes und des Dienstes erhöht werden.

Ein weiterer wichtiger Aspekt ist das Netzmanagement. Die dabei eingesetzten Komponenten werden für die in Phase 4 beschriebene Administration und Betrieb benötigt. Allerdings muss bereits bei der Konzeption festgelegt werden, welche Strategie hinsichtlich Sicherheitsaspekten verfolgt werden soll. Dazu gehört neben der Anordnung der Komponenten auch die Entscheidung, welche Daten relevant sind.

Eine detaillierte Beschreibung für die einzelnen Dienste ist in den ISi-Modulen des Themenbereichs 2 „Dienste und Anwendungen im Internet“ im jeweiligen Abschnitt „Sichere Grundarchitektur für normalen Schutzbedarf“ zu finden. Aspekte des hohen Schutzbedarfs werden in der Aktivität 5.2.4 betrachtet.

5.2.3 Aktivität „Vorgaben für die sichere Beschaffung, Konfiguration und den sicheren Betrieb anpassen“

Voraussetzungen:	Dokumentation der vorhandenen IT-Struktur (Aktivität 5.1.3)
	Schutzbedarfsfeststellung (Aktivität 5.1.4)
	Grundvorgaben für Beschaffung, Konfiguration und Betrieb (sofern vorhanden)
Hilfsmittel:	Abschnitt „Komponenten sicher auswählen, konfigurieren und betreiben“ und Varianten im ISi-S der Module der ISi-Reihe
Ergebnisse:	Konzepte für Beschaffung, Konfiguration und Betrieb

Im Anschluss an die Anpassung der Architektur muss ermittelt werden, welche Maßnahmen bei der Beschaffung, Konfiguration und dem Betrieb zur Absicherung des internen Netzes getroffen werden müssen. Diese Maßnahmen werden in den Vorgaben für Beschaffung, Konfiguration und Betrieb dokumentiert. Für alle drei Bereiche bietet der ISi-S umfassende Erläuterungen, die in den Checklisten ISi-Check zusammengefasst sind.

Diese Anforderungen ergeben sich in der Regel aus den in den vorangegangenen Aktivitäten gewählten Architekturen. So ist z. B.der Einsatz von Virenschutzprogrammen nach dem heutigen Stand der Technik unverzichtbar. Diese generelle Anforderung wird nun konkretisiert, indem beschrieben wird, welche Methoden zur Schadprogrammsuche das Programm beherrschen muss. Auch „organisatorische“ Aspekte wie die zentrale Managebarkeit können eine solche Anforderung darstellen.

Zusammen mit evtl. bereits vorhandenen, institutionsweiten allgemeinen Vorgaben können so spezielle Konzepte für Beschaffung, Konfiguration und Betrieb erstellt werden. Diese beziehen sich dabei auf die einzelnen Komponenten der entwickelten Architektur.

5.2.4 Aktivität „Weitere Empfehlungen sichten und einarbeiten“

Voraussetzungen:	Konzepte für Beschaffung, Konfiguration und Betrieb, Grundarchitektur, Schutzbedarfsfeststellung
Hilfsmittel:	Varianten im ISi-S der Module der ISi-Reihe
Ergebnisse:	angepasste Konzepte für Beschaffung, Konfiguration und Betrieb
	angepasste Grundarchitektur

Bis zu diesem Zeitpunkt sind Maßnahmen ausgewählt worden, die für ein Netz oder einen Dienst mit normalem Schutzbedarf ausreichend sind. Nun kann es aber Teilbereiche im internen Netz geben, die einen hohen Schutzbedarf in Bezug auf einen der Sicherheitsgrundwerte Integrität, Vertraulichkeit oder Verfügbarkeit haben. Oder die auf dem Papier erstellte Architektur ist noch sehr weit weg von der bereits in der Institution umgesetzten Architektur. Oder gewisse Anforderungen werden als übertrieben bzw. als nicht ausreichend eingeschätzt.

Um diese Aspekte aufzugreifen, werden zu diesem Zeitpunkte die Varianten, die im jeweiligen ISi-S den Gefährdungen zugeordnet dargestellt sind, gesichtet und bei Bedarf den Konzepten oder der Grundarchitektur hinzugefügt. Hier werden ganz bewusst andere Lösungsmöglichkeiten dargestellt, unter Abwägung der damit verbundenen Restrisiken. Die entworfene Architektur kann damit ganz individuell an die Bedürfnisse angepasst und verändert werden.

Die ISi-Reihe gibt zu jeder Variante ausreichend Informationen hinsichtlich des Umsetzungsaufwands und des Risikos, um in eigener Verantwortung eine gute Entscheidung treffen zu können.

5.2.5 Aktivität „Maßnahmen konsolidieren“

Voraussetzungen:	Konzepte für Beschaffung, Konfiguration und Betrieb, Grundarchitektur
Hilfsmittel:	Varianten und Abdeckungsmatrizen im ISi-S der Module der ISi-Reihe
Ergebnisse:	angepasste Konzepte für Beschaffung, Konfiguration und Betrieb sowie die Grundarchitektur und /oder Widersprüche in den Maßnahmen

Nach der Anpassung der Grundarchitektur, der Erstellung der Konzepte für Beschaffung, Konfiguration und Betrieb und der Auswahl weiterer Empfehlungen, muss bei dieser Aktivität überprüft werden, welche Auswirkungen daraus resultieren. Dabei müssen zum einem die Wechselwirkungen zwischen dem Dienst, den ausgewählten Maßnahmen und der bestehenden Architektur beurteilt werden. Zum anderen kann es auch zu Wechselwirkungen zwischen verschiedenen (geplanten und bereits umgesetzten) Maßnahmen kommen. Dabei kann beispielsweise ermittelt werden, dass sich Maßnahmen gegenseitig aufheben, stören oder gegen die gleiche Gefährdung wirken. Zumindest in den ersten beiden Fällen muss dem entgegengewirkt werden.

Wird beispielsweise als eine Maßnahme zum Schutz der Integrität der übertragenen Daten eine Ende-zu-Ende-Verschlüsselung eingesetzt, so muss beachtet werden, dass sich die damit übertragenen Datenströme nicht mehr ohne weiteres am Sicherheits-Gateway kontrollieren lassen. Eine zentrale Filterung von E-Mails, um Viren zu erkennen, wird damit wesentlich erschwert. Bei einigen (verschlüsselten) Protokollen kann es auch zu Problemen kommen, wenn diese zusammen mit NAT eingesetzt werden sollen. Entsprechende Hinweise werden häufig bei den Varianten erläutert, jedoch können diese aufgrund der Vielzahl der Kombinationsmöglichkeiten nicht vollständig sein.

5.2.6 Entscheidung „Korrektur an Architektur erforderlich“

Ergeben sich bei den vorangegangenen Aktivitäten zur Betrachtung der einzelnen Dienste Widersprüche oder kann eine Aktivität nicht erfolgreich durchgeführt werden, so muss geprüft werden, ob eine grundlegende Korrektur an der bisher erarbeiteten Architektur notwendig ist, um die Probleme zu beseitigen.

Ist eine solche Korrektur notwendig, so muss zu Aktivität 5.2.1 zurückgekehrt werden und alle folgenden Maßnahmen erneut durchlaufen werden, um zu überprüfen, ob die vorgenommene Korrektur weitere Auswirkungen nach sich zieht.

Es kann jedoch auch sein, dass eine Korrektur der Architektur nicht mit vertretbarem Aufwand möglich ist bzw. das Problem durch eine solche nicht gelöst werden kann. In diesem Fall muss zur Phase 1 zurückgekehrt werden, um dort zum Beispiel die Anforderungen an die Dienste anzupassen. Die Anpassung des Schutzbedarfs ist hierbei kein geeignetes Mittel, da der Schutzbedarf ausschließlich von möglichen Schäden bei einer Verletzung der Schutzwerte abhängt.

Haben sich bei der Abarbeitung der vorangegangenen Maßnahmen keine Probleme ergeben, so ist die Betrachtung für den aktuellen Dienst abgeschlossen und für den nächsten benötigten Dienst werden die Aktivitäten 5.2.2 bis 5.2.4 erneut durchlaufen. Sollen keine weiteren Dienste eingeführt werden, so kann mit der Aktivität Fehler: Referenz nicht gefunden fortgefahren werden.

5.2.7 Aktivität „IT-Grundschutz-Modellierung durchführen “

Voraussetzungen:	Konzepte für Beschaffung, Konfiguration und Betrieb, Grundarchitektur, Erhebung der vorhandenen IT-Struktur, Schutzbedarfsfeststellung
Hilfsmittel:	BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“, Abschnitt 4.4, sowie IT-Grundschutz-Kataloge
Ergebnisse:	umfassende Konzepte für Beschaffung, Konfiguration und Betrieb und Grundarchitektur

Nach der Auswahl der Maßnahmen, die in der ISi-Reihe gegeben werden, sollte eine Modellierung nach IT-Grundschutz durchgeführt werden. Ziel ist es, die fehlenden IT-Grundschutz-Maßnahmen, die sich im Wesentlichen auf übergeordnete, organisatorische und personelle Maßnahmen beschränken, zu ergänzen. Dazu wird die geplante und bestehende Architektur mit Hilfe der vorhandenen Bausteine aus den IT-Grundschutz-Katalogen nachgebildet. Als Ergebnis entsteht ein IT-Grundschutzmodell des Informationsverbunds, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des Informationsverbunds beinhaltet. Eine detaillierte Beschreibung dieser Modellierung ist dem BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“ im Abschnitt 4.3 zu entnehmen.

Aus den IT-Grundschutz-Bausteinen können nun die fehlenden IT-Grundschutz-Maßnahmen ermittelt werden, die im bisherigen Konzept noch nicht berücksichtigt wurden. Dazu zählen im Wesentlichen Maßnahmen, die den Bausteinen der Schichten „Übergeordnete Aspekte“ und „Infrastruktur“ zugeordnet werden.

5.2.8 Aktivität „Umsetzungsentscheidung fällen“

Voraussetzungen:	Ergebnisse über Erfolg der vorangegangenen Phase
Hilfsmittel:	keine
Ergebnisse:	Entscheidung über Fortführung des Projekts und Benennung von Verantwortlichen

Die Umsetzungsentscheidung umfasst, ob das Projekt in der konzipierten Form überhaupt umgesetzt werden soll. Zeichnet es sich ab, dass aufgrund der Konzeption die Umsetzung problematisch oder sehr teuer sein wird, oder treten Widersprüche auf, so müssen diese gelöst werden, bevor zur nächsten Phase übergegangen wird. Fehler, die in dieser Phase auftreten, werden in die nächsten Phasen übernommen und können dort weitreichende Folgen haben. In späteren Phasen können diese Probleme nicht mehr beseitigt werden, lediglich die Auswirkungen können mit hohem Aufwand abgemildert werden. Daher sollte die Konzeption mit großer Sorgfalt durchgeführt werden. Eine Entscheidung in diesem Schritt kann auch sein, dass ein konzipierter Dienst in dieser Form nicht umgesetzt wird.

Darüber hinaus umfasst die Umsetzungsentscheidung auch die Benennung der Verantwortlichen. Es muss festgelegt werden, wer die Konzeption umsetzt und wer dabei Entscheidungsträger ist. Dies muss nicht für das gesamte Projekt global festgelegt werden. Vielmehr müssen Entscheidungsträger für die einzelnen Bestandteile des Projekts, einzelne Dienste oder Maßnahmen festgelegt werden.

5.2.9 Aktivität „Konzepte zusammenstellen“

Voraussetzungen:	umfassende Konzepte für Beschaffung, Konfiguration und Betrieb und Grundarchitektur (Aktivität 5.2.7)
Hilfsmittel:	keine
Ergebnisse:	Technisches Feinkonzept

In zeitlicher Nähe zur Umsetzungsentscheidung wird das technische Feinkonzept entwickelt. Obwohl diese beiden Aktivitäten in dieser Beschreibung getrennt wurden, bedeutet dies nicht, dass sie sequenziell abgearbeitet werden müssen. Vielmehr wird in der Praxis die in Abbildung 5.4 gewählte Darstellung umgesetzt werden. Die Aktivitäten können teilweise parallel durchgeführt werden, da getroffene Entscheidungen Einfluss auf beide Aktivitäten haben.

Das technische Feinkonzept basiert auf den in den vorangegangenen Aktivitäten getroffenen Entscheidungen und stellt gleichzeitig die Grundlage für die in der nächsten Phase beschriebene Realisierung dar. Während in den Aktivitäten der Hauptschleife noch allgemeinere Aussagen, basierend auf den Empfehlungen der ISi-Module zu den Maßnahmen gemacht wurden, werden diese im Feinkonzept konkretisiert und auf das konkrete Projekt angepasst. Allerdings müssen an dieser Stelle noch nicht alle Details zur Umsetzung angegeben werden, die Darstellung erfolgt jedoch auf einem hohen technischeren Niveau. Dabei müssen dienstspezifische, aber noch keine produktspezifischen Aspekte enthalten sein.

Wird beispielsweise zunächst nur von einer Whitelist-Strategie für die Einrichtung der Paketfilter gesprochen, so enthält das Feinkonzept eine Auflistung, welche Kommunikationsverbindungen zugelassen und damit in die Whitelist aufgenommen werden sollen.

Die Erstellung des technischen Feinkonzepts sollte mit größter Sorgfalt durchgeführt werden. Alle für die folgende Realisierung relevanten Punkte müssen betrachtet werden. Natürlich müssen die Vorgaben des Feinkonzepts während der Realisierungsphase streng eingehalten werden.

Darüber hinaus werden in dieser Aktivität auch die sogenannten Betriebskonzepte erstellt, die beim Betrieb und der Administration zur Anwendung kommen. Es sollte außerdem überlegt werden, wie mit Tests während des Betriebs umgegangen werden soll. Eine Möglichkeit dazu stellt die Bereitstellung von Referenzsystemen dar, auf denen neue Software-Bestandteile und Hardware-Komponenten ausgiebig getestet werden können, bevor sie im gesamten System eingesetzt werden. Allerdings können solche Referenzplattformen aus Kostengründen oft nicht für alle Systeme bereitgehalten werden.

Eine Lösungsmöglichkeit für diese Probleme stellt die Virtualisierung dar, die sowohl für Hardware als auch für Software durchgeführt werden kann. Eine weitere Möglichkeit bietet das Outsourcing der Tests. Dies kann zum einen dadurch realisiert werden, dass nur vom Hersteller getestete Patches, Updates oder Pattern eingespielt werden. Zum anderen können die Tests von einem externen Dienstleister durchgeführt werden, der die entsprechenden Referenzplattformen, oftmals für mehrere Kunden, bereithält. Beide Varianten ermöglichen es jedoch nicht, eigene Tests durchzuführen. Außerdem entsteht dadurch ein Zeitverzug bis zum Einsatz der neuen Software. Dieser Nachteil ist jedoch oftmals tolerierbar, da der Einsatz ungetesteter Software ein Sicherheitsrisiko mit sich bringt. Alternativ dazu können die Tests auch in der Produktivumgebung durchgeführt werden. Um den normalen Betrieb jedoch nicht zu gefährden, müssen Vorkehrungen dagegen getroffen werden. Dazu können die Tests zu einem Zeitpunkt durchgeführt werden, an dem kein oder kaum normaler Betrieb des Systems stattfindet. Durch die Tests darf die Produktivumgebung nicht mehr als unbe-

dingt notwendig beeinflusst werden. Es muss sichergestellt werden, dass nach den Tests die Produktivumgebung den gleichen Zustand besitzt wie vor den Tests. Diese Variante bietet den Vorteil, dass die Tests in der realen Umgebung durchgeführt werden, allerdings nicht unter Betriebsbedingungen.

Zusätzlich zur Erstellung der Betriebskonzepte sollte auch der Aspekt des Notfallmanagements berücksichtigt werden. Dabei werden Szenarien entwickelt, Prozesse definiert und die notwendigen Voraussetzungen geschaffen, um diese im Notfall abarbeiten zu können, ohne erst durch lange Planungen Zeit zu verlieren. Zu solchen Maßnahmen kann es gehören, Wartungsverträge mit entsprechend definierten Ausfall- und Wiederherstellungszeiten zu definieren oder auch selbst bereits vorkonfigurierte Geräte bereitzuhalten. Ausführliche Informationen zur Erstellung eines Notfallkonzeptes sind im BSI-Standard 100-4 zu finden.

5.3 Phase 3: Realisierung

Nach einer gründlichen Analyse der Rahmenbedingungen und des Bedarfs in Phase 1 und der sorgfältigen Konzeption der Internet-Anbindung und der benötigten Dienste in Phase 2 kann nun mit der Umsetzung begonnen werden.

Die ersten Aktivitäten in dieser Phase behandeln die benötigte Hardware und Software. Neben der Auswahl geeigneter Komponenten spielen die Beschaffung, Konfiguration und Tests eine entscheidende Rolle. Ausgehend von dem erstellten Konzept muss das Sicherheitskonzept weiter ausgearbeitet werden. Die im technischen Feinkonzept festgehaltenen Ergebnisse müssen als ein weiterer Schritt umgesetzt werden. Vor der Inbetriebnahme der neuen Komponenten sollten weitere Tests, die auch Sicherheitsaspekte mit einschließen, durchgeführt werden.

Obwohl der in Abbildung 5.5 dargestellte Plan für den Ablauf dieser Phase keine expliziten Rücksprünge in vorangegangene Phasen vorsieht, sind diese bei Bedarf möglich. Dies kann auch bedeuten, dass ein Dienst nicht wie geplant realisiert wird, sondern eine neue Konzeption erfolgt.

Während der gesamten Phase müssen die in Phase 2 des Ablaufplans getroffenen Entscheidungen der Konzeption streng eingehalten und umgesetzt werden. Es ist nicht möglich, Vorgaben während der Realisierung einfach abzuändern, nur weil deren Umsetzung nicht möglich oder zu schwierig scheint. Werden Probleme oder Fehler der Konzeption erkannt, so müssen diese natürlich korrigiert werden. Dazu ist es aber notwendig, zu Phase 2 zurückzukehren und die entsprechenden Aktivitäten erneut zu durchlaufen. Durch dieses geplante Vorgehen kann die Gefahr verringert werden, im Zuge der Beseitigung eines Fehlers viele weitere Fehler zu erzeugen. So können beispielsweise auch Wechselwirkungen zwischen Maßnahmen und Auswirkungen auf die gesamte Architektur erkannt werden.

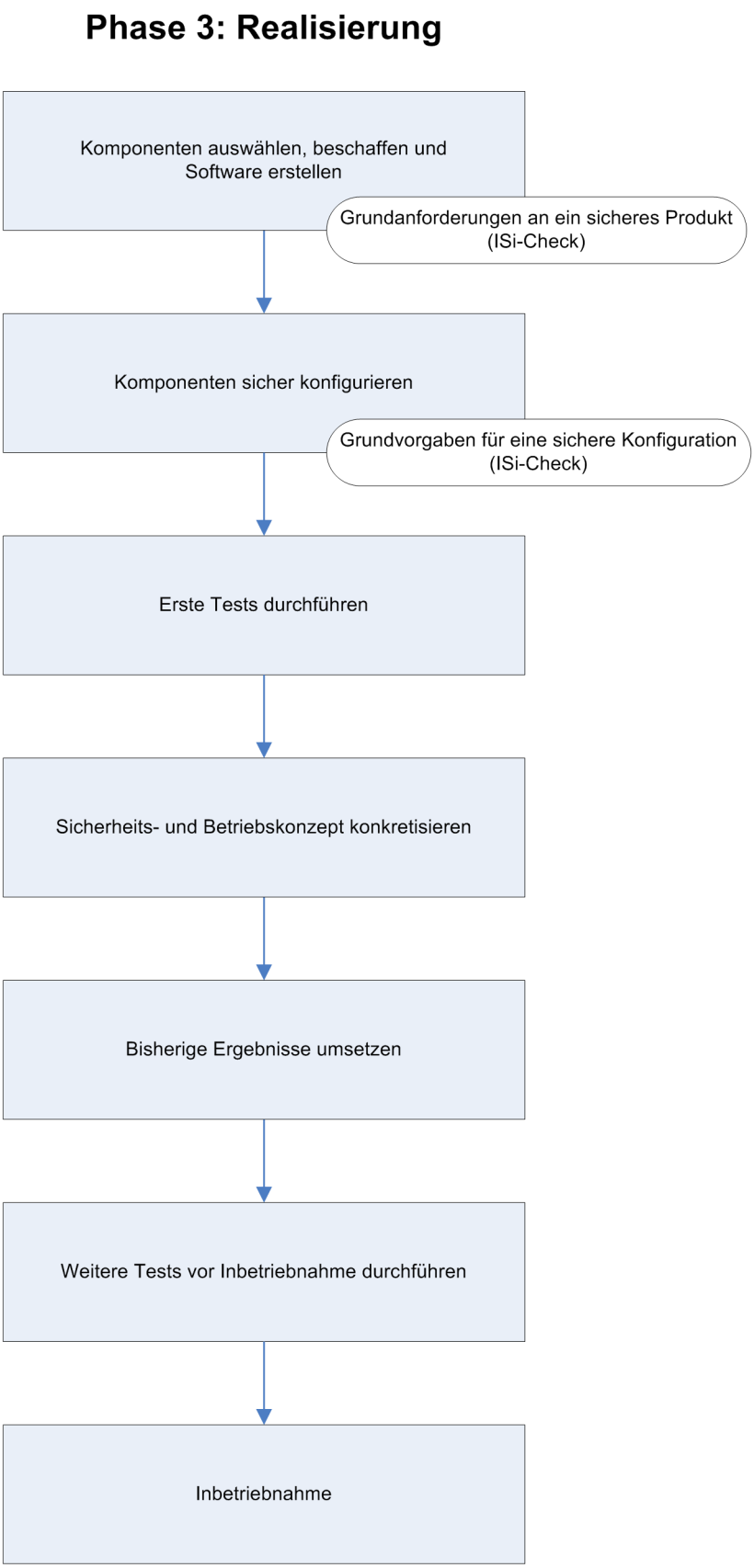

Abbildung 5.5: Aktivitäten der Phase 3: Realisierung

5.3.1 Aktivität „Komponenten auswählen, beschaffen und Software erstellen“

Voraussetzungen:	Konzept für Beschaffung
Hilfsmittel:	Checklisten der ISi-Reihe
Ergebnisse:	Geeignete Komponenten liegen vor

Als erster Schritt bei der Realisierung der Internet-Anbindung oder eines neuen Dienstes steht die Auswahl geeigneter Hardware und Software an. Die zu treffende Entscheidung basiert auf den Vorgaben des technischen Feinkonzepts. Die dort geforderten Maßnahmen müssen mit den ausgewählten Produkten umsetzbar sein.

Innerhalb der ISi-Reihe werden diese Anforderungen in dem jeweiligen Modul im ISi-S im Abschnitt „Grundanforderungen an ein sicheres Produkt“ detailliert erläutert. Des Weiteren werden für diesen Schritt auch die alternativen Empfehlungen bzw. bei Bedarf die Empfehlungen für den hohen Schutzbedarf aus den gleichnamigen Abschnitten des ISi-S benötigt. All diese Empfehlungen werden im (ISi-Check) zusammengefasst dargestellt, der für diese Aktivität ebenfalls herangezogen werden sollte.

Die Produktauswahl für eine Internet-Anbindung enthält, abgesehen von den fachlichen Anforderungen, kaum Aspekte, die es von der Auswahl anderer IT-Produkte unterscheidet. Daher können die bereits vorhandenen Abläufe verwendet werden, sofern diese den allgemeinen Sicherheitsanforderungen genügen.

Eine Möglichkeit besteht darin, alle benötigten Produkte von einem Anbieter als Komplettlösung zu beziehen. Ein potentieller Auftragnehmer würde in diesem Fall auch die Konfiguration und Installation vornehmen, die in den Aktivitäten 5.3.2 und 5.3.5 beschrieben werden. Dies kann für die Institution eine Arbeitserleichterung mit sich bringen. Allerdings stehen die im Vergleich zu einer internen Umsetzung meist höheren Kosten, die Abhängigkeit von einem Auftragnehmer und geringere Kontrollmöglichkeiten, insbesondere bezüglich der Sicherheit, dagegen.

Oftmals kann Standard-Software und -Hardware eingesetzt werden. Um diese auszuwählen, sollte zunächst eine Markterhebung durch einen Experten durchgeführt werden. Als Resultat liegt dann eine Liste mit Produkten vor, die die benötigten Anforderungen erfüllen. Anhand dieser können die Vor- und Nachteile der einzelnen Produkte gegeneinander abgewogen werden, um eine Produktentscheidung zu fällen. Dabei spielen nicht nur die benötigten Eigenschaften des Produkts eine Rolle, sondern darüber hinausgehend u. a. erwünschte Zusatzfunktionen, Sicherheits- und Kompatibilitätseigenschaften sowie die Konformität zu Standards. Insbesondere bei teureren Anschaffungen existieren häufig interne sowie allgemeine rechtliche Vorgaben für die Beschaffung oder Ausschreibung, die ebenfalls berücksichtigt werden müssen.

Wird keine geeignete Software gefunden, die die Anforderungen erfüllt und ist es auch nicht möglich, durch eine Anpassung in den Phasen 1 oder 2 die Anforderungen geeignet zu ändern, so muss die Software individuell erstellt werden. Dabei muss die Entscheidung getroffen werden, ob eigene Kapazitäten zur Verfügung stehen, um die Software zu erstellen, oder ob dies durch einen Auftragnehmer realisiert wird. Allerdings gelten für beide Erstellungsarten die gleichen Anforderungen, die lediglich auf unterschiedlichem Wege durchgesetzt werden können; bei der externen Erstellung kommt der Institution in erster Linie eine begleitende und kontrollierende Rolle zu.

Die neue Software sollte die im ISi-S des jeweiligen Moduls aufgeführten Grundanforderungen erfüllen. Darüber hinaus müssen auch die allgemeinen Programmierrichtlinien der Institution einge-

halten werden. Diese enthalten neben den Anforderungen an die sichere Programmierung auch formale Kriterien bezüglich der Benutzerfreundlichkeit, Interoperabilität und Dokumentation. Soll die erstellte Software an die darunterliegende Hardware angepasst werden, um die Performance zu erhöhen, so sollte die Kompabilität zu anderen Architekturen erhalten bleiben.

Bei der Erstellung neuer Software sollte, wie bei jedem Software-Projekt, die Dokumentation nicht vernachlässigt werden. Auch bei der Beschaffung sollte darauf geachtet werden, dass die zugehörigen Dokumente enthalten sind. Darüber hinaus sollten für alle relevanten Komponenten Dokumente für alle Benutzergruppen erstellt werden: für technisches und nichttechnisches Fachpersonal sowie für externe Nutzer.

5.3.2 Aktivität „Komponenten sicher konfigurieren“

Voraussetzungen:	Konzept für Konfiguration
Hilfsmittel:	Checklisten der ISi-Reihe
Ergebnisse:	Komponenten sind sicher konfiguriert

Die sichere Konfiguration der Komponenten stellt eine wichtige Voraussetzung für den sicheren Betrieb dar. Nachlässigkeiten oder Fehler können das gesamte System in einen unsicheren Zustand überführen. Daher ist es wichtig, die Konfiguration aufbauend auf den in Phase 2 erstellten Betriebs- und Sicherheitskonzepten auszuführen. Die jeweiligen Studie ISi-S enthalten umfassende Empfehlungen zur Konfiguration der Komponenten, die im Zuge der Phase 2 in die Konzepte überführt wurden.

An dieser Stelle können die im Zuge der Konzeption individualisierten Checklisten (ISi-Check) der entsprechenden Module herangezogen werden, die die Anforderungen an die Konfiguration für jede Komponente in kompakter Form enthalten. Da außer diesen Vorgaben keine spezifischen Aspekte im Vergleich zu herkömmlichen IT-Projekten zu beachten sind, wird an dieser Stelle für detailliertere Informationen auf die Standardliteratur verwiesen.

5.3.3 Aktivität „Erste Tests durchführen“

Voraussetzungen:	beschaffte und konfigurierte Komponenten
Hilfsmittel:	IT-Grundschutz-Kataloge, Maßnahmen M2.82 „Entwicklung eines Testplans für Standardsoftware“ und M2.83 „Testen von Standardsoftware“
Ergebnisse:	Testplan und Testergebnis

Nachdem die entsprechenden Komponenten beschafft und konfiguriert wurden, sollten sie gründlichen Tests unterzogen werden. Bevor die Komponenten tatsächlich eingesetzt werden, wird überprüft, ob die sie den in der Konzeption gestellten Anforderungen genügen und ob sie korrekt zusammenarbeiten.

Grundlage dieser Tests ist ein Testplan. Dieser muss vor Beginn der Tests erstellt werden. Der Testplan ist nicht nur die Basis für die in dieser Aktivität durchgeführte Überprüfung der beschafften Produkte, sondern auch für die weiteren in Aktivität 5.3.6 beschriebenen Tests.

Mit Hilfe der Tests muss sichergestellt werden, dass jedes Programm nur die erforderlichen Funktionen erfüllt und keine unerwünschten Nebenwirkungen mit sich bringt. Tests müssen unter Berücksichtigung aller Hard- und Software-Komponenten so durchgeführt werden, dass der Produktivbetrieb nicht beeinträchtigt wird. Daher sollte zum Testen eine Testumgebung genutzt werden.

Die effiziente Umsetzung des Testplans erfordert ein systematisches Vorgehen beim Testen. Ziel des vorliegenden Ablaufplans ist es nicht, das Testverfahren in seinen Details zu beschreiben. Eine ausführliche und praxisnahe Darstellung für Standard-Software ist in den IT-Grundschutz-Katalogen des BSI, insbesondere Maßnahmen M 2.82 „Entwicklung eines Testplans für Standardsoftware“ und M 2.83 „Testen von Standardsoftware“, zu finden. Im Folgenden sollen nur die wesentlichen Punkte des Verfahrens beschrieben werden.

Um ein systematisches Vorgehen bei der Testdurchführung sicherzustellen, ist als Erstes ein Testplan zu erstellen, der folgende Punkte umfassen sollte:

- Testinhalte,
- Testziele,
- Testmethoden,
- Testumgebung,
- Personal,
- Testablauf und Zeitplanung sowie
- Entscheidungskriterien.

Die Testinhalte ergeben sich aus dem Anforderungskatalog für die Hardware und Software, der in Phase 2 erstellt wurde und der auch die Grundlage für die Beschaffung bildete. Die Testfälle sind so zu konzipieren, dass sie hinsichtlich aller im Betrieb denkbaren Konstellationen eine möglichst hohe Abdeckung erreichen. Bei Tests von Software sind dabei die Eingabedaten und die, bei korrekter Ausführung zu erwartenden Ausgaben festzulegen. Die Testfälle müssen auf jeden Fall auch unzulässige Daten als Eingaben und Fehlbedienungen des Systems beinhalten, um zu überprüfen, ob das System korrekt reagiert und kein Sicherheitsrisiko auftritt. Um zu überprüfen, ob das System auch den Bedingungen des Produktivbetriebs genügen kann, sollten für die Tests realistische Daten und Datenmengen verwendet werden. Darüber hinaus sollten auch Überlasttests durchgeführt wer-

den, um die Grenzen des neuen Systems kennenzulernen. Dabei werden die Werte der geplanten Betriebsparameter solange erhöht, bis das System nicht mehr arbeitsfähig ist. Die Bedingungen, unter denen die Tests durchgeführt wurden, und die ermittelten Grenzwerte müssen dokumentiert werden.

Um den Produktionsbetrieb durch die Tests nicht zu beeinflussen, soll der Testbetrieb in einer eigenen, vom Produktivsystem vollständig abgeschotteten, Testumgebung stattfinden. Diese sollte einerseits ein möglichst vollständiges Abbild der späteren Betriebsumgebung modellieren, andererseits darf sie aber auch nicht so aufwändig sein, dass die Grenzen der Wirtschaftlichkeit überschritten werden. Eine Alternative dazu stellen Tests in der Produktivumgebung dar, die zu einem Zeitpunkt durchgeführt werden, bei dem die Umgebung nicht produktiv genutzt wird - wie beispielsweise nachts. Entsprechend muss diese Testumgebung im Testplan genau spezifiziert werden. Dabei ist anzugeben, welche Ressourcen (Betriebsmittel, IT-Infrastruktur) hierfür in welchem Umfang zur Verfügung stehen müssen. Eine solche Testumgebung ist auch für spätere Tests während des Betriebs notwendig.

Bei der Verteilung der Aufgaben ist darauf zu achten, dass die Funktionen „Testdurchführung“ und „Überprüfung der Ergebnisse“ von verschiedenen Personen nach dem sogenannten Vier-Augen-Prinzip ausgeführt werden. Unter dieser Randbedingung ist im Testplan für jeden Testinhalt festzuschreiben, wer für welche Aufgabe verantwortlich ist. Um die Tests zielgerichtet und koordiniert durchzuführen, sind die Abfolge der Testschritte sowie deren zeitlicher Rahmen möglichst genau zu spezifizieren. Der Testplan muss Kriterien festlegen, wie auftretende Fehler zu bewerten sind.

Nach der Erstellung des Testplans kann mit der Durchführung der Tests begonnen werden, die sich an den Vorgaben des Testplans orientiert. Werden bei den Tests Mängel festgestellt, so müssen diese beseitigt werden. Dazu gehören auch erneute Tests, die den Erfolg der Fehlerbeseitigung überprüfen. Wurden konzeptionelle Fehler gefunden, so müssen diese in die Dokumentation und das Konzept einfließen. Dazu ist ein Rücksprung in Phase 2 notwendig.

5.3.4 Aktivität „Sicherheits- und Betriebskonzept konkretisieren“

Voraussetzungen:	bestehendes Sicherheits- und Betriebskonzept
Hilfsmittel:	keine
Ergebnisse:	angepasstes Sicherheits- und Betriebskonzept

Nach der Beschaffung und Konfiguration der benötigten Hardware und Software sowie den Tests muss das bestehende Sicherheitskonzept konkretisiert werden. Es wird davon ausgegangen, dass in der Institution bereits ein Sicherheitskonzept existiert. Dieses wird durch Hinzufügen oder Anpassen aktualisiert. Dabei werden die neuen Sicherheitsmaßnahmen dokumentiert.

Im Gegensatz zu den Betriebskonzepten, die sich mit spezifischen Aspekten des IT-Betriebs befassen, werden im Sicherheitskonzept nur die sicherheitstechnischen Aspekte betrachtet. Dazu gehören beispielsweise Regelungen für den Umgang mit Sicherheitsvorfällen. Viele Aspekte, wie die Datensicherung, der Virenschutz oder die Notfallvorsorge spielen sowohl für den Betrieb als auch für die Sicherheit eine Rolle. Häufig muss auch das Kryptokonzept erweitert werden, in dem beispielsweise das Schlüsselmanagement geregelt wird. Bei dieser Aktivität sollten bei Bedarf auch die Betriebskonzepte, die in Phase 2 erstellt wurden, weiter konkretisiert werden.

Viele der getroffenen Regelungen sind nicht internet-spezifisch. Sie müssen allerdings die neuen Gefährdungen mit berücksichtigen, die durch die Internet-Anbindung entstehen. Darüber hinaus existieren jedoch auch internet-spezifische Konzepte, die vor der Internet-Anbindung nicht immer vorhanden oder notwendig waren. Ein Beispiel dafür ist das Konzept für das Sicherheits-Gateway. Im technischen Feinkonzept wurden die allgemeinen Regeln für das Sicherheits-Gateway erstellt. Für diese Aktivität wird auf die im ISi-S des jeweiligen Moduls getroffenen Aussagen zur sicheren Grundkonfiguration der Komponenten zurückgegriffen. Da als Ergebnis der Beschaffung nun ein konkretes Produkt feststeht, kann das Konzept weiter konkretisiert und um produktspezifische Details erweitert werden. Diese Details liegen für einige Module in den Grundvorgaben für den sicheren Betrieb (ISi-Check) bereits vor. Anderenfalls müssen sie aus den produktunabhängigen Vorgaben des ISi-S und der Checklisten für das in der Institution eingesetzte Produkt erstellt werden.

5.3.5 Aktivität „Bisherige Ergebnisse umsetzen“

Voraussetzungen:	Ergebnisse der vorangegangenen Aktivitäten
Hilfsmittel:	keine
Ergebnisse:	keine

Durch die Tests aus Aktivität 5.3.3 und die Konkretisierung des Sicherheitskonzepts in Aktivität 5.3.4 können Änderungen an dem bisher vorhandenen System notwendig werden. Diese müssen in dieser Aktivität umgesetzt werden, um das System vor den abschließenden Tests auf den geplanten Stand zu bringen. Dazu kann es notwendig sein, Hardware und Software-Komponenten neu zu installieren, anzupassen oder zu konfigurieren. Für dieses Vorgehen gelten die gleichen Vorgaben wie für die Konfiguration in Aktivität 5.3.2. Da außer diesen Vorgaben keine spezifischen Aspekte im Vergleich zu herkömmlichen IT-Projekten zu beachten sind, wird an dieser Stelle für detaillierte Informationen auf die Standardliteratur verwiesen.

Diese Aktivität umfasst nicht nur die technischen Aspekte. Dazu gehören auch Anpassungen bei der Organisation und die Umsetzung administrativer Regelungen.

5.3.6 Aktivität „Weitere Tests vor Inbetriebnahme durchführen“

Voraussetzungen:	Testplan
Hilfsmittel:	keine
Ergebnisse:	betriebsbereites System

Nach der Installation und Konfiguration der Soft- und Hardware müssen weitere Tests durchgeführt werden, bevor das System in Betrieb genommen werden kann. Im Gegensatz zu den in Aktivität 5.3.3 beschriebenen Tests, werden hier die vollständig installierten und konfigurierten Komponenten getestet, die in Betrieb genommen werden sollen. Damit soll überprüft werden, ob die Installation und Konfiguration so durchgeführt wurde, dass alle funktionalen und sicherheitskritischen Aspekte erfüllt sind. Es muss außerdem ermittelt werden, ob die in der Konzeption erstellte und getestete Konfiguration der Systeme vorliegt oder ob Abweichungen aufgetreten sind. Auch Änderungen aufgrund der vorangegangenen Tests, die in Aktivität 5.3.5 umgesetzt wurden, werden hier getestet. Diese Tests zeigen, ob das eingesetzte System die gestellten Anforderungen tatsächlich erfüllen kann. Bei diesen Tests können auch Wechselwirkungen zwischen alten und neuen Komponenten des Systems entdeckt werden, die den Produktivbetrieb beeinflussen könnten. Grundlage dieser Tests ist wiederum das Testkonzept.

Einen weiteren wichtigen Punkt stellt die Überprüfung hinsichtlich der Sicherheit der Systeme dar. Sicherheitskritische Komponenten sollen dabei überprüft werden, insbesondere deren Zusammenspiel. Beispielsweise kann auf diese Weise der Paketfilter überprüft werden. Hilfreich ist es oft, die Position eines potenziellen Angreifers einzunehmen und die Internet-Anbindung aus dessen Sichtweise zu betrachten.

Schwachstellen oder Fehler, die bei den Tests entdeckt werden, müssen beseitigt werden. Ist eine Beseitigung nicht möglich, muss eine entsprechende Maßnahme umgesetzt werden, so dass Bedrohungen nicht mehr wirksam werden können. Solche Maßnahmen müssen in das Sicherheitskonzept einfließen. Dazu muss zur Phase 2 zurückgekehrt werden.

Verlaufen die Tests erfolgreich, so liegt als Ergebnis dieser Aktivität die Freigabe der Systeme für den Produktivbetrieb vor.

5.3.7 Aktivität „Inbetriebnahme“

Voraussetzungen:	Ergebnisse der vorangegangenen Aktivitäten
Hilfsmittel:	keine
Ergebnisse:	keine

Nachdem die installierten und konfigurierten Komponenten erfolgreich getestet wurden, kann das System in den Produktivbetrieb übergehen. Wie dabei vorgegangen wird, ist vom System selbst und den Begleitumständen abhängig.

Eine Möglichkeit ist die sukzessive Einführung der Dienste nach dem sogenannten one-some-many-Prinzip. Nach der erfolgreichen Inbetriebnahme auf einem System erhält erst eine kleinere Gruppe, zum Beispiel eine Fachabteilung, die neuen Komponenten. Während dieses sogenannten Pilotbetriebs können weitere Erfahrungen mit dem System unter realen Einsatzbedingungen gewonnen werden. In dieser Phase des Projekts sollten die Systeme sehr gründlich überwacht werden, um Probleme technischer, organisatorischer oder personeller Natur zu erkennen. So kann zum Beispiel erkannt werden, wie stark die Systeme ausgelastet sind und ob die Systeme von den Benutzern angenommen werden. Mit einer solchen Überwachung ist auch eine Kontrolle des Nutzerverhaltens möglich, auch wenn dies nicht bezweckt wird. Daher müssen solche Aktionen mit dem Betriebs- bzw. Personalrat abgestimmt werden.

Die gewonnenen Erkenntnisse sollten dazu genutzt werden, die Probleme zu beseitigen. Erst danach wird das System in allen Bereichen umgesetzt. Während des Pilotbetriebs, an dem nur wenige Nutzer beteiligt sind, laufen beide Systeme parallel zueinander. Dies ist allerdings nur dann problemlos möglich, wenn ein vollkommen neuer Dienst eingeführt wird oder ein Dienst, der keinen Schreibzugriff auf gemeinsam genutzte Daten benötigt.

Alternativ können die Dienste zum gleichen Zeitpunkt eingeführt werden. Bei dieser Methode können sofort alle Mitarbeiter die neuen Dienste nutzen und es müssen nicht zwei Systeme parallel gepflegt werden. Es müssen außerdem keine Schnittstellen zwischen den Systemen entwickelt werden. Allerdings bringt diese Lösung ein höheres Einführungsrisiko mit sich, da alle Bereiche betroffen sind. Auch kann der organisatorische Aufwand höher sein.

Falls notwendig, sollten die Nutzer parallel zur Einführung der neuen Dienste geschult werden. Wird eine schrittweise Einführung gewählt, so sollten die Nutzergruppen erst zu dem Zeitpunkt geschult werden, wenn sie das System erhalten. Hier ist eine gründliche Planung erforderlich, so dass es vermieden wird, dass die Schulung zu dem neuen Dienst erst deutlich nach dessen Einführung erfolgt. Dies würde die Akzeptanz verringern und kann auch zu Sicherheitsproblemen führen, wenn der Dienst nicht in der vorgesehenen Weise genutzt wird.

5.4 Phase 4: Administration und Betrieb

Nachdem die Internet-Anbindung oder die neuen Dienste erfolgreich in Betrieb genommen worden sind, müssen der störungsarme Betrieb und die Administration sichergestellt werden. Diese Phase ist nach Abschluss der vorangegangenen Phasen permanent zu durchlaufen. Natürlich können auch Situationen entstehen, bei denen Änderungen notwendig werden, die Rücksprünge in vorangegangenen Phasen notwendig machen.

Zentrales Element dieser Phase ist die Überwachung der Betriebsparameter und das Einspielen von Updates und Patches. Werden bei der Überwachung Abweichungen vom Normalzustand erkannt, erfordert dies mehr oder weniger umfangreiche Änderungen am System. Gleiches gilt für die Reaktion auf die entsprechenden Sicherheitswarnungen. Eine solche Änderung kann auch Änderungen am Sicherheitskonzept erfordern, die einen Rücksprung zur Phase 2 notwendig machen. Vor der Umsetzung komplexer Änderungen sollten erneut Tests durchgeführt werden. Nach dem erfolgreichen Test kann die Änderung während des nächsten Wartungsfensters durchgeführt werden. Dabei sollte das sogenannte Vier-Augen-Prinzip angewendet werden. Im Anschluss muss geprüft werden, ob die Umsetzung erfolgreich war und das angestrebte Ziel erreicht wurde. Unter Umständen können sich aus der Änderung auch Anpassungen der Betriebsparameter ergeben.

Eine grafische Darstellung der einzelnen Aktivitäten dieser Phase zeigt Abbildung 5.6.

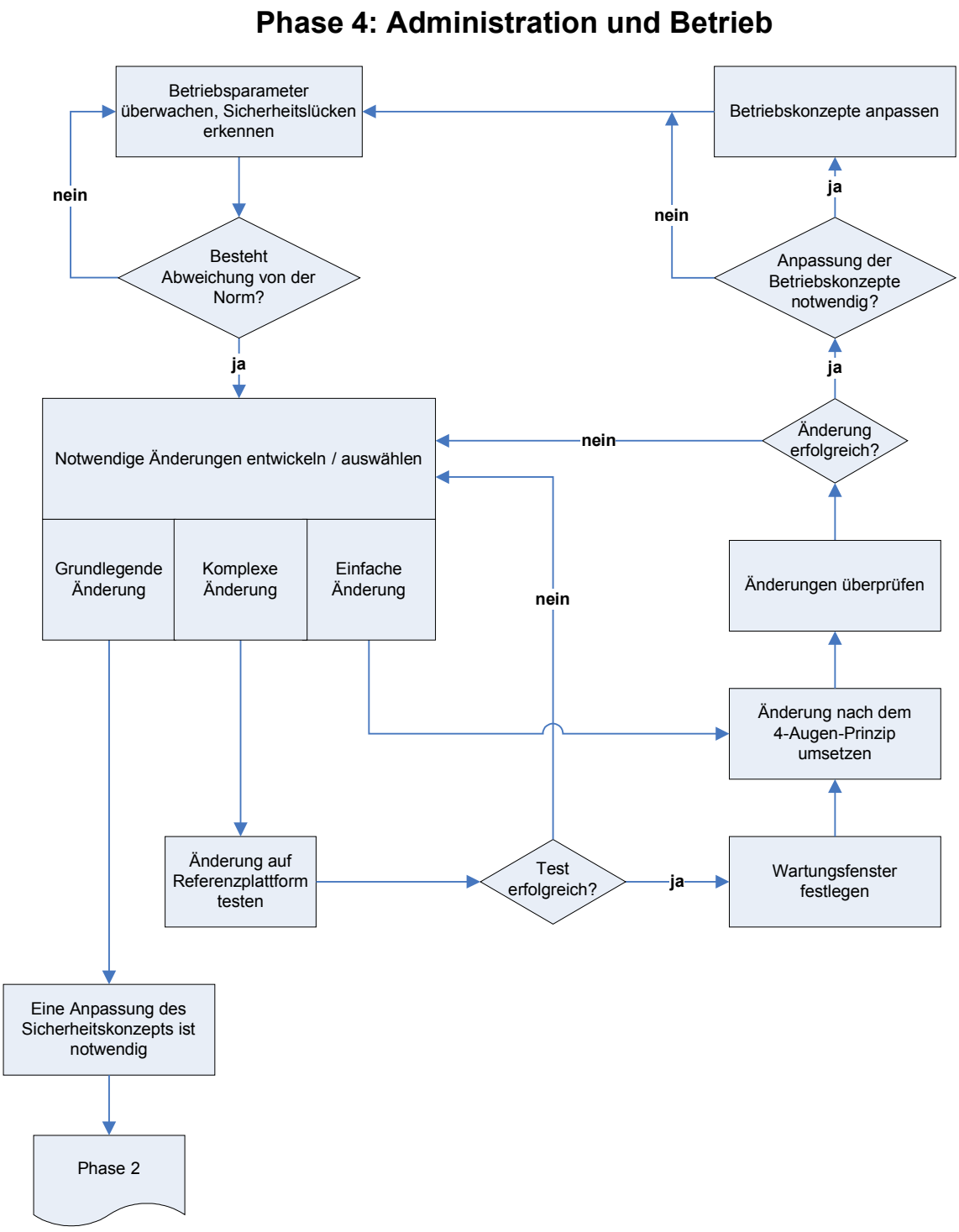

Abbildung 5.6: Aktivitäten der Phase 4: Administration und Betrieb

5.4.1 Aktivität „Betriebsparameter überwachen, Sicherheitslücken erkennen“

Nachdem das System in den Regelbetrieb übernommen wurde, beginnt die kontinuierliche Arbeit der Administratoren. Das einmal entwickelte System wird nicht auf Dauer statisch bestehen bleiben, sondern muss auf kleinere oder größere Änderungen flexibel reagieren können. Ursache solcher Änderungen können sein:

- externe Anforderungswünsche
- betriebliche Änderungen und
- sicherheitstechnische Änderungen.

Externe Anforderungen kommen häufig von den Benutzern selbst. Für diese sollte eine zentrale Anlaufstelle eingerichtet werden, bei der Anregungen, Kritik oder Probleme gesammelt werden. Durch die Zentralisierung können die notwendigen Änderungen gezielt ausgewählt und durchgeführt werden. Dazu gehören beispielsweise die Freischaltung benötigter Ports oder die Einführung neuer Server, die externe Anforderungen darstellen. Auch die Ergebnisse einer Fehlersuche können eine Änderung notwendig machen. Diese Ereignisse treten in unregelmäßigen Abständen auf.

Ein weiterer wesentlicher Punkt bei dem Betrieb ist die kontinuierliche Überwachung des Systems. Aus den in Phase 2 und 3 erstellten Betriebskonzepten gehen Parameter für den Betrieb hervor. Diese müssen jedoch um die Parameter ergänzt werden, die auf den ersten Blick rein betrieblichen Aspekten zugeordnet werden. Diese können aber als Folge auch einen beträchtlichen Einfluss auf die Sicherheit haben. Mögliche Betriebsparameter sind die Auslastung der Server, des Speichers oder der Netzverbindungen. Des Weiteren können beispielsweise die Anzahl der Benutzer oder der Durchsatz beobachtet werden.

Für jeden Betriebsparameter werden Schwellwerte definiert. Werden Abweichungen von diesen Schwellwerten erkannt, müssen Änderungen am System durchgeführt werden. Für die Festlegung der Schwellwerte kann insbesondere auf Erfahrungswerte der Administratoren zurückgegriffen werden.

Die Logdaten der Paketfilter oder des Intrusion Detection Systems können weitere Hilfsmittel zur Überwachung des Systems sein. Falls aufgrund der gewonnenen Daten eine Kontrolle des Nutzerverhaltens möglich ist, muss vorab die Zustimmung des Betriebs- oder Personalrats für die entsprechenden Maßnahme eingeholt werden.

5.4.2 Aktivität „Notwendige Änderungen entwickeln/auswählen“

Nachdem die Notwendigkeit einer Änderung erkannt wurde, muss deren Durchführung geplant werden. Dabei gibt es die Möglichkeit auf eine bereits existierende Sicherheitsmaßnahme zurückzugreifen oder eine neue zu entwickeln.

Die Änderungen werden dabei in drei Kategorien unterteilt, je nachdem welche Auswirkungen sie mit sich bringen können. Im Ablaufplan der ISi-Reihe wird zwischen einfachen, komplexen und grundlegenden Änderungen unterschieden. Die Abgrenzung zwischen diesen Kategorien ist nicht streng definiert. Im Zweifelsfall sollte eine Änderung zumindest als komplex betrachtet werden.

Generell lässt sich jedoch sagen, dass eine einfache Änderung keine Tests auf einer Referenzplattform (siehe Aktivität 5.4.3) erfordert. Bei einer solchen einfachen Änderung kann direkt mit der Aktivität 5.4.4 fortgefahren werden. Häufig wurden diese Änderungen schon öfters durchgeführt und nicht speziell neu entwickelt. Ein Beispiel für eine einfache Änderung ist das Hinzufügen eines neuen Benutzers.

Eine komplexe Änderung ist umfangreicher gegenüber einer einfachen Änderung und erfordert daher den Test auf einer Referenzplattform und die Durchführung innerhalb eines Wartungsfensters. Eine komplexe Änderung stellt beispielsweise das Einspielen von Patches oder der Hardware-Austausch eines Servers dar.

Darüber hinausgehende Änderungen werden als grundlegende Änderungen bezeichnet. Sie erfordern eine Änderung des Sicherheitskonzepts. In diesem Fall wird zur Phase 2 zurückgekehrt. Dort können beispielsweise Änderungen an der Architektur vorgenommen werden.

5.4.3 Aktivität „Änderungen auf Referenzplattform testen“

Wurde eine komplexe Änderung ausgewählt, um eine Abweichung von der Norm zu beseitigen, so muss diese Änderung zunächst getestet werden. Dabei wird überprüft, ob die Änderung den gewünschten Zweck erzielt und ob unerwünschte Nebenwirkungen auftreten. Grundlage der Tests ist das Testkonzept.

Zur Durchführung der Tests wird in den meisten Fällen eine Referenzplattform in der Testumgebung benötigt. Bereits in Aktivität 5.3.3 wurde diskutiert, in welcher Form eine solche genutzt werden kann. Dabei kann die benötigte Hardware intern oder extern bereitgestellt, Techniken zur Nachbildung der Hardware genutzt oder die Tests durch externe Dienstleister durchgeführt werden.

Je nach Art der Änderung und deren möglichen Auswirkungen können unterschiedliche Tests durchgeführt werden. In der Praxis ist es meist nicht möglich, alle Änderungen bis ins letzte Detail zu testen, bevor diese umgesetzt werden. Jedoch kann dies nicht bedeuten, dass die Tests vollkommen entfallen dürfen. Tests sind ein wichtiges Instrument zur Erhöhung der Sicherheit des IT-Systems. Die Abwägung, für welche Maßnahme welche Tests durchgeführt werden müssen, sollte anhand von Erfahrungswerten und den möglichen Auswirkungen der Maßnahmen erfolgen. Um eine konsistente Durchführung zu erreichen, sollte die Regelung hierzu dokumentiert werden.

5.4.4 Aktivität „Wartungsfenster festlegen“ und „Änderungen nach dem Vier-Augen-Prinzip umsetzen“

Nachdem die ausgewählte komplexe Änderung getestet bzw. eine einfache Änderung ausgewählt wurde, kann die Änderung umgesetzt werden. Handelte es sich um eine komplexe Änderung, so sollte diese innerhalb eines Wartungsfensters durchgeführt werden.

Ein Wartungsfenster ist ein Zeitraum, der regelmäßig oder bei Bedarf auftritt und währenddessen Änderungen am System durchgeführt werden können. Die Wartungsfenster müssen den Benutzern frühzeitig bekannt gemacht werden. Es ist ebenfalls sinnvoll, ein Wartungsfenster nicht so zu platzieren, dass es kurz vor der Abwesenheit der IT-Mitarbeiter liegt. So sollten Änderungen beispielsweise nicht freitags durchgeführt werden, wenn am Wochenende niemand anwesend ist. Gerade Wochenenden bieten sich hingegen für größere Änderungen an. In diesem Fall muss aber sichergestellt werden, dass genügend Personal vorhanden ist, falls die Änderungen nicht wie geplant durchgeführt werden können oder es bei der Durchführung der Änderungen zu Problemen kommt. Auch für den Zeitraum nach dem Wartungfenster, an dem der normale Betrieb wieder aufgenommen wird, müssen genügen IT-Mitarbeiter anwesend sein, um bei Problemen reagieren zu können. Nach einem Wartungsfenster am Wochenende sollten daher montags ein großer Teil aller IT-Mitarbeiter zur Verfügung stehen. Die Planung der Durchführung sollte nicht nur die eigentlichen Aktionen umfassen, sondern auch auf Regelungen für den Nichterfolgsfall zurückgreifen können. Von vornherein sollten dazu Zeitpunkte oder Zustände des Systems definiert werden, an denen die Aktionen rückgängig und das System in den Zustand vor dem Wartungsfenster zurückgesetzt wird. Nur so kann garantiert werden, dass am Ende des Wartungsfensters der Normalbetrieb wieder starten kann. Je nach Umfang der Änderung sollte der Plan auch Start- und Endzeiten der einzelnen Aktionen und die Verantwortlichen enthalten.

Änderungen sollten grundsätzlich nach dem Vier-Augen-Prinzip durchgeführt werden. Dies bedeutet, dass Änderungen nicht von einer Person allein durchgeführt werden dürfen, eine zweite Person muss stets mitwirken. Damit kann das Risiko des Missbrauchs oder von Fehlern verringert werden. Wenn im Einzelfall von diesem Prinzip abgewichen werden soll, muss dies unter Berücksichtigung der möglichen Auswirkungen der Aktion erfolgen.

Soll nur eine einfache Änderung durchgeführt werden, so wurde diese im Vorfeld nicht getestet. Bei der Durchführung sollte daher, wenn möglich, auch das Vier-Augen-Prinzip angewendet werden. Einfache Änderungen können in der Regel zeitnah erfolgen, eine Verschiebung in das nächste Wartungsfenster ist nicht notwendig.

Die Dokumentation der vorgenommenen Änderungen am System ist für die weitere Administration notwendig. Andere Administratoren können diese Dokumentation für ihre Arbeit nutzen, um beispielsweise Probleme leichter zu identifizieren. Auch bei der eigenen Arbeit können auf diese Weise Änderungen aus der Vergangenheit nachvollzogen werden. Zu diesem Zweck empfiehlt sich auch das Führen eines Betriebshandbuchs, in das alle Änderungen am System und die aufgetretenen Probleme und Lösungen für alle IT-Mitarbeiter leserlich und nachvollziehbar eingetragen werden. Darin kann im Bedarfsfall beispielsweise nachgeschlagen werden, ob ein Problem in der Vergangenheit bereits einmal aufgetreten ist oder welche Änderungen am System vor dem Auftreten des Problems durchgeführt wurden.

5.4.5 Aktivität „Änderungen überprüfen“

Obwohl zumindest komplexe Änderungen bereits im Vorfeld auf ihre gewünschte Wirkung und unerwünschte Nebenwirkungen getestet wurden, kann nicht garantiert werden, dass dieses Verhalten auch in der realen Umgebung eintritt. Probleme können sich beispielsweise ergeben, wenn Fehler bei der Durchführung oder Abweichungen der Referenzplattform in der Testumgebung vom Produktivsystem aufgetreten sind.

Einfache Änderungen, die nicht getestet wurden, müssen zu diesem Zeitpunkt ebenfalls überprüft werden. Auf diese Art und Weise können bei der Durchführung aufgetretene Fehler oder andere Probleme schnell erkannt und Schäden minimiert werden.

5.4.6 Aktivität „Betriebskonzepte anpassen“

Mit der Anpassung der Betriebskonzepte schließt sich der Regelkreislauf der Phase 4. Eine solche Anpassung kann bei bestimmten, meist komplexen, Änderungen notwendig werden.

Die Betriebskonzepte stellen neben den Sicherheitskonzepten wichtige Grundlagen für den Betrieb der IT-Systeme dar. Dazu gehören u. a. das Datensicherungskonzept, das Notfallvorsorgekonzept, das Virenschutzkonzept und das Firewallkonzept. Diese Konzepte wurden bereits in Phase 2 und 3 erstellt bzw. aktualisiert.

Wurde eine Änderung an einem oder mehreren IT-Systemen durchgeführt, so können dadurch auch Änderungen an den Betriebskonzepten notwendig werden. Diese sind ebenso vielfältig wie die Änderungen an dem System selbst. Wurden die Betriebskonzepte angepasst, so kann dies auch Änderungen der Betriebsparameter und den entsprechenden Schwellwerten nach sich ziehen.

Daher schließt sich an diese Aktivität wiederum Aktivität 5.4.1 an.

6 Glossar

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computer-Netze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzer-Kennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

Angriff (engl. attack)

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Anwendungsschicht (engl. application layer)

Die Anwendungsschicht ist die oberste Schicht im TCP/IP-Referenzmodell. Sie umfasst alle Protokolle, die von Anwendungsprogrammen, z. B. Browser oder E-Mail-Client, verarbeitet und für den Austausch anwendungsspezifischer Daten genutzt werden. Beispiele für Protokolle der Anwendungsschicht sind das Hypertext Transfer Protocol (HTTP) oder das Simple Mail Transfer Protocol (SMTP).

Authentisierung (engl. authentication)

Unter einer Authentisierung versteht man die Vorlage eines Nachweises eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Baustein

Der Begriff dient im IT-Grundschutz zur Strukturierung von Informationstechnik und ihrer Einsatzumgebung. Bausteine sind die Einheiten innerhalb einer Schicht (z. B. IT-Systeme, Netze). Sie beschreiben teils technische Komponenten (wie Verkabelung), teils organisatorische Verfahren (wie Notfallvorsorge-Konzept) und besondere Einsatzformen (wie häuslicher Arbeitsplatz). In jedem Baustein werden die betrachtete IT-Komponente und die Gefährdungslage beschrieben sowie organisatorische und technische Sicherheitsmaßnahmen empfohlen.

Bedrohung (engl. threat)

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen bedrohen kann, wodurch dem Besitzer der Informationen ein Schaden entsteht.

Betriebssystem (engl. operating system)

Das Betriebssystem ist ein Steuerungsprogramm, das es dem Benutzer ermöglicht, seine Dateien zu verwalten, angeschlossene Geräte (z. B. Drucker, Festplatte) zu kontrollieren oder Programme zu starten. Weit verbreitet sind z. B. Windows, Linux oder MacOS.

Bot-Netz

Ein fernsteuerbares Rechnernetz, das für Spam-Verbreitung oder DDoS-Angriffe verwendet werden kann.

Browser [engl.]

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (engl. Federal Office for Information Security)

Bundesbehörde im Geschäftsbereich des Bundesministerium des Innern.

CERT (Computer Emergency Response Team [engl.])

Anlauf- und Beratungsstelle für Computer-Notfälle, z. B. CERT-Bund.

Client [engl.]

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme eines Servers zugreift.

Datenschutz

Mit Datenschutz wird der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Datensicherung (engl. backup)

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren. Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustands von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

DDoS (Distributed Denial of Service [engl.])

Ein koordinierter DoS Angriff auf die Verfügbarkeit von IT mittels einer größeren Anzahl von angreifenden Systemen.

DMZ (Demilitarisierte Zone)

Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz. DMZ werden bei einfachen Sicherheits-Gateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheits-Gateway aus Paketfilter - Application-Level Gateway - Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

DNS (Domain Name System [engl.])

Das Domain Name System übersetzt alphanumerische Adressnamen (z. B. www.bsi.bund.de) in numerische Adressen (z. B. 194.95.177.86). Auch eine Übersetzung in die umgekehrte Richtung ist mit dem DNS möglich. Alphanumerische Namen für Rechner sind für die Benutzer einfach zu behalten und einzugeben. Da allerdings IPv4 und IPv6 Adressen in numerischer Form verlangen, ist eine Adressumsetzung durch das DNS notwendig.

DoS (Denial of Service [engl.])

Angriffe, mit dem Ziel, die Verfügbarkeit von IT zu schädigen.

FTP (File Transfer Protocol [engl.])

Das File Transfer Protocol umfasst Funktionen, mit denen man Dateien auf einfache Weise zwischen zwei Rechnern austauschen kann.

Hacking [engl.]

Hacking bezeichnet im Kontext von Informationssicherheit Angriffe, die darauf abzielen, vorhandene Sicherheitsmechanismen zu überwinden, um in ein IT-System einzudringen, seine Schwächen offen zulegen und es gegebenenfalls - bei unethischem Hacking - zu übernehmen.

HTTP (Hypertext Transfer Protocol [engl.])

Das Hypertext Transfer Protocol dient zur Übertragung von Daten - meist Webseiten - zwischen einem HTTP-Server und einem HTTP-Client, also z. B. einem Browser. Die Daten werden Über Uniform Resource Locators (URL) eindeutig bezeichnet. URLs werden meist in der Form Protokoll://Rechner/Pfad/Datei angegeben. Protokoll steht dabei für Protokolle der Anwendungsschicht, Rechner für den Namen oder die Adresse des Servers und der Pfad der Datei gibt den genauen Ort der Datei auf dem Server an. Ein Beispiel für eine URL ist http://www.bsi.bund.de/fachthem/sinet/index.htm.

HTTPS (HTTP secure [engl.])

Protokoll zur sicheren Übertragung von HTML-Seiten im Internet. SSL/TLS dient dabei zur Absicherung der Client-Server-Kommunikation.

Hypertext

Elektronisches Dokumentenformat, das Querverweise (Hyperlinks) zwischen unterschiedlichen Dokumenten vorsieht, die Standard-Darstellungsform im WWW.

IDS (Intrusion Detection System [engl.])

Ein Intrusion Detection System ist ein System zur Erkennung von Angriffen auf ein Rechnersystem oder Rechnernetz.

Informationssicherheit (engl. information security)

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist umfassender und wird daher zunehmend verwendet.

IP (Internet Protocol [engl.])

Verbindungsloses Protokoll der Internet-Schicht im TCP/IP-Referenzmodell. Ein IP-Header enthält in der Version IPv4 u. a. zwei 32-Bit-Nummern (IP-Adressen) für Ziel und Quelle der kommunizierenden Rechner.

IT-Grundschutz

IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von IT-Verbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen für IT-Systeme mit normalem Schutzbedarf umgesetzt sind. Für Systeme mit hohem oder sehr hohem Schutzbedarf sind möglicherweise darüber hinausgehende Sicherheitsmaßnahmen notwendig.

IT-Sicherheit (engl. IT Security)

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschätzt sind.

IT-Sicherheitsbeauftragter

Personen mit eigener Fachkompetenz zur IT-Sicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde, die für alle IT-Sicherheitsfragen, Mitwirkung im IT-Sicherheitsprozess und IT-Sicherheitsmanagement-Team zuständig sind, die IT-Sicherheitsleitlinie, das IT-Sicherheitskonzept

und andere Konzepte z. B. für Notfallvorsorge koordinierend erstellen und deren Umsetzung planen und überprüfen.

IT-Strukturanalyse

In einer IT-Strukturanalyse werden die erforderlichen Informationen Über den ausgewählten Informationsverbund, die IT-Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

Informationsverbund

Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei die gesamte IT einer Institution oder auch nur einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

JavaScript [engl.]

JavaScript ist eine Programmiersprache, die oft auf Webseiten eingesetzt wird. Mit ihr ist es z. B. möglich, Pop-Up-Fenster zu öffnen, Berechnungen durchzuführen oder Formulareingaben zu überprüfen. JavaScript ist Bestandteil aller neuen Browser. JavaScript zählt zu den Aktiven Inhalten.

Kommunikationstechnik

Technik zur Übermittlung von Informationen, also im Kontext E-Government insbesondere Computer-Netze wie das Internet und sonstige Datenverbindungen, aber auch Fax, Telefon, Mobiltelefon, vgl. auch IT (Informationstechnik).

NAT (Network Address Translation [engl.])

Network Address Translation (NAT) bezeichnet ein Verfahren zum automatischen und transparenten Ersetzen von Adressinformationen in Datenpaketen. NAT-Verfahren kommen meist auf Routern und Sicherheits-Gateways zum Einsatz, vor allem, um den beschränkten IPv4-Adressraum möglichst effizient zu nutzen und um lokale IP-Adressen gegenüber öffentlichen Netzen zu verbergen.

Netzplan

Ein Netzplan ist eine grafische Übersicht über die Komponenten eines Netzes und ihre Verbindungen.

Paketfilter (engl. packet filter)

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr anhand spezieller Regeln filtern. Ihre Aufgabe ist es, Datenpakete anhand der Informationen in den Header-Daten der IP- und Transportschicht (z. B. Quell- und Ziel-Adresse, -Portnummer, TCP-Flags) weiterzuleiten oder zu verwerfen. Der Inhalt des Pakets bleibt dabei unberücksichtigt.

Passwort

Geheimes Kennwort, das Daten, Rechner, Programme u. a. vor unerlaubtem Zugriff schützt.

Patch [engl.]

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Software-Fehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Phishing [engl.]

Versuch von Betrügern, IT-Anwender irrezuführen und zur Herausgabe von Authentisierungsdaten zu bewegen. Dies wird in den meisten Fällen bei Online-Banking-Verfahren eingesetzt.

Protokoll (engl. protocol)

Beschreibung (Spezifikation) des Datenformats für die Kommunikation zwischen elektronischen Geräten.

Restrisiko (engl. residual risk)

Risiko, das grundsätzlich bleibt, auch wenn Maßnahmen zum Schutz des IT-Einsatzes ergriffen worden sind.

Revision

Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-) Richtlinien. Eine Revision sollte unabhängig und neutral sein.

Risiko (engl. risk)

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Router [engl.]

Ein (IP-)Router ist ein Vermittlungsrechner, der Netze auf IP-Ebene koppelt und Wegewahlentscheidungen anhand von IP-Protokollschicht-Informationen trifft. Router trennen Netze auf der Netzzugangsschicht und begrenzen daher die Broadcast-Domäne eines Ethernets.

Schutzbedarf (engl. protection requirements)

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der IT-Sicherheits-Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch".

Schwachstelle (engl. vulnerability)

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Server [engl.]

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server.

Sicherheits-Gateway

Ein Sicherheits-Gateway (oft auch Firewall genannt) gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. Ein Sicherheits-Gateway für normalen Schutzbedarf besteht im Allgemeinen aus mehreren, in Reihe geschalteten Filterkomponenten. Dabei ist zwischen Paketfilter und Application-Level Gateway (ALG) zu unterscheiden.

Sicherheitsgrundwerte

synonym zu Grundwert(e) der IT-Sicherheit

Sicherheitskonzept (engl. security concept)

In einem Sicherheitskonzept werden die konzeptionellen Sicherheitsanforderungen systematisch festgelegt und das Vorgehen zu ihrer Umsetzung in Maßnahmen beschrieben.

Sicherheitsleitlinie (engl. security policy)

In einer Sicherheitsleitlinie werden Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

SigG (Signaturgesetz)

Gesetz über Rahmenbedingungen für elektronische Signaturen.

Spam [engl.]

Gängige Bezeichnung für unverlangt zugesandte Werbepost per E-Mail.

Spoofing [engl.]

Spoofing (von to spoof, zu deutsch: manipulieren, verschleiern oder vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

Spyware [engl.]

Software, die persönliche Daten des Benutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software oder an Dritte sendet.

Standard-Software

Unter Standard-Software wird Software (Programme, Programm-Module, Tools etc.) verstanden, die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell von einem Auftragnehmer für einen Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich außerdem dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

Switch [engl.]

Ein Switch (zu deutsch Schalter) ist eine Netzwerk-Komponente zur Verbindung mehrerer Netz-Segmente in einem lokalen Netz. Da Switches den Netzverkehr analysieren und logische Entscheidungen treffen, werden sie auch als intelligente Hubs bezeichnet.

Tag [engl.]

Als Tag wird im Rahmen einer Auszeichnungssprache eine Bereichsmarkierung bezeichnet, die Beginn und Ende eines Dokumentabschnitts kennzeichnet und diesem eine Bedeutung zuweist.

TAN (Transaktionsnummer)

Geheimzahl, die die Freigabe für einen einzelnen Vorgang erteilt. Die Geheimzahl verliert hiernach ihre Gültigkeit. Wird insbesondere beim Internet-Banking in Kombination mit einer PIN eingesetzt.

TCP (Transmission Control Protocol [engl.])

Verbindungsorientiertes Protokoll der Transportschicht im TCP/IP-Referenzmodell, welches auf IP aufsetzt.

Trojanisches Pferd (engl. trojan horse)

Programm, welches sich als nützliches Werkzeug tarnt, jedoch schädlichen Programmcode einschleust und im Verborgenen unerwünschte Aktionen ausführt.

Vertraulichkeit (engl. confidentiality)

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Vertraulichkeit ist ein Grundwert der IT-Sicherheit.

Virenschutzprogramm

Ein Virenschutzprogramm ist eine Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Virus (engl. virus)

Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich nach ihrer Ausführung selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

VLAN (Virtual Local Area Network [engl.])

Virtuelle lokale Netze (Virtual LANs, VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden.

Webserver [engl.]

Ein Webserver ist eine Software-Komponente, mit der Web-Angebote über HTTP und HTTPS bereitgestellt werden können. Er nimmt Anfragen von Clients, wie z.B. Browsern, entgegen und beantwortet diese, indem er angefragte Dokumente ausliefert. Häufig wird auch die Hardware, auf dem eine Webserver-Software installiert ist, als Webserver bezeichnet.

WLAN (Wireless Local Area Network [engl.])

Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

Wurm

Selbstständiges, sich selbst reproduzierendes Programm, das sich in einem System (vor allem in Netzen) ausbreitet.

7 Stichwort- und Abkürzungsverzeichnis