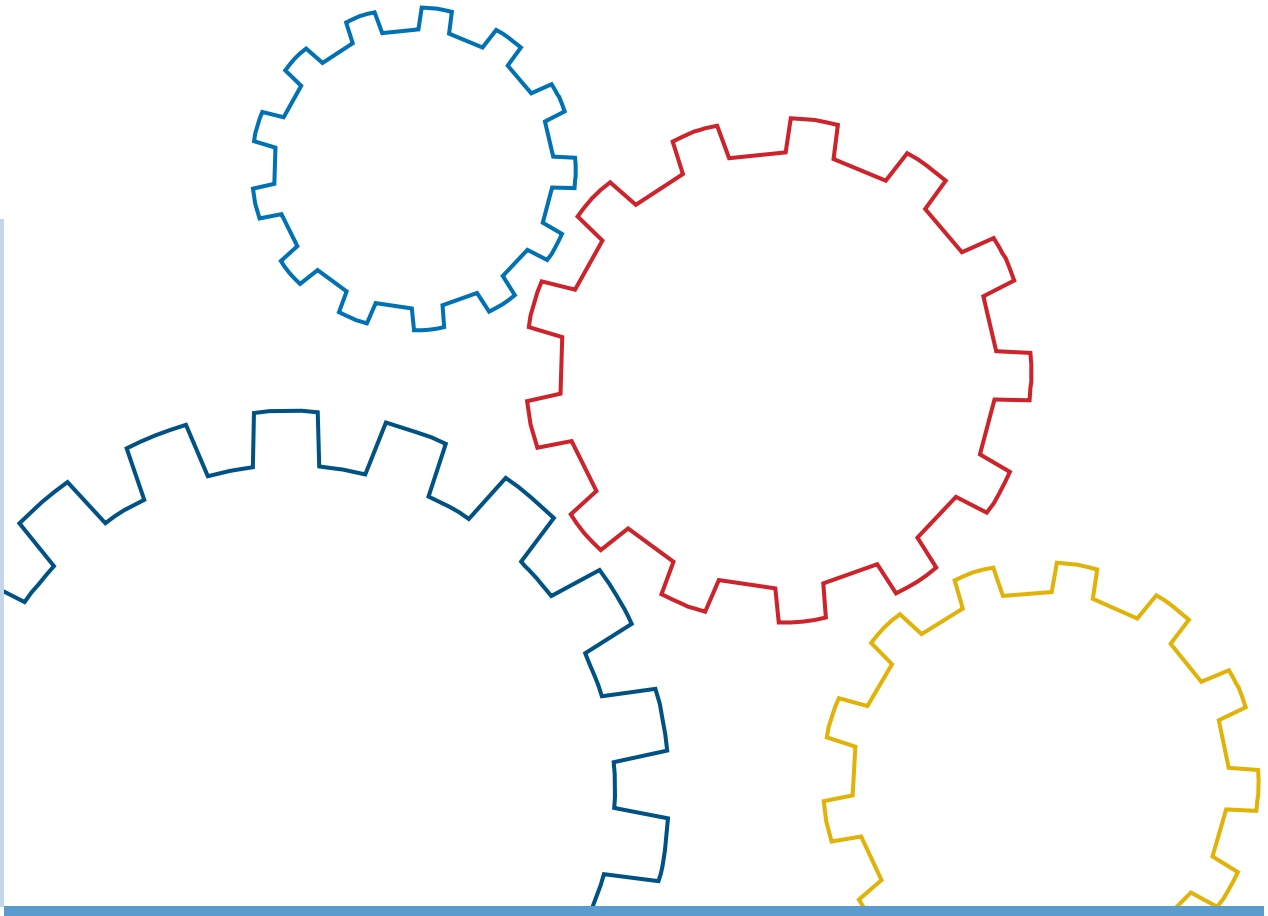
Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz-Profile

Anwendungsbeispiel für IT-Grundschutz im produzierenden Gewerbe



www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik

Referat 114 - IT-Sicherheitsmanagement und IT-Grundschutz
Postfach 20 03 63
53133 Bonn
Tel:+49 (0) 22899 9582-0
E-Mail: grundschutz@bsi.bund.de
Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

1.1 Zielsetzung des Profils

Nahezu alle Geschäftsprozesse in Unternehmen und Behörden werden heutzutage durch Informationstechnik (IT) unterstützt. Dies gilt auch für das produzierende Gewerbe und nicht nur für die dort ausgeübten administrative Tätigkeiten, wie das Rechnungswesen oder die Personalverwaltung, sondern auch für die Fertigung und die unmittelbar mit dieser verknüpften Prozesse, beispielsweise Lagerhaltung und Logistik oder Arbeitsvorbereitung und Entwicklung.

Für die Steuerung und Überwachung von Produktionsanlagen dienten anfänglich hochgradig spezialisierte, kaum standardisierte proprietäre Systeme, die untereinander nur in geringem Umfang und mit der übrigen IT im Unternehmen überhaupt nicht vernetzt waren. Dies ändert sich, wie einige aktuelle Trends belegen:

- Als Alternative und Ergänzung zu der herkömmlichen Verkabelung automatisierter Systeme per Feldbus wird zunehmend eine auf Industriebedingungen abgestimmte Variante des Ethernets eingesetzt (*Industrial Ethernet*).
- Immer häufiger wird für die Leitsysteme von Produktionsanlagen Standard-IT eingesetzt, also beispielsweise PCs mit einer Microsoft Windows- oder einer Unix/Linux-Variante als Betriebssystem und darauf zugeschnittener Software zur Anlagensteuerung und -überwachung.
- Damit einher geht ein Trend zu einer verstärkten Vernetzung der verschiedenen Leitsysteme untereinander sowie mit der übrigen Unternehmens-IT.
- Die Systeme werden zunehmend mit Optionen zur Fernwartung und -steuerung ausgestattet. Web-Schnittstellen erlauben die Anwendung dieser Funktionen auch mittels üblicher Webbrowser über das Internet.

Diese Entwicklungen ermöglichen es einerseits, die verschiedenen Teilprozesse in einem Produktionsunternehmen stärker zu integrieren und damit effizienter zu gestalten. Andererseits wird der Produktionsbereich damit aber auch zusätzlichen Gefährdungen ausgesetzt, da dieser in zunehmendem Maße mit den klassischen Sicherheitsproblemen von Computernetzen, wie Schadsoftware (Viren, Würmer, Trojanische Pferde) oder Hackerangriffen, konfrontiert wird. Dies führt auch zu der Frage, ob und inwieweit sich die gegen diese Gefährdungen entwickelten Konzepte und Schutzmechanismen auch für vernetzte Systeme im Produktionsbereich eignen.

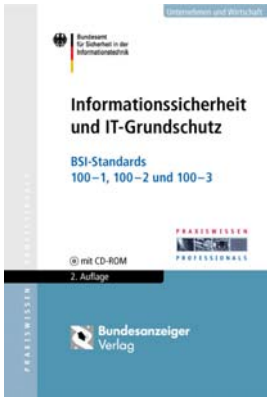
Als Verfahren zur effektiven und effizienten Absicherung informationstechnisch gestützter Geschäftsprozesse haben sich die IT-Grundschutz-Vorgehensweise und die zugehörigen Maßnahmenempfehlungen der IT-Grundschutz-Kataloge bewährt. In diesem Profil wird anhand eines einfachen Beispiels gezeigt, wie sich IT-Grundschutz auch für den Bereich der Produktion anwenden lässt, also einem

Bereich mit teilweise sehr speziellen IT-Systemen, Anwendungen und Einsatzumgebungen. Das Beispiel ist bewusst einfach gewählt, damit wichtige Aspekte in Produktionsumgebungen deutlich werden. Dazu gehören Probleme wie der lokale Schutz gegen Schadsoftware, oder Herausforderungen, die aus der langen Laufzeit von Produktionsanlagen und einer engen Bindung an die für Steuerung und Kontrolle eingesetzte Hard- und Software resultieren.

In diesem Profil wird nicht näher auf solche Informationstechnik eingegangen, die unmittelbar Bestandteil von im Produktionsbereich eingesetzten Maschinen ist, etwa speicherprogrammierbare Steuerungen (SPS). Für diese spezialisierte Hard- und Software sind gegebenenfalls gesonderte Risikoanalysen erforderlich.

Die wesentlichen Dokumente, Hilfsmittel sowie weitere Informationen zur IT-Grundschutz-Vorgehensweise und den IT-Grundschutz-Katalogen bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter www.bsi.bund.de/gshb/ an.

1.2 BSI-Standards zur Informationssicherheit



Informationssicherheit hat den Schutz von Informationen jeglicher Art und Herkunft als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert sein. Dies erfordert die Umsetzung von organisatorischen und technischen Sicherheitsmaßnahmen und einen kontinuierlichen Prozess, in dem immer wieder geprüft wird, ob diese Maßnahmen noch einen hinreichenden Schutz bieten. Die BSI-Standards zur Informationssicherheit enthalten dazu Empfehlungen für Herangehensweisen, die sich national und international bewährt haben.

Im Einzelnen behandeln die BSI-Standards die folgenden Themen:

- **BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)**

  Dieser Standard beschreibt allgemeine Anforderungen an ein ISMS. Er ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der ISO-Standards 27000 und 27002. Er bietet Lesern eine leicht verständliche und systematische Einführung und Anleitung, unabhängig davon, mit welcher Methode sie die Anforderungen umsetzen möchten.

- **BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise**

  Dieses Dokument beschreibt detailliert die IT-Grundschutz-Vorgehensweise und enthält damit eine sehr konkrete Anleitung dazu, wie ein ISMS in der Praxis aufgebaut und betrieben werden kann. Wichtige Themen sind:

  - die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Informationssicherheitsorganisation,

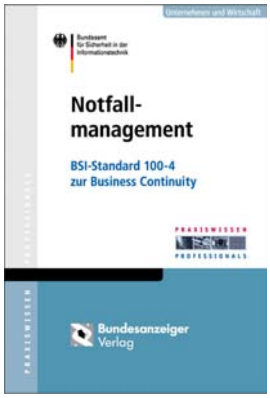
- die Anfertigung von Sicherheitskonzepten sowie die Auswahl und Umsetzung angemessener Sicherheitsmaßnahmen,
- die Aufrechterhaltung der Informationssicherheit im laufenden Betrieb und deren kontinuierliche Verbesserung.

- **BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz**

  Bei der Auswahl der geeigneten Sicherheitsmaßnahmen wird ein Anwender durch die IT-Grundschutz-Kataloge unterstützt. Diese enthalten Empfehlungen für organisatorische und technische Maßnahmen, die bei normalen Sicherheitsanforderungen und für typische IT-Umgebungen einen angemessenen und ausreichenden Schutz bieten. Der BSI-Standard 100-3 beschreibt eine Vorgehensweise, mit der unter Verwendung der IT-Grundschutz-Kataloge IT-Risiken analysiert werden können. Eine solche Analyse kommt immer dann infrage, wenn ein Objekt

  - einen höheren Schutzbedarf hat oder
  - (noch) nicht ausreichend in den IT-Grundschutz-Katalogen behandelt wird oder
  - zwar behandelt wird, aber in einem Einsatzszenario, das für den IT-Grundschutz eher untypisch ist.

- **BSI-Standard 100-4: Notfallmanagement**

  In diesem Standard wird ein systematischer Weg aufgezeigt, die Fähigkeit einer Organisation zur angemessenen Reaktion auf krisenhafte Ereignisse (Notfälle) und zur möglichst raschen Wiederaufnahme ihrer wichtigen Geschäftsprozesse zu steigern. Notfallmanagement ist besonders wichtig für die Geschäftsprozesse einer Organisation, bei denen längere Ausfallzeiten unbedingt zu vermeiden sind. In einem Fertigungsunternehmen dürften dazu alle Prozesse zählen, die für die Erzeugung der Produkte und die Abwicklung der Aufträge wesentlich sind. Der Standard beschreibt insbesondere auch, wie mit Hilfe einer so genannten Business-Impact-Analyse diese **kritischen Geschäftsprozesse** sowie die Ressourcen bestimmt werden, die von ihnen im Normalbetrieb und zur Wiederherstellung benötigt werden.

1.3 Die IT-Grundschutz-Kataloge

Während die BSI-Standards sinnvolle Vorgehensweisen und Organisationsformen beschreiben, wie Informationssicherheit und Notfallmanagement in einer Institution geschaffen und gelebt werden kann, enthalten die nach dem Baukastenprinzip gegliederten IT-Grundschutz-Kataloge konkrete Hinweise zu den Gefährdungen und erforderlichen Sicherheitsmaßnahmen. Sie sind in drei Bestandteile gegliedert:

- Die **Gefährdungs-Kataloge** enthalten Zusammenstellungen wesentlicher Gefährdungen für die Informationssicherheit und sind entlang der möglichen Ursachen „Höhere Gewalt“, „Organisatorische Mängel“, „Menschliche Fehlhandlungen“, „Technisches Versagen“ und „Vorsätzliche Handlungen“ gegliedert.
- Die **Maßnahmen-Kataloge** enthalten detaillierte Maßnahmenbeschreibungen, die in die Bereiche „Infrastruktur“, „Organisation“, „Personal“, „Hardware und Software“, „Kommunikation“ und „Notfallvorsorge“ unterschieden sind.

Die **Baustein-Kataloge** bilden die Klammer zwischen Gefährdungs- und Maßnahmenkatalogen. Ein Baustein beschreibt jeweils einen bestimmten Teilaspekt der Informationstechnik einer Organisation. Dies kann ein bestimmtes technisches System, ein zu regelnder organisatorischer Sachverhalt oder eine bestimmte Anwendung sein. Die Bausteine sind sortiert in die Schichten „Übergreifende Aspekte“ (z. B. Hard- und Softwaremanagement), „Infrastruktur“ (z. B. Verkabelung, Gebäude), „IT-System“ (z. B. Client unter Windows XP), „Netze“ (z. B. WLAN oder Remote Access) und „Anwendungen“ (z. B. Telearbeit, SAP System). Jeder Baustein enthält neben einer kurzen Darstellung seines Anwendungsgebiets Zusammenstellungen der für den beschriebenen Sachverhalt relevanten Gefährdungen und empfohlenen Schutzmaßnahmen.

Mit Hilfe der IT-Grundschutz-Kataloge kann eine Organisation auf einfache Weise ein Sicherheitskonzept erstellen, indem die jeweils erforderlichen Maßnahmen aus den anwendbaren Bausteinen ausgewählt und bei Bedarf ergänzt werden.

1.4 Gestaltungselemente in diesem Profil

In diesem Profil werden die folgenden Gestaltungselemente verwendet:

Absätze, die mit diesem Logo gekennzeichnet sind, enthalten Erläuterungen und Beispiele zu dem Musterunternehmen, das in diesem Profil zur Veranschaulichung der IT-Grundschutz-Vorgehensweise herangezogen wird („Beispiele“).

Ein Ausrufezeichen verweist auf wichtige Regeln und Handlungsanleitungen bei der Anwendung der IT-Grundschutz-Vorgehensweise („Regeln“).

Mit einer Glühbirne markierte Abschnitte enthalten Hinweise auf mögliche Arbeitserleichterungen oder einen zusätzlichen Nutzen („Tipps“).

Um die Lesbarkeit des Dokuments zu erhöhen und einen rascheren Überblick über den Inhalt eines Dokuments zu ermöglichen, werden wichtige Begriffe bei ihrer Einführung durch **Fettdruck** hervorgehoben.

Referenzen auf andere Dokumente werden mit einem Kürzel in eckigen Klammern (z. B. [GSK]) angegeben. Anhang D enthält die ausführlichen Literaturhinweise zu diesen Bezeichnungen.

Zwei Hinweise noch zu sprachlichen Konventionen:

- Die IT-Grundschutz-Vorgehensweise ist für beliebige Organisationen anwendbar, also Unternehmen, Behörden, Vereine usw. Da Gegenstand dieses Profils ein Produktionsunternehmen ist, werden in diesem Dokument bei den Erläuterungen zur IT-Grundschutz-Methodik auch dann die Begriffe „Unternehmen“, „Unternehmensleitung“ oder „Geschäftsführung“ verwendet, wenn die beschriebenen Sachverhalte auf andere Organisationsarten übertragbar sind.
- Wird im Text für die Bezeichnung von Funktionsträgern oder Rollen die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

2 Rahmenbedingungen

Informationssicherheit ist eine Managementaufgabe. Dies bedeutet, dass die für ein angemessenes Sicherheitsniveau in einer Organisation erforderlichen organisatorischen Strukturen, Abläufe und Einzelmaßnahmen systematisch geplant, eingeführt, überprüft und weiterentwickelt werden müssen. Welche Anforderungen ein solches **Informationssicherheitsmanagementsystem** (ISMS) erfüllen muss, ist in [ISO 27001] und [BSI 100-1] dargestellt. Diese Regelwerke gelten für beliebige Organisationen und zwar unabhängig von ihrer Größe, ihrer Rechtsform sowie der Art ihrer Tätigkeit. Die IT-Grundschutz-Vorgehensweise [BSI 100-2] gibt in Verbindung mit den IT-Grundschutz-Katalogen [GSK] Empfehlungen und konkrete Anleitungen dazu, wie die allgemein gehaltenen Anforderungen der ISMS-Standards in einer bestimmten Organisation umgesetzt werden können. Auch diese Empfehlungen sind organisationsunabhängig und müssen, wenn sie umgesetzt werden, auf die besonderen Bedingungen und Anforderungen der jeweiligen Institution zugeschnitten werden.

Zu den wesentlichen Aufgaben im Rahmen des Sicherheitsprozesses gehört die Entwicklung von Sicherheitskonzepten für die gesamte Organisation oder sinnvoll abgegrenzte Ausschnitte aus dieser. Der Geltungsbereich eines Sicherheitskonzepts wird in [BSI 100-2] als **Informationsverbund** bezeichnet.

In den folgenden Abschnitten werden die Rahmenbedingungen beschrieben, unter denen das in diesem Dokument dargestellte IT-Grundschutz-Profil auf einen Informationsverbund in einem Fertigungsunternehmen angewendet werden kann.

2.1 Erläuterungen zum Schutzbedarf

Die IT-Grundschutz-Vorgehensweise und die in den IT-Grundschutz-Katalogen empfohlenen Sicherheitsmaßnahmen zielen darauf ab, Geschäftsprozesse so abzusichern, dass sie möglichst störungsfrei bleiben. Eine Störung liegt immer dann vor, wenn die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen, Daten, Anwendungen und IT-Systemen verletzt werden.

Diese drei so genannten **Grundwerte der Informationssicherheit** bedeuten folgendes:

- **Vertraulichkeit** ist gewährleistet, wenn Informationen nicht unbefugt und ungewollt preisgegeben worden sind. Beispielsweise können innovative Produktionsverfahren und neuartige Produkte einem Unternehmen Wettbewerbsvorteile sichern. Sie sind deshalb, ebenso wie Informationen zu den Kunden und vorbereiteten Angeboten, ein mögliches Ziel von Wirtschaftsspionage. Maßnahmen, mit denen derartigen Angriffen gegen geheime Geschäftsinformationen begegnet werden, zielen also darauf ab, deren Vertraulichkeit zu sichern.
- Die **Verfügbarkeit** von Dienstleistungen, Funktionen eines IT-Systems, Anwendungen, Netzen oder auch von Informationen ist vorhanden, wenn

diese von den Anwendern stets wie vorgesehen genutzt werden können. Fertigungsbetriebe streben eine möglichst hohe, effiziente Ausnutzung ihrer Kapazitäten an. In der Produktion ist die Verfügbarkeit oftmals das höchste Sicherheitsziel. Ist diese nicht gewährleistet, können beispielsweise je nach Anlage sehr hohe Folgekosten für den Wiederanlauf entstehen.

- Der Grundwert **Integrität** bedeutet, dass Informationen unversehrt, also vollständig und nicht unbefugt oder unbemerkt verändert vorliegen und Systeme korrekt funktionieren. Beispielsweise müssen Fertigungsanlagen wie geplant arbeiten, damit die Produkte in der gewünschten Zeit, Quantität und Qualität hergestellt werden können. Dazu müssen die Mechanik der Anlagen in Ordnung und deren Bedienung fehlerfrei sein. Bei Maschinen, die mittels Informationstechnik gesteuert werden, hängt die Funktionssicherheit insbesondere aber auch davon ab, dass die beteiligte Software und die von ihr verwendeten Informationen unverfälscht und korrekt, also integer sind. Fehlerhafte Steuerungssoftware kann nicht nur schwerwiegende wirtschaftliche Nachteile für ein Unternehmen nach sich ziehen, je nach Art der Produktionsanlage ist sie auch ein mehr oder weniger hohes Risiko für die Unversehrtheit der Personen und der Umwelt in der Umgebung der Produktionsstätte.

Die Gewährleistung der Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität ist wichtig für die Fehlerfreiheit und Zuverlässigkeit informationstechnisch gesteuerter Anlagen in Fertigung und Logistik (**funktionale Sicherheit**). Sie ist außerdem eine Voraussetzung für die Erfüllung weiterer gegebenenfalls wichtiger Schutzziele, wie der **Authentizität**, also dem Nachweis der Echtheit einer Person oder eines bestimmten technischen Systems, oder der **Nachweisbarkeit** und **Nichtabstreitbarkeit** von Handlungen und Ereignissen.

2.2 Rechtliche und andere externe Randbedingungen

Die Notwendigkeit, für Informationssicherheit zu sorgen, ergibt sich nicht nur aus dem Eigeninteresse eines Unternehmens, dass seine Geschäftsprozesse störungsfrei und effizient funktionieren, sondern auch aufgrund rechtlicher Rahmenbedingungen, vertraglicher Verpflichtungen und sonstiger äußerer Gegebenheiten.

Was alles zu diesen Anforderungen zählt, hängt von der Rechtsform des Unternehmens, der Art seiner Geschäftsprozesse und den speziellen Beziehungen zu externen Organisationen und Gruppen beispielsweise Kunden, Lieferanten, Geschäftspartnern, Banken oder Versicherungen ab. Für das produzierende Gewerbe wichtige Gesetze, Vorschriften und Verpflichtungen sind beispielsweise:

- das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), ein im Jahr 1998 verabschiedeten Artikelgesetz, das die Leitungen von Aktiengesellschaften und anderen größeren Kapitalgesellschaften dazu verpflichtet, ein eigenes Risikomanagementsystem für ihr Unternehmen einzurichten,

- die unter dem Namen „Basel II“ bekannt gewordenen Regelungen zur Eigenkapitalhinterlegung der Kreditinstitute, die sich indirekt auch auf Unternehmen auswirken können, da Banken bei der Kreditvergabe auch darauf achten müssen, wie gut ein Unternehmen seine operativen Risiken im Griff hat,
- Vorschriften aus dem Bundesdatenschutzgesetz und anderen Rechtsnormen, die den Umgang mit personenbezogenen Informationen regeln,
- die Arbeitsstättenverordnung und zugehörige Richtlinien,
- spezielle Gesetze, die den Umgang mit gefährlichen Gütern oder Fertigungsweisen regeln, beispielsweise das Bundes-Immissionsschutzgesetz,
- das Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz), das regelt inwieweit ein Hersteller bei Produktfehlern haftbar gemacht werden kann,
- Anforderungen, von deren Erfüllung Versicherungsgesellschaften ihre Auszahlungen im Schadensfall abhängig machen,
- Anforderungen der Hersteller von Fertigungsanlagen, die eingehalten werden müssen, damit Gewährleistungsansprüche nicht verfallen,
- das Betriebsverfassungsgesetz und die dort formulierten Mitwirkungs- und Mitbestimmungsvorschriften des Betriebsrats bei allen geplanten Maßnahmen, bei denen eine Verhaltens- und Leistungskontrolle der Beschäftigten möglich ist.

Diese äußeren Rahmenbedingungen erfordern nicht nur die Einrichtung eines Informationssicherheitsmanagementsystems. Sie geben darüber hinaus auch Hinweise auf Sachverhalte, deren Regelung besonders dringlich ist, und beeinflussen die konkrete Ausgestaltung von Sicherheitsmaßnahmen. Beispielsweise schreibt das Bundesdatenschutzgesetz angemessene Maßnahmen zum Schutz personenbezogener Informationen vor. Eine in diesem Zusammenhang wichtige Maßnahme ist es, die Zugriffe auf IT-Systeme zu protokollieren, auf denen solche Informationen verarbeitet werden. Gleichzeitig setzt es aber auch Grenzen für Art-, Umfang und Umgang mit den Informationen, die bei einer aus Sicherheitsgründen eingeführten Protokollierung erfasst werden.

Eine wichtige Grundlage bei der Entwicklung von Sicherheitskonzepten ist daher eine sorgfältige Übersicht, welche Rechtsnormen und vertraglichen Regelungen zu berücksichtigen sind. Hierzu empfiehlt sich gegebenenfalls die Rücksprache mit der zuständigen Rechts- und Vertragsabteilung.

2.3 Verantwortlichkeiten und Vorgehensweise

Gemäß [BSI 100-2] gehören zum Informationssicherheitsprozess die folgenden Schritte:

- Initiierung des Prozesses:
  - Verantwortung der Leitungsebene
  - Konzeption und Planung des Prozesses
  - Erstellung der Leitlinie zur Informationssicherheit
  - Auswahl und Etablierung einer geeigneten Organisationsstruktur für das Management des Prozesses
  - Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen
- Erstellung eines Sicherheitskonzepts
- Umsetzung des Sicherheitskonzepts:
  - Realisierung der Sicherheitsmaßnahmen
  - Schulung und Sensibilisierung
- Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit im laufenden Betrieb

Verantwortung der Unternehmensleitung und Sicherheitsleitlinie

Die Geschäftsführung trägt die grundlegende Verantwortung für die Informationssicherheit eines Unternehmens. Sie wird gegebenenfalls auch haftbar gemacht, wenn aufgrund unzureichender Schutzvorkehrungen Dritte geschädigt werden. Die Delegation von Aufgaben und die Einberufung spezieller Zuständigkeiten sind wichtige Voraussetzungen dafür, Informationssicherheit als wesentliche Aufgabe in einem Unternehmen zu verankern. Dies entbindet die Geschäftsführung aber nicht von ihrer Grundverantwortung. Zusätzlich gilt: Je aktiver eine Leitung die Ziele der Informationssicherheit unterstützt, desto einfacher und nachhaltiger fällt die Etablierung der zugehörigen Prozesse im Unternehmen. Eine Möglichkeit, diese aktive Unterstützung auszudrücken, ist eine **Sicherheitsleitlinie** als Grundlagendokument zum Stellenwert der Informationssicherheit in einem Unternehmen.

Der IT-Sicherheitsbeauftragte und seine Aufgaben

Informationssicherheit verlangt angemessene organisatorische Strukturen, damit die erforderlichen Aufgaben dauerhaft wahrgenommen werden. Dazu gehört insbesondere, eine zentrale Zuständigkeit für die Informationssicherheit in Gestalt eines **IT-Sicherheitsbeauftragten** einzurichten. Zu dessen Aufgaben gehört es,

- alle für die Informationssicherheit erforderlichen Teilprozesse zu steuern und zu koordinieren,

- die Unternehmensleitung bei der Formulierung der Sicherheitsleitlinie zu unterstützen,
- Sicherheitskonzepte und zugehörige Teilkonzepte, Richtlinien und Regelungen zu verfassen beziehungsweise deren Entwicklung zu koordinieren,
- die Umsetzung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- Sicherheitsvorfälle und deren Auswirkungen zu untersuchen,
- der Unternehmensleitung sowie gegebenenfalls weiteren Gremien über den Status der Informationssicherheit zu berichten,
- Sensibilisierungs- und Schulungsmaßnahmen für Informationssicherheit zu initiieren und zu koordinieren.

Vielfalt und Komplexität der Aufgaben erfordern umfangreiche Kenntnisse sowie ein großes Verständnis für die Geschäftsprozesse des Unternehmens und deren organisatorische und technische Grundlagen. IT-Sicherheitsbeauftragte sollten daher eng mit den IT-Leitern und den Fachverantwortlichen beispielsweise der Produktionsleitung zusammenarbeiten. Eine gute Kommunikation zwischen den verantwortlichen Personen erleichtert es, die Belange der Informationssicherheit frühzeitig in die Entscheidungsprozesse zu den Geschäftsprozessen einzubinden, und fördert die Akzeptanz für als erforderlich erachtete Sicherheitsmaßnahmen.

In größeren Organisationen oder bei bestimmten Aufgaben bietet es sich gegebenenfalls an, einen größeren Personenkreis in einem **Sicherheitsmanagement-Team** an der Koordinierung der verschiedenen Arbeiten, die zur Gewährleistung der Informationssicherheit erforderlich sind, zu beteiligen.

Entscheidungen zur Informationssicherheit sollten möglichst in Übereinstimmung mit den betroffenen Fachverantwortlichen getroffen werden. Ist dies in einzelnen Fällen nicht möglich, weil die Interessen und Standpunkte zu weit auseinander klaffen, ist es Aufgabe der Geschäftsführung, zu vermitteln und eine Entscheidung herbeizuführen.

3 Definition und Abgrenzung des Informationsverbunds

Als Beispiel dient in diesem Profil das fiktive Unternehmen RECPLAST GmbH, mit dessen Hilfe auch im Webkurs IT-Grundschutz veranschaulicht wird, wie gemäß BSI-Standard 100-2 ein Informationssicherheitsmanagementsystem aufgebaut und Sicherheitskonzepte entwickelt werden können. Geschäftsgegenstand, Standorte und die grundsätzliche Struktur des Unternehmensnetzes und der eingesetzten Informations- und Kommunikationstechnik werden für das IT-Grundschutz-Profil so übernommen, wie sie im Webkurs beschrieben sind. Aufgrund des speziellen Blickwinkels wird die Informationstechnik im Fertigungsbereich sowie den vor- und nachgelagerten Prozessen in diesem Profil jedoch präzisiert.

Um die Lesbarkeit und Übersichtlichkeit zu wahren, wird die Informationstechnik in dem Beispielunternehmen gegenüber einem realen Produktionsbetrieb gleichwohl vereinfacht dargestellt. Aus denselben Gründen werden nicht alle Problembereiche berücksichtigt, die in einem realen Sicherheitskonzept behandelt werden sollten. Dies gilt etwa für die Themen Datensicherung und Archivierung.

Geschäftsgegenstand

Das Unternehmen RECPLAST stellt aus wiederverwertbaren gebrauchten Verpackungsmaterialien rund 400 unterschiedliche Kunststofferzeugnisse her, zum Beispiel Rund- und Brettprofile, Zäune, Blumenkübel oder Abfallbehälter. Der Herstellungsprozess gliedert sich in zwei Teile:

- Zunächst werden aus den vorsortierten Materialien mit Hilfe von Recyclinganlagen so genannte Regranulate gewonnen.
- Diese Regranulate dienen in den anschließenden Fertigungsprozessen als Rohstoff für die verschiedenen Kunststofferzeugnisse der Firma.

Die Produkte werden meist in hohen Stückzahlen hergestellt und über den Groß- und Einzelhandel vertrieben, aber auch kundenspezifisch angepasste Sonderfertigungen und der Direktvertrieb an Geschäftskunden gehören zum Angebot des Unternehmens. Es gibt einige wenige Stamm- und Großkunden, die mehr oder weniger regelmäßig und mit unterschiedlichen Auftragsvolumina bedient werden, und zahlreiche Einmalkunden. Der jährliche Gesamtumsatz der RECPLAST GmbH beläuft sich auf rund 50 Millionen Euro bei einem Gewinn von etwa einer Millionen Euro.

Standorte und organisatorische Gliederung

Abbildung 1 veranschaulicht die organisatorische Gliederung der RECPLAST GmbH. Eine graue Hinterlegung kennzeichnet diejenigen Bereiche, die für dieses Profil relevant sind.

Verwaltung sowie Produktion und Lager befinden sich in Bonn, allerdings an unterschiedlichen Standorten: Die Geschäftsführung hat zusammen mit den

Verwaltungsabteilungen und den Abteilungen für Einkauf sowie Marketing und Vertrieb vor kurzem ein neues Gebäude in Bad Godesberg bezogen, während Produktion, Material- und Auslieferungslager am ursprünglichen Firmensitz im Stadtteil Beuel verblieben sind. Zusätzlich hat das Unternehmen Vertriebsbüros in Berlin, Hamburg und München. Das Unternehmen beschäftigt insgesamt 180 Mitarbeiter, von denen 40 in der Verwaltung in Bad Godesberg, 134 in Produktion und Lager in Beuel und jeweils 2 Mitarbeiter in den Vertriebsbüros in Berlin, Hamburg und München tätig sind.

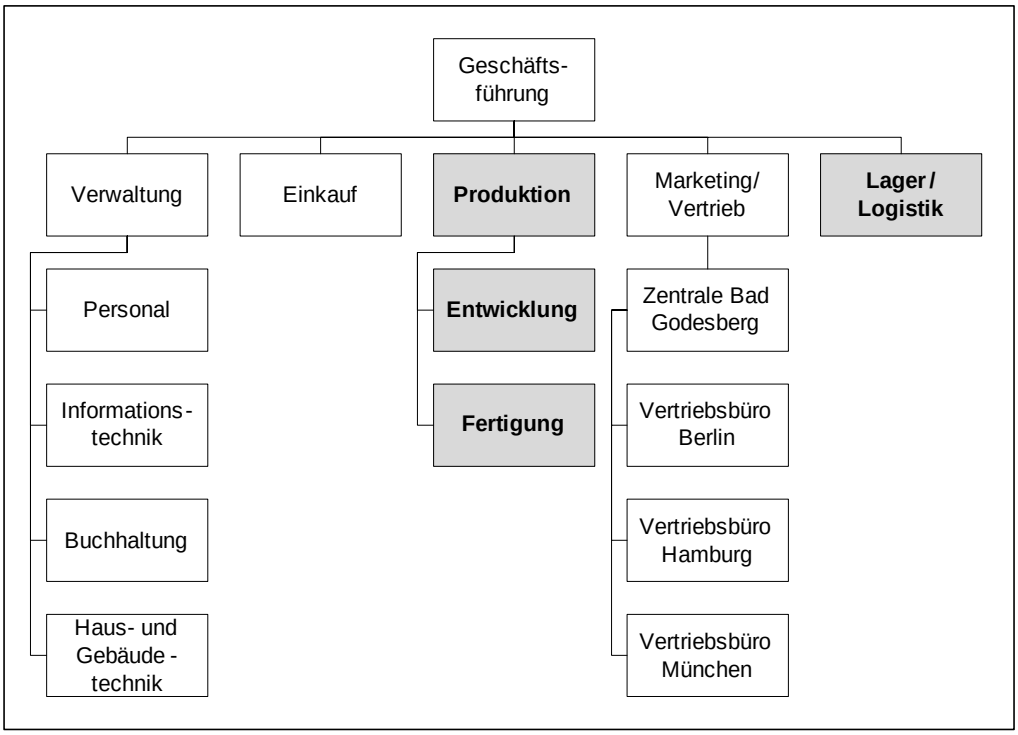


Abbildung 1: Organisatorische Gliederung der RECPLAST GmbH

Der betrachtete Informationsverbund: die Produktionsstätte in Bonn-Beuel

Alle wesentlichen Geschäftsprozesse bei der RECPLAST GmbH werden durch Informationstechnik unterstützt, auch der Produktionsbereich, der eine elementare Bedeutung für das Unternehmen hat. Aus diesem Grund wurde von der Unternehmensleitung beschlossen, den Stand der Informationssicherheit in diesem Bereich gesondert zu untersuchen. Es soll geprüft werden, ob die vorhandenen Sicherheitsvorkehrungen dem Schutzbedarf der betrachteten Geschäftsprozesse entsprechen. Für erkannte Schwachstellen sollen Maßnahmen gesucht und umgesetzt werden, die den dadurch gegebenen Gefährdungen entgegenwirken. Aufgrund der engen funktionalen Verzahnung soll die gesamte Informationstechnik in der Produktionsstätte in Bonn-Beuel in die Untersuchung einbezogen werden. Die nachfolgende Skizze stellt die Situation des Informationsverbunds zu Beginn dieses Prozesses dar.

Räumliche Gegebenheiten

Die Produktionsstätte in Bonn-Beuel besteht aus insgesamt fünf miteinander verbundenen Hallen, einer Reihe von zugeordneten Räumlichkeiten (Büroräume, Sozialräumen etc.) sowie Außenflächen mit weiteren Werkstätten, Lagerplätzen und Garagen für den unternehmenseigenen Fuhrpark (siehe Abbildung 2). Nach außen hin ist das Firmengelände durch Mauern und Zäune gesichert. Die Pforte ist ständig besetzt, die Zufahrt durch Schranken geregelt.

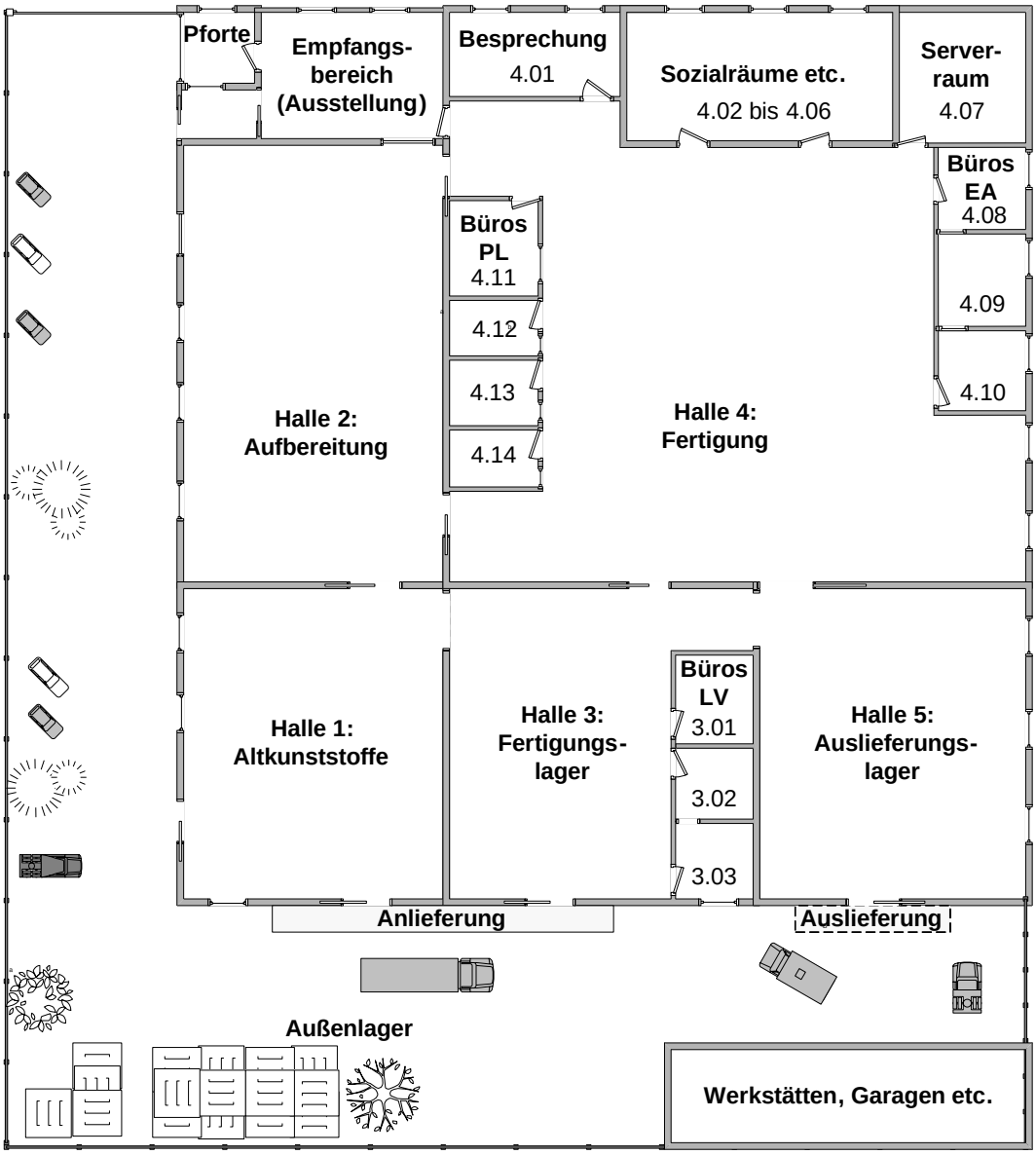


Abbildung 2: Werksgelände und räumliche Aufteilung der Betriebsstätte Bonn-Beuel (Legende; PL = Produktionsleitung; EA = Entwicklungsabteilung; LV = Lagerverwaltung)

Die Produktions- und Lagerhallen sind wie folgt organisiert:

- **Halle 1 („Altkunststoffe“)**
  Diese Halle beherbergt das Lager für die wiederverwertbaren Verpackungsmaterialien sowie Geräte für vorbereitende Aktivitäten,

beispielsweise eine Sortieranlage zur groben Sortierung der angelieferten Materialien. In dieser Halle befinden sich keine PCs.

- **Halle 2 („Aufbereitung“)**
  Hier werden die vorsortierten Altkunststoffe zu den Regranulaten verarbeitet. Kern ist eine Recyclinganlage, in der die gebrauchten Verpackungen zerkleinert, gesäubert, geschmolzen und granuliert werden. Diese Anlage wird mit Hilfe eines speziellen, vom Hersteller der Anlage gelieferten und sich ebenfalls in der Halle befindlichen Industrie-PCs gesteuert.

- **Halle 3 („Fertigungslager“)**
  In dieser Halle befindet sich ein Lager für die unterschiedlichen gewonnenen Regranulate sowie weitere Hilfsstoffe und Betriebsmittel, die zur Herstellung der Produkte erforderlich sind. Die Halle beherbergt außerdem die Büros der Lagerverwaltung. In den Büros der Lagerverwaltung befinden sich insgesamt vier PCs, ein weiterer PC steht im offenen Lagerbereich.

- **Halle 4 („Fertigung“)**
  In dieser Halle werden aus den Regranulaten und ergänzenden Materialien in verschiedenen technischen Verfahrensweisen die Fertigteile erzeugt. Sie beherbergt daher die für diesen Zweck erforderlichen Geräte und Anlagen, darunter mehrere elektronisch gesteuerte Spritzgussanlagen. Mittels handelsüblicher Web-Browser und auf die entsprechenden Maschinen abgestimmter Spezialsoftware sind die Steuerung der Maschinen sowie deren Fernwartung via Modem auch von entfernten Terminals aus möglich. Zu diesem Zweck befindet sich ein spezieller Industrie-PC in der Fertigungshalle, der sowohl eine Schnittstelle zu den Produktionsanlagen als auch zum Unternehmensnetz besitzt.
  In der Fertigungshalle ist eine Reihe von Büroräumen abgetrennt. Diese werden von der Produktionsleitung, der Netz- und Systemadministration und, in einem eigenen Trakt, der Entwicklungsabteilung genutzt. In diesen Räumlichkeiten befinden sich insgesamt zehn PCs. Alle sind als Client in das Unternehmensnetz integriert. Außerdem enthält die Halle einen abgetrennten Serverraum für zentrale IT-Systeme und die Telekommunikationsanlage.

- **Halle 5 („Auslieferungslager“)**
  Hier befindet sich das Lager für die erzeugten Fertigteile. Im Auslieferungslager befindet sich ein weiterer PC für den Zugriff auf die verwendete Lagerverwaltungssoftware.

Neben Sozialräumen, Umkleiden, Sanitäreinrichtungen etc. gibt es in der Fertigungshalle noch einen größeren Besprechungsraum. Dieser enthält Steckdosen zum Anschluss zusätzlicher IT-Systeme, beispielsweise Laptops, an das lokale Netz des Unternehmens.

Während das Firmengelände nach außen hin gut gesichert ist, gibt es innerhalb des Geländes nahezu keine weiteren Abgrenzungen. Eine Ausnahme bilden die in einem eigenen Trakt befindlichen Räumlichkeiten der Entwicklungsabteilung. Dieser Trakt kann nur mit Schlüssel betreten oder muss von innen geöffnet werden. Auch alle anderen Büroräume können abgeschlossen werden. Es gibt die

Vorschrift, dies auch zu tun, wenn sie nicht besetzt sind. Ansonsten haben alle Betriebsangehörige ungehinderten Zutritt zu allen Hallen – aber auch Betriebsfremde beispielsweise die Fahrer von anliefernden LKWs.

Software/Anwendungen

Die folgenden Anwendungen sind besonders wichtig für Fertigung und Logistik des Unternehmens:

- **Konstruktionssoftware**
  Auf vier von den sechs in der Entwicklungsabteilung angesiedelten PCs ist eine CAD/CAM-Software installiert, mit der die Konstruktion der Werkzeuge, Formteile und Produkte unterstützt wird.

- **Enterprise Resource Planning (ERP)**
  Für Produktionsplanung und -steuerung dient eine gekaufte ERP-Software mit einer integrierten Lagerverwaltungskomponente. Letztere unterstützt die innerbetrieblichen Materialflüsse sowie die Wareneingänge und den Versand an Kunden, beispielsweise durch den Druck von Lieferscheinen oder Bestellanforderungen. Das System ermöglicht es, jederzeit über Art, Umfang und Position der gelagerten Materialien und Güter informiert zu sein. Im Prinzip haben alle PC-Benutzer über eine entsprechende Clientsoftware Zugriff auf die ERP-Software, wenn auch mit bedarfsabhängig unterschiedlichen Rechten.

- **Steuerung des Materialflusses mittels RFID und WLAN**
  Für die Organisation ihrer Lagerbereiche setzt das Unternehmen Funktechnik ein. Zur Kennzeichnung der Lagerposition sind die verschiedenen Lagerorte in den drei Innenlagern und im Außenbereich mit RFID-Transpondern ausgestattet. Der Transport von und zu den Lagerorten geschieht mittels Gabelstaplern, die über angebrachte RFID-Antennen und -Lesegeräte die Informationen der Transponder auslesen können. Die insgesamt vier Gabelstapler sind zusätzlich mit Computer-Terminals ausgestattet, die über eine WLAN-Schnittstelle Zugriff auf die Lagerverwaltungssoftware und die dort abgespeicherten Lagerpositionen haben. Dies ermöglicht es, auf effiziente Weise einen Gabelstaplerfahrer darüber zu informieren, welche Lagerposition er anfahren soll, oder ihn mittels Signalen zu warnen, wenn er eine falsche Position ansteuert.

- **Anlagensteuerung und -kontrolle**
  Auf den beiden Industrie-PCs befindet sich Spezialsoftware zur Steuerung und Kontrolle der zugehörigen Anlagen. Die PCs wurden von den Anlagenherstellern geliefert, installiert und konfiguriert. Aufgrund der Gefahr, dass es zu Funktionsstörungen bei der Steuerungssoftware kommt, sowie der Gewährleistungsregelungen sind beide Geräte nicht in das Patch- und Änderungsmanagement des Unternehmens einbezogen.

Neben diesen grundlegenden produktionsbezogenen und logistischen Anwendungen ist auf den PCs in den Büroräumen Standardsoftware im Einsatz, sprich die üblichen Büroanwendungen, E-Mail-Clients und Webbrowser.

Netze und IT-Systeme

Die Firma RECPLAST betreibt ein internes Netz auf der Basis von Ethernet, TCP/IP und Microsoft Windows-Betriebssystemen, das zentral von der im Verwaltungsbereich in Bad Godesberg angesiedelten IT-Abteilung administriert wird. Die beiden Server – der Datei- und Druckserver sowie der Server für die ERP-Anwendung – werden mit Microsoft Windows Server 2003 betrieben, die Clients sind mit Ausnahme der beiden Leitrechner für die Recycling- und die Spritzgussanlage sowie die mobilen Computer auf den Gabelstaplern einheitlich mit Windows XP ausgestattet.

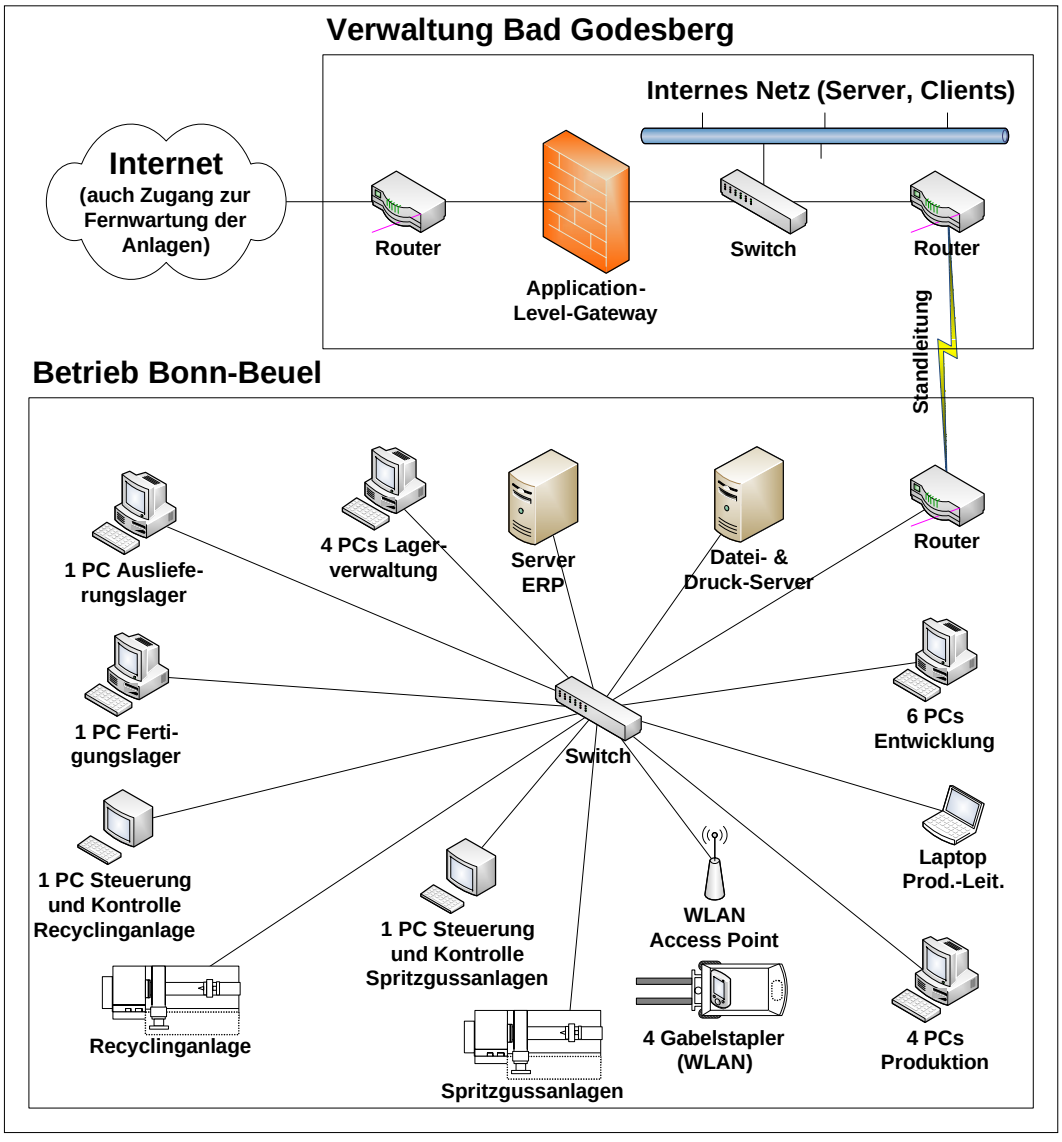


Abbildung 3: Netzplan der RECPLAST GmbH.
Peripherie- (z. B. Drucker und Scanner) und Telekommunikationsgeräte (z. B. TK-Anlage und Faxgeräte) sind nicht im Netzplan aufgeführt, um die Darstellung übersichtlich zu halten.

Ein Mitarbeiter und eine Mitarbeiterin der Entwicklungsabteilung sind ergänzend zu ihren eigentlichen Aufgaben mit der Aufgabe betraut, die zentrale IT-Administration bei den lokal anfallenden Aufgaben zu unterstützen, beispielsweise bei der

Anwenderbetreuung oder Wartungsarbeiten an Servern und den Clients. Sie haben daher Administratorrechte auf allen IT-Systemen am Standort.

In dieses Firmennetz ist der Standort Bonn-Beuel mit zwei eigenen Servern und achtzehn angeschlossenen PCs über eine angemietete Standleitung eingebunden. Der Netzplan in Abbildung 3 veranschaulicht die Struktur des Netzes.

Die achtzehn Clients am Standort Bonn-Beuel verteilen sich wie folgt auf die ansässigen Organisationseinheiten:

- **Lager/Logistik**
  Vier PCs befinden sich in den abschließbaren Büroräumen der Lagerverwaltung im Fertigungslager in Halle 3. Zusätzlich steht jeweils ein PC mit angeschlossenem Drucker in den offenen Hallenbereichen des Fertigungs- sowie des Auslieferungslagers (Halle 5). Diese beiden IT-Systeme bieten den Beschäftigten des jeweiligen Lagers die Möglichkeit, schnell auf die Lagerverwaltungssoftware zugreifen zu können, zum Beispiel um Bestände abzufragen oder Belege zu drucken.

- **Produktion**

  - **Fertigung**
    Fünf PCs befinden sich in Halle 4, davon vier in den Büroräumen der Produktionsleitung und einer, der Industrie-PC zur Steuerung und Kontrolle der Produktionsanlagen im offenen Hallenbereich. Ein weiterer Industrie-PC befindet sich in der Recyclinghalle (Halle 2). Beide Industrie-PCs wurden von den Herstellern der jeweiligen Anlage bereitgestellt und mit älteren Betriebssystemen ausgestattet, der Leitrechner für die Spritzgussanlagen mit Windows NT und der Leitrechner für die Recyclinganlage sogar nur mit Windows 98. Für die Kommunikation zwischen den Leitrechnern und den Produktionsanlagen dienen spezielle industrielle Bussysteme, so genannte Feldbusse, die Integration ins Firmen-LAN erfolgt mittels Ethernet. Die Leitrechner erlauben den Zugriff auf Informationstechnik, die unmittelbarer Bestandteil der Produktionsanlagen ist, beispielsweise deren speicherprogrammierbare Steuerungen (SPS).

  - **Entwicklung**
    In den Räumlichkeiten der Entwicklungsabteilung in Halle 4 befinden sich insgesamt sechs PCs samt angeschlossener Peripherie (Drucker, Scanner etc.).

Im Serverraum in Halle 4 befinden sich ein Switch, ein Router, ein WLAN-Access-Point und zwei Server. Ein Server dient als zusätzlicher Domänen-Controller sowie als örtlicher Datei- und Druckserver, der zweite beherbergt die ERP-Anwendung und deren Datenbank.

Das WLAN dient der Kommunikation zwischen der Lagerverwaltungssoftware und den Computer-Terminals auf den Gabelstaplern und ist daher auf eine entsprechend große Reichweite hin ausgelegt. Dabei wurde in Kauf genommen, dass die Funksignale über das Firmengelände hinaus empfangen werden können.

An zusätzlicher Informationstechnik sind die Telekommunikationsanlage, ein Faxgerät sowie ein dem Produktionsleiter zugeteilter Laptop, der zeitweilig auch in das lokale Netz eingebunden ist, vorhanden. Außerdem werden verschiedene Arten mobiler Datenträger (CDs, DVDs, USB-Sticks) verwendet, zum Beispiel um Daten lokal zu sichern oder Softwareupdates einzuspielen.

4 Leitlinie zur Informationssicherheit und Sicherheitskonzept

In diesem Kapitel werden mit den Themen „Formulierung einer Leitlinie zur Informationssicherheit“ und „Entwicklung eines Sicherheitskonzepts“ zwei wesentliche Schritte beim Aufbau eines Informationssicherheits-managementsystems für ein Unternehmen dargestellt.

Zwar unterscheiden sich Sicherheitsleitlinien und Sicherheitskonzepte eines produzierenden Unternehmens inhaltlich von denen einer administrativ tätigen Einrichtung, nicht aber in den Verfahren, mit denen man zu dem jeweiligen Ergebnis gelangt. Die in [BSI 100-2] dargestellten Vorgehensmodelle zur Entwicklung beider Dokumente können daher unabhängig von der Art einer Organisation und ihrer Geschäftsprozesse angewendet werden.

4.1 Leitlinie zur Informationssicherheit

Eine Leitlinie zur Informationssicherheit ist ein von der Unternehmensleitung in Kraft gesetztes und allen betroffenen Mitarbeitern bekannt gemachtes Grundlagendokument mit prinzipiellen Aussagen zum Stellenwert der Informationssicherheit für das Unternehmen sowie Regelungen zur Organisation und den Verantwortlichkeiten im Sicherheitsprozess.

Inhalt

Gemäß [BSI 100-2] sollten in einer Sicherheitsleitlinie die folgenden Sachverhalte dargestellt werden:

- der Stellenwert der Informationssicherheit für das Unternehmen und die Bedeutung der Informationen und Informationstechnik für die Aufgabenerfüllung,
- der Bezug der Sicherheitsziele zu den Geschäftszielen oder Aufgaben des Unternehmens,
- die Sicherheitsziele und die Kernelemente der Sicherheitsstrategie für die eingesetzte Informationstechnik,
- die Zusicherung, dass die Sicherheitsleitlinie von der Unternehmensleitung durchgesetzt wird, und Leitaussagen zur Erfolgskontrolle sowie
- die Organisationsstruktur, die für die Umsetzung des Sicherheitsprozesses etabliert wird.

Zusätzlich können beispielsweise

- zur Motivation realistische Gefährdungen für die Geschäftsprozesse angerissen und wichtige gesetzlichen Regelungen und Rahmenbedingungen (etwa vertragliche Verpflichtungen) genannt werden,

- die wesentlichen Aufgaben und Zuständigkeiten im Sicherheitsprozess aufgezeigt und Ansprechpartner für Sicherheitsfragen benannt werden,
- Programme zur Förderung der Informationssicherheit durch Schulungs- und Sensibilisierungsmaßnahmen angekündigt werden.

Um die Bedeutung der Informationssicherheit für ein Unternehmen als Ganzes oder einzelne seiner Geschäftsprozesse einschätzen zu können, ist es hilfreich, sich zu überlegen, welche Folgen Ausfälle oder Beschädigungen der Informationstechnik nach sich ziehen könnten: Werden gesetzliche Bestimmungen verletzt? Oder vertragliche Verpflichtungen? Wie viel Aufwand erfordern Ersatzprozesse, falls technische Systeme versagen und die Geschäftsprozesse nicht mehr in der vorgesehenen Weise durchgeführt werden können? Drohen wirtschaftliche Verluste? Welche Störungen sind tragbar, welche nicht?

Die in einer Leitlinie zur Informationssicherheit formulierten Absichtserklärungen der Unternehmensleitung können als Begründung bei der Anforderung weiterer Budgetmittel, der Planung konkreter Sicherheitsmaßnahmen oder auch dem Wunsch nach zusätzlichen Schulungen verwendet werden. Sie können ebenfalls dazu beitragen, das Sicherheitsbewusstsein der Beschäftigten zu erhöhen – dies umso mehr, je zielgruppengerechter die Sicherheitsleitlinie formuliert ist und je besser für ihre Bekanntmachung gesorgt wird.

Erarbeitung

Wenngleich die Sicherheitsleitlinie ein Positionspapier der Unternehmensleitung ist, so wird dieses Dokument in der Regel nicht von der Geschäftsführung selber entwickelt, sondern von dem IT-Sicherheitsbeauftragten gemeinsam mit anderen Personen aus verschiedenen Unternehmensbereichen vorbereitet. Es empfiehlt sich, dazu eine feste Arbeitsgruppe einzurichten. Dieses Team sollte so zusammengesetzt sein, dass möglichst vielfältige Kenntnisse und Erfahrungen zur Informationstechnik und -sicherheit sowie den Erfordernissen der Geschäftsprozesse eingebracht werden können. Als Mitglieder bieten sich daher verantwortliche oder kompetente Mitarbeiter an, die in einem der wesentlichen Geschäftsprozesse, der Informationstechnik oder im Leitungsbereich des Unternehmens tätig sind. In Betrieben mit Produktion ist vor allem auf eine intensive Beteiligung von für die Produktion verantwortlichen Mitarbeitern zu achten.

Diese feste Arbeitsgruppe sollte nicht zu groß sein und bei Bedarf weitere Mitarbeiter aus anderen Unternehmensbereichen hinzuziehen.

Wichtig ist es auch, die Unternehmensleitung regelmäßig über den Fortgang der Arbeiten zu unterrichten – schließlich muss diese sich die Ergebnisse der Arbeitsgruppe zu eigen machen und verantworten. Ebenso sollten die Unterrichtungs-, Beratungs- und Mitbestimmungsrechte des Betriebsrats beachtet werden. So sind gemäß des deutschen Betriebsverfassungsgesetzes Maßnahmen und technische Verfahren mitbestimmungspflichtig, wenn sie es prinzipiell ermöglichen, das Verhalten oder die Leistungen der Mitarbeiter zu überwachen. Eine rechtzeitige, umfassende Beteiligung und Information des Betriebsrats empfiehlt sich aber

auch grundsätzlich, da dies möglichen Zeitverzögerungen vorbeugen kann, wenn aus der Sicherheitsleitlinie abgeleitete Maßnahmen eingeführt werden sollen.

Eine möglichst breite Beteiligung an der Erarbeitung der Sicherheitsleitlinie trägt zur Akzeptanz der in ihr formulierten und aus ihr abgeleiteten Regeln bei. Daher sollten möglichst alle maßgeblichen Geschäftsbereiche in die Entwicklung des Dokuments einbezogen werden.

Das Beispielunternehmen

Das Beispielunternehmen, die RECPLAST GmbH, ist bestrebt, ein Managementsystem für Informationssicherheit einzurichten. Es hat dazu bereits einige wesentliche Arbeiten geleistet. So wurde ein Mitarbeiter der Abteilung „Informationstechnik“ als IT-Sicherheitsbeauftragter ernannt, eine erste Leitlinie zur Informationssicherheit entworfen, außerdem ein Sicherheitskonzept angefertigt. Dieses Konzept bezieht sich aber im Wesentlichen auf den Verwaltungsbereich des Unternehmens und die dort genutzten Anwendungen und IT-Komponenten. Die Besonderheiten der Informationstechnik in der Produktionsstätte in Bonn-Beuel sind kein Gegenstand dieses Planungsdokuments.

Daher wird entschieden, für den Informationsverbund „Produktionsstätte Bonn-Beuel“ ein Sicherheitskonzept mit Hilfe der IT-Grundschutz-Vorgehensweise zu entwickeln – dies insbesondere auch, weil die dort angesiedelten Geschäftsprozesse mehr und mehr durch Informationstechnik unterstützt werden. Es wird außerdem entschieden, zu prüfen, ob der Produktionsbereich hinreichend in der vorhandenen Sicherheitsleitlinie berücksichtigt ist, und diese gegebenenfalls zu erweitern oder abzuändern.

Die Geschäftsführung beschließt, zur Durchführung dieser Arbeiten eine Arbeitsgruppe mit den folgenden vier festen Mitgliedern einzurichten:

- dem IT-Sicherheitsbeauftragten, der als Mitarbeiter der IT-Abteilung auch das erforderliche informationstechnische Know-how einbringt,
- dem Produktionsleiter als Verantwortlichem für die Abteilungen Fertigung und Entwicklung,
- dem Leiter der ebenfalls in Bonn-Beuel angesiedelten Abteilung „Lager/Logistik“,
- dem Assistenten der kaufmännischen Geschäftsführung, um einen engen Kontakt zur Unternehmensleitung zu sichern.

Zwischenergebnisse sollen auf gemeinsamen Sitzungen mit den Geschäftsprozessverantwortlichen und der Unternehmensleitung beraten werden.

In einem ersten Schritt untersucht die Arbeitsgruppe die vorhandene Leitlinie zur Informationssicherheit des Unternehmens und prüft, ob für die Produktionsstätte in Bonn-Beuel eine eigene Leitlinie erforderlich ist. Dies wird verneint, da für die beiden Standorte grundsätzlich übereinstimmende Ziele und Regelungen zur Informationssicherheit gelten sollten. Dies würde durch eine generelle Leitlinie

für das gesamte Unternehmen besser ausgedrückt als durch getrennte Grundsatzdokumente.

Die vorhandene Sicherheitsleitlinie soll gleichwohl dahingehend überarbeitet werden, dass die besondere Bedeutung des Produktionsbereichs für die RECPLAST GmbH hervorgehoben wird und die für diesen Bereich spezifischen Gesichtspunkte dargestellt werden. In den Diskussionen dazu, welche Besonderheiten in der Sicherheitsleitlinie des Unternehmens berücksichtigt werden sollen, kristallisieren sich die folgenden Aspekte heraus:

- **Notfall-Management für den Produktionsbereich planen**
  Im Produktionsbereich sind mit der Fertigung und der Entwicklung die wesentlichen wertschöpfenden Prozesse des Unternehmens angesiedelt. Dies bedeutet auch, dass hier in besonderer Weise auf Notfallvorsorge zu achten ist und darauf, dass im Falle von Störungen diese Geschäftsprozesse möglichst schnell wieder funktionsfähig sind. Es sind Konzepte zu entwickeln, um diesen Anforderungen gerecht zu werden.

- **Moderne Fertigungstechnik fördern**
  Um seine Wettbewerbsposition zu halten, ist das Unternehmen bestrebt, seine Produktion mit neuesten technischen Verfahren und Geräten zu unterstützen. Dies schließt ein, dass es Informationstechnik einsetzt, mit der sich die Leistungsfähigkeit des Unternehmens, die Effizienz seiner Prozesse und die Qualität der dabei entstehenden Erzeugnisse erhöhen lassen. In diesem Kontext wird auch die grundsätzliche Vernetzung der verschiedenen Geschäftsprozesse positiv gesehen. Informationssicherheit soll daher nicht bedeuten, Möglichkeiten zur Optimierung der Produktionsprozesse ungenutzt zu lassen, sondern dafür sorgen, dass diese sicher gestaltet werden.

- **Informationssicherheit bei Investitionsplanung berücksichtigen**
  Die Produktionsanlagen und sonstigen technischen Systeme des Unternehmens müssen eine hohe funktionale Zuverlässigkeit aufweisen, also ausfallsicher und präzise arbeiten. Dies stellt nicht nur Anforderungen an die Robustheit der Maschinen, sondern auch an die Zuverlässigkeit der Steuerungs- und Kontrollsoftware. Letztere hängt wiederum auch davon ab, wie gut sie gegen mögliche Gefährdungen geschützt ist. Bei der Planung und Beschaffung von Produktionsanlagen und anderen technischen Systemen für die Produktion sind daher die Anforderungen der Informationssicherheit frühzeitig zu berücksichtigen. Organisatorisch bedeutet dies, dass der IT-Sicherheitsbeauftragte von Beginn an in Investitionsplanungen und -entscheidungen einbezogen wird, wenn diese die Informationssicherheit betreffen.

- **Sicherheitsanforderungen an Hersteller von Produktionsanlagen stellen**
  Moderne Produktionsanlagen kommen ohne Informationstechnik nicht aus. Damit wird die Sicherheit dieser Technik zu einer wichtigen Anforderung bei der Beschaffung solcher technischer Systeme. Dies muss sich in den Verhandlungen mit den Herstellern und den Auswahlkriterien beim Kauf von Anlagen wiederfinden. Zwei Beispiele:

  - **Fernwartung von Anlagen und Steuerungssoftware regeln**
    Aus Gewährleistungsgründen und wegen des dort vorhandenen Know-hows verbleibt die Aufgabe, eine Anlage und deren Steuerungssoftware zu warten, oftmals beim Hersteller. Dies geschieht häufig per Fernwartung über eine dazu an der Anlage vorgesehene Schnittstelle (Netzanschluss, Modem). Die genauen Einzelheiten sind in zwischen Hersteller und Kunde bei dem Kauf einer Anlage auszuhandelnden Wartungsverträgen geregelt. Hier ist etwa danach zu fragen, welche Sicherheiten ein Hersteller bietet, dass Fernwartungszugänge nicht missbraucht werden.

  - **Auf Aktualität und Sicherheit der Steuerungssoftware achten**
    Produktionsanlagen sind üblicherweise über einen vergleichsweise langen Zeitraum von mindestens zehn bis fünfzehn Jahren im Einsatz – also deutlich länger als normale Computer-Systeme. Dies kann bei Anlagen, die mittlerweile häufig mit Standard-IT-Komponenten betrieben werden, zu sicherheitsrelevanten Wartungsproblemen führen. Steuerungssoftware ist häufig an eine bestimmte Betriebssystemversion gebunden. Für ältere Betriebssysteme sehen sich deren Hersteller aber nicht mehr unbedingt verpflichtet, Sicherheitspatches herauszugeben. Und selbst wenn, so garantiert dies nicht, dass damit die Steuerungssoftware noch funktioniert. Bei der Auswahl dieser Software sind derartige Abhängigkeiten und die daraus resultierenden Gefährdungen daher zu berücksichtigen.

- **Zusammenarbeit zwischen IT-Administration und Produktion regeln**
  Nicht nur die Fernwartung, sondern auch die innerbetriebliche IT-Administration der Produktionsanlagen ist zu regeln. Dabei ist zu beachten, dass sich die Vorgehensweisen in Büro- und Produktionsnetzen deutlich unterscheiden – so können beispielsweise Zugriffe im laufenden Betrieb zur Wartung einer Anlage oder die Durchführung von Penetrationstests im Produktionsnetz die Produktionsanlagen empfindlich stören. Es muss in der Sicherheitsleitlinie deutlich werden, dass eine enge Abstimmung zwischen der IT-Administration und den Verantwortlichen für den Produktionsbereich wichtig ist. Es gibt einige Begriffe, die in Produktion und IT-Administration unterschiedlich gebraucht werden (z. B. „Programmierung“). Es wird daher entschieden, ein Glossar zu erstellen, in dem die Bedeutung wichtiger Begriffe, die in IT-Administration und Produktion gebräuchlich sind, festgelegt wird. Dieses Glossar soll bei Bedarf den Arbeitsanweisungen für die Mitarbeiter beider Bereiche beigefügt werden, um die wechselseitige Kommunikation zu erleichtern und Missverständnissen vorzubeugen.

- **Entwicklungsergebnisse vor Wirtschaftsspionage schützen**
  Die Kalkulation und weitere Einzelheiten zu Angeboten, Kundenkarteien, Prototypen neuartiger Produkte, geplante Innovationen in der Fertigungstechnik – diese und weitere Informationen sollte man vor der Kenntnisnahme durch Konkurrenten schützen. Nahezu jedes Unternehmen kann von Wirtschaftsspionage betroffen sein. Im Bereich der Betriebsstätte in Bonn-Beuel haben diesbezüglich die Dateien und Unterlagen der Entwicklungs-

abteilung einen besonders hohen Schutzbedarf und erfordert ein entsprechendes Augenmerk bei der Entwicklung von Sicherheitskonzepten.

Beispieldokument

Anhang A enthält als Muster für ein solches Grundsatzdokument zur Informationssicherheit die Sicherheitsleitlinie der RECPLAST GmbH. Die vorstehend genannten Aspekte sind in dieses Dokument eingearbeitet.

4.2 Sicherheitskonzept

Während eine Sicherheitsleitlinie die grundsätzlichen Ziele, organisatorischen Strukturen und Verantwortlichkeiten zur Gewährleistung der Informationssicherheit in einer Organisation enthält, wird in einem Sicherheitskonzept festgelegt, wie diese Rahmenvorgaben umgesetzt werden. Weil sich jede konkrete Sicherheitsmaßnahme letztlich auf diese Planungen zurückführen lassen beziehungsweise mit diesen vereinbar sein muss, wird das Sicherheitskonzept damit zum zentralen Bezugspunkt zur Informationssicherheit in einem Unternehmen.

Geltungsbereich eines Sicherheitskonzepts

Eine wichtige Festlegung bei der Entwicklung eines Sicherheitskonzepts gemäß IT-Grundschutz ist die Entscheidung, welcher **Informationsverbund** betrachtet werden soll, also der Geltungsbereich des Konzepts. Zwar ist es grundsätzlich wünschenswert, wenn dieser das gesamte Unternehmen umfasst, aber insbesondere bei größeren Institutionen und wenn Sicherheitsmaßnahmen bislang eher punktuell und ohne ein zugrunde liegendes systematisches Konzept vorgenommen wurden, ist es oft praktikabler sich zunächst auf Teilbereiche zu konzentrieren. Dies verhindert nicht nur ein Verzetteln angesichts zu großer Aufgabenstellungen. Die Einführung von Strukturen, Maßnahmen und Regelungen für Informationssicherheit im gesamten Unternehmen fällt auch leichter, wenn ein systematisches Vorgehen dazu bereits in einem wichtigen Teilbereich erfolgreich eingeübt wurde.

Ein Informationsverbund sollte allerdings sinnvoll gewählt werden, also

- eine gewisse Mindestgröße haben,
- aufgrund seiner organisatorischen Strukturen oder Anwendungen gut abgrenzbar sein sowie
- wesentliche Aufgaben einer Organisation unterstützen.

Ungeeignet als Informationsverbund sind damit beispielsweise einzelne Clients, Server oder Netzverbindungen.

Alle drei Kriterien für einen sinnvollen Informationsverbund werden von der in diesem Profil betrachteten Produktionsstätte in Bonn-Beuel mit den

Geschäftsbereichen „Fertigung“, „Entwicklung“ und „Lager/Logistik“ erfüllt.

Verfahrensschritte

Die IT-Grundschutz-Vorgehensweise ist ein strukturiertes Verfahren zur Entwicklung von Sicherheitskonzepten. Sie stützt sich auf die IT-Grundschutz-Kataloge [GSK] als Baukasten zur Auswahl von Sicherheitsmaßnahmen und enthält die in Abbildung 4 dargestellten Verfahrensschritte.

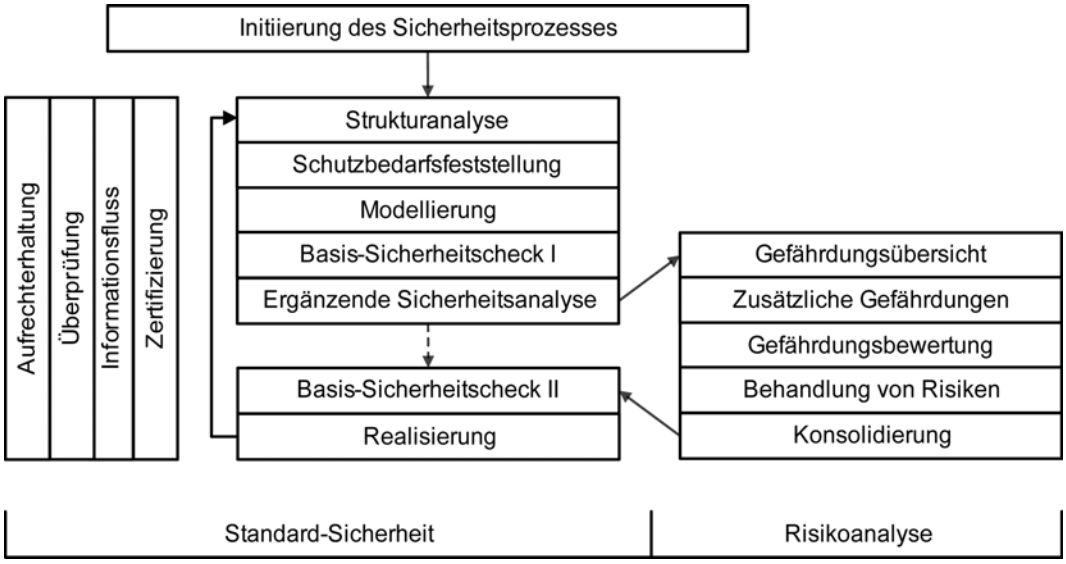


Abbildung 4: Schritte zur Entwicklung eines Sicherheitskonzepts gemäß IT-Grundschutz

Die Bedeutung der einzelnen Schritte ist wie folgt:

1. In einer **Strukturanalyse** wird ermittelt und strukturiert zusammengestellt, welche Anwendungen, IT-Systeme, Kommunikationsnetze und infrastrukturellen Gegebenheiten zu dem betrachteten Informationsverbund gehören. Ergebnis dieses Schritts ist eine Übersicht der Objekte, die mit dem Sicherheitskonzept zu schützen sind. Diese Objekte werden als **Zielobjekte** bezeichnet.

2. Bei der **Schutzbedarfsfeststellung** wird auf der Grundlage möglicher Schadensauswirkungen unter Berücksichtigung verschiedener Schutzziele entschieden, welche Sicherheitsanforderungen die zuvor identifizierten Zielobjekte haben. Art und Ausmaß der für ein Zielobjekt umzusetzenden Sicherheitsmaßnahmen hängen wesentlich von den in diesem Schritt getroffenen Entscheidungen ab.

3. Bei der **Modellierung gemäß IT-Grundschutz** werden erstmals die IT-Grundschutz-Kataloge zur Unterstützung des Prozesses eingesetzt. Diese sind nach dem Baukastenprinzip gegliedert. Ein Baustein beschreibt eine typische IT-Komponente (Anwendung, IT-System oder Kommunikationsverbindung), eine infrastrukturelle Gegebenheit oder einen zu regelnden übergreifenden Aspekt bei der Anwendung von Informationstechnik. Jeder Baustein enthält eine Sammlung an Empfehlungen dazu, wie die darin

beschriebene Komponente sicher betrieben oder der dargestellte Sachverhalt sicher geregelt werden sollte. Diese Empfehlungen sind so ausgerichtet, dass ihre Umsetzung für Zielobjekte mit normalem Schutzbedarf ein ausreichendes Sicherheitsniveau bietet, das gegebenenfalls bei höherem Schutzbedarf durch zusätzliche Maßnahmen auszubauen ist. Bei der Modellierung wird geprüft, welche Bausteine für den betrachteten Informationsverbund relevant sind. Die im weiteren Vorgehen zu berücksichtigenden Bausteine werden ausgewählt und bilden zusammengenommen ein **IT-Grundschutz-Modell** des Informationsverbunds.

4. Dieses IT-Grundschutzmodell ist Grundlage für den nächsten Schritt, dem **Basis-Sicherheitscheck**. Bei diesem wird in einem Soll-Ist-Vergleich geprüft, ob und in welchem Ausmaß die Empfehlungen der ausgewählten IT-Grundschutz-Bausteine für die vorhandenen Zielobjekte umgesetzt sind und wo aufgrund nicht oder nur unzureichend umgesetzter Maßnahmen noch ein Handlungsbedarf besteht.

5. Nicht alle Zielobjekte können hinreichend durch die vorhandenen IT-Grundschutz-Bausteine abgebildet werden, so dass gegebenenfalls weitere Sicherheitsmaßnahmen erforderlich sind. Zusätzliche oder wirksamere Schutzmaßnahmen können auch für Zielobjekte mit höherem Schutzbedarf notwendig werden. In beiden Fällen wird für die betroffenen Zielobjekte in einer **ergänzenden Sicherheitsanalyse** und gegebenenfalls erforderlichen **Risikoanalysen** geprüft, ob ein Bedarf an zusätzlichen Schutzmaßnahmen besteht. Wenn als Ergebnis dieser Analysen das bestehende Sicherheitskonzept verändert wird, ist der Umsetzungsstand der ergänzten oder modifizierten Sicherheitsmaßnahmen in einem weiteren Basis-Sicherheitscheck zu prüfen.

6. Als Ergebnis der vorangegangenen Sicherheitsüberprüfungen ergibt sich eine Menge an zwar notwendigen, bislang allerdings noch nicht oder nur unzureichend umgesetzten Sicherheitsmaßnahmen. Bei der **Realisierungsplanung** geht es darum, die praktische Behebung dieser Defizite zu planen. Die tatsächlich umzusetzenden Maßnahmen werden konsolidiert und konkretisiert, Kostenpläne und Zeitpläne aufgestellt sowie Verantwortliche für die Umsetzung und deren Kontrolle bestimmt. Ergebnis dieses Planungsschritts ist ein abgestimmter und von der Geschäftsführung unterstützter Realisierungsplan.

Inhalt und die Reihenfolge der Schritte sind nicht spezifisch für bestimmte Organisationsarten und Geschäftsprozesse. Besonderheiten ergeben sich gegebenenfalls dadurch, dass die eingesetzte Informationstechnik mehr oder weniger gut durch die IT-Grundschutz-Kataloge abgebildet werden kann. Der Schwerpunkt der IT-Grundschutz-Kataloge liegt auf häufig genutzten IT-Komponenten und Anwendungen. Je heterogener die IT-Landschaft eines Unternehmens ist, je spezieller die Hard- und Software und die Anwendungen, für die sie eingesetzt werden, desto größer ist in der Regel die Anzahl der Zielobjekte, für die ein zusätzlicher Analysebedarf besteht.

In den folgenden Kapiteln werden diese Phasen am Beispiel der RECPLAST GmbH näher beschrieben. Verantwortlich für die Durchführung der einzelnen Schritte ist wieder die von der Unternehmensleitung einberufene und vom IT-Sicherheitsbeauftragten koordinierte vierköpfige Arbeitsgruppe, die sich bereits darum gekümmert hat, die Leitlinie zur Informationssicherheit des Unternehmens zu überarbeiten. Als Zeitvorgabe wird festgelegt, dass die Ergebnisse innerhalb von vier Monaten erzielt werden sollen.

Sicherheitskonzept und Notfallvorsorge-Konzept

Notfall-Management und Informationssicherheitsmanagement sind sich ergänzende Prozesse. So ist es auch für das Notfall-Management erforderlich, gewisse Planungsdaten zu erheben, zum Beispiel welche Verfügbarkeitsanforderungen die einzelnen Anwendungen und Systeme stellen oder welche Ressourcen für einen Notbetrieb und die Wiederherstellung des regulären Betriebs erforderlich sind. Diese Informationen überschneiden sich teilweise mit denen, die bei den verschiedenen Phasen der IT-Grundschutz-Vorgehensweise erhoben werden, etwa im Rahmen der Strukturanalyse oder bei der Schutzbedarfsfeststellung. In [BSI 100-4] sind Möglichkeiten beschrieben, wie die Aktivitäten zur Entwicklung von Notfallvorsorge- und Sicherheitskonzepten miteinander verzahnt und Doppelarbeiten vermieden werden können.

Hilfsmittel

Die Ergebnisse der einzelnen Schritte sind zu dokumentieren, damit getroffene Entscheidungen zu späteren Zeitpunkten und auch von Dritten nachvollzogen werden können. Als Hilfsmittel hierfür gibt es Formulare und Checklisten in den Anhängen und ergänzenden Dokumenten zu [GSK]. Diese Vorlagen decken einzelne Schritte der IT-Grundschutz-Vorgehensweise ab. Eine umfassende Unterstützung aller Phasen bietet das GSTOOL des BSI. Für mehr Informationen zu diesem Werkzeug siehe www.bsi.bund.de/gstool/. Unter dem Menüpunkt *Download* gibt es dort auch die Möglichkeit, eine dreißig Tage lang gültige Testversion der Software herunterzuladen sowie unter *Andere Tools* eine Liste weiterer Werkzeuge, die verschiedene Hersteller zur Unterstützung der IT-Grundschutz-Vorgehensweise anbieten.

5 Strukturanalyse

Ziel der Informationssicherheit ist ein störungsfreier Geschäftsbetrieb. Dazu ist es wichtig, zu wissen, welche Informationen für die Prozesse eines Unternehmens bedeutsam sind und auf welchen technischen Systemen diese Informationen übertragen, gespeichert und verarbeitet werden.

Der erste Schritt bei der Entwicklung eines Sicherheitskonzepts besteht folglich darin, zu ermitteln, aus welchen Komponenten sich der betrachtete Informationsverbund zusammensetzt. Dieser Schritt wird in der IT-Grundschutz-Vorgehensweise als Strukturanalyse bezeichnet. Sein Ergebnis ist eine Zusammenstellung derjenigen Objekte, für die Schutzmaßnahmen vorzusehen sind, also der **Zielobjekte** des Sicherheitskonzepts.

5.1 Vorgehensweise

Ausgangspunkt der Strukturanalyse sind die Geschäftsprozesse des Unternehmens. Gemäß [BSI 100-2] werden die Zielobjekte daher in folgender Reihenfolge erfasst:

1. Zunächst werden die **Geschäftsprozesse**, **Anwendungen** und **Informationen** erfasst, die zum Geltungsbereich des betrachteten Informationsverbunds gehören.
2. danach erfolgt die **Netzplanerhebung**.
3. Daran anschließend wird untersucht und zusammengestellt, welche **IT-Systeme** für die Anwendungen benötigt werden und im Einsatz sind.
4. Im nächsten Schritt wird das räumliche Umfeld der IT-Systeme betrachtet und dokumentiert, also **Gebäude** und **Räume**, in denen die erhobene Informationstechnik angesiedelt ist.

Um die notwendigen Angaben zu erfassen, sind die im Unternehmen vorhandenen Unterlagen zur Informationstechnik zu sichten, beispielsweise Netzpläne, Inventare oder Raumpläne. Die daraus bezogenen Informationen sind zusätzlich in Gesprächen mit den Geschäftsprozessverantwortlichen oder anderen kompetenten Personen aus dem Unternehmen auf Vollständigkeit, Korrektheit und Aktualität zu prüfen und zu ergänzen.

Bei der Strukturanalyse werden zwar umfangreiche Informationen erhoben, jedoch nicht, um ein umfassendes Inventar der Anwendungen des Unternehmens und der dafür eingesetzten Informationstechnik zu erhalten. Ziel ist vielmehr eine mit Blick auf ein Sicherheitskonzept hin geordnete Zusammenstellung der wesentlichen IT-Komponenten. Eine wichtige Aufgabe bei der Strukturanalyse ist es daher, die Komplexität der insgesamt vorhandenen Informationen angemessen zu reduzieren. Dazu trägt insbesondere die **Gruppierung** gleichartiger und im Sicherheitskonzept gleichartig zu behandelnder Zielobjekte bei.

Dokumentation

Ergebnisdokumente der Strukturanalyse sind graphische und tabellarische Übersichten, in denen die Anwendungen, IT-Systeme, Kommunikationsverbindungen und räumlichen Gegebenheiten des Informationsverbunds beschrieben sind. Tabelle 1 zeigt, welche Informationen für die verschiedenen Typen von Zielobjekten erforderlich sind.

Aus dieser Dokumentation muss auch deutlich werden, welche Zielobjekte zu Gruppen zusammengefasst wurden. Dies bedeutet beispielsweise für einen Netzplan, in dem die Kommunikationsverbindungen zwischen den IT-Systemen visualisiert werden, dass gruppierte Client-PCs als ein einziges Objekt dargestellt werden (**bereinigter Netzplan**).

Anhang B.1 enthält als Beispiel für die Dokumentation einer Strukturanalyse die diesbezüglichen Ergebnisse der RECPLAST GmbH.

Typ des Zielobjekts	Zu dokumentierende Information
Anwendung und dazugehörige Informationen	eindeutige Bezeichnung, unterstützte Fachaufgabe/Geschäftsprozess, IT-Systeme, die direkt und indirekt erforderlich sind, ggf. zusätzliche Abhängigkeiten zwischen den Anwendungen, ggf. Verweis, ob personenbezogene Informationen gespeichert oder verarbeitet werden
Kommunikationsverbindung	Art der Verkabelung bzw. Kommunikationsanbindung (z. B. Lichtwellenleiter, WLAN basierend auf IEEE 802.11), maximale Datenübertragungsrate (z. B. 10 MB/s), verwendete Netzprotokolle (z. B. Ethernet, TCP/IP), bei Außenanbindungen: Details zum externen Netz (z. B. Internet, Name des Providers)
IT-System	eindeutige Bezeichnung, Typ und Funktion, zugrunde liegende Plattform (Hardware, Betriebssystem), Standort (z. B. Gebäude- und Raumnummer), Status (in Betrieb, im Test, in Planung), zuständiger Administrator, Benutzer, vorhandene Kommunikationsschnittstellen (z. B. Internet-Anschluss, Bluetooth, WLAN-Adapter), Art der Netzanbindung und Netzadresse, bei Gruppen: Anzahl der gleichartigen IT-Systeme
Raum	eindeutige Bezeichnung, Art und Funktion (z. B. Büroraum, Serverraum, Datenträgerarchiv), Standort/Gebäude, bei Gruppen: Anzahl der gleichartigen Räume

Tabelle 1: Informationen, die bei der Strukturanalyse zu den verschiedenen Zielobjekt-Typen zu dokumentieren sind.

5.2 Besonderheiten und Probleme

Welche Anwendungen?

In der Regel werden in einem Informationsverbund zahlreiche Anwendungen eingesetzt, angefangen mit allgemeinen Büroanwendungen, wie Textverarbeitung, Präsentationserstellung oder Tabellenkalkulation, bis hin zu hochgradig spezialisierter Software für einzelne Geschäftsprozesse. Da die Erfassung jeder einzelnen eingesetzten Software im Rahmen der Strukturanalyse wenig effizient ist, sollte man sich darauf konzentrieren, die besonders sicherheitskritischen Anwendungen zu erheben, also diejenigen, die aufgrund der Anforderungen der betrachteten Geschäftsprozesse ein Mindestniveau an

- Geheimhaltung (Vertraulichkeit),
- Korrektheit und Unverfälschtheit (Integrität) oder
- Verfügbarkeit

erfordern.

Für eine angemessene Auswahl der Anwendungen bietet es sich an, Anwender und Geschäftsprozessverantwortliche zu befragen.

Als in diesem Sinne besonders wichtig identifiziert das Sicherheits-management-Team der RECPLAST GmbH beispielsweise die folgenden in der Produktionsstätte in Bonn-Beuel genutzten Anwendungen:

- Anlagensteuerung und -kontrolle,
- Produktionsplanung und -steuerung,
- Lagerverwaltung (einschließlich der logistischen Unterstützung mittels RFID),
- Entwicklung (neuer Fertigungstechniken und Produkte)
- Entwurf (der für die Produktion benötigten Formteile).

Neben diesen produktionsspezifischen Anwendungen sollen im Sicherheits-konzept weitere Anwendungen betrachtet werden, da diese, beziehungsweise deren sicherheitsgerechter Einsatz, für das Unternehmen wichtig sind. Zu diesen Anwendungen gehören Standard-Büroanwendungen (Textverarbeitung, Präsentation, Tabellenkalkulation), E-Mail und Internet-Recherche.

Gruppenbildung

Ein Sicherheitskonzept muss zwar für jedes einzelne Zielobjekt angemessene und wirksame Schutzmechanismen vorsehen. Umgekehrt braucht aber nicht jedes Zielobjekt auch sein eigenes Kapitel in diesem Planungsdokument. In der Praxis unterliegen viele Komponenten nämlich ähnlichen Bedingungen und können daher mit den gleichen Sicherheitsmaßnahmen geschützt werden. Beispielsweise stimmen in der Regel bei den Clients eines Netzes Betriebssystem und installierte

Software überwiegend überein, ebenso deren räumliche Umgebung und Netzanbindung. Derartige IT-Systeme können zu einer Gruppe zusammengefasst und damit einheitlich im Sicherheitskonzept behandelt werden – es sei denn, diese Geräte unterscheiden sich maßgeblich im Schutzbedarf der Informationen und Anwendungen, für die sie genutzt werden.

Grundsätzlich können Komponenten immer dann zu einer Gruppe zusammengefasst werden, wenn sie

- vom gleichen Typ sind,
- gleich oder nahezu gleich konfiguriert sind,
- den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen,
- die gleichen Anwendungen unterstützen,
- in gleicher oder ähnlicher Weise in ein Netz eingebunden sind (sofern es sich um IT-Systeme handelt) und
- den gleichen Schutzbedarf aufweisen.

Die Bildung angemessener Gruppen ist eine der wesentlichen Aufgaben bei der Strukturanalyse. Die Verringerung der Anzahl der unterschiedenen Zielobjekte leistet einen Beitrag zu einer effizienten Erarbeitung eines Sicherheitskonzepts. Es ist jedoch auch wichtig, dass die vorgenommene Gruppenbildung tatsächlich angemessen ist. Werden Objekte zusammengefasst, die unterschiedliche Schutzanforderungen haben, kann dies zu großen Sicherheitslücken führen.

Zur Veranschaulichung, wann Zielobjekte sinnvoll zu einer Gruppe zusammengefasst werden können und wann nicht, dienen nachfolgend einige Entscheidungen der Strukturanalyse der RECPLAST GmbH.

Beispiel 1: Industrie-PCs zur Anlagensteuerung und -kontrolle

Sowohl die Recycling- als auch die Spritzgussanlagen werden mit Hilfe von Industrie-PCs und einer speziellen Software gesteuert. Beide PCs unterstützen damit vergleichbare Anwendungszwecke (Anlagensteuerung und -kontrolle) und sind auch identisch in das Netz eingebunden. Es verbietet sich jedoch aus verschiedenen Gründen, die Geräte zu einer Gruppe zusammenzufassen:

- Sie haben unterschiedliche Betriebssystemvarianten. Dies kann unter Sicherheitsaspekten bedeutsam sein, weil für ältere Betriebssysteme möglicherweise keine Sicherheitspatches mehr angeboten werden. Bei gravierenden auf Softwarefehlern beruhenden Sicherheitslücken sind in solchen Fällen Ersatzmaßnahmen zum Schutz einer Anlagensteuerung und -kontrolle notwendig.
- Die Anlagen sind unterschiedlich wichtig für die RECPLAST GmbH. Einen Ausfall der Recyclinganlage kann das Unternehmen zur Not und bei erschöpf-

ten Lagerbeständen dadurch kompensieren, dass es Granulate, die für die Produktion erforderlich sind, bei einem Drittunternehmen einkauft. Ein Ausfall einer Spritzgussanlage könnte hingegen zu größeren finanziellen Verlusten führen, wenn bei einer Auftragsproduktion festgelegte Terminvorgaben nicht eingehalten werden können.

- Für beide Anlagen gibt es Wartungsverträge mit den Herstellern. Diese sehen aber unterschiedliche Regularien vor, etwa für den Zeitraum, in dem ein Hersteller seiner Wartungsverpflichtung nachkommen muss, oder bezüglich der Art und Weise wie Fernwartung durchgeführt wird.

Es wird daher entschieden, die beiden Steuerungs-PCs einschließlich der auf ihnen befindlichen Software nicht zu einer Gruppe zusammenzufassen.

Beispiel 2: Gabelstapler

Bei den vier Gabelstaplern, die zur Unterstützung der Lagerverwaltung mit eigenen Computern, WLAN- und RFID-Schnittstellen ausgestattet sind, ist eine Gruppenbildung hingegen unstrittig. Sie bedienen dieselbe Anwendung und dies mit völlig identischer Technik und Netzanbindung – es gibt folglich keinen Grund, diese nicht zu einer Gruppe zusammenzufassen.

Beispiel 3: Client-PCs

Die verschiedenen PCs, die als Clients des Unternehmensnetzes in den Abteilungen „Fertigung“, „Entwicklung“ und „Lager/Logistik“ betrieben werden, sind alle mit einem identischen Betriebssystem ausgestattet. Auch ihre räumliche Umgebung (Unterbringung in Büroräumen) unterscheidet sich mit Ausnahme der beiden PCs in den offenen Lagerbereichen nicht. Es wird folglich erwogen, diese IT-Systeme als eine Gruppe zu behandeln und nicht weiter zu differenzieren, zumal die Datenbestände, auf die mit ihnen zugegriffen werden kann, viele Übereinstimmungen aufweisen. Im weiteren Verlauf der Beratungen entscheidet man sich jedoch dazu, zwei Ausnahmen zu machen:

- Auf den sechs PCs der Entwicklungsabteilung befinden sich Konstruktionspläne und unter Umständen kundenspezifische Entwicklungen und Verfahrensbeschreibungen, die beispielsweise vor Wirtschaftsspionage und damit möglichen gravierenden wirtschaftlichen Folgen für die Firma zu schützen sind. Hier ist der hohe Schutzbedarf der Informationen der Grund dafür, diese sechs IT-Systeme in der Strukturanalyse zu einer eigenen Gruppe zusammenzufassen und gesondert im Sicherheitskonzept zu behandeln.
- Die beiden PCs in den offenen Bereichen des Fertigungs- und des Auslieferungslagers befinden sich in einer anderen räumlichen Umgebung wie die in Büroräumen untergebrachten Clients des Fertigungs- und Lagerbereichs. Da Zugangs- und Zugriffsschutz für diese IT-Systeme besonders zu überlegen sind, werden beide PCs zu einer Gruppe „Lager-PCs“ zusammengefasst.

Die verbliebenen PCs fasst das Sicherheitsmanagement-Team in einer Gruppe „Büro-PCs“ zusammen.

Abbildung 5 zeigt, wie sich die gebildeten Gruppen auf den Netzplan auswirken.

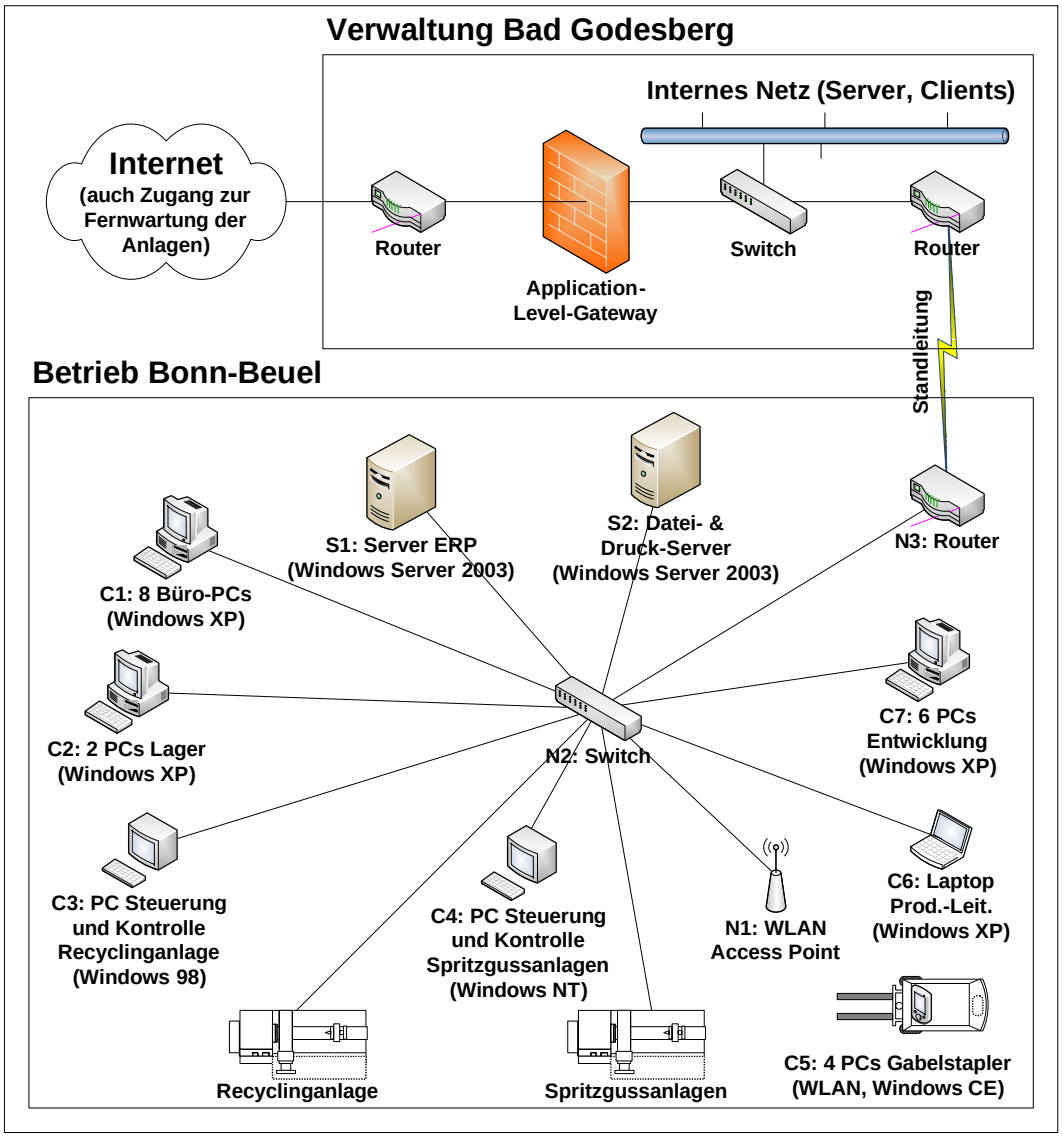


Abbildung 5: Bereinigter Netzplan der RECPLAST GmbH mit gruppierten IT-Systemen und Angaben zu deren Betriebssystem. Der vorangestellte Buchstabe kennzeichnet den Typ des IT-Systems (S = Server; C = Client; N = Netzkopplungskomponente).

6 Schutzbedarfsfeststellung

Bei der Strukturanalyse werden die verschiedenen Objekte eines Informationsverbunds, also Anwendungen und IT-Systeme sowie deren Vernetzung und räumliche Umgebung, geordnet zusammengestellt. Im darauf folgenden Schritt, der Schutzbedarfsfeststellung, wird in einem systematischen Prozess bewertet und abgeleitet, wie wichtig aus Sicht des Unternehmens der Schutz von **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** dieser Zielobjekte ist. Da sich die Maßnahmen, die zum Schutz der Vertraulichkeit von Informationen angemessen sind, von denen unterscheiden, mit denen die Verfügbarkeit oder Integrität gesichert werden, müssen die Bewertungen und Ableitungen getrennt für die verschiedenen Grundwerte erfolgen.

Das Ergebnis der Schutzbedarfsfeststellung

- gibt Hinweise auf diejenigen Aspekte und Bereiche, die im Rahmen eines Sicherheitskonzepts in besonderer Weise berücksichtigt werden sollten, und
- unterstützt die Entscheidung, für welche Zielobjekt die Umsetzung der IT-Grundschutz-Maßnahmen bereits eine hinreichende und angemessene Sicherheit bietet und für welche zusätzliche Risikobetrachtungen und gegebenenfalls stärker wirksame Schutzvorkehrungen erforderlich sind.

Wegen ihrer grundlegenden Bedeutung für die Auswahl und Einführung von Sicherheitsmaßnahmen sollten die Schutzbedarfsfeststellung sehr sorgfältig vorgenommen und ihre Ergebnisse mit der Unternehmensleitung sowie den Fachverantwortlichen abgestimmt werden.

6.1 Vorgehensweise

Die Schutzbedarfsfeststellung gliedert sich in die folgenden Teilschritte:

1. die Definition von **Schutzbedarfskategorien**,
2. die Feststellung des Schutzbedarfs der **Anwendungen** des Informationsverbunds mit Hilfe dieser Kategorien,
3. daraus abgeleitet die Feststellung des Schutzbedarfs der **IT-Systeme**, die für diese Anwendungen im Einsatz sind, und
4. davon abhängig die Ableitung des Schutzbedarfs der der **Räume**, in denen die IT-Systeme untergebracht sind, sowie
5. der **Kommunikationsverbindungen** zwischen diesen IT-Systemen.

Schutzbedarfskategorien definieren

Wie hoch der Schutzbedarf eines Zielobjekts ist, hängt vom Ausmaß des möglichen Schadens bei Verletzungen eines seiner Schutzziele ab.

Welche Verluste entstehen, wenn ein Server nicht in dem erforderlichen Maß verfügbar ist? Welche Nachteile erwachsen einem Unternehmen, wenn ein Konkurrent Kenntnis von vertraulichen Informationen erhält? Wie gravierend können sich unbefugte Änderungen an einem Datenbestand auswirken? – Diese und vergleichbare Fragen zu den Auswirkungen von Schadensereignissen lassen sich vorab nur in Ausnahmefällen präzise quantifizieren. Eine exakte Berechnung ist allerdings in der Regel auch nicht erforderlich. [BSI 100-2] empfiehlt, sich auf drei **Schutzbedarfskategorien** zu beschränken, nämlich

- **normal**, wenn die Schadensauswirkungen begrenzt und überschaubar sind,
- **hoch**, wenn die Schadensauswirkungen beträchtlich sein können, und
- **sehr hoch**, wenn die Schadensauswirkungen ein existenziell bedrohliches, katastrophales Ausmaß erreichen können.

Bei einem normalen Schutzbedarf genügt es im Allgemeinen für eine hinreichende Sicherheit, die IT-Grundschutz-Maßnahmen umzusetzen. Bei einem hohen Schutzbedarf sind möglicherweise zusätzliche oder stärker wirksame Sicherheitsmaßnahmen notwendig. Bei einem sehr hohen Schutzbedarf sind solche Maßnahmen sogar mit großer Wahrscheinlichkeit erforderlich (vgl. Tabelle 2).

Schutzbedarfskategorie	Schadensauswirkung	Bewertung
normal	begrenzt, überschaubar	IT-Grundschutz-Maßnahmen genügen im Allgemeinen
hoch	beträchtlich	gegebenenfalls sind höherwertige Sicherheitsmaßnahmen erforderlich
sehr hoch	katastrophal, existenzgefährdend	höherwertige Sicherheitsmaßnahmen sehr wahrscheinlich erforderlich

Tabelle 2: Zusammenhang zwischen Schutzbedarfskategorien und Sicherheitsmaßnahmen

Wenn in einem Unternehmen eine differenziertere Unterscheidung von Schutzklassen und damit mehr als drei Schutzbedarfskategorien verwendet werden, können diese für die Entwicklung eines Sicherheitskonzepts gemäß IT-Grundschutz auf die drei Schutzbedarfskategorien *normal*, *hoch* und *sehr hoch* abgebildet werden.

Ob ein Schaden als *normal*, *hoch* oder *sehr hoch* einzuschätzen ist, hängt einerseits von seiner Art, andererseits von der Fähigkeit eines Unternehmens ab, Verletzungen der Informationssicherheit zu verkraften. Verliert es beispielsweise aufgrund von Wirtschaftsspionage einen Auftrag im Volumen von mehreren hunderttausend Euro an einen Konkurrenten, so kann dies für ein kleineres Unternehmen existenzgefährdend sein, während für einen weltweit operierenden großen Konzern finanzielle Einbußen in einer solchen Höhe nur ein geringes Problem darstellen.

Daher sind auf den jeweils betrachteten Informationsverbund zugeschnittene Kriterien zu definieren, anhand derer mögliche Schadensauswirkungen und damit

die Schutzbedarfsfeststellung nachvollziehbar eingestuft werden kann. In [BSI 100-2] werden zur Unterstützung dieser Entscheidungen die folgenden **Schadensszenarien** unterschieden:

- **Verstoß gegen Gesetze, Vorschriften oder Verträge**, z. B. gegen die Anforderungen an eine ordnungsgemäße Archivierung von Geschäftsunterlagen, die Auflagen der Gewerbeaufsichtsämter oder Vereinbarungen in Lieferverträgen mit Kunden,
- **Beeinträchtigung des informationellen Selbstbestimmungsrechts**, z. B. bei Preisgabe von Personal- oder anderen Arbeitnehmerdaten,
- **Beeinträchtigung der persönlichen Unversehrtheit**, z. B. aufgrund von Fehlern in der Steuerungssoftware von Maschinen und Produktionsanlagen,
- **Beeinträchtigung der Aufgabenerfüllung**, z. B. bei durch den Ausfall wichtiger IT-Systeme verursachtem Maschinenstillstand,
- **negative Innen- oder Außenwirkung**, z. B. wenn Kunden, Konkurrenten oder eine breite Öffentlichkeit von häufigen Unregelmäßigkeiten im Unternehmen Kenntnis erhalten, oder das Unternehmen aufgrund von Sicherheitsvorfällen an Wertschätzung bei den eigenen Mitarbeitern verliert,
- **finanzielle Auswirkungen**, z. B. Einnahmeausfälle und Vertragsstrafen, wenn sich die Produktion verzögert und dadurch Liefertermine nicht eingehalten werden können, oder Wiederbeschaffungs- und Wiederherstellungskosten, wenn Hard- oder Software beschädigt werden.

[BSI 100-2] enthält einen allgemeinen Vorschlag dazu, wie diese Schadensszenarien bei der Definition der Schutzbedarfskategorien verwendet werden. Dieser ist an die speziellen Bedingungen des betrachteten Informationsverbunds anzupassen. Als Beispiel dazu zeigt Tabelle 3 die Definition der Schutzbedarfskategorien bezüglich der Schadensszenarien „Beeinträchtigung der Aufgabenerfüllung“ und „finanzielle Auswirkungen“ bei der RECPLAST GmbH.

Schadenszenario	**Schutzbedarfskategorie**		
	normal	**hoch**	**sehr hoch**
Beeinträchtigung der Aufgabenerfüllung	Die Abläufe bei RECPLAST werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.	Die Abläufe bei RECPLAST werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.	Die Abläufe bei RECPLAST werden so stark beeinträchtigt, dass Ausfallzeiten, die über zwei Stunden hinausgehen, nicht toleriert werden können.
Finanzielle Auswirkungen	Der mögliche finanzielle Schaden ist geringer als 50.000 Euro.	Der mögliche finanzielle Schaden liegt zwischen 50.000 und 500.000 Euro	Der mögliche finanzielle Schaden liegt über 500.000 Euro.

Tabelle 3: Definition der Schutzbedarfskategorien bei der RECPLAST GmbH (Auszug)

Schutzbedarf von Anwendungen feststellen

Mit Hilfe der zuvor festgelegten Kriterien wird zunächst der Schutzbedarf der Anwendungen bestimmt. Dazu ist jeweils zu untersuchen, für welche Geschäftsprozesse eine Anwendung eingesetzt wird und welche Informationen sie verwendet. Für die Bestimmung des Schutzbedarfs sollten die bei den verschiedenen Schadensszenarien möglichen Schäden betrachtet werden: Werden beispielsweise personenbezogene oder -beziehbare Informationen verarbeitet oder wichtige Geschäftsgeheimnisse? In diesen Fällen könnte der Schutzbedarf einer Anwendung bezüglich Vertraulichkeit als *hoch* oder *sehr hoch* bewertet werden. Gleiches gilt beispielsweise für das Schutzziel Verfügbarkeit, wenn der Ausfall einer Anwendung unvertretbare Produktionsverzögerungen nach sich ziehen würde, oder das Schutzziel Integrität, wenn aufgrund falscher Informationen gravierende Fehlentscheidungen getroffen werden.

Schutzbedarf von IT-Systemen, Räumen und Kommunikationsverbindungen ableiten

Der Schutzbedarf von IT-Systemen hängt im Wesentlichen von dem Schutzbedarf der Anwendungen ab, für die ein IT-System relevant ist. Dabei kommen Vererbungsprinzipien zum Tragen. In der IT-Grundschutz-Vorgehensweise werden die folgenden drei Fälle unterschieden:

- **Maximumprinzip:** In der Regel richtet sich der Schutzbedarfs eines IT-Systems in einem Grundwert nach dem höchsten Schutzbedarf der Anwendungen, für die es genutzt wird.
- **Kumulationseffekte:** Aufgrund der Vielzahl an Anwendungen, die das IT-System benötigen, ist dessen Schutzbedarf in einem Grundwert höher als der höchste Schutzbedarf der einzelnen Anwendungen.
- **Verteilungseffekte:** Der insgesamt höhere Schutzbedarf einer Anwendung verteilt sich so, dass ein beteiligtes IT-System einen geringeren Schutzbedarf hat.

In ähnlicher Weise werden der Schutzbedarf von Räumen aufgrund der in ihnen untergebrachten IT-Systeme und der Schutzbedarf von Kommunikationsverbindungen aufgrund der über sie gesendeten Daten abgeleitet.

Kommunikationsverbindungen sind immer dann als besonders kritisch zu betrachten, wenn

- auf ihnen Informationen mit einem hohen Schutzbedarf übertragen werden, da diese besonders wirksam gegen Angriffe oder Ausfälle zu sichern sind,
- sie auf keinen Fall für die Übertragung hochschutzbedürftiger Informationen genutzt werden dürfen, um zu verhindern, dass diese von unbefugten Dritten eingesehen werden können, oder
- sie über unkontrollierte Bereiche führen, was etwa bei Außenverbindungen über das Internet der Fall ist, aber auch auf WLANs, deren Reichweite nicht

an der Umzäunung eines Unternehmens endet, oder auf angemietete Standleitungen zutreffen kann.

In [BSI 100-2] wird empfohlen, die **kritischen Kommunikationsverbindungen** im Netzplan so zu markieren, dass auch deutlich wird, warum ein Netzsegment als kritisch eingestuft wurde.

Dokumentation der Schutzbedarfsfeststellung

Zur Dokumentation der Schutzbedarfsfeststellung bieten sich tabellarische Übersichten an. Diese sollten sowohl die getroffenen Entscheidungen als auch die zugehörigen Begründungen enthalten. Mit Hilfe von Software-Werkzeugen zum IT-Grundschutz, etwa dem GSTOOL, lassen sich solche Listen einfach generieren. Derartige Tools bieten darüber hinaus den Vorteil, dass sie die Bestimmung des Schutzbedarfs von IT-Systemen, Kommunikationsverbindungen und Räumen durch Vorschläge unterstützen, die zum Beispiel aus dem Vererbungsprinzip abgeleitet werden können.

Anhang B.2 enthält als Beispiel für die Dokumentation der Schutzbedarfsfeststellung die diesbezüglichen Ergebnisse der RECPLAST GmbH.

6.2 Besonderheiten und Probleme

Grundsätzlich unterscheidet sich die Vorgehensweise bei der Schutzbedarfsfeststellung eines Produktionsunternehmens nicht von der bei beliebigen anderen Organisationen. Auch die dabei häufig auftretenden Probleme sind ähnlich. Die diesbezüglichen Empfehlungen in [BSI 100-2] gelten daher uneingeschränkt auch für die RECPLAST GmbH.

Korrektur der Strukturanalyse bei der Schutzbedarfsfeststellung

Einigen Entscheidungen bei der Strukturanalyse liegen implizit bereits Annahmen zum Schutzbedarf zugrunde. So bei der Auswahl der Anwendungen, bei denen die Konzentration auf solche mit einem besonderen Schutzbedarf gelegt wird. Gleiches gilt für die gebildeten Gruppen: Ein übereinstimmender Schutzbedarf in allen Grundwerten ist ein wesentliche Kriterium dafür, Zielobjekte in einer Gruppe zusammenzufassen.

Die Schutzbedarfsfeststellung bedeutet eine vertiefte Betrachtung des Werts einer Anwendung oder einer sie unterstützenden IT-Komponente für ein Unternehmen. Sie kann folglich auch dazu führen, in der Strukturanalyse getroffene Entscheidungen zurückzunehmen, also

- vorgenommene Gruppenbildungen wieder aufzulösen, weil die Diskussionen zur Einstufung des Schutzbedarfs ergeben haben, dass die zusammengefassten Zielobjekte unterschiedliche Sicherheitsanforderungen haben, oder auch

- neue Gruppen zu bilden, da sich gezeigt hat, dass dies aufgrund der Übereinstimmungen im Schutzbedarf für die beteiligten Zielobjekte problemlos möglich ist.

Schutzziel Verfügbarkeit

Der Schutzbedarf wird getrennt für die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität festgestellt. Je nach Informationsverbund und betrachtetem Objekt haben diese Ziele eine unterschiedliche Wertigkeit. Beispielsweise streben Produktionsunternehmen in der Regel eine möglichst hundertprozentige Auslastung ihrer Fertigungsanlagen an. Auch kurzzeitige Ausfälle sind oftmals mit hohen Kosten für den Wiederanlauf verbunden, zudem kann die Wiederanlaufzeit mehrere Tage beanspruchen. Daher ist es erforderlich, dass die zur Steuerung und Kontrolle benötigte Informationstechnik eine entsprechend hohe Verfügbarkeit hat, Ausfälle und Ausfallzeiten also auf ein absolutes Minimum reduziert sind. Aber auch hier empfiehlt es sich, genau zu differenzieren:

Wie bereits im Kapitel zur Strukturanalyse beschrieben, haben die bei der RECPLAST GmbH eingesetzten Industrie-PCs zur Anlagensteuerung und -kontrolle unterschiedliche Verfügbarkeitsanforderungen:

- Weil ein vorübergehender Ausfall der Recycling-Anlage keine größeren wirtschaftlichen Verluste nach sich zieht, wird der Schutzbedarf des zur Steuerung und Kontrolle dieser Anlage eingesetzten PCs bezüglich Verfügbarkeit als *normal* eingestuft.
- Anders verhält es sich bei dem PC, mit dem die Spritzgussanlage gesteuert wird. Bei diesem hält das Sicherheitsmanagement-Team Ausfälle von wenigen Stunden noch für vertretbar, nicht aber solche, die länger dauern als einen Tag. Ein mehr als 24-stündiger Produktionsausfall könnte neben unmittelbaren Einnahmeausfällen auch bedeuten, dass bei bestimmten Auftraggebern Konventionalstrafen drohen und die Gefahr besteht, dass diese zu Konkurrenten abwandern. Das Team entscheidet sich also dafür, den Verfügbarkeitsbedarf dieses IT-Systems als *hoch* einzustufen.

Als *normal* wird auch der Verfügbarkeitsbedarf der RFID-gestützten Lagerverwaltung eingeschätzt. Zwar trägt diese Anwendung zur Effizienz der Arbeitsprozesse bei und bringt dem Unternehmen damit betriebswirtschaftliche Vorteile, die auf einige zehntausend Euro jährlich geschätzt wurden. Aufgrund manueller Ausweichverfahren rechtfertigen die Verluste auch eines mehrtägigen Ausfalls der Technik, zum Beispiel aufgrund einer Nicht-Verfügbarkeit des WLANs, keine höhere Schutzbedarfseinstufung.

Schutzziel Integrität

Eine **hohe Integrität** der Informationen, die im Produktionsumfeld verarbeitet werden, ist unerlässlich für die Effizienz der Fertigung und die Erfüllung der Qualitätsanforderungen an deren Erzeugnisse. Fehlerhafte Steuerungsdaten

können beispielsweise zum Ausfall einer Anlage führen, aber auch dazu, dass Qualitätsmängel erst zu spät erkannt werden und unnötig viel Ausschussware produziert wird. Aber auch gravierendere Auswirkungen sind möglich: Anlagen und – schlimmer noch – in deren Umgebung anwesende Personen können geschädigt werden, zum Beispiel bei Überhitzung oder Überdruck einer Maschine.

So enthält die Steuersoftware des Leitrechners für die Spritzgussanlagen bei der RECPLAST GmbH Überwachungsfunktionen, die bei Überschreitung vorgegebener Toleranzwerte für die Maschinenparameter unterschiedliche Aktionen auslösen können. Je nach Art und Grad der Abweichung reichen diese von einer bloßen Alarmierung, über die Aussonderung fehlerhafter Teile bis hin zu einem sofortigen Stillstand der betroffenen Anlage. Da fehlerhafte Grenzwerte die vorstehend beschriebenen unter Umständen gravierenden Auswirkungen haben können, wird der Schutzbedarf bezüglich der Integrität der Steuerungs- und Kontrollsoftware und damit auch des betreffenden IT-Systems als *hoch* eingestuft. Mit einer vergleichbaren Begründung wird diese Einschätzung auch für die Steuerung und Kontrolle der Recyclinganlage getroffen.

Die Anwendung zur RFID-gestützten Lagerverwaltung wird auch bezüglich des Schutzziels Integrität als weniger kritisch gesehen. Fehlerhafte Informationen, zum Beispiel eine falsche Lagerposition, können leicht erkannt und einfach korrigiert werden. Daher entscheidet sich das Sicherheitsmanagement-Team dafür, den Schutzbedarf der Anwendung bezüglich Integrität als *normal* zu bewerten.

Schutzziel Vertraulichkeit

In jedem Unternehmen gibt es eine Vielzahl an Informationen, bei denen in besonderer Weise darauf zu achten ist, dass sie nur von Berechtigten eingesehen werden können. Informationen, deren Vertraulichkeit in besonderer Weise geschützt werden muss, sind beispielsweise solche

- zu deren Geheimhaltung sich ein Unternehmen gegenüber Kunden verpflichtet hat,
- aus deren Kenntnis die Konkurrenz Vorteile beziehen könnte, beziehungsweise bei deren Preisgabe eigene Wettbewerbsvorteile verloren gingen,
- deren unbefugte Weitergabe gesetzliche Vorschriften zum betrieblichen Datenschutz verletzen würde.

Informationen mit einem höheren Schutzbedarf befinden sich bei der RECPLAST GmbH insbesondere auf den Rechnern der Entwicklungsabteilung, wo nicht nur Formteile für die Gussanlagen entwickelt werden, sondern auch an gegebenenfalls patentierfähigen Rezepturen für neuartige Kunststoffe gearbeitet wird. Der Schutzbedarf dieser IT-Systeme wird daher unter dem Grundwert Vertraulichkeit als *hoch* eingestuft.

Eine längere Diskussion gibt es im Sicherheitsmanagement-Team über die Einstufung der PCs in den Büros der Produktions- und Lagerleitung bezüglich Vertraulichkeit. Mit Hilfe dieser IT-Systeme kann auf das ERP-System zugegriffen werden. Daneben ist auf ihnen übliche Standardsoftware (Büroanwendungen, E-Mail, Webbrowser) installiert. Die Vertraulichkeit des überwiegenden Teils der gespeicherten und verarbeiteten Informationen wird als *normal* eingestuft. Da ein Zugriff auf den PC aber auch den Zugang zu Firmengeheimnissen (z. B. in einzelnen E-Mails oder Dokumenten) öffnen könnte, wird gemäß Maximalprinzip der Schutzbedarf dieser IT-Systeme bezüglich Vertraulichkeit als *hoch* eingestuft.

Angemessenheit der Entscheidungen zur Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung gilt es, zwei Extreme zu vermeiden. Zum einen kann es die Neigung geben, den Schutzbedarf einer Komponente in einem beliebigen Grundwert als **zu gering** einzuschätzen. Dies kann verschiedene Ursachen haben:

- Ein möglicher Grund kann darin liegen, dass die Bedeutung einer Komponente unterschätzt wird, weil sie nur in Teilbereichen überblickt wird. Ein Geschäftsprozessverantwortlicher weiß zum Beispiel nicht unbedingt, in welchen anderen Unternehmensbereichen eine Anwendung auch noch benötigt wird, die nur sporadisch für seinen Geschäftsprozess relevant ist. Ein Mitglied der IT-Abteilung hätte vielleicht diesen Überblick, weiß jedoch nicht so gut über die tatsächliche fachliche Relevanz der Anwendung Bescheid.
- Eine zu niedrige Bewertung kann aber auch dadurch motiviert sein, dass man sich um einen Mehraufwand drücken will, den ein höherer Schutzbedarf bei der Entwicklung und Umsetzung eines Sicherheitskonzepts nach sich ziehen kann. Dies kann dadurch verstärkt werden, dass Schutzbedarf und Gefährdung fälschlicherweise miteinander verwechselt werden. Weil keine Gefahr gesehen wird, wird auch kein besonderer Schutzbedarf angenommen.

Welche Motivation oder Ursache ein zu gering eingeschätzter Schutzbedarf auch immer haben mag, er bedeutet stets ein unnötiges Risiko für die Informationssicherheit im Unternehmen.

Dies gilt umgekehrt zwar nicht bei einem zu hoch eingeschätzten Schutzbedarf, ein daraus resultierender unnötiger Aufwand für Informationssicherheit kann jedoch ebenfalls nicht im Interesse des Unternehmens liegen. Ursache für eine **Überschätzung des Schutzbedarfs** kann wie bei dessen Unterschätzung eine lediglich partielle Sicht auf ein betrachtetes Zielobjekt sein. Mitarbeiter der IT-Abteilung können zum Beispiel den Verfügbarkeitsbedarf einer Anwendung zu hoch bewerten, weil sie aufgrund einer eher technischen Sicht die fachliche Dringlichkeit einer Anwendung über- oder Ausweichverfahren bei deren Ausfall unterschätzen.

Zur möglichst genauen Feststellung des Schutzbedarfs empfehlen sich Workshops mit kompetenter Beteiligung aus den relevanten Geschäftsprozessen (im Beispiel der RECPLAST GmbH mit Mitarbeitern aus der Entwick-

lungsabteilung, dem Fertigungsbereich und dem Bereich Lager/Logistik) und der IT-Abteilung. Dabei sollte der Zweck der Schutzbedarfsfeststellung den Beteiligten prägnant beschrieben sowie die Schutzbedarfskategorien und Zuordnungskriterien verbindlich definiert und mit der Geschäftsführung abgestimmt sein.

Im Sicherheitsmanagement-Team der RECPLAST GmbH sind Mitarbeiter aus allen relevanten Bereichen des betrachteten Informationsverbunds vertreten. Dadurch gelingt es zügig, zu übereinstimmenden Bewertungen des Schutzbedarfs der einzelnen Zielobjekte des Informationsverbunds zu kommen. Diese sind in Anhang B.2 wiedergegeben.

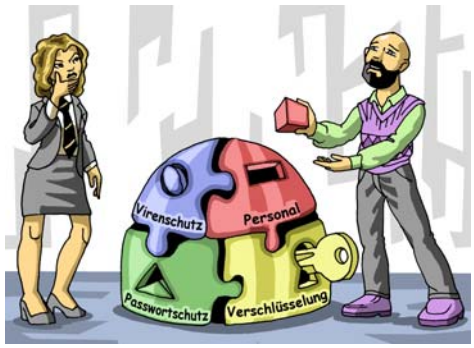
Schutzbedarfsfeststellung und Notfallplanung

Angesichts der existenziellen Bedeutung der Fertigung für ein Produktionsunternehmen bietet es sich an, für und mit einem besonderen Fokus auf diesen Bereich ein Notfall-Management zu etablieren. Ein Vorgehensmodell und Einzelempfehlungen dazu sind in den Dokumenten [BSI 100-4] und [GSK], Baustein B 1.3 *Notfallvorsorge-Konzept*, beschrieben. Bestandteil der dort dargestellten Methodik ist mit der **Business Impact Analyse (BIA)** auch ein Verfahren, mit dem Folgeschäden von Krisen und anderen Notfällen ermittelt und bewertet werden können. Zwischen dieser und der Schutzbedarfsfeststellung bestehen die folgenden Unterschiede:

- Von den verschiedenen bei einer Schutzbedarfsfeststellung betrachteten Schadensszenarien werden bei einer BIA insbesondere, wenn auch nicht ausschließlich, die finanziellen Auswirkungen betrachtet.
- Im Mittelpunkt der BIA steht die Verfügbarkeit eines Prozesses sowie der dafür erforderlichen IT-Systeme und Ressourcen. Vertraulichkeit und Integrität von Informationen und Systemen werden allenfalls am Rande betrachtet.
- Die BIA schließt auch eine zeitliche Betrachtung mit ein, da untersucht wird, ab wann ein Ausfall für ein Unternehmen kritisch werden kann.
- Im Rahmen einer BIA werden zusätzliche Werte geschätzt und Informationen erhoben, zum Beispiel die maximal tolerierbare Ausfallzeit und die anzustrebende Wiederanlaufzeit eines Systems nach einer schwerwiegenden Unterbrechung.

Wenn ein Unternehmen nicht nur den IT-Grundschutz, sondern auch ein Notfall-Management gemäß [BSI 100-4] umsetzen will, empfiehlt es sich die für die Schutzbedarfsfeststellung und die BIA erforderlichen Informationen im Zusammenhang zu ermitteln und zu betrachten. Dies erhöht die Effizienz des Vorgehens und trägt dazu bei, dass die beiden Untersuchungsverfahren nicht zu widersprüchlichen Ergebnissen bezüglich der Verfügbarkeitsanforderungen von Prozessen und Systemen führen.

7 Modellierung gemäß IT-Grundschutz



In der Strukturanalyse werden die Zielobjekte eines Sicherheitskonzepts ermittelt, anschließend bei der Schutzbedarfsfeststellung deren Bedarf an Vertraulichkeit, Verfügbarkeit und Integrität. Die Resultate beider Schritte fließen in die **Modellierung gemäß IT-Grundschutz** ein. Bei dieser wird entschieden, welche IT-Grundschutz-Bausteine für den betrachteten Informationsverbund anzuwenden sind. Das Ergebnis dieses Vorgangs ist ein **IT-Grundschutz-Modell**, das

- als **Prüfplan** für die in einem bestehenden Informationsverbunds umgesetzten Sicherheitsmaßnahmen und
- als **Entwicklungskonzept** für die in einem geplanten Informationsverbund umzusetzenden Sicherheitsmaßnahmen

dienen kann.

7.1 Vorgehensweise

Die Bausteine sind in [GSK] in die **fünf Schichten** *Übergreifende Aspekte*, *Infrastruktur*, *IT-Systeme*, *Netze* und *Anwendungen* gegliedert. [BSI 100-2] empfiehlt, bei der Modellierung entlang dieser Reihenfolge vorzugehen und für jeden Baustein zu prüfen, auf welche Zielobjekte im betrachteten Informationsverbund er anzuwenden ist.

Fehlende Bausteine

Auch wenn die IT-Grundschutz-Kataloge fortlaufend aktualisiert werden, so lässt sich doch nicht ausschließen, dass ein Informationsverbund Zielobjekte enthält, die nur unzureichend oder überhaupt nicht durch die vorhandenen Bausteine abgebildet werden können. In diesen Fällen müssen entweder bestehende Bausteine modifiziert oder aber neue, benutzerdefinierte Bausteine angefertigt werden, um angemessene und hinreichende Sicherheitsmaßnahmen für diese Zielobjekte im Sicherheitskonzept zu berücksichtigen. Die Abwandlung vorhandener und die Formulierung neuer Bausteine können durch eine Risikoanalyse unterstützt werden (siehe Kapitel 9 dieses Profils).

Dokumentation

Zur Dokumentation des Modellierungsergebnisses bietet sich eine tabellarische Zusammenstellung des zum betrachteten Informationsverbund gebildeten IT-Grundschutz-Modells an. Diese sollte die anzuwendenden Bausteine mit

Bezeichnung und Nummer enthalten und für jeden Baustein angeben, auf welche Zielobjekte er anzuwenden ist. In weiteren Spalten einer solchen Tabelle können die Namen von Ansprechpartnern für die Durchführung des Basis-Sicherheitschecks (siehe dazu das nächste Kapitel) sowie ergänzende Anmerkungen zur vorgenommenen Zuordnung angeführt werden. Es ist ebenfalls zu vermerken, wenn für ein Zielobjekt neue oder angepasste Bausteine erforderlich sind, weil eine vollständige Entsprechung (bislang) in [GSK] fehlt.

Es ist abschließend anhand der Dokumentation zu prüfen, ob das IT-Grundschutz-Modell vollständig ist, ob also alle Zielobjekte des Informationsverbunds in Übereinstimmung mit den Modellierungshinweisen in den [GSK], Kapitel 2.2 durch IT-Grundschutz-Bausteine abgebildet sind. Wenn für die hinreichende Absicherung eines Zielobjekts die vorhandenen IT-Grundschutz-Bausteine nicht ausreichen, ist dies ebenfalls zu vermerken.

Werkzeuge zum IT-Grundschutz wie das GSTOOL unterstützen die Modellierung, indem sie für den betrachteten Informationsverbund und die mit ihm verknüpften Zielobjekte Vorschläge für die anzuwendenden Bausteine liefern. Das GSTOOL ermöglicht es beispielsweise auch, Problemebereiche und technische Systeme zu modellieren, die keine ausreichende Entsprechung in den [GSK] haben. Zu diesem Zweck können vorhandene Bausteine angepasst sowie neue, benutzerdefinierte Bausteine angelegt werden.

7.2 Besonderheiten und Probleme

Kapitel 2.2 der IT-Grundschutz-Kataloge enthält detaillierte Hinweise dazu, welche Bausteine auf einen Informationsverbund und seine unterschiedlichen Zielobjekte anzuwenden sind. Im Allgemeinen sind diese Empfehlungen einfach umzusetzen. Besonderheiten und Probleme ergeben sich immer dann, wenn für einen Zielobjekttyp Bausteine fehlen oder die angebotenen nicht vollständig zu passen scheinen.

Nachfolgend wird mit Hilfe ausgewählter Bausteine am Beispiel der RECPLAST GmbH auf einige wichtige Aspekte eingegangen, die bei der Modellierung gemäß IT-Grundschutz zu berücksichtigen sind.

Sachverhalte sind übergeordnet geregelt

Wenn wie bei der RECPLAST GmbH der betrachtete Informationsverbund nicht das gesamte Unternehmen, sondern nur einen Ausschnitt daraus umfasst, bedeutet dies nicht, dass für diesen Ausschnitt Regelungen gelten müssen, die sich von denen für das gesamte Unternehmen unterscheiden. Dies gilt insbesondere für die Bausteine der Schicht 1. Dazu gehören die in B 1.0 *Sicherheitsmanagement* beschriebenen grundlegenden Maßnahmen zum Aufbau einer Sicherheitsorganisation oder die übergreifenden Regelungen zu speziellen technischen und organisatorischen Problembereichen, etwa zum Schutz vor Schadsoft-

ware (in B 1.6 *Computer-Virenschutzkonzept*) oder zur Schulung und Sensibilisierung der Benutzer (in B 1.13 *IT-Sicherheitssensibilisierung und -schulung*).

Das Sicherheitsmanagement-Team der RECPLAST GmbH entscheidet sich daher dazu, bei der Anwendung der Bausteine der Schicht 1 darauf zu achten, dass die jeweils angesprochenen Sachverhalte möglichst unternehmensweit geregelt sind, und dass besondere Regelungen für die Betriebsstätte in Bonn-Beuel nur für spezielle Sachverhalte gelten sollen.

Besondere Einsatzbedingungen: Virenschutz

Eine dieser Besonderheiten ist der Schutz vor Schadsoftware. Das zentrale Virenschutz-Konzept der RECPLAST GmbH sieht vor, dass die in das Unternehmensnetz eingebundenen Client-PCs automatisiert und durch zentrale Systemrichtlinien erzwungen mit einer jeweils aktuellen Version der Virenschutz-Software und seiner Datenbasis (Virendefinitionen) ausgestattet werden. Dieses Verfahren verbietet sich bei den PCs zur Anlagensteuerung und -kontrolle, da jegliche Veränderung, also auch eine Aktualisierung seines Virenschutzes, ein Problem für die Funktionsfähigkeit dieser wichtigen IT-Systeme sein kann.

Gleichwohl sollte der Schutz vor Schadsoftware nicht vernachlässigt werden, zumal die PCs vernetzt sind, von außen gewartet werden und Betriebssysteme verwenden, die von Schadsoftware betroffen sein können. Das Sicherheitsmanagement-Team entscheidet sich daher dafür, spezielle Lösungen für den Virenschutz zu suchen und das vorhandene Konzept zum Schutz vor Schadsoftware um die gefundenen Lösungen zu ergänzen.

Als erschwerender Faktor kommt hinzu, dass für den mit Windows 98 betriebenen PC zur Steuerung und Kontrolle der Recyclinganlage keine angemessene aktuelle Schutzsoftware angeboten wird. Für den Leitrechner der Spritzgussanlagen sind zwar Virenschutzlösungen erhältlich, die möglichen Kosten eines Ausfalls der Produktionsanlage, zum Beispiel aufgrund fehlerhafter Updates dieser Software, werden jedoch als so hoch angesehen, dass auch für dieses IT-System alternative Lösungen zum Schutz vor Schadsoftware vorgezogen werden.

Besondere Einsatzbedingungen: Belastungen durch Umgebungseinflüsse

Auch andere, in Büroumgebungen selbstverständliche Anforderungen lassen sich in Produktionsbereichen nicht vollständig umsetzen. So sollten IT-Systeme üblicherweise so aufgestellt werden, dass schädigende Umgebungseinflüsse minimiert sind. Im Produktionsumfeld müssen jedoch höhere Belastungen in Kauf genommen werden, etwa durch Staub, Erschütterung, Luftfeuchtigkeit oder störende Magnetfelder. IT-Systeme, die in solch problematischen Umgebungen betrieben werden, müssen auf diese Belastungen hin ausgerichtet sein. Dies ist bereits bei der Beschaffung der Geräte zu berücksichtigen. Um dieser Anforderung gerecht zu werden, entscheidet man sich in der RECPLAST GmbH dazu, zu prüfen, ob der Baustein B 1.9 *Hard- und Software-Management* um eine zusätzliche, benutzerdefinierte Maßnahme *Auswahlkriterien für die Beschaffung*

eines geeigneten Industrie-PCs zu ergänzen ist. In vergleichbarer Weise soll geprüft werden, ob die Bausteine zur Verkabelung (B 2.2 *Elektrotechnische Verkabelung* und B 2.12 *IT-Verkabelung*) auch den speziellen Anforderungen industrieller Umgebungen gerecht werden können oder ergänzt werden müssen.

Modellierung der räumlichen Gegebenheiten

Eine weitere Frage, die das Sicherheitsmanagement-Team der RECPLAST GmbH bei der Entwicklung des Sicherheitskonzepts beantworten will, ist die danach, inwieweit die in [GSK] vorhandenen Bausteine B 2.3 *Gebäude* sowie zu den verschiedenen Arten von Räumen (beispielsweise B 2.3 *Büroraum*, B 2.4 *Serverraum* oder B 2.6 *Raum für technische Infrastruktur*) den Sicherheitsanforderungen in Produktions- und Lagerhallen gerecht werden können. Ein Merkmal dieser Hallen ist, dass sie offener gehalten sind als Büroräume und der Zutritt im Prinzip jedem Betriebsangehörigen problemlos möglich ist. Aber auch Externe, etwa Fahrer bei der Anlieferung oder Abholung von Gütern, haben Zutritt zu diesen Hallen. Diese vergleichsweise große Offenheit steht in einem gewissen Kontrast zu dem teilweise hohen Schutzbedarf der dort befindlichen IT-Systeme.

Das Team entscheidet sich dafür, in einer ergänzenden Sicherheitsanalyse die Notwendigkeit eines eigenen Bausteins *Produktions- und Lagerhalle* zu prüfen und dazu die Bausteine auszuwerten, die in [GSK] zu den räumlichen Gegebenheiten enthalten sind.

Fernwartung durch Externe

Eine längere Diskussion gibt es über die Anwendung des Baustein B 1.11 *Outsourcing*, der sich mit den Sicherheitsaspekten von ausgelagerten Geschäfts- und Produktionsprozessen befasst. Es wird die Frage aufgeworfen, ob dieser Baustein anzuwenden ist, weil die Software der Spritzgussanlagen sowie der Recyclinganlage von deren jeweiligen Herstellern gewartet wird und nicht von Mitarbeitern der RECPLAST GmbH. Zu diesem Zweck haben die Anlagen Fernwartungszugänge, die in unregelmäßigen Abständen für die Techniker der Anlagenhersteller geöffnet werden, zum Beispiel um die Steuerungssoftware zu aktualisieren. Letztlich wird die Frage, ob der Baustein B 1.11 *Outsourcing* anzuwenden ist, jedoch verneint, da man der Meinung ist, dass

- die Wartung einer Anlage kein eigenständiger Geschäftsprozess, sondern nur eine vergleichsweise kleine, wenn auch wichtige Teilaktivität darstellt,
- die Arbeiten nicht selbsttätig ausgeführt werden, sondern nur nach Freigabe und unter Kontrolle von Mitarbeitern der IT-Administration des eigenen Unternehmens,
- die von dieser Fernwartung adressierten Sicherheitsaspekte in anderen Bausteinen zusammengenommen hinreichend behandelt werden, beispielsweise in

- B 1.1 *Organisation* mit der Maßnahme M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*,
- B 1.9 *Hard- und Software-Management* mit der Maßnahme M 5.87 *Vereinbarung über die Anbindung an Netze Dritter* sowie
- B 4.4 *Remote Access Dienste*.

Das Sicherheitsmanagement-Team entscheidet sich daher dafür, den Baustein B 1.11 *Outsourcing* nicht in das IT-Grundschutz-Modell des Informationsverbunds aufzunehmen.

Bausteine der Schicht 5: Anwendungen

Zum Schutz einiger wesentlicher und häufig vorkommender Anwendungen gibt es in Schicht 5 geeignete Bausteine. Für den betrachteten Informationsverbund, die Betriebsstätte Bonn-Beuel der RECPLAST GmbH, sind davon die folgenden Bausteine relevant:

- der Baustein B 5.3 *E-Mail*, wobei die Betriebsstätte in das umfassende E-Mail-System des Unternehmens eingebunden ist, die beschriebenen Regelungen und technischen Vorkehrungen folglich nicht nur für das Werk in Bonn-Beuel gelten,
- ergänzend dazu der Baustein B 5.12 *Exchange 2000 / Outlook 2000*, da diese Software im Betrieb eingesetzt wird, wenn auch in einer neueren Version,
- der Baustein B 5.7 *Datenbanken* für die datenbankbasierte ERP-Software des Unternehmens,
- der Baustein B 5.8 *Telearbeit* für den auch außerhäusig und im privaten Umfeld für betriebliche Zwecke verwendeten Laptop des Betriebsleiters,
- der Baustein B 5.14 *Mobile Datenträger* anwendungsübergreifend für den gesamten Informationsverbund, da USB-Sticks, CDs, DVDs und andere Arten mobiler Datenträger an vielen Stellen des Betriebs und für unterschiedliche Zwecke im Einsatz sind.

Das Sicherheitsmanagement-Team entscheidet sich darüber hinaus dafür, in einer ergänzenden Sicherheitsanalyse (siehe Kapitel 9) zu prüfen, ob zur Sicherheit der folgenden Anwendungen zusätzliche Untersuchungen notwendig sind:

- die **Steuerungssoftware** für die Recycling- und Spritzgussanlagen, da zwar einzelne Aspekte zur Sicherheit dieser Software in verschiedenen anderen Bausteinen erfasst werden, beispielsweise B 1.6 *Computer-Viren-Schutzkonzept*, aber in [GSK] kein Baustein explizit der Anlagensteuerung und -kontrolle gewidmet ist,
- die **RFID-gestützte Lagerverwaltung**, die nur partiell (etwa durch den Baustein B 4.6 *WLAN* für das für die genutzte Datenübertragungstechnik oder den Baustein B 5.7 *Datenbanken*) durch einen entsprechenden Baustein abgebildet

werden kann, nicht aber in solch wesentlichen Teilen wie den Risiken der eingesetzten RFID-Technik.

Es wird erwogen, für beide Anwendungen gegebenenfalls eigene Bausteine anzulegen. Grundlage für diese Bausteine sollten herstellerspezifische Sicherheitshinweise sein, die durch Ergebnisse von Internet-Recherchen und die Auswertung von wichtigen themenbezogenen Publikationen ergänzt werden sollten, beispielsweise [RFID] zu den Sicherheitsaspekten dieser Funk-Chips.

8 Basis-Sicherheitscheck

Mit einem Basis-Sicherheitscheck können der Stand der Informationssicherheit in einem Unternehmen überprüft und Möglichkeiten identifiziert werden, diesen zu verbessern. Mittels Interviews und stichprobenartigen Kontrollen wird dazu in einem **Soll-Ist-Vergleich** untersucht, ob und inwieweit die technischen und organisatorischen Sicherheitsmaßnahmen umgesetzt sind, die in dem IT-Grundschutz-Modell des Informationsverbunds empfohlen werden.

8.1 Vorgehensweise

Zur **Vorbereitung** des Basis-Sicherheitschecks sind

- die im Unternehmen vorhandenen **Dokumente zu sichten**, in denen sicherheitsrelevante Sachverhalte dargestellt sind, beispielsweise Arbeitsanweisungen, Ablaufbeschreibungen oder Handbücher,
- **Gesprächspartner festzulegen**, die kompetent Auskunft zu den übergreifenden Regelungen und infrastrukturellen Gegebenheiten, den IT-Systemen und den zwischen ihnen vorhandenen Kommunikationsverbindungen sowie den Anwendungen im Informationsverbund geben können,
- gegebenenfalls **externe Stellen zu identifizieren**, die ergänzende Hinweise zum Umsetzungsstand der Maßnahmen liefern können, beispielsweise die Hersteller dazu, wie sie ihre Wartungsarbeiten an den Fertigungsanlagen absichern,
- mit den ausgewählten Ansprechpartnern **Termine abzustimmen** und
- **Befragungsteams zusammenzustellen**.

Die **Interviews**, in denen mit den ausgewählten Gesprächspartnern der Umsetzungsstand der Maßnahmenempfehlungen der [GSK] für die betrachteten Zielobjekte ermittelt wird, sollten in einer entspannten, sachbezogenen Atmosphäre stattfinden. Bei Bedarf können die Befragungen durch **Begehungen** zum Beispiel zu infrastrukturellen Sachverhalten wie dem Schutz vor unbefugtem Zutritt oder der Aufstellung von Servern und **stichprobenartige Kontrollen** etwa der Konfiguration eines IT-Systems ergänzt werden.

Als Ergebnis der Überprüfung einer Maßnahme kommen die folgenden Antworten infrage:

- **„entbehrlich“**, wenn eine Maßnahme nicht umgesetzt werden muss, entweder weil diese nicht relevant ist oder aber andere Maßnahmen für einen hinreichend wirksamen Schutz sorgen,
- **„ja“**, wenn eine Maßnahme vollständig, wirksam und angemessen umgesetzt ist,

- **„teilweise“**, wenn einzelne Empfehlungen einer Maßnahme nicht oder nur unvollständig umgesetzt sind,
- **„nein“**, wenn der größte Teil der Empfehlungen einer Maßnahme nicht oder nur unzureichend umgesetzt ist.

Ein Basis-Sicherheitscheck muss nachvollziehbar **dokumentiert** werden. Neben der Dokumentation der Einzelentscheidungen zu den verschiedenen Maßnahmen gehören dazu auch einige allgemeine Angaben: Wann fand die Befragung statt? Wer hat daran teilgenommen? Welche Zielobjekte waren Gegenstand? Welcher Baustein wurde betrachtet?

Sorgfältige Begründungen tragen zur Nachvollziehbarkeit der Entscheidungen und Feststellungen bei. Falls eine Maßnahme die Regelung eines Sachverhalts fordert, kann beispielsweise darauf verwiesen werden, in welcher Unternehmensrichtlinie dies erfolgt ist. Begründungen und zusätzliche Erläuterungen sind insbesondere dann erforderlich, wenn Maßnahmen nicht oder nur unvollständig umgesetzt sind. Warum wurde eine Maßnahme als entbehrlich eingestuft? Welche Ersatzmaßnahme wurde stattdessen eingeführt? Welche Teilempfehlungen einer Maßnahme sind umgesetzt und welche nicht? – diese Fragen müssen sich mit Hilfe der Dokumentation beantworten lassen.

Werkzeuge wie das GSTOOL erleichtern die Dokumentation des Basis-Sicherheitschecks. Als Hilfsmittel bietet das BSI außerdem zu jedem Baustein ein Formular an, mit dem für die zugehörigen Maßnahmen die Ergebnisse des Soll-Ist-Vergleichs tabellarisch erfasst werden können.

8.2 Besonderheiten und Probleme

Wie schon bei den vorangegangenen Schritten unterscheidet sich das Vorgehen in einem Produktionsunternehmen auch beim Basis-Sicherheitscheck nicht von dem bei einer beliebigen anderen Organisation. Die Besonderheiten ergeben sich aus Eigenheiten, die bei der Umsetzung von Maßnahmen zu berücksichtigen sind. In vielen Fällen sind die IT-Grundschutz-Maßnahmen so formuliert, dass sie auch auf die Bedingungen eines Produktionsunternehmens angewendet werden können und allenfalls vergleichsweise geringfügige Anpassungen oder Erweiterungen erforderlich sind. Dies wird nachfolgend anhand einiger ausgewählter Bausteine aus den Schichten 1 bis 4 der [GSK] erläutert.

Die Bausteine der Schicht 5 beschreiben anwendungsbezogene Sicherheitsmaßnahmen beispielsweise zu E-Mail, Datenbanken oder Datenträgeraustausch. Da die anwendungsbezogenen Bausteine im Grundschutz-Modell der RECPLAST GmbH nicht spezifisch für den Produktionsbereich sind, wird nachfolgend nicht auf den Basis-Sicherheitscheck zu den Bausteinen der Schicht 5 eingegangen.

8.2.1 Bausteine der Schicht 1: Übergreifende Aspekte

Baustein B 1.3 *Notfall-Vorsorgekonzept*

Die Maßnahmen dieses Bausteins sollen ein Unternehmen in die Lage versetzen, umgehend und adäquat auf Sicherheitsvorfälle, die zu schwerwiegenden Betriebsstörungen führen, reagieren zu können. Unterbrochene Geschäftsprozesse sollen möglichst schnell wiederaufgenommen und der entstandene Schaden in einem vertretbaren Ausmaß gehalten werden. Um diese Ziele erreichen zu können, ist es erforderlich, dass ein Unternehmen

- die Verfügbarkeitsanforderungen seiner Geschäftsprozesse und deren Abhängigkeiten untereinander sowie die von diesen benötigten Ressourcen (Personal, Infrastruktur, Technik, Informationen) untersucht,
- die Verantwortlichkeiten für Notfälle festlegt und
- Konzepte für die beim Eintritt eines Notfalls erforderlichen Handlungsschritte erarbeitet, dokumentiert und erprobt.

Ein Notfall-Vorsorgekonzept erfordert einen nicht unerheblichen Aufwand. Schon alleine aus Wirtschaftlichkeitserwägungen sollte bei der Entwicklung das Augenmerk auf Anwendungen und Systeme gelegt werden, die besonders hohen Verfügbarkeitsanforderungen unterliegen. Solche Systeme sind in einem Produktionsunternehmen in erster Linie die Fertigungsanlagen und andere unmittelbar mit der Produktion verknüpfte IT-Systeme.

Die Maßnahmen des Bausteins B 1.3 *Notfall-Vorsorgekonzept* werden im Basis-Sicherheitscheck der RECPLAST GmbH überwiegend als *umgesetzt* eingestuft. Hohe Verfügbarkeitsanforderungen stellen beispielsweise diejenigen Zielobjekte, die zur Steuerung der Fertigungsanlagen beitragen. Mögliche Maßnahmen zur Notfallvorsorge für derartige IT-Systeme sind etwa:

- sie regelmäßig warten zu lassen und deren korrektes Funktionieren kontinuierlich zu testen,
- eine Anlage zur unterbrechungsfreien Stromversorgung (USV) zur Überbrückung von Stromausfällen bereitzustellen,
- vollständige Ersatzsysteme oder zumindest wichtige Einzelkomponenten vorzuhalten,
- Pläne für einen manuellen Ersatzbetrieb bei einem völligen Ausfall der IT-Systeme zu entwickeln,
- Vereinbarungen mit den Lieferanten oder Herstellern der IT-Systeme zur kurzfristigen Bereitstellung von Ersatzsystemen abzuschließen.

Letzteres wird von den Verantwortlichen der RECPLAST GmbH als wesentliche Maßnahme für den Fall eines Ausfalls der Fertigungsanlagen bevorzugt. Daher enthalten die Verträge mit den Herstellern der Anlagen und den Lieferanten der zur ihrer Steuerung und Kontrolle eingesetzten Hardware und Software

Vereinbarungen über eine 24-stündige Rufbereitschaft zur Wartung der Geräte sowie die Verpflichtung zur kurzfristigen Lieferung von fehlerhaften Komponenten spätestens nach einem Werktag.

Alle vorhandenen sowie weitergehende Maßnahmen zur Notfall-Vorsorge, die auch solche Ereignisse berücksichtigen wie die vollständige Zerstörung einer Fertigungsanlage, plant die RECPLAST GmbH in einem umfassenden Konzept zum Notfall-Management mit Hilfe der in [BSI 100-4] empfohlenen Vorgehensweise zu entwickeln und zusammenzufassen – allerdings erst zu einem späteren Zeitpunkt nach der Umsetzung des in Arbeit befindlichen Sicherheitskonzepts.

Baustein B 1.6 *Computer-Virenschutz-Konzept*

Dieser Baustein enthält ein Maßnahmenbündel für ein systematisches Vorgehen zum Schutz gegen Schadsoftware. Es soll damit verhindert werden, dass ein Informationsverbund von Viren, Würmern oder Trojanischen Pferden befallen wird, beziehungsweise der mögliche Schaden begrenzt werden, falls es trotz aller Vorkehrungen zur Infiltration mit Schadsoftware kommt.

Ein effektiver Schutz vor Schadsoftware erfordert, dass

- die **verschiedenen Arten** berücksichtigt werden, in denen sie auftreten kann,
- alle **möglichen Einfallswege** identifiziert werden, über die sie sich verbreitet,
- sowohl **technische Vorkehrungen** als auch **organisatorische Regelungen** getroffen werden, um die möglicherweise betroffenen Systeme vor Schadsoftware zu schützen,
- die Schutzvorkehrungen **kontinuierlich aktualisiert** werden, da fast täglich neue Varianten von Schadsoftware auftreten.

Mit der vermehrten Verwendung von Standard-IT und deren zunehmender Vernetzung steigt auch die Wahrscheinlichkeit, dass die Informationstechnik im Produktionsbereich von Schadsoftware betroffen wird. Insofern wird auch hier der Virenschutz immer dringlicher – vor allem auch, weil der mögliche Schaden, den Schadsoftware etwa bei Leitrechnern in der Fertigung ausrichten kann, besonders hoch ist. Andererseits bereiten hier die üblichen Konzepte zum Virenschutz Probleme. Stand der Technik ist ein regelmäßig aktualisierter und zentral administrierter Virenschutz in Echtzeit auf allen potenziell von Schadsoftware betroffenen IT-Systemen. Dieses Verfahren lässt sich aber aus folgenden Gründen nicht unmittelbar auf alle IT-Systeme im Produktionsbereich übertragen:

- Üblicherweise werden Fertigungsanlagen gemeinsam mit der Steuerungssoftware von den Herstellern geliefert. Sicherheitsfunktionalitäten, dazu zählen auch Virenscanner, sind in diesem Paket nicht vorhanden und müssten nachträglich installiert werden. Eine solche Nachrüstung könnte aber gegebenenfalls unvereinbar mit den Haftungsregelungen und Service-Verpflichtungen des Anlagenherstellers sein.

- Virenschutz und insbesondere auch dessen automatische Aktualisierung vertragen sich nicht mit IT-Systemen, die Echtzeitanforderungen genügen müssen. Es ist offensichtlich problematisch, wenn ein Virenscanner Aktionen der Steuerungssoftware zum Beispiel zur Notabschaltung einer Fertigungsanlage unterbindet, oder aber ein nicht hinreichend getestetes Update des Scanners zu Funktionsstörungen in der Steuerungssoftware führt.
- Während normale Computer rund fünf Jahre im Einsatz sind, sind im Fertigungsbereich 15 bis 25 Jahre Einsatzdauer keine Seltenheit. Die Lebensdauer von Fertigungsanlagen übersteigt damit deutlich die von üblichen IT-Systemen. Dies bedeutet auch, dass unter Umständen für die Betriebssystemvariante eines Leitrechners in der Produktion kein aktueller Virenschutz mehr auf dem Markt angeboten wird.

Ein lokaler Virenschutz auf IT-Systemen für die Anlagensteuerung und -kontrolle ist daher auch dann problematisch, wenn er technisch möglich wäre. Da es jedoch auch nicht sinnvoll ist, auf jeglichen Schutz zu verzichten, müssen andere Mechanismen diese IT-Systeme hinreichend schützen. Eine Lösung kann darin bestehen, für einen entsprechenden Schutz nicht auf dem IT-System selber zu sorgen, sondern auf einem vorgelagerten System, das den Datenverkehr zu dem kritischen System kontrolliert.

Der Basis-Sicherheitscheck bei der RECPLAST GmbH ergibt, dass der Virenschutz im Unternehmen grundsätzlich den geltenden Standards entspricht: Auf den Servern und den Clients (mit Ausnahme der beiden Leitrechner C3 und C4) ist Schutzsoftware installiert, die jeglichen eingehenden Datenverkehr (Dateien, E-Mails, Webseiten) auf Schadfunktionen hin untersucht und mindestens täglich aktualisiert wird. Auch die PCs auf den Gabelstaplern sind über eine Spezialversion der unternehmensweit eingesetzten Anti-Virensoftware ausreichend geschützt. Da auf den Leitrechnern für die Recycling- und Spritzgussanlagen jedoch jeglicher Virenschutz fehlt, werden Maßnahmen wie

- M 2.156 *Auswahl einer geeigneten Computer-Virenschutz-Strategie* und
- M 4.3 *Regelmäßiger Einsatz eines Anti-Viren-Programms*

nur als *teilweise umgesetzt* bewertet.

Dies wird insbesondere auch deshalb als kritisch gesehen, weil diese IT-Systeme innerhalb des lokalen Netzes kein eigenes, geschütztes Segment bilden. Das Sicherheitsmanagement-Team der RECPLAST GmbH wird daher damit beauftragt, Vorschläge für einen besseren Schutz dieser IT-Systeme zu entwickeln.

Baustein B 1.9 *Hard- und Software-Management*

Dieser Baustein enthält grundlegende Regelungen für einen ordnungsgemäßen und sicherheitsgerechten Betrieb von Hardware- und Software-Komponenten während ihres gesamten Lebenszyklus. In ihm werden diejenigen übergreifenden Sicherheitsaspekte behandelt, die für alle Arten von IT-Systemen und Anwendungen gleichermaßen gelten.

Einer dieser Aspekte ist es dafür zu sorgen, dass nur **Berechtigte** und nur im Rahmen ihrer Berechtigung **Zugriffsmöglichkeiten** auf ein IT-System und die dort gespeicherten Informationen haben. Dazu ist es beispielsweise erforderlich, bei der Planung und Konzeption des IT-Betriebs

- Vorgaben für die Einrichtung von Benutzern und Benutzergruppen zu entwickeln (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*),
- die Zugriffs- und Zugangskontrolle zu regeln (M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*) und
- passende Authentikationsmechanismen auszuwählen (siehe M 4.133 *Geeignete Auswahl von Authentikationsmechanismen*) sowie
- den Umgang mit Fremdpersonal zu klären (siehe M 2.226 *Regelungen für den Einsatz von Fremdpersonal*).

Bei der RECPLAST GmbH werden diesbezügliche allgemeine Regelungen für den IT-Betrieb aufgestellt. Auf der Grundlage dieser Vorgaben ist die IT-Administration beispielsweise bestrebt, Berechtigungen zur Nutzung der IT-Systeme lediglich einzuräumen, soweit dies von den Arbeitsaufgaben her erforderlich ist und unbefugte Zugriffe durch zentrale Systemrichtlinien zu erschweren.

Diskussionen gibt es im Sicherheitsmanagement-Team um die Frage, wie die in den offenen Hallenbereichen aufgestellten IT-Systeme gegen unberechtigte Zugriffe zu schützen sind, zumal sich häufig auch betriebsfremde Personen in den Fertigungs- und Lagerhallen aufhalten, insbesondere Wartungstechniker für die Maschinen und Automaten aber auch Fahrer von anliefernden und abholenden Lieferfahrzeugen. Im Einzelnen sind dazu bereits vor der Durchführung des Basis-Sicherheitschecks die folgenden Regelungen getroffen worden:

- Die beiden **PCs in den Lagern** sind so eingerichtet, dass außer der Gruppe der Administratoren nur eine zweite Benutzergruppe („Lagermitarbeiter“) mit stark eingeschränkten Rechten zugriffsberechtigt ist. Mitglieder dieser Gruppe können den PC nur für den Zugriff auf die Lagerverwaltungssoftware nutzen und müssen sich dazu vorher mit Benutzernamen und Passwort authentisieren. Die PCs werden nur sporadisch benötigt. Daher werden sie automatisch gesperrt, wenn sie zwei Minuten lang nicht benutzt werden. Gleiches gilt für den Zugriff auf die ERP-Software.
- Als problematischer wird der Zugriffsschutz auf die **Leitrechner für die Recycling- und Spritzgussanlagen** angesehen. Auch auf diesen IT-Systemen wurden entsprechend den Erfordernissen eingeschränkte Benutzergruppen eingerichtet und die Zugriffsmöglichkeit an eine Authentisierung mittels Benutzerkennung und Passwort gekoppelt. Das zuständige Personal muss jedoch ständig auf die Software zugreifen sowie auf dem Bildschirm angezeigte Statusinformationen einsehen können. Daher verbietet sich eine automatische Sperrung des IT-Systems und zwar unabhängig davon, wie lange es nicht mehr aktiv benutzt wurde. Im Unterschied zu den PCs in den Lager-

hallen sind die Leitrechnern jedoch kontinuierlich vom zuständigen Personal zu überwachen, um Funktionsstörungen der Anlagen erkennen und umgehend auf diese reagieren zu können. Diese Vorschrift ist Bestandteil der Arbeitsanweisungen für den Betrieb der Anlagen.

Die oben erwähnten Maßnahmen werden im Basis-Sicherheitscheck daher für diese IT-Systeme als *umgesetzt* bewertet. Aufgrund des höheren Schutzbedarfs der beiden PCs zur Anlagensteuerung und -kontrolle sieht das Sicherheitsmanagement-Team jedoch grundsätzlich den Bedarf nach stärkeren Authentisierungstechniken für beide IT-Systeme. Es entschließt sich daher dazu, Alternativen zu prüfen, beispielsweise Chipkarten oder biometrische Verfahren.

Baustein B 1.14 *Patch- und Änderungsmanagement*

Viele Sicherheitslücken und Funktionsstörungen von Anwendungen, IT-Systemen oder Kommunikationsnetzen beruhen auf Mängeln oder Fehlern in der eingesetzten Software. Daher gehört es zu den wichtigen Aufgaben der IT-Administration, die installierte Software regelmäßig zu aktualisieren, denn neue Versionen versprechen neben der Bereitstellung zusätzlicher Funktionen immer auch die Behebung vorhandener und bekannt gewordener Schwachstellen. Insbesondere sollten *Patches*, *Hotfixes* oder *Service Packs*, die darauf abzielen, Sicherheitslücken zu schließen, unverzüglich eingespielt werden, zumal das Zeitfenster zwischen dem Bekanntwerden einer Schwachstelle und deren Ausnutzung immer geringer wird.

Zwar gehört die regelmäßige Aktualisierung der installierten Software zu den elementaren Sicherheitsmaßnahmen. Dies kann jedoch unter Umständen auch zu unvorhergesehenen Funktionsstörungen eines IT-Systems führen. Daher sollte die vorhandene Software immer erst nach ausreichenden Tests und in Abstimmung mit den Verantwortlichen für die jeweils betroffenen Geschäftsprozesse geändert werden.

Der Baustein B 1.14 *Patch- und Änderungsmanagement* enthält Empfehlungen für ein systematisches und auf die Erfordernisse der jeweiligen Organisation hin zugeschnittenes Vorgehen. Die Gesamtheit der dort beschriebenen Maßnahmen kann in der Regel zwar nur bei größeren Informationsverbünden umgesetzt werden, jedoch erhalten auch kleine Unternehmen Hinweise dazu, worauf sie bei der Aktualisierung ihrer Software achten müssen.

In der RECPAST GmbH wird detailliert in einem Software-Inventar dokumentiert, welche Software eingesetzt wird, welchen Versionsstand diese hat sowie wie viele Lizenzen verfügbar sind. Für die Führung dieses Verzeichnisses ist die IT-Administration zuständig. Ferner ist auf den IT-Systemen des Informationsverbunds nur solche Software zugelassen, die von den betroffenen Abteilungsleitern und der IT-Administration (sowie im Konfliktfall der Geschäftsführung) gemeinsam freigegeben wurde. Vor Erteilung einer Freigabe sind Tests erforderlich, deren Ausrichtung und Umfang sich nach der Art der zu prüfenden Software richtet. Sowohl die Verteilung von Patches und neuen Versionen einer Software an die Clients und Server des Netzes als auch die

Inventarisierung der vorhandenen Software wird mit Hilfe entsprechender Softwarewerkezuge weitgehend automatisiert durchgeführt.

Bei der Verteilung der eingesetzten Software muss auch auf die speziellen Anforderungen einzelner IT-Systeme eingegangen werden. So ist es aus verschiedenen Gründen nicht möglich, die Leitrechner für die Anlagensteuerung und -kontrolle in die automatisierte Software-Verteilung zu integrieren.

- Ein spezielles, wenngleich bei derartigen Systemen nicht seltenes Problem besteht darin, dass die beiden zur Anlagensteuerung und -kontrolle eingesetzten PCs mit älteren Betriebssystemversionen ausgestattet sind, für die keine weiteren Sicherheitspatches mehr entwickelt werden. Ein aktuelles Betriebssystem zu installieren ist nicht möglich, da die Anlagensoftware auf neueren Betriebssystemen nicht lauffähig ist.
- Grundsätzlich verbietet es sich, die Software von Produktionsanlagen nach einem festen Zeitschema (etwa jeden dritten Dienstag eines Monats spätestens um 11.00 Uhr) zu aktualisieren, weil dies zu kostspieligen Unterbrechungen eines IT-Systems und damit von Fertigungsprozessen führen kann.
- Aufgrund der mit den Herstellern geschlossenen Wartungsverträge ist es zudem auch nicht zulässig, die Software eigenmächtig ohne Rücksprache mit den Herstellern durch die unternehmenseigene IT-Administration zu aktualisieren.
- Des Weiteren kommt hinzu, dass keine Änderungen an der Software – auch nicht das Einspielen von Patches zum Betriebssystem – vorgenommen werden sollten, solange nicht sichergestellt ist, dass die Steuerungssoftware anschließend noch einwandfrei funktioniert.

Die relevanten Anforderungen der Maßnahmen des Bausteins B 1.14 *Patch- und Änderungsmanagement* werden im Basis-Sicherheitscheck damit zwar weitgehend als umgesetzt bewertet. Dennoch offenbart sich – wie schon beim Baustein B 1.6 *Computer-Virenschutz-Konzept* – auch hier ein Handlungsbedarf aufgrund der ungeschützten PCs zur Steuerung und Kontrolle der Recycling- und Spritzgussanlagen. Beide Rechner sind einem erhöhten Angriffsrisiko ausgesetzt.

8.2.2 Bausteine der Schicht 2: Infrastruktur

B 2.1 *Gebäude*

Der Baustein B 2.1 *Gebäude* enthält Maßnahmen, die dazu dienen, dem Schutzbedarf der Informationstechnik angemessene räumliche Bedingungen zu schaffen. Die Maßnahmen sollen ein Gebäude gegen physische Schäden aufgrund von Feuer, Wasser oder Blitzschlag sichern, dafür sorgen, dass nur befugte Personen Zutritt zu schützenswerter Informationstechnik und vertraulichen Informationen haben und gegen vorsätzliche Handlungen wie Diebstahl oder Vandalismus schützen.

Wichtige Aspekte, die in diesem Baustein berücksichtigt werden, sind

- das **Bauwerk** selber, also dessen Wände, Decken, Böden, Dach sowie Fenster und Türen,
- die gebäudeweiten **Versorgungseinrichtungen** (Strom, Wasser, Heizung etc.) sowie
- die **Aufteilung der Nutzungen** auf ein Gebäude.

Insgesamt ist der Bereich der Gebäudesicherheit ein stark geregelter Bereich: Neben den Anforderungen der Informationssicherheit sind hier weitere Vorschriften zu beachten, beispielsweise gesetzliche Auflagen zur Arbeitssicherheit oder zum Brandschutz, sowie technische Richtlinien, etwa des Deutschen Instituts für Normung (DIN), des Verbands der Elektrotechnik, Elektronik und Informationstechnik (VDE) oder des Verbands deutscher Maschinen- und Anlagenbau (VDMA). Die Einhaltung dieser Vorschriften, insbesondere solchen zum Brandschutz und zur Arbeitssicherheit, wird auch durch dafür zuständige Einrichtungen überprüft (Feuerwehr, Berufsgenossenschaft).

Bei den gebäudebezogenen Maßnahmen zur Informationssicherheit empfiehlt sich eine enge Zusammenarbeit mit anderen verantwortlichen Mitarbeitern, beispielsweise den Beauftragten für Arbeitssicherheit und Brandschutz. Dies kann auch dazu beitragen, mögliche Zielkonflikte zu vermeiden, beispielsweise zwischen Zugangsschutz (Absperren von Gebäudeteilen) und vorbeugendem Brandschutz (Freihalten von Fluchtwegen).

Der Idealzustand ist, dass die aus Sicht der Informationssicherheit erforderlichen Maßnahmen bereits bei der Planung eines Gebäudes ausreichend berücksichtigt werden. Dies ist in der Praxis allerdings oft nicht gegeben, insbesondere bei alten und zu anderen Zwecken errichteten Gebäuden, so dass für eine sicherheitsgerechte Ausgestaltung gegebenenfalls sehr aufwändige und kostspielige Umbauten erforderlich sind oder Kompromisslösungen in Kauf genommen werden müssen.

Dies gilt auch für die zu einem zusammenhängenden Gebäudekomplex verbundenen und daher als ein einziges Gebäude behandelten Hallen der RECPLAST GmbH. So empfiehlt die Maßnahmen M 1.13 *Anordnung schützenswerter Gebäudeteile*, dass Räume oder Gebäudeteile, die höhere Sicherheitsanforderungen stellen, nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein sollen. Kritisch sind beispielsweise

- Erdgeschossräume, die an öffentliche Verkehrsflächen grenzen, weil diese beispielsweise leichter zum Ziel von Anschlägen oder zum Opfer von Verkehrsunfällen werden können, sowie
- Räume unterhalb von Flachdächern, weil diese durch möglicherweise eindringendes Regenwasser gefährdet sind.

Ein Teil der Aspekte, die in dieser Maßnahme angesprochen werden, ist in den Räumen der RECPLAST GmbH erfüllt. So haben die Hallen zwar Flachdächer. Jedoch ist durch eingezogene Zwischendecken dafür gesorgt worden, dass die in den Räumlichkeiten der Entwicklungsabteilung und dem Serverraum befindlichen

IT-Systeme vor eindringendem Regenwasser geschützt sind. Aufgrund der Randlage des Serverraums und der Räumlichkeiten der Entwicklungsabteilung wird diese Maßnahme beim Basis-Sicherheitscheck jedoch insgesamt als *nicht umgesetzt* bewertet. Das Sicherheitsmanagement-Team wird damit beauftragt, verschiedene Alternativen für die Anordnung dieser Räumlichkeiten zu prüfen und dabei insbesondere auch auf die Wirtschaftlichkeit der einzelnen Varianten zu achten.

Längere Diskussionen gibt es auch um die Frage, wie gut die Anforderungen der Maßnahme M 2.17 *Zutrittsregelung und -kontrolle* im Unternehmen umgesetzt sind. Diese Maßnahme fordert, dass der **Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen** zu regeln und zu kontrollieren ist. Eine solche Regelung erfordert, dass

- der betroffene Bereich eindeutig bestimmt wird,
- nur diejenigen Personen zutrittsberechtigt sind, für die es eine Erfordernis gibt,
- unberechtigt sich in dem betreffenden Bereich aufhaltende Personen einfach als solche erkennbar sein müssen,
- bei Besuchern die Notwendigkeit des Zutritts geprüft werden muss,
- erteilte Zutrittsberechtigungen dokumentiert werden.

Im Prinzip sind diese Fragen in der Betriebsstätte in Bonn-Beuel geregelt. Zutritt zum Werksgelände haben nur Betriebsangehörige, die sich gegebenenfalls mit ihrem Werksausweis an der Pforte als solche ausweisen müssen, und Besucher, die sich an der Pforte angemeldet, ausgewiesen sowie den Grund ihres Besuchs und den verantwortlichen Ansprechpartner benannt haben. Die in den Büroräumen arbeitenden Mitarbeiter sind angehalten, die Räume abzuschließen, sobald sie nicht mehr besetzt sind.

Ein Problem stellen die offenen Hallenbereiche dar, in denen sich – wie schon zum Baustein B 1.9 *Hard- und Software-Management* angemerkt wurde – häufig auch betriebsfremde Personen aufhalten (z. B. Wartungstechniker und Fahrer von anliefernden und abholenden Lieferfahrzeugen). Das Sicherheitsmanagement-Team bewertet die Maßnahme M 2.17 *Zutrittsregelung und Kontrolle* trotz der Risiken, die sich aus der Anwesenheit von Betriebsfremden in den Fertigungs- und Lagerhallen ergeben können, als umgesetzt, da es eine Betriebsanweisung gibt, gemäß der betriebsfremde Personen (Besucher) verpflichtet sind, einen Besucherausweis deutlich erkennbar zu tragen, und sich in den Werkshallen nur in Begleitung aufhalten dürfen. Die Werksangehörigen müssen gemäß dieser Anweisung ihren Werksausweis ebenfalls sichtbar mit sich führen, so dass Besucher und Werksangehörige leicht voneinander unterschieden werden können.

Da sich zwei Mitglieder des Sicherheitsmanagement-Teams jedoch daran erinnern, dass sie in den zurückliegenden Monaten zwei- bis dreimal Betriebsfremde in den Hallen unbeaufsichtigt angetroffen haben, wird beschlossen, dass

die Mitarbeiter von der Unternehmensleitung in einem Rundschreiben nochmals auf die geltenden Regelungen hingewiesen werden sollen.

B 2.2 *Elektrotechnische Verkabelung* und B 2.12 *IT-Verkabelung*

Die beiden Bausteine enthalten Maßnahmen für eine sichere elektro- und informationstechnische Verkabelung. Beide Verkabelungsarten müssen hinreichend leistungsfähig und gegen Missbrauch sowie beabsichtigte oder unbeabsichtigte Beschädigungen geschützt verlegt sein. Neben anderen Maßnahmen ist es dazu auch erforderlich, solche Kabeltypen, auszuwählen, die an die jeweiligen Umgebungsbedingungen angepasst sind. Dazu enthält die Maßnahme M 1.20 *Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht* Empfehlungen. Außerdem ist es wichtig, dass die Arbeiten zur Verkabelung die einschlägigen Normen und Vorschriften befolgen und fachmännisch ausgeführt werden. Bei der IT-Verkabelung ist zusätzlich noch auf deren Abhörsicherheit zu achten.

Beim Basis-Sicherheitscheck ist festgestellt worden, dass in der RECPLAST GmbH die Maßnahmenempfehlungen beider Bausteine weitgehend umgesetzt sind. Sowohl die elektrotechnische Verkabelung als auch die IT-Verkabelung in der RECPLAST GmbH wurde mit Hilfe von Mitarbeitern der Haustechnik entworfen und von Fachfirmen ausgeführt und dokumentiert. Die ausgewählten Kabel und deren Führung werden daher den speziellen Anforderungen in den Fertigungs- und Lagerhallen der Betriebsstätte in Bonn-Beuel gerecht. So werden grundsätzlich alle Kabel geordnet in Kabeltrassen und überwiegend in Deckenbereichen sowie gegen Brände abgeschottet und nicht in unmittelbarer Nähe zu Wasserleitungen geführt. Verteiler und Netzkopplungsgeräte sind in Schutzschränken untergebracht, um sie gegen nicht autorisierte Zugriffe zu sichern. Die IT-Verkabelung in den Fertigungshallen und Lagerhallen entspricht der Norm [ISO 24702] an die Verkabelung in industriellen Umgebungen. Die beteiligten Komponenten zeichnen sich durch eine hohe mechanische Stabilität und Temperaturunempfindlichkeit und elektromagnetische Verträglichkeit aus.

8.2.3 Bausteine der Schicht 3: IT-Systeme

B 3.201 *Allgemeiner Client*

Die Maßnahmen dieses Bausteins gelten für alle IT-Systeme, die (zumindest zeitweise) als Client in einem Client-Server-Netz betrieben werden, unabhängig von deren Betriebssystem, den integrierten Netzschnittstellen und zugeordneten Peripheriegeräten. Der Baustein ist für jedes Zielobjekt beziehungsweise jede Gruppe von Zielobjekten gesondert anzuwenden. Die Maßnahmen müssen ferner durch die in anderen Bausteinen enthaltenen betriebssystemspezifischen Maßnahmen ergänzt werden.

Wichtige Maßnahmen des Bausteins sind beispielsweise:

- M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates,*
- M 3.18 *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung,*
- M 4.2 *Bildschirmsperre,*
- M 4.3 *Regelmäßiger Einsatz eines Anti-Viren-Programms,*
- M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme.*

Diese Übersicht zeigt, dass eine Reihe von Maßnahmen, deren Umsetzung für „normale“ Clients selbstverständlich zu sein scheint, bei den Leitrechnern für Fertigungsanlagen problematisch ist:

- Wie dargestellt, ist birgt ein zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (M 2.273) die Gefahr von Funktionsstörungen und ist auf vielen derartigen IT-Systemen darüber hinaus auch nicht möglich. Gleiches gilt für die Anforderung, regelmäßig ein Anti-Viren-Programm einzusetzen (M 4.3), sowie für eine Reihe der Empfehlungen zum Einsatz angemessener Sicherheitsprodukte für IT-Systeme (M 4.41).
- Die automatische oder manuelle Aktivierung einer Bildschirmsperre (M 4.2) verbietet sich, da die Kontrollinformationen und gegebenenfalls Warnhinweise jederzeit und unmittelbar einsehbar sein müssen.
- Es ist zwar sinnvoll, dass auch auf solchen Systemen Benutzer oder Benutzergruppen gemäß ihrer Berechtigungen unterschieden und insbesondere Administrator-Rollen herausgehoben werden. Oftmals besteht jedoch die Situation, dass ein Steuerungsprogramm von mehreren gleichberechtigten Benutzern bedient werden muss. Es ist in solchen Fällen wenig zweckmäßig, wenn ein einzelner Benutzer sich vom IT-System abmeldet (M 3.18), da er damit unter Umständen den erforderlichen raschen Zugriff eines anderen Benutzers erschwert.

Während die Empfehlungen des Bausteins für die meisten betrachteten Zielobjekte bei der RECPLAST GmbH überwiegend als *umgesetzt* bewertet werden, verbieten sich solche Einstufungen für die angeführten Maßnahmen bei den Leitrechnern für die Recycling- und Spritzgussanlagen. Während die anderen oben erwähnten Maßnahmen ohne Diskussion als *nicht umgesetzt* bewertet werden, gibt es im Sicherheitsmanagement-Team unterschiedliche Meinungen darüber, ob die Maßnahme M 4.2 *Bildschirmsperre* als *nicht umgesetzt* oder *entbehrlich* eingestuft werden soll. Man einigt sich schließlich darauf, sie als *nicht umgesetzt* zu bewerten – und zwar mit folgender Begründung:

Sinn der Maßnahme ist es, nicht autorisierte Zugriffe auf ein IT-System zu verhindern und gegebenenfalls die Vertraulichkeit der auf dem Bildschirm einsehbaren Informationen zu schützen. Diese Schutzziele werden nicht dadurch irrelevant, dass die Maßnahme aus anderen Gründen unzweckmäßig ist. Die Einstufung als *nicht umgesetzt* weist – anders als die Einstufung als *entbehrlich* – auch darauf hin, dass nach anderen Möglichkeiten gesucht werden muss, um unberechtigte Zugriffe auf die betreffenden IT-Systeme zu verhindern.

Maßnahmen sind entbehrlich, wenn sie keine Schutzwirkung entfalten oder aber die Schutzwirkung durch höherwertige Maßnahmen hinreichend gewährleistet ist. Unwirtschaftlichkeit oder Unzweckmäßigkeit sind hingegen Begründungen dafür, den Umsetzungsstand einer Maßnahme im Basis-Sicherheitscheck als *nicht umgesetzt* einzustufen.

8.2.4 Bausteine der Schicht 4: Netze

Die Bausteine dieser Schicht enthalten Maßnahmen zum Schutz der Kommunikationsverbindungen eines Informationsverbunds. Die Umsetzung der empfohlenen Maßnahmen trägt dazu bei, die Verfügbarkeit, Integrität und Vertraulichkeit der in einem Netz übertragenen Informationen zu wahren. Die Maßnahmen erschweren gleichzeitig, dass eine Kommunikationsverbindung zu einer Schwachstelle für die Sicherheit des gesamten Informationsverbunds wird.

B 4.1 *Heterogene Netze*

Zu den wesentlichen Aufgaben bei der Planung und dem Aufbau eines Netzes gehört es, dieses dem Schutzbedarf angemessen logisch und physisch zu segmentieren. Differenzierungen im Schutzbedarf in unterschiedlichen Teilen eines Netzes müssen sich auch in dessen Topographie und Topologie widerspiegeln. Insbesondere bei höherem Schutzbedarf empfiehlt es sich, ein Netz in einzelne Teilnetze aufzuteilen.

Der Basis-Sicherheitscheck bei der RECPLAST GmbH ergibt, dass in dieser Hinsicht das Netz in Bonn-Beuel deutliche Schwachstellen aufweist. Obwohl sich die angeschlossenen IT-Systeme zum Teil deutlich im Schutzbedarf unterscheiden, drückt sich dies nicht in der Struktur des Netzes aus, denn alle IT-Systeme sind an demselben Switch angeschlossen. Die im Baustein B 4.1 *Heterogene Netze* empfohlenen Maßnahmen

- M 5.77 *Bildung von Teilnetzen,*
- M 5.61 *Geeignete physikalische Segmentierung* und
- M 5.62 *Geeignete logische Segmentierung*

werden daher als *nicht umgesetzt* bewertet. Es wird beschlossen, das Netz zumindest mit Hilfe zusätzlicher Switches und am jeweiligen Schutzbedarf orientiert zu unterteilen. Die Netzadministration soll hierzu und gegebenenfalls weiteren zweckmäßigen Sicherheitsmaßnahmen einen Vorschlag ausarbeiten. Bei der Segmentierung sollen ferner die Empfehlungen der Bausteine B 3.301 *Sicherheitsgateway (Firewall)* und B 3.302 *Router und Switches* berücksichtigt werden. Ein wesentlicher Aspekt bei den Überlegungen zur Umstrukturierung des Netzes ist der Schutz der Anlagensteuerungen. Daher soll der Sicherheitsbedarf der beteiligten IT-Systeme in einer Risikoanalyse näher geprüft werden. Siehe dazu Kapitel 9 *Ergänzende Sicherheitsanalyse und Risikoanalyse*.

B 4.6 *WLAN*

Zu den Bausteinen aus der Schicht 4, die das Sicherheitsmanagement-Team der RECPLAST GmbH anzuwenden hat, gehört auch der Baustein B 4.6 *WLAN*. Zielobjekt ist das Funknetz, das für die Kommunikation zwischen der zentralen Lagerverwaltungssoftware und den PCs auf den Gabelstaplern eingerichtet wurde.

Die Maßnahmen des Bausteins zielen darauf ab, Funknetze nach den Standards IEEE 802.11 so zu betreiben, dass einerseits die Verfügbarkeit dieser Kommunikationsverbindungen gewährleistet ist, andererseits aber auch unerwünschte Zugriffe und das Eindringen in das Firmennetz unter Umgehung der Schutzsysteme über ein WLAN verhindert werden. Dazu sollte beispielsweise die Reichweite eines Funknetzes so gewählt werden, dass zwar die funktionalen Erfordernisse gewahrt bleiben, andererseits die Funkwellen jedoch möglichst wenig in Bereiche außerhalb des Unternehmens abstrahlen. Die IT-Systeme, mit deren Hilfe das Netz aufgebaut wird, sollten ferner so aufgestellt werden, dass Unbefugte keine Zugriffsmöglichkeiten auf die Geräte haben. Zu beiden Aspekten enthält die Maßnahme M 1.63 *Geeignete Aufstellung von Access Points* Empfehlungen.

Diese Maßnahme wird beim Basis-Sicherheitscheck in der RECPLAST GmbH als *nicht umgesetzt* bewertet, weil der Access Point in dem am Rande des Firmengeländes gelegenen Serverraum untergebracht ist. Zwar trägt dies dazu bei, den physischen Zugriff auf das Gerät auf dazu berechtigte Personen zu begrenzen, führt andererseits aber zu einer unnötig großen Ausbreitung der Funkwellen außerhalb des Firmengeländes. Der IT-Sicherheitsbeauftragte und der Leiter der Abteilung „Lager/Logistik“ sollen in einer gemeinsamen Begehung einen besser geeigneten Aufstellort in einer der Lagerhallen oder deren Umgebung suchen, außerdem Maßnahmen zum physischen Schutz des Access Points an seinem neuen Standort vorschlagen.

Nicht nur die physische Unterbringung des Access-Points wird als problematisch beurteilt, sondern – stärker noch – auch dessen Anbindung an das interne Netz. Die Anwendung „RFID-gestützte Lagerverwaltung“, für die das WLAN genutzt wird, setzt Zugriffe in das interne Firmennetz zwingend voraus. In Maßnahme M 5.139 *Sichere Anbindung eines WLANs an ein LAN* wird empfohlen, Zugriffe aus dem WLAN wie solche aus dem Internet zu behandeln und nur zuzulassen, wenn sie durch ein Sicherheitsgateway geschützt sind. Ein solcher Schutz fehlte jedoch in der vorhandenen Netzstruktur vollständig. Daher wird entschieden, auch diese Maßnahme als *nicht umgesetzt* zu bewerten. Das Sicherheitsmanagement-Team soll verschiedene Varianten zur Anbindung des WLANs prüfen. Angesichts des insgesamt hohen Schutzbedarfs des WLANs wird als Sofortmaßnahme beschlossen, den Access Point logisch und physisch vor den Router (N3) und nicht mehr hinter dem Switch (N1) zu platzieren (siehe Abbildung 6).

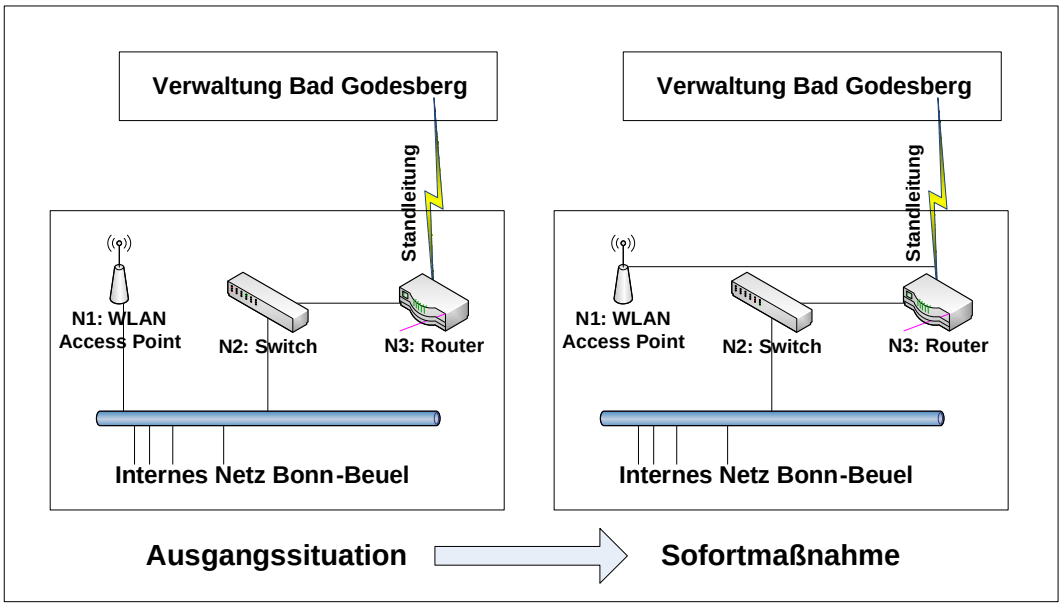


Abbildung 6: Geänderte WLAN-Anbindung als Sofortmaßnahme aufgrund des Basis-Sicherheitschecks

9 Ergänzende Sicherheitsanalyse und Risikoanalyse

Die Maßnahmen der [GSK] bieten für typische Geschäftsprozesse, Anwendungen und IT-Systeme, die in üblichen Einsatzumgebungen betrieben werden und einen normalen Schutzbedarf haben, eine angemessene Sicherheit. Für Zielobjekte, die diesen Kriterien nicht genügen, sind unter Umständen zusätzliche oder stärker wirksame Schutzmaßnahmen erforderlich. Deren Notwendigkeit ist in einer ergänzenden Sicherheitsanalyse und gegebenenfalls einer Risikoanalyse zu prüfen.

9.1 Vorgehensweise

Gemäß [BSI 100-2] wird in einer **ergänzenden Sicherheitsanalyse** geprüft, ob für einzelne Zielobjekte ein zusätzlicher Analysebedarf zur Auswahl stärker wirksamen Sicherheitsmaßnahmen besteht. Sie ist für alle Zielobjekte des Informationsverbundes durchzuführen,

- die einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- für die es keinen Baustein in den [GSK] gibt beziehungsweise die mit den Bausteinen der [GSK] nicht modellierbar sind oder
- die in Einsatzszenarien betrieben werden, die für den IT-Grundschutz untypisch sind.

Für jedes Zielobjekt, auf das eines dieser Kriterien zutrifft, muss in der ergänzenden Sicherheitsanalyse entschieden werden, ob weitere Risikobetrachtungen erforderlich sind oder nicht. Diese Festlegungen sind in einem **Management-Report** nachvollziehbar zu begründen. Dieser Bericht ist der Unternehmensleitung vorzulegen und von dieser zu verabschieden.

Eine **Risikoanalyse** hat die Aufgabe, relevante Gefährdungen zu identifizieren und deren Auswirkungen auf den Informationsverbund abzuschätzen, um eine Grundlage für die Entscheidungen zur Absicherung der betrachteten Zielobjekte zu erhalten. Es gibt zahlreiche Verfahren zur Durchführung solcher Untersuchungen. Besonders aufwändig, aber auch fehleranfällig, sind quantitative Risikoanalysen. Bei diesen wird versucht, Risiken anhand einer möglichst exakten Bestimmung von Eintrittswahrscheinlichkeiten von Schadensereignissen und dabei entstehenden Schadensausmaßen zu bewerten.

Die in [BSI 100-3] detailliert beschriebene **Risikoanalyse auf Basis von IT-Grundschutz** bietet eine vereinfachte Methode, bei der die in den Bausteinen der [GSK] enthaltenen Übersichten zur Gefährdungslage das wesentliche Hilfsmittel sind. Im Einzelnen wird in den folgenden Schritten vorgegangen (siehe auch Abbildung 4, Seite 25):

1. Erstellung der Gefährdungsübersicht
2. Ermittlung zusätzlicher Gefährdungen

3. Gefährdungsbewertung
4. Behandlung von Risiken
5. Konsolidierung des Sicherheitskonzepts

Diese Schritte werden im nächsten Kapitel anhand eines Beispiels aus dem Informationsverbund der RECPLAST GmbH erläutert. Bei dem in der Risikoanalyse betrachteten Zielobjekt handelt es sich um den PC zur Steuerung und Kontrolle der Spritzgussanlagen.

9.2 Besonderheiten und Probleme

Im betrachteten Informationsverbund der RECPLAST GmbH gibt es eine Reihe an Zielobjekten, auf die wenigstens eines der Kriterien zutrifft, die eine ergänzende Sicherheitsanalyse erforderlich machen:

- So haben viele Zielobjekte einen **hohen Schutzbedarf** in mindestens einem der drei Grundwerte Vertraulichkeit, Verfügbarkeit oder Integrität, beispielsweise
  - die Anwendungen A1 „Steuerung Recyclinganlage“, A2 „Steuerung Spritzgussanlagen“ und A7 „Entwicklung“,
  - die IT-Systeme S1 „Server ERP“, C3 „PC Steurung und Kontrolle Recyclinganlage“ und C4 „PC Steuerung und Kontrolle Spritzgussanlagen“,
  - die Produktions- und Lagerhallen aufgrund der in ihnen untergebrachten Informationstechnik sowie
  - verschiedene Kommunikationsverbindungen zwischen Computern und Netzkopplungskomponenten.
- Die beiden IT-Systeme C3 und C4 werden darüber hinaus aufgrund des industriellen Umfelds und der an sie geknüpften Echtzeitanforderungen in einer für den IT-Grundschutz eher **untypischen Einsatzumgebung** betrieben.
- Es gibt ebenfalls Zielobjekte, die **keinen hinreichend passenden Baustein** haben, etwa die Anwendung A4 „Lagerverwaltung“, die mit RFID eine Technik verwendet, die bislang in den [GSK] noch nicht behandelt wird.

Für alle Zielobjekte eine Risikoanalyse durchzuführen, hätte einen erheblichen Aufwand bedeutet. Daher wird zunächst geprüft, für welche Zielobjekte solche Bemühungen tatsächlich gerechtfertigt sind. Aufgrund des hohen Schutzbedarfs des Leitrechners zur Steuerung und Kontrolle der Spritzgussanlagen (Zielobjekt C4), entscheidet das Sicherheitsmanagement-Team sich dafür, dieses Zielobjekt einer Risikoanalyse zu unterziehen. Die Untersuchung soll insbesondere auch die Sicherheit der Schnittstellen und Kommunikationsbeziehungen zu diesem IT-System einbeziehen. Aufgrund der verwandten Problemstellung wird außerdem

überlegt, die Ergebnisse der Risikoanalyse auf das Zielobjekt C3, den PC zur Steuerung und Kontrolle der Recyclinganlage, zu übertragen.

Die getroffenen Entscheidungen dokumentiert das Sicherheitsmanagement-Team in einem Bericht, der von der Unternehmensleitung unterschrieben wird (siehe Anhang B.5).

Unter Umständen empfiehlt es sich, für mehrere Zielobjekte eine Risikoanalyse durchzuführen. In diesen Fällen ist es sinnvoll, zunächst die Sicherheit der Zielobjekte zu untersuchen, bei denen der zu erwartende Schaden bei einer Verletzung von Vertraulichkeit, Integrität oder Verfügbarkeit besonders hoch ist.

Erstellung der Gefährdungsübersicht

Ausgangspunkt für den ersten Schritt, die Erstellung der Gefährdungsübersicht, ist das Grundschutzmodell des Informationsverbunds. Aus diesem werden alle Zielobjekte gestrichen, die in der Risikoanalyse nicht berücksichtigt werden, anschließend alle Bausteine, für die es kein Zielobjekt mehr gibt. Die in den verbliebenen Bausteinen angeführten Gefährdungen werden anschließend zusammengestellt und thematisch sortiert, wobei gegebenenfalls doppelt vorkommende Gefährdungen gestrichen werden.

Die Gefährdungsübersicht für das betrachtete Zielobjekt C4 enthält folglich sowohl Gefährdungen, die in den direkt auf das Zielobjekt anzuwendenden Bausteinen B 3.201 *Allgemeiner Client* und B 3.205 *Client unter Windows NT* referenziert werden, als auch solche aus relevanten übergeordneten Bausteinen, beispielsweise B 1.9 *Hard- und Software-Management* und den meisten anderen Bausteinen der Schicht 1.

Für Auszüge aus dieser Gefährdungsübersicht und weiteren Dokumenten zur Risikoanalyse siehe Anhang B.6.

Ermittlung zusätzlicher Gefährdungen

Im nächsten Schritt, der Ermittlung zusätzlicher Gefährdungen, ist zu prüfen, ob weitere Gefährdungen zu berücksichtigen sind, die sich aus dem spezifischen Einsatzszenario des betrachteten Zielobjekts ergeben.

Zur Ermittlung zusätzlicher Gefährdungen empfiehlt sich ein Workshop, der vom IT-Sicherheitsbeauftragten oder einem anderen Sicherheitsexperten moderierter wird. Ferner können Quellen hilfreich sein wie Herstellerdokumentationen oder Publikationen im Internet. Auch die Gefährdungskataloge der [GSK] sollten durchgesehen werden, denn sie können relevante Gefährdungen enthalten, die bislang mit dem betrachteten Zielobjekt noch nicht verknüpft sind.

Es sollte ferner darauf geachtet werden,

- sich auf solche Gefährdungen zu konzentrieren, die Grundwerte bedrohen, in denen das betrachtete Zielobjekt einen hohen oder sehr hohen Schutzbedarf hat,
- alle Gefahrenbereiche zu berücksichtigen, also höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen von Außen- und Innentätern,
- unrealistische Gefährdungen und solche, die keinen nennenswerten Schaden verursachen, auszuschließen sowie
- die Gefährdungen angemessen zu verallgemeinern, um den Aufwand für die folgenden Schritte zu verringern.

Die Gefährdungsübersicht ist um die identifizierten Gefährdungen zu ergänzen.

In dem Workshop, den das Sicherheitsmanagement-Team der RECPLAST GmbH veranstaltet, werden beispielsweise die folgenden zusätzlichen Gefährdungen ermittelt (siehe auch Tabelle 21 in Anhang B.6):

- G 2.70 *Manipulation durch Familienangehörige und Besucher*
  Diese Gefährdung stammt aus den Grundschutzkatalogen, war allerdings in der Modellierung für das betrachtete Zielobjekt nicht berücksichtigt worden. Sie wird aufgenommen, weil Familienangehörige und Besucher relativ häufig in der Fertigungshalle anwesend sind.
- G 4.B1 *Mangelnde Verfügbarkeit eines Leitrechners aufgrund von Netzüberlastung*
  Eine außergewöhnlich hohe Netzauslastung schränkt die Verfügbarkeit eines Leitrechners so ein, dass nicht mehr schnell genug auf Störungen reagiert werden kann.
- G 5.B1 *Gezielter Hacker-Angriff auf eine Produktionsanlage*
  Aufgrund von Schwachstellen der externen Schnittstellen gelingt es einem Angreifer, Fehlfunktionen bei der Fertigungsanlage auszulösen.
- G 5.B2 *Produktionsausfall durch ungezielten Denial-of-Service-Angriff*
  Ein ungezielter Hackerangriff überlastet das Netz und führt zum Ausfall einer Produktionsanlage.

Gefährdungsbewertung

Anschließend ist in der **Gefährdungsbewertung** für jede Gefährdung zu prüfen, inwiefern die bislang vorhandenen oder geplanten Sicherheitsmaßnahmen einen ausreichenden Schutz bieten. Das Ergebnis dieser Prüfung wird einschließlich seiner Begründung wie folgt in der Gefährdungsübersicht dokumentiert:

- Ein **„OK=J“** kennzeichnet Gefährdungen, die hinreichend durch vorhandene oder geplante Maßnahmen abgesichert sind oder die nicht relevant sind, zum Beispiel, weil ein anderer Grundwert betroffen ist.

- Ein **„OK=N“** bedeutet, dass die vorhandenen oder geplanten Maßnahmen keinen ausreichenden Schutz vor der jeweiligen Gefährdung bieten. Bei diesen Gefährdungen besteht folglich noch Handlungsbedarf.

Bei der RECPLAST GmbH wird insbesondere der Schutz gegen diejenigen Gefährdungen als unzureichend bewertet, die aus der Art der Netzanbindung des betrachteten IT-Systems resultieren. Gefährdungen wie die vorstehend genannten G 4.B1 *Mangelnde Verfügbarkeit eines Leitrechners aufgrund von Netzüberlastung* oder G 5.B1 *Gezielter Hacker-Angriff auf eine Produktionsanlage* erhalten folglich das Prädikat „OK=N“. Siehe dazu auch Tabelle 22 in Anhang B.6.

Behandlung der Risiken

Im letzten Schritt ist zu entscheiden, in welcher Weise mit Gefährdungen zu verfahren ist, für die die bislang umgesetzten Sicherheitsmaßnahmen noch keinen ausreichenden Schutz bieten. Zwischen den folgenden Risiko-Strategien ist eine begründete Entscheidung zu treffen:

A: Risiko-Reduktion durch weitere Sicherheitsmaßnahmen
Die Risiken werden durch zusätzliche Sicherheitsmaßnahmen verringert.

B: Risiko-Vermeidung durch Umstrukturierung
Die Risiken werden vermieden, indem der Informationsverbund so umstrukturiert wird, dass die Gefährdung nicht mehr wirksam werden kann.

C: Risiko-Übernahme
Die Risiken werden akzeptiert, beispielsweise weil die Gefährdung nur unter äußerst speziellen Bedingungen zu einem Schaden führen kann, weil keine hinreichend wirksamen Gegenmaßnahmen bekannt sind oder aber weil der Aufwand für mögliche Schutzmaßnahmen unangemessen hoch ist.

D: Risiko-Transfer
Die Risiken werden verlagert. Durch Abschluss von Versicherungen oder durch Auslagerung der risikobehafteten Aufgabe an einen externen Dienstleister kann zum Beispiel ein möglicher finanzieller Schaden (zumindest teilweise) auf Dritte abgewälzt werden.

Unter Umständen können Risiken auch nur vorübergehend in Kauf genommen werden. Solche **Risiken unter Beobachtung** werden zunächst akzeptiert (Handlungsalternative C), allerdings nur unter dem Vorbehalt, bei einer verschärften Gefährdungslage durch eine der drei anderen Alternativen (A, B oder D) auf sie zu reagieren. In der Regel sind übernommene Risiken als Risiken unter Beobachtung zu behandeln.

Ergebnis der Gefährdungsbewertung bei der RECPLAST GmbH ist, dass die vorhandenen Sicherheitsmaßnahmen insbesondere bezüglich der Risiken aufgrund der vorhandenen Netzanbindung keinen hinreichenden Schutz

für das betrachtete Zielobjekt bieten (siehe auch Tabelle 23 in Anhang B.6). Im Sicherheitsmanagement-Team werden daher die verschiedenen Handlungsalternativen diskutiert:

- Insbesondere auch aufgrund der engen Bindung an den Anlagenhersteller gibt es so gut wie keine Möglichkeit, den Risiken durch **zusätzliche Sicherheitsmaßnahmen** auf dem betreffenden IT-System zu begegnen, etwa einem lokalen Virenschutz.
- Der bislang vorhandene Versicherungsschutz des Unternehmens schließt IT-bezogene Risiken nicht mit ein. Die Risiken **zu verlagern** würde in diesem Fall daher bedeuten, sich gegen mögliche finanzielle Schäden aufgrund des Ausfalls oder der Störung einer Produktionsanlage durch den Abschluss einer zusätzlichen Versicherung abzusichern. Eine kurze Recherche bei verschiedenen Industrieversicherern ergibt, dass dies nur mit zusätzlichen Auflagen und zu hohen Konditionen möglich ist. Daher wird diese Möglichkeit verworfen.
- Es besteht Einigkeit darüber, dass die ermittelten Risiken vermeidbar sind. Ihre **Übernahme** kommt daher allenfalls dann infrage, wenn die Vorteile aus der bestehenden Netzanbindung der Steuerungssysteme in einem einigermaßen positiven Verhältnis zu den Gefährdungen stehen. Dies wird letztlich jedoch verneint: Weder die Möglichkeit zu einem zentralen Management der IT-Systeme, noch die zum Abruf von Statusinformationen – auch von entfernten Standorten aus – rechtfertigen die Inkaufnahme der Risiken.
- Das Sicherheitsmanagement-Team entscheidet sich daher für die **Umstrukturierung** des Netzes und eine strikte Trennung des IT-Systems vom Büro-Netz der RECPLAST GmbH, um Hacker und Schadsoftware, aber auch unbeabsichtigte Überlastungen oder Integritätsverletzungen, von den Anlagen des Unternehmens fernzuhalten.

In diese Umstrukturierung sollen grundsätzliche alle Systeme zur Anlagensteuerung und -kontrolle einbezogen werden. Auf Einzelheiten zur Umsetzung dieser Entscheidung wird in Kapitel 10 *Umsetzung des Sicherheitskonzepts* eingegangen.

Konsolidierung des Sicherheitskonzepts

Zusätzliche Sicherheitsmaßnahmen, die sich aufgrund der ergänzenden Sicherheitsanalyse beziehungsweise einer Risikoanalyse ergeben haben, müssen konkretisiert und mit dem vorhandenen Sicherheitskonzept in Einklang gebracht **(„konsolidiert“**) werden. Dies hat gleichzeitig Rückwirkungen auf den Sicherheitsprozess: Wurde beispielsweise entschieden, Risiken durch eine Umstrukturierung des Geschäftsprozesses zu vermeiden, so macht dies häufig eine Aktualisierung der Strukturanalyse und der sich anschließenden Schritte der IT-Grundschutz-Vorgehensweise erforderlich. Auf jeden Fall ist der Umsetzungsstand von zusätzlichen oder geänderten Sicherheitsmaßnahmen in einem zweiten Basis-Sicherheitscheck zu überprüfen.

10 Umsetzung des Sicherheitskonzepts

Basis-Sicherheitscheck, ergänzende Sicherheits- und Risikoanalyse zeigen auf, für welche Zielobjekte und bezüglich welcher Aspekte ein Bedarf an zusätzlichen Sicherheitsmaßnahmen besteht. Diese Sicherheitslücken gilt es wirksam und unter Berücksichtigung der wirtschaftlichen und sonstigen Rahmenbedingungen des betrachteten Informationsverbunds zu schließen. Eine sorgfältige Planung trägt wesentlich zur Effizienz und Effektivität dieser Aktivität bei.

10.1 Vorgehensweise

In [BSI 100-2] wird empfohlen, die Umsetzung von Sicherheitsmaßnahmen in folgenden Schritten zu planen:

- **Schritt 1: Untersuchungsergebnisse sichten**
  Um einen Überblick über die insgesamt erforderlichen Sicherheitsmaßnahmen zu erhalten, werden die beim Basis-Sicherheitscheck als fehlend identifizierten Standard-Sicherheitsmaßnahmen sowie diejenigen, deren Erfordernis in ergänzenden Sicherheitsanalysen ermittelt wurde, zusammengestellt.
- **Schritt 2: Maßnahmen konsolidieren**
  In diesem Schritt werden die umzusetzenden Sicherheitsmaßnahmen aufeinander abgestimmt und konkretisiert sowie an die organisatorischen und technischen Gegebenheiten des Unternehmens angepasst.
- **Schritt 3: Kosten und Aufwand schätzen**
  Für jede konkretisierte Maßnahme werden die einmaligen und fortlaufenden Sachkosten und Personalaufwände bei Einführung und Betrieb ermittelt. Die Maßnahmen und benötigten finanziellen und personellen Ressourcen sind mit der Unternehmensleitung abzustimmen.
- **Schritt 4: Umsetzungsreihenfolge festlegen**
  Unter Berücksichtigung der sachlogischen Zusammenhänge zwischen den Maßnahmen, ihrer Schutzwirkung und der verfügbaren Ressourcen ist daher eine sinnvolle Umsetzungsreihenfolge festzulegen.
- **Schritt 5: Verantwortliche bestimmen und Termine setzen**
  Es ist eindeutig festzulegen, wer bis zu welchem Zeitpunkt für welche Aufgaben zuständig ist, damit die beschlossenen Maßnahmen fristgerecht umgesetzt werden, ferner von wem die Umsetzung kontrolliert wird.
- **Schritt 6: Begleitende Aktivitäten planen**
  Dazu gehört insbesondere, den betroffenen Mitarbeiter in geeigneter Weise die Ziele der Maßnahmen und die damit verbundenen Folgen zu vermitteln sowie sie, soweit erforderlich, in deren Handhabung zu schulen.

Wenn nur wenige Maßnahmen umzusetzen sind und dafür nur ein geringer Aufwand erforderlich ist, können die Schritt 1, 3 und 4 entfallen.

Die [GSK] enthalten eine Reihe von Hilfestellungen für die Realisierungsplanung:

- Die Festlegung der Umsetzungsreihenfolge wird in den **Bausteinen** durch die Sortierung der Maßnahmen anhand eines Lebenszyklus-Modells unterstützt,
- die **Maßnahmentexte** enthalten Vorschläge für die Zuordnung der Verantwortlichkeiten und geben viele Umsetzungshinweise,
- die **Gefährdungsbeschreibungen** können eine nützliche Argumentationshilfe in Diskussionen mit der Unternehmensleitung zur Erforderlichkeit von Maßnahmen sein.

10.2 Besonderheiten und Probleme

Der Basis-Sicherheitscheck und die ergänzende Sicherheitsanalyse haben ergeben, dass für den betrachten Informationsverbund der RECPLAST GmbH eine Reihe von Sicherheitsmaßnahmen umzusetzen sind. Auf einige davon wurde in den vorherigen Kapiteln bereits detailliert eingegangen. Im Einzelnen wird ein Handlungsbedarf insbesondere bei folgenden Zielobjekten gesehen:

- Für die **Anbindung des Funknetzes** an das kabelgebundene Netz soll die Empfehlung der Maßnahme M 5.139 *Sichere Anbindung eines WLANs an ein LAN* dahingehend umgesetzt werden, zwischen den beiden Netzen ein Sicherheitsgateway einzurichten. Dies soll es ermöglichen, den Datenverkehr ins LAN vollständig zu sperren, sobald ein Angriff auf das WLAN erkannt wird. Darüber hinaus wird entschieden, den Access Point so aufzustellen, dass die Abstrahlung in Bereiche außerhalb des Firmengeländes minimiert wird (Maßnahme M 1.63 *Geeignete Aufstellung von Access Points*).
- Aufgrund der hohen Vertraulichkeit der Informationen auf den **Clients der Entwicklungsabteilung** sollen diese in einem eigenen Netzsegment angeordnet werden. Dieses Segment wird auch einen neu zu beschaffenden eigenen Server für die Ablage der Dateien der Abteilung aufnehmen.
- Die Lage der **Räumlichkeiten der Entwicklungsabteilung** im Außenbereich der Werksgebäude ist aus Sicherheitssicht als ungünstig bewertet worden (siehe M 1.13 *Anordnung schützenswerter Gebäudeteile*). Eine grundlegende Änderung wird allerdings von der Unternehmensleitung aufgrund der baulichen Gegebenheiten als nicht finanzierbar gesehen. Stattdessen werden kostengünstige, aber wirksame kleinere Verbesserungen wie robustere Fenstergitter ins Auge gefasst.
- Die Sicherheitsprobleme der **PCs für die Anlagensteuerung** und -kontrolle (Zielobjekte C3 und C4) sollen durch eine strikte Trennung von Produktions- und Büronetz behoben werden. Als Sofortmaßnahme wurde vom Sicherheitsmanagement-Team beschlossen, die Kommunikationsverbindung zwischen den beiden PCs und dem internen Netz solange so lange zu kappen, bis Maßnahmen zum Schutz dieser IT-Systeme umgesetzt sind. Der

Netzanschluss zu den beiden PCs soll nur bei konkretem Bedarf und nur temporär geöffnet werden – zum Beispiel für die zuvor angekündigte Fernwartung einer der Anlagen durch den jeweiligen Hersteller.

Die endgültige Lösung, die völlige Trennung zwischen Büro- und Produktionsnetz, soll mit Hilfe eines Sicherheitsgateways, das aus einem Application-Level-Gateway sowie einem vor- und einem nachgelagerten Paketfilter besteht, realisiert werden, der gemäß Maßnahme M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways* bevorzugten Methode zur Trennung von Teilnetzen mit unterschiedlich hohem Schutzbedarf. In das Sicherheitsgateway soll auch ein Testsystem integriert werden, auf dem Updates und eingespielte Dateien, beispielsweise solche der Entwicklungsabteilung, geprüft und getestet werden können. Fernwartungszugänge sollten restriktiv gehandhabt werden, die in die Anlagen integrierten Modems beispielsweise nur bei dringendem Bedarf aktiviert werden.Das Sicherheitsgateway soll ferner einen Datenfluss zwischen Recycling- und Spritzgussanlagen verhindern und damit auch für eine Separierung der Komponenten des Produktionsnetzes sorgen.

- Die Datenübertragung über die angemietete **Standleitung zwischen den beiden Standorten** der RECPLAST GmbH in Bonn-Beuel und Bad Godesberg soll mittels Sicherheitsgateway und VPN geschützt werden. Der vorhandene Router N3 wird daher durch ein komplexeres Sicherheitssystem ersetzt, das ebenfalls aus einem Application-Level-Gateway, einem inneren und einem äußeren Paketfilter gebildet wird.

Die gewählten Lösungen erfordern umfangreiche Neuanschaffungen von Hard- und Software und bedeuten eine wesentliche Umstrukturierung des bisherigen Unternehmensnetzes. Die Umsetzung der Entscheidungen führt aber auch dazu, die Sicherheit des gesamten Netzes zu erhöhen. Mit deutlichen Hinweisen auf die vermiedenen Risiken und dem zusätzlichen Argument, dass die neue Netzstruktur auch die Chance bietet, geplante Neuanschaffungen im Anlagenbereich sicher zu integrieren, gelingt es jedoch relativ schnell, die Zustimmung der Unternehmensleitung zu den Investitionen zu erhalten.

Abbildung 7 veranschaulicht die neue Struktur des Netzes nach der Umsetzung aller beschlossenen Sicherheitsmaßnahmen.

Neben diesen konkreten Maßnahmen wird beschlossen, bei künftigen Beschaffungen stärker zu berücksichtigen, welche Möglichkeiten ein Anlagenhersteller für das **Einspielen von Patches und Updates** sowie zum Schutz vor Schadsoftware anbietet und wie groß die Bereitschaft und Fähigkeit sind, notwendige Sicherheitspatches zeitnah bereitzustellen.

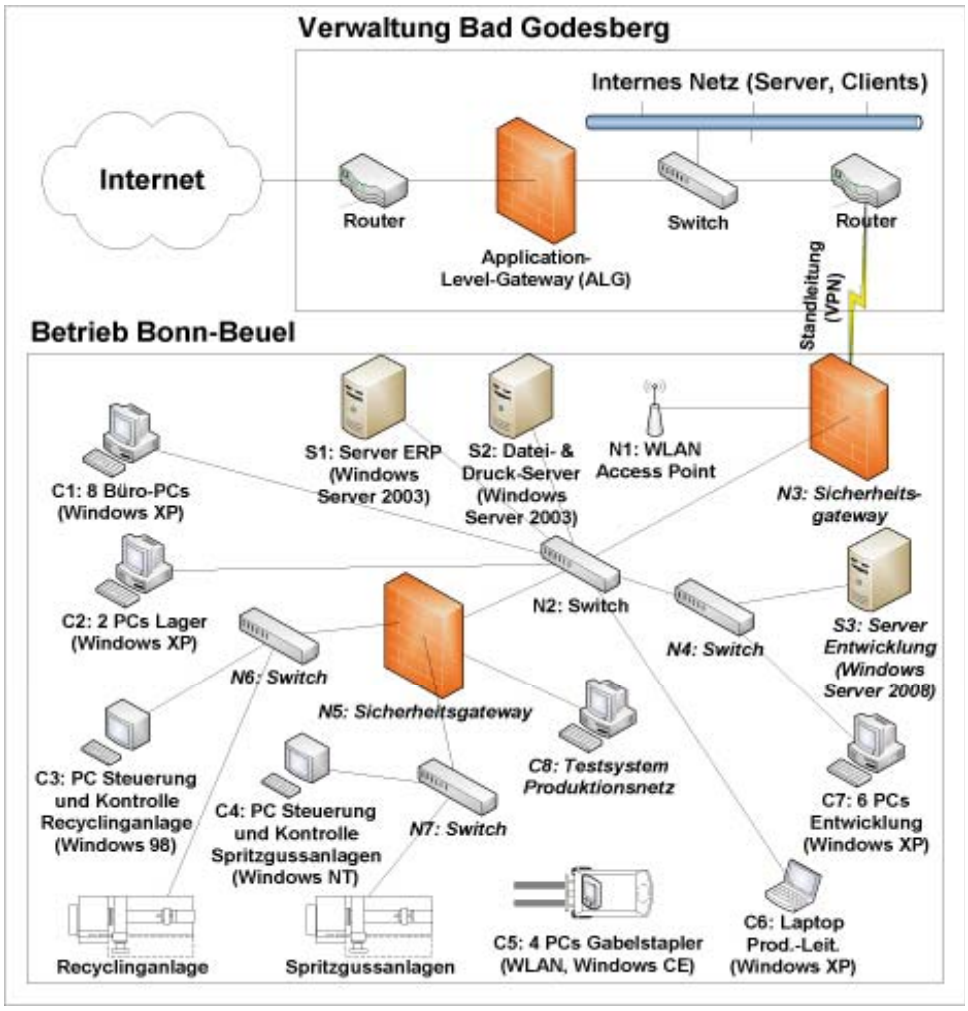


Abbildung 7: Netzstruktur in der Betriebsstätte Bonn-Beuel der RECPLAST GmbH nach der Umstrukturierung. Der vorangestellte Buchstabe kennzeichnet den Typ des IT-Systems (S = Server; C = Client; N = Netzkopplungskomponente). Die zusätzlichen oder geänderten IT-Systeme sind *kursiv* beschriftet.
Die Recycling- und die Spritzgussanlagen können über integrierte Modems ferngewartet werden. Dieser Zugang wird ausschließlich bei Bedarf und nur temporär geöffnet. Um die Abbildung übersichtlich zu halten, ist diese Kommunikationsverbindung nicht im Netzplan eingetragen.

Begleitende Maßnahmen

Die beschlossenen Sicherheitsmaßnahmen erfordern einige begleitende Maßnahmen. Insbesondere ist es notwendig, aufgrund der zusätzlichen Informationstechnik für **mehr IT-bezogenes Know-how** am Standort zu sorgen. Daher wird ein in der Netzadministration erfahrener Mitarbeiter der IT-Abteilung zum Standort Bonn-Beuel hin versetzt und zusätzlich in der Bedienung der Produktions- und Sicherheits-Hardware und -Software geschult.

Außerdem müssen die vorhandenen Regelwerke zur Bedienung der Leitrechner aktualisiert werden. Dies betrifft insbesondere die Vorschriften zur Fernwartung sowie zum Einspielen von Daten auf die IT-Systeme und zu den dafür obligatorischen Tests.

11 Aufrechterhaltung und Verbesserung der Informationssicherheit

Geschäftsprozesse, Informationstechnik, Bedrohungsszenarien und Sicherheitstechnik unterliegen einem kontinuierlichen Wandel, ebenso das äußere Umfeld, in dem ein Unternehmen tätig ist, zum Beispiel durch neue Gesetze und Verordnungen. Informationssicherheit ist daher kein einmal erreichter Zustand, sondern ein Prozess, dessen Angemessenheit und Wirksamkeit regelmäßig zu prüfen sind und der gegebenenfalls zu verbessern und an geänderte Bedingungen anzupassen ist.

In diesem Kapitel werden Mittel und Verfahren skizziert, die zur Aufrechterhaltung und kontinuierlichen Weiterentwicklung eines Managementsystems für Informationssicherheit beitragen.

11.1 Überprüfung des Sicherheitsprozesses

Ein Sicherheitsprozess kann zu unterschiedlichen Zwecken überprüft werden:

- Zum einen kann untersucht werden, ob und inwieweit die beschlossenen Sicherheitsmaßnahmen **umgesetzt sind und wie geplant funktionieren**. Werden die Maßnahmen von den Mitarbeitern akzeptiert und eingehalten? Sind zusätzliche Sensibilisierungsmaßnahmen erforderlich?
- Zum anderen kann die **Angemessenheit** des vorhandenen Sicherheitskonzepts geprüft werden. In diesem Zusammenhang sind sowohl interne als auch externe Faktoren zu berücksichtigen. Gibt es betriebliche Änderungen, beispielsweise in der Technik oder den räumlichen Gegebenheiten? Hat sich die Organisation des Unternehmens geändert, beispielsweise durch neue oder die Auslagerung von bestehenden Geschäftsprozessen? Entspricht das Sicherheitskonzept noch den gesetzlichen Anforderungen?
- Auch die **Wirtschaftlichkeit** eines Sicherheitskonzepts ist regelmäßig zu beobachten. Wurde der in der Realisierungsplanung angesetzte Kostenrahmen eingehalten? Gibt es gegebenenfalls zwischenzeitlich kostengünstigere Maßnahmen mit vergleichbarer Schutzwirkung? Welchen Nutzen haben die vorhandenen Maßnahmen?

Zur Überprüfung und Bewertung der Wirksamkeit und Angemessenheit eines Sicherheitskonzepts können verschiedene Methoden beitragen. So verweisen **Sicherheitsvorfälle** immer auch auf Schwachstellen in den vorhandenen Schutzmechanismen. Eine gründliche Auswertung kann deshalb einen bedeutenden Beitrag zur Verbesserung eines Sicherheitskonzepts leisten. In vergleichbarer Weise können **Penetrationstests** oder **Security Scanner** dazu beitragen, Sicherheitslücken in einem Netz oder auf IT-Systemen zu entdecken. Systematisch kann ein Sicherheitsmanagement im Rahmen von internen oder externen **Audits** oder einer **Sicherheitsrevision** untersucht werden.

Welche Verfahrensweisen ein Unternehmen wählen sollte, um sein Sicherheitsmanagement zu überprüfen, hängt von seiner Größe und dem Schutzbedarf seiner Geschäftsprozesse ab. Bei der RECPLAST GmbH entscheidet man sich für folgende Regelungen:

- Die **Wirksamkeit** jeder im Realisierungsplan vorgesehenen Maßnahme wird spätestens vier Wochen nach ihrer Umsetzung geprüft.
- Es werden regelmäßige Veranstaltungen und Aktionen zur Sensibilisierung und Schulung der Mitarbeiter (auch aus der Produktion) zu den verschiedenen Aspekten der Informationssicherheit durchgeführt. Außerdem wird das Thema verstärkt in den Mitarbeiterinformationen und in Betriebsversammlungen berücksichtigt. Dabei soll auch auf Probleme bei der Umsetzung des Sicherheitskonzepts eingegangen werden. Gegebenenfalls sollten Mitarbeiter aus der Produktion sogar speziell sensibilisiert werden.
- Alle drei Monate wird ein **Workshop** abgehalten, in dem das Sicherheitsmanagement-Team und gegebenenfalls weitere Teilnehmer ihre Erfahrungen und Probleme mit dem Sicherheitskonzept untereinander austauschen.
- Die Netzsicherheit wird mit Hilfe von **Penetrationstests** durch eine darauf spezialisierte und vertrauenswürdige externe Firma jährlich geprüft.
- Der IT-Sicherheitsbeauftragte wird beauftragt, ebenfalls jährlich die Angemessenheit der vorhandenen **Dokumentation** zum Sicherheitskonzept zu prüfen. Die Ergebnisse sowie gegebenenfalls Empfehlungen zur Weiterentwicklung des Konzepts sind der Unternehmensleitung zu berichten.

Die Regelungen gelten Unternehmensweit, also nicht nur in der Produktionsstätte in Bonn-Beuel.

Größere Sicherheitsvorfälle sind immer auch ein Indikator für Unzulänglichkeiten im vorhandenen Sicherheitskonzept. Sie sollten daher zum Anlass genommen werden, dieses außerplanmäßig zu überprüfen und gegebenenfalls zu verbessern.

11.2 Informationsflüsse

Das Engagement und die Beteiligung der Unternehmensleitung sind für ein erfolgreiches Sicherheitsmanagement unabdingbar. Dies setzt auch voraus, dass die Führungsebene in **Management-Berichten** regelmäßig und prägnant über die wesentlichen Eckpunkte zum Stand der Informationssicherheit unterrichtet wird.

Ein erfolgreiches Informationssicherheitsmanagement erfordert auch eindeutige Regelungen zu den **Informationsflüssen und Meldewegen**. Welche Informationen sind weiterzuleiten? Von wem und an wen? Wer muss welche Informationen einholen? – Solche Fragen sollte eine Unternehmensleitung in entsprechenden Richtlinien regeln.

Für die Nachhaltigkeit des Informationssicherheitsprozesses ist ferner eine sorgfältige, zielgruppengerechte und aktuell gehaltene **Dokumentation** der technischen Abläufe, getroffenen Entscheidungen und organisatorischen Vorgaben wichtig. Sie trägt dazu bei, dass

- getroffene Entscheidungen nachvollzogen,
- Prozesse vereinheitlicht sowie
- Schwächen und Fehler erkannt und behoben

werden können. Ein besonderes Augenmerk sollte dabei darauf gelegt werden, dass Änderungen von Abläufen, technischen Gegebenheiten und anderen Sachverhalten auch in der vorhandenen Dokumentation nachgezogen werden.

Bei der RECPLAST GmbH wird entschieden, dass der IT-Sicherheitsbeauftragte in einem kurzen halbjährlichen Bericht die wesentlichen Aussagen über den Stand der Informationssicherheit im Unternehmen darstellt. Dieser Bericht wird mit dem Sicherheitsmanagement-Team abgestimmt und auch die Ergebnisse der Sicherheitsuntersuchungen (Workshops, Penetrationstests etc.) enthalten. Es wird zusätzlich festgelegt, dass bei größeren Sicherheitsvorfällen die Unternehmensleitung unmittelbar benachrichtigt werden muss. Außerdem werden Verantwortliche für die Pflege aller Dokumente benannt, die für den Sicherheitsprozess wichtig sind.

11.3 ISO 27001-Zertifizierung auf Basis von IT-Grundschutz

Unternehmen, die sich erfolgreich darum bemüht haben, den IT-Grundschutz umzusetzen, können dies extern überprüfen und durch ein Zertifikat bestätigen lassen. Ein solches Zertifikat kann sowohl gegenüber Kunden als auch Geschäftspartnern als Qualitätsmerkmal dienen und somit Wettbewerbsvorteile bewirken. Für ein Fertigungsunternehmen kann ein Zertifikat beispielsweise bedeutsam sein, weil es belegt, dass aufgrund der umgesetzten Sicherheitsmaßnahmen mit höherer Wahrscheinlichkeit

- Liefertermine eingehalten werden, da das Unternehmen resistenter gegen Ausfälle oder Störungen der Produktion ist (geschützte Verfügbarkeit),
- die gelieferten Produkte die gewünschte Qualität haben (geschützte Integrität) und
- die Vertraulichkeit von Kundendaten im erforderlichen Umfang gewahrt bleibt, da diese vor unbefugter Einsichtnahme geschützt sind (geschützte Vertraulichkeit).

Unter Umständen kann ein Unternehmen durch günstigere Konditionen bei eingeräumten Krediten oder abgeschlossenen Versicherungsverträgen auch direkte wirtschaftliche Vorteile aus einem Zertifikat ziehen. Und nicht zuletzt kann der Zertifizierungsprozess auch einen Anreiz dafür bieten, die eigenen Prozesse zu überdenken und zu verbessern.

Für diesen Zweck wurde vom BSI gemeinsam mit anderen Experten für Informationssicherheit und Anwendern das **ISO 27001-Zertifikat auf Basis von IT-Grundschutz** entwickelt. Das Zertifikat ist nicht auf einen bestimmten Einsatzbereich, eine Organisationsgröße oder eine Branche hin ausgerichtet. Es kann sowohl von Dienstleistungs- als auch von Fertigungsunternehmen erworben werden, ebenso von Behörden, Verbänden oder Forschungseinrichtungen.

Grundlage für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist der Nachweis, dass in dem betreffenden Informationsverbund die IT-Grundschutz-Maßnahmen umfassend umgesetzt sind. Für diesen Nachweis ist ein Audit durch einen externen, beim BSI zertifizierten Auditor und die Überprüfung des Auditberichts durch die Zertifizierungsstelle erforderlich.

Weitere Informationen zur Zertifizierung nach ISO 27001 finden sich in [ZERT].

Der Aufwand für die Zertifizierung ist umso geringer, je umfassender ein Unternehmen die IT-Grundschutz-Maßnahmen bereits umgesetzt hat. Wenngleich die RECPLAST GmbH eine Zertifizierung noch nicht plant, so ist sie doch bestrebt, eine solche im Bedarfsfall relativ unkompliziert erlangen zu können. Daher wird entschieden, die Sicherheitskonzepte auch künftig mit Hilfe der IT-Grundschutz-Vorgehensweise weiterzuentwickeln.

12 Fazit

In diesem Profil wurde anhand eines Beispiels veranschaulicht, wie die IT-Grundschutz-Vorgehensweise auf ein Produktionsunternehmen angewendet werden kann. Es zeigt sich, dass dies in weiten Teilen problemlos möglich ist. Die grundsätzlichen Empfehlungen des Standards [BSI 100-2] zum Aufbau und zur Weiterentwicklung eines Informationssicherheitsmanagementsystems sowie zur Methodik der Entwicklung von Sicherheitskonzepten gelten für beliebige Organisationen, damit uneingeschränkt auch für Produktionsunternehmen. Auch die [GSK] bieten vielfältige Hilfestellungen zur Absicherung derartiger Informationsverbünde. Dies gilt insbesondere für diejenigen Anwendungen und IT-Systeme, die für Aufgabenstellungen wie Lagerverwaltung, Produktionsplanung, Entwicklung und Konstruktion oder Auftragsverwaltung eingesetzt werden. Anders verhält es sich mit der Hard- und Software, die zur Steuerung und Kontrolle von Anlagen eingesetzt wird. Sie unterliegt Anforderungen, die besondere Risikoanalysen und ergänzende oder modifizierte Sicherheitsmaßnahmen erforderlich machen.

Zur Begrenzung der Risiken wird in diesem Profil das Produktionsnetz mit Hilfe eines Sicherheitsgateways strikt von dem Büronetz getrennt. Der Netzverkehr im Produktionsnetz wird, soweit technisch möglich, auf das notwendige Maß beschränkt. Dies verhindert, dass die Fertigungsanlagen von sicherheitsrelevanten Vorfällen im Büronetz betroffen werden, ebenso, dass sich Probleme im Produktionsnetz auf das Büronetz oder andere Bereiche des Produktionsnetzes auswirken. Anwendungen, IT-Systeme und Produktionsanlagen sind in realen Unternehmen komplexer als im hier dargestellten Beispiel. Die empfohlene Netztrennung und die Art, wie sie umgesetzt wird, sind eine Möglichkeit, für Informationssicherheit in einem Produktionsunternehmen zu sorgen. Im konkreten Einzelfall können auch andere und weitergehende Lösungen notwendig sein, um für eine angemessene Informationssicherheit zu sorgen und unnötige Gefährdungen zu vermeiden. Je nach Gefährdungspotenzial ist die physische Trennung zwischen den beiden Netzen unter Umständen die einzig akzeptable und angemessene Vorgehensweise.

Anhang A: Leitlinie zur Informationssicherheit

Die Geschäftsführung der RECPLAST GmbH verabschiedet mit dieser Leitlinie die folgenden für alle Abteilungen und Mitarbeiter verbindlichen Grundsätze zur Informationssicherheit im Unternehmen.

Stellenwert von Informationen, Informationstechnik und deren Sicherheit für die RECPLAST GmbH

Der Erfolg unseres Unternehmens ist abhängig von aktuellen und korrekten Informationen. Diese werden zunehmend elektronisch verarbeitet, gespeichert und übermittelt. In allen Geschäftsprozessen und Abteilungen spielt Informationstechnik eine wichtige, unterstützende Rolle, ebenso in der Kommunikation mit Kunden, Geschäftspartnern und anderen Organisationen.

Die folgenden Beispiele veranschaulichen die Bedeutung von Informationssicherheit:

- Insbesondere in unserer Personalabteilung, aber auch in anderen Abteilungen und Arbeitsbereichen werden personenbezogene Daten verarbeitet. Zum Schutz dieser Informationen sind wir im Interesse der Betroffenen und aus gesetzlichen Gründen verpflichtet.
- An vielen Stellen unseres Unternehmens werden vertrauliche Informationen von Kunden und Geschäftspartnern vorrätig gehalten. Ein Missbrauch dieser Informationen kann das Ansehen und damit den geschäftlichen Erfolg der RECPLAST GmbH nachhaltig beschädigen und ist daher zu verhindern.
- Unsere Wettbewerbsposition beruht auch auf den innovativen Ideen unserer Entwicklungsabteilung zu Produkten und Fertigungsverfahren. Zwischen- und Endergebnisse ihrer Arbeiten unterliegen daher der Geheimhaltung und sind unter anderem vor Wirtschaftsspionage zu schützen.
- Auch in Fertigung und Logistik wird Informationssicherheit für die Effizienz unserer Prozesse und die Qualität unserer Erzeugnisse immer wichtiger. So sind wir bestrebt, unsere Produktion mit neuesten technischen Verfahren und Geräten zu unterstützen, um unserer Wettbewerbsfähigkeit zu halten oder sogar zu verbessern. Moderne Produktionsanlagen und Logistiksysteme sind immer stärker digitalisiert und vernetzt. Informationssicherheit wird daher auch hier zu einer wichtigen Aufgabe.

Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind wesentliche Voraussetzungen dafür, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen zu gewährleisten. Aufgrund unserer Verantwortung für die Informationssicherheit haben wir einen Sicherheitsprozess in Gang gesetzt. Dazu gehören die Entwicklung und Umsetzung dieser Leitlinie und eines Sicherheitskonzepts. Die Einhaltung der Leitlinie sowie Aktualität und Angemessenheit des Sicherheitskonzepts werden regelmäßig überprüft.

Ziele der Informationssicherheit und Kernelemente unserer Sicherheitsstrategie

Die Informationstechnik dient unserem Unternehmen wesentlich zur Erfüllung des Massengeschäfts im Vertrieb und Einkauf, für die Aufgaben der Finanz- und Lohnbuchhaltung und für qualitative Aufgaben in der Entwicklung, Auftragsabwicklung und im Management. Insbesondere für die Erledigung der auftragsbezogene Entscheidungen und Investitionen sind aktuelle und korrekte Unternehmensdaten erforderlich. Ein Ausfall wichtiger IT-Systeme ist bis zu einem Tag überbrückbar, darüber hinaus wären Beeinträchtigungen der Managementdispositionen, der Auftragsabwicklung und der Unternehmenskommunikation zwischen Verwaltung, Produktion und Lager riskant.

In Abwägung der Gefährdungen, der Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln sind uns die folgenden Aspekte zur Informationssicherheit besonders wichtig:

1. Geschäftsprozesse, Anwendungen und Informationstechnik müssen sorgfältig durchdacht werden und einfach zu steuern bleiben. Komplexe Strukturen, die zu unnötigen Risiken führen, sind zu vermeiden.

2. Informationssicherheit erfordert nicht nur organisatorische und technische Maßnahmen, sondern auch dass sich alle Mitarbeiter der möglichen Gefährdungen bewusst sind und sich sicherheitsgerecht verhalten. Dazu sollen regelmäßige Fortbildungsmaßnahmen zur Informationssicherheit beitragen.

3. Die Vertraulichkeit und Integrität der für das Unternehmen wichtigen Informationen sind zu schützen. Auch im Umgang mit elektronischen Dokumenten und Informationen sind Geheimhaltungsanweisungen strikt zu befolgen.

4. Die für das Unternehmen relevanten Gesetze und Vorschriften sowie vertragliche und aufsichtsrechtliche Verpflichtungen müssen eingehalten werden.

5. Ziel ist, die Sicherheit der Informationstechnik (gleichwertig neben Leistungsfähigkeit und Funktionalität) im Unternehmen aufrechtzuerhalten, so dass die Geschäftsinformationen bei Bedarf verfügbar sind. Ausfälle der IT haben Beeinträchtigungen des Unternehmens zur Folge. Lang andauernde Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag führen, sind nicht tolerierbar.

6. Durch Sicherheitsmängel im Umgang mit IT verursachte Ersatzansprüche, Schadensregulierungen und Image-Schäden müssen verhindert werden.

7. Gebäude und Räumlichkeiten unseres Unternehmens werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu den IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Informationen durch ein restriktives Berechtigungskonzept geschützt.

8. Es ist darauf zu achten, dass bei Investitionen die Belange der Informationssicherheit angemessen berücksichtigt sind. Anbieter elektronisch gesteuerter Fertigungsanlagen müssen in der Lage und bereit sein, aus Sicherheitsgründen

erforderliche Änderungen der integrierten Software während der gesamten Einsatzzeit einer Anlage vorzunehmen.

9. Die Übergänge zu externen Kommunikationsnetzen sind besonders zu schützen. Dies betrifft auch Fernwartungszugänge, die Anlagenherstellern gegebenenfalls eingeräumt werden. Solche Eingänge in das Netz der RECPLAST GmbH dürfen nur abgestimmt geöffnet werden. Zugriffe und durchgeführte Aktionen sind zu protokollieren.

10. Die Informationstechnik in der RECPLAST GmbH wird zentral von der IT-Abteilung administriert. Dabei muss die IT-Abteilung die Anforderungen der unterstützten Geschäftsprozesse berücksichtigen. Für die Administration von IT-Systemen, die unmittelbar für die Fertigung benötigt werden, bedeutet dies, dass alle Wartungsaktivitäten nur in Abstimmung mit der Produktionsleitung erfolgen dürfen.

11. Die RECPLAST GmbH muss in der Lage sein, rasch auf Krisen reagieren zu können. Das Unternehmen plant daher ein umfassendes Notfall-Management zu entwickeln, um auch bei gravierenden Unterbrechungen seine wesentlichen Geschäftsprozesse so schnell wie möglich wiederaufnehmen zu können. Eine besondere Priorität besitzt dabei die Wiederherstellung unserer Fertigungskapazitäten.

12. Bei der Entwicklung von Konzepten und der Einführung von Maßnahmen zur Informationssicherheit orientieren wir uns an allgemein anerkannten Standards, zum Beispiel der IT-Grundschutz-Vorgehensweise und den Empfehlungen des BSI-Standards 100-4 zum Notfall-Management.

Organisationsstruktur für Informationssicherheit

- Damit Informationssicherheit in unserem Unternehmen dauerhaft den erforderlichen Stellenwert besitzt, wird ein **IT-Sicherheitsbeauftragter** alle Arbeiten zur Informationssicherheit koordinieren. Der Inhaber dieser Aufgabe ist in dieser Funktion unmittelbar der Unternehmensleitung unterstellt und ist verpflichtet, ihr regelmäßig über den Stand, Probleme und aktuelle Vorhaben zur Informationssicherheit zu berichten. Der IT-Sicherheitsbeauftragte ist frühzeitig bei allen Investitionsentscheidungen und Projekten zu beteiligen, die Belange der Informationssicherheit berühren.

- Der IT-Sicherheitsbeauftrage arbeitet eng mit dem **Sicherheitsmanagement-Team** zusammen, das aus Mitarbeitern verschiedener Abteilungen des Unternehmens gebildet wird. Zu den Aufgaben dieser Arbeitsgruppe gehört es, Konzepte zur Informationssicherheit zu entwickeln und diesbezügliche Entscheidungen vorzubereiten.

- Für alle geschäftlich relevanten Informationen werden verantwortliche Mitarbeiter (**Informationseigentümer)** benannt. Sie sind verantwortlich für die Einschätzung der geschäftlichen Bedeutung (der Information, Technik), für die sichere Nutzung und Kontrolle, inklusive der Einhaltung von Sicherheitsgrundsätzen, Standards und Richtlinien. Die „Eigentümer“ definieren die

erforderliche Zugänglichkeit (der Information, Technik) sowie Art und Umfang der Autorisierung. Sie sind für die Verwaltung der zustehenden Zugriffsrechte der Benutzer verantwortlich und gegenüber der Leitung in Rechenschaftspflicht.

- Ein **Informationstreuhänder**, der z. B. aufgrund eines Serviceauftrags für das Unternehmen Leistungen erbringt, hat die Vorgaben des Informationseigentümers und diese Leitlinie zur Informationssicherheit einzuhalten. Damit ist er verantwortlich für die Einhaltung der Sicherheitsziele (Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Rechenschaftspflicht und Verbindlichkeit der Informationen). Bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen hat er den Informationseigentümer zu informieren.
- Jeder **Mitarbeiter** soll im Rahmen seines Umgangs mit Informationen und Informationstechnik (als Benutzer, Berater, Geschäftspartner) die erforderliche Integrität und Vertraulichkeit von Informationen sowie Verbindlichkeit und Beweisbarkeit von Geschäftskommunikation gewährleisten und die Richtlinien des Unternehmens einhalten. Unterstützt durch sensibilisierende Schulung und Benutzerbetreuung am Arbeitsplatz soll jeder im Rahmen seiner Möglichkeiten, Sicherheitsvorfälle von innen und außen vermeiden. Erkannte Fehler sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.
- Für die Überprüfung der Informationssicherheit bei der Bearbeitung, Nutzung und Kontrolle von Informationen werden jeweils unabhängige Verantwortliche eingesetzt, die z. B. Zugriffsmöglichkeiten auf Finanzdaten und den Umgang mit Finanztransaktionen und zugehörige Sicherheitsmaßnahmen kontrollieren.

Verstöße und Sanktionen

Jeder Beschäftigte der RECPLAST GmbH ist zu einem sorgfältigen Umgang mit den Informationen, Anwendungen, IT-Systemen und Kommunikationsnetzen der RECPLAST GmbH verpflichtet. Beabsichtigte oder grob fahrlässige Verletzungen der Informationssicherheit, zum Beispiel

- der Missbrauch von Daten, der finanziellen Verlust verursachen kann,
- der unberechtigte Zugriff auf Informationen oder ihre Änderung und unbefugte Übermittlung,
- die illegale Nutzung von Informationen aus dem Unternehmen oder
- die Gefährdung der Informationssicherheit anderer Unternehmen oder Institutionen,

können disziplinarische Folgen bis hin zur Kündigung des Arbeitsverhältnisses, gegebenenfalls auch straf- und zivilrechtliche Konsequenzen haben. Bei finanziellem Schaden können Haftungsansprüche und Regressforderungen geltend gemacht werden.

Anhang B: Dokumente zum Sicherheitskonzept

Die nachfolgenden Abschnitte enthalten die Ergebnisdokumente der RECPLAST GmbH für die Schritte zur Entwicklung eines Sicherheitskonzepts gemäß [BSI 100-2]. Um den Umfang vertretbar und die Darstellung übersichtlich zu halten, wird dabei auf eine vollständige Dokumentation verzichtet. Dies bedeutet, dass in den nachfolgenden Tabellen

- viele Anwendungen und IT-Systeme nicht berücksichtigt sind, selbst wenn sie Bestandteil so gut wie jeden Informationsverbunds sind – beispielsweise solche Anwendungen wie Faxen, Telefonieren oder Datenträgeraustausch und die zugeordneten IT-Systeme Faxgerät, Telekommunikationsanlage oder mobile Datenträger,
- Basis-Sicherheitscheck sowie ergänzende Sicherheits- und Risikoanalyse auch zu den angesprochenen Zielobjekten nur in kurzen Auszügen wiedergegeben werden.

B.1 Dokumentation der Strukturanalyse

Anwendungen

Nr.	Anwendung	Art der Information	Benutzer	Geschäftsprozesse
A1	Steuerung Recyclinganlage	T	Fertigung	Aufbereitung Altkunststoffe
A2	Steuerung Spritzgussanlagen	T	Fertigung	Produktfertigung
A3	Produktionsplanung und -steuerung (Komponente der ERP-Software)	T/K/V	Produktionsleitung	Produktfertigung
A4	Lagerverwaltung inklusive RFID-Unterstützung, (Komponente der ERP-Software)	T	Abteilung Lager/Logistik	Lagerverwaltung, indirekt: Aufbereitung Altkunststoffe, Fertigung
A5	ERP-Datenbank (Basis für A3 und A4)	T/K/V	Berechtigte Mitarbeiter aus allen in Bonn-Beuel ansässigen Abteilungen	Alle Geschäftsprozesse aus Fertigung, Entwicklung sowie Lager und Logistik
A6	Entwurf von Formteilen (mit Hilfe von CAD/CAM-Software)	T/V	Entwicklungsabteilung	Entwicklung; Voraussetzung für Produktion

Nr.	Anwendung	Art der Information	Benutzer	Geschäftsprozesse
A7	Entwicklung (mit Hilfe der CAD/CAM-Software und weiterer Software-Tools)	T/V	Entwicklungsabteilung	Produktfertigung
A8	Standard-Büroanwendungen	P/K	Lagerleitung, Produktionsleitung, Entwicklungsabteilung	Fertigung, Entwicklung, Lager/Logistik
A9	E-Mail	P/K	Lagerleitung, Produktionsleitung, Entwicklungsabteilung	Fertigung, Entwicklung, Lager/Logistik
A10	Internet-Recherche	P	Lagerleitung, Produktionsleitung, Entwicklungsabteilung	Fertigung, Entwicklung, Lager/Logistik

Tabelle 4: Anwendungen des betrachteten Informationsverbunds (Legende: A = Anwendung; P = personenbezogene Informationen; V = besonders vertrauliche Informationen; T = Technische Daten für Produktion; K = Kundendaten)

Erläuterungen:

- Für alle Anwendungen ist in technischer Hinsicht die IT-Administration verantwortlich. Daneben gibt es für die Anwendungen A1 bis A7 Fachverantwortliche aus den Abteilungen, in denen die jeweilige Anwendung eingesetzt wird.

IT-Systeme

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender
S1	Server ERP	Windows 2003 Server	1	Raum 4.07, Halle 4 (Serverraum)	In Betrieb	Berechtigte IT-Benutzer
S2	Datei- und Druckserver	Windows Server 2003	1	Raum 4.07, Halle 4 (Serverraum)	In Betrieb	Alle IT-Benutzer
C1	Büro-PCs	Windows XP	8	Räume 3.01 bis 3.03 (Halle 3) sowie 4.11 bis 4.14 (Halle 4)	In Betrieb	Prod.-Leitung, Lager-verwaltung
C2	PCs Lager	Windows XP	2	Halle 3, Halle 5	In Betrieb	Mitarbeiter Lager
C3	PC Steuerung und Kontrolle Recyclinganlage	Windows 98	1	Halle 2	In Betrieb	Mitarbeiter Recycling
C4	PC Steuerung und Kontrolle Spritzgussanlagen	Windows NT	1	Halle 4	In Betrieb	Mitarbeiter Fertigung
C5	PCs Gabelstapler	Windows CE	4	Mobil	In Betrieb	Mitarbeiter Lager

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender
C6	Laptop Prod.-Leitung	Windows XP	1	Mobil	In Betrieb	Prod.-Leitung
C7	PCs Entwicklung	Windows XP	6	Räume 4.08 bis 4.10 (Halle 4)	In Betrieb	Entwickl.-Abteilung
N1	WLAN Access Point	IEEE 802.11g	1	Raum 4.07 (Serverraum)	In Betrieb	Mitarbeiter Lager
N2	Switch	Hersteller-spezifisch	1	Raum 4.07 (Serverraum)	In Betrieb	Alle IT-Benutzer
N3	Router	Hersteller-spezifisch	1	Raum 4.07 (Serverraum)	In Betrieb	Alle IT-Benutzer

Tabelle 5: IT-Systeme des betrachteten Informationsverbunds (Legende: S = Server; C = Client; N = Netzkopplungskomponente)

Abhängigkeiten der Anwendungen von den IT-Systemen (Auszug)

Anwendung	IT-System Nr.								
	S1	S2	C3	C4	C5	C7	N1	N2	N3
A1 Steuerung Recyclinganlage			X					X	
A2 Steuerung Spritzgussanlagen				X				X	
A3 Prod.-Planung und -steuerung	X	X						X	
A4 Lagerverwaltung	X	X			X		X	X	
A5 ERP-Datenbank	X							X	
A6 Entwurf von Formteilen						X		X	
A7 Entwicklung						X		X	
A8 Standard-Büroanwendungen		X							
A9 E-Mail								X	X
A10 Internet-Recherche								X	X

Tabelle 6: Zuordnung der Anwendungen zu den IT-Systemen (Legende: S = Server; C = Client; N = Netzkopplungskomponente; X = Anwendung benutzt IT-System Ai X Sj = Die Ausführung der Anwendung Ai hängt vom IT-System Sj ab)

Kommunikationsverbindungen

Die Kommunikationsverbindungen können mit Hilfe eines Netzplans dokumentiert werden, in dem die IT-Systeme gruppiert und hinreichend gekennzeichnet sind. Siehe Abbildung 5, Seite 33.

Räume

Raum		IT/Informationen	Schutzbedarf		
Bezeich-nung	**Art**	**IT-Systeme/ Datenträger**	**Vertrau-lichkeit**	**Integrität**	**Verfüg-barkeit**
R 4.01	Besprechungs-raum	Möglichkeit zum Anschluss von Laptops etc. an das Netz			
R 3.01 bis 3.03; R 4.11 bis 4.14	Büroräume	C1 Büro-PCs; Faxgerät in Raum 4.11			
R 4.08 bis 4.10	Büroräume	C7 PCs Entwicklung			
R 4.07	Serverraum	Server S1 und S2, Access Point N1, Switch N2, Router N3, TK-Anlage			
Halle 1 (offener Bereich)	Lagerhalle	RFID-Chips zur Kennzeichnung der Lagerpositionen			
Halle 2 (offener Bereich)	Produktions-halle	C3 PC Steuerung und Kontrolle Recyclinganlage			
Halle 3 (offener Bereich)	Lagerhalle	RFID-Chips zur Kennzeichnung der Lagerpositionen 1 PC Lager			
Halle 4 (offener Bereich)	Produktions-halle	C4 PC Steuerung und Kontrolle Spritzgussanlagen			
Halle 5 (offener Bereich)	Lagerhalle	RFID-Chips zur Kennzeichnung der Lagerpositionen 1 PC Lager			

Tabelle 7: Räume des betrachteten Informationsverbunds (Legende: R = Raum).

Erläuterungen:

- Die Spalten „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ werden erst bei der Schutzbedarfsfeststellung ausgefüllt.

B.2 Dokumentation der Schutzbedarfsfeststellung

Schutzbedarfskategorien

Schadenszenario	Schutzbedarfskategorie		
	normal	**hoch**	**sehr hoch**
1. Verstoß gegen Gesetze, Vorschriften oder Verträge	Es drohen allenfalls geringfügige juristische Konsequenzen oder Konventionalstrafen.	Es drohen schwerwiegende juristische Konsequenzen oder Konventionalstrafen.	Die juristischen Konsequenzen oder Konventionalstrafen gefährden die Existenz des Unternehmens.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	Nur geringfügige Auswirkungen drohen, die von den Betroffenen toleriert würden.	Den Betroffenen drohen beträchtliche soziale oder wirtschaftliche Folgen, die sie nicht tolerieren.	Den Betroffenen drohen ruinöse Auswirkungen auf ihre soziale oder wirtschaftliche Stellung.
3. Beeinträchtigung der persönlichen Unversehrtheit	Mitarbeiter und andere Personen im Betrieb und seiner Umgebung werden nicht beeinträchtigt.	Mitarbeiter und andere Personen im Betrieb und seiner Umgebung werden beeinträchtigt, aber nicht dauerhaft geschädigt.	Mitarbeiter und andere Personen im Betrieb und seiner Umgebung werden dauerhaft geschädigt.
4. Beeinträchtigung der Aufgabenerfüllung	Die Abläufe im Unternehmen werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.	Die Abläufe im Unternehmen werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.	Die Abläufe im Unternehmen werden so stark beeinträchtigt, dass Ausfallzeiten von mehr als 2 Stunden nicht toleriert werden können.
5. Negative Innen- oder Außenwirkung	Es droht kein Ansehensverlust bei Kunden und Geschäftspartnern.	Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird erheblich beeinträchtigt.	Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird grundlegend und nachhaltig beschädigt.
6. Finanzielle Auswirkungen	Der mögliche finanzielle Schaden ist geringer als 50.000 Euro.	Der mögliche finanzielle Schaden liegt zwischen 50.000 und 500.000 Euro	Der mögliche finanzielle Schaden liegt über 500.000 Euro.

Tabelle 8: Definition der Schutzbedarfskategorien bei der RECPLAST GmbH

Schutzbedarf der Anwendungen

Anwendung		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
A1	Steuerung Recyclinganlage	Vertraulichkeit	normal	Die Informationen, die zur Steuerung der Anlage beitragen und bei deren Betrieb erzeugt werden, haben keinen besonderen Bedarf an Vertraulichkeit.
		Integrität	hoch	Zwar ist der finanzielle Schaden, der als Folge von Integritätsverletzungen droht, vergleichsweise gering. Aufgrund der Auswirkungen, die Fehlfunktionen der Anlage für die Umgebung und die Personen in ihrer Nähe haben können, wird der Schutzbedarf jedoch als *hoch* eingestuft.
		Verfügbarkeit	normal	Ausfälle führen erst nach mehreren Tagen zu höheren Schäden. Es gibt hinreichende Lagerbestände an erzeugten Regranulaten. Außerdem können bei Bedarf für die Fertigung erforderliche Granulate kurzfristig zugekauft werden.
A2	Steuerung Spritzgussanlagen	Vertraulichkeit	hoch	In die Steuerung der Fertigungsanlagen fließen Firmengeheimnisse ein. Die Informationen, die für den Betrieb erforderlich sind, sowie diejenigen, die beim Betrieb erzeugt werden, sind deswegen als vertraulich zu behandeln.
		Integrität	hoch	Fehlerhafte Steuerungsdaten können zum Ausfall einer Anlage führen und diese beschädigen, aber auch dazu, dass Qualitätsmängel erst zu spät erkannt werden und unnötig viel Ausschussware produziert wird. Die körperliche Unversehrtheit anwesender Personen kann ebenfalls beeinträchtigt werden.
		Verfügbarkeit	hoch	Ein mehr als 24-stündiger Produktionsausfall kann unmittelbare Einnahmeausfälle bewirken. Bei bestimmten Auftraggebern drohen ferner Konventionalstrafen und die Abwanderung zur Konkurrenz.

Anwendung		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
A3	Produktions-planung und -steuerung	Vertraulichkeit	hoch	Zu dieser Anwendung gehören Informationen, die als Betriebs-geheimnisse einzuschätzen sind.
		Integrität	hoch	Bei fehlerhaften oder verfälsch-ten Informationen drohen Fehlentscheidungen und damit verbunden direkte und indirekte finanzielle Verluste
		Verfügbarkeit	hoch	Ein weniger als 24 Stunden langer Ausfall der zur Planung und -Steuerung der Produktion eingesetzten Software kann zu entsprechend hohen Verlusten führen.
A4	Lagerverwaltung	Vertraulichkeit	normal	Es entstehen keine größeren Schäden, wenn Informationen dieser Anwendung bekannt werden.
		Integrität	normal	Fehlerhafte Informationen, zum Beispiel eine falsche Lager-position, können leicht erkannt und einfach korrigiert werden.
		Verfügbarkeit	normal	Ausfälle des IT-gestützten Ver-fahrens können mit vertretba-rem Aufwand durch manuelle Verfahren ersetzt werden. Erst bei einem mehrtägigen Ausfall drohen höhere Verluste.
A5	ERP-Datenbank	Vertraulichkeit	hoch	Aufgrund der Anwendungen A3 und A4, denen diese Datenbank zugrunde liegt, ergibt sich ein hoher Schutzbedarf (Maximumprinzip).
		Integrität	hoch	Aufgrund der Anwendungen A3 und A4, denen diese Datenbank zugrunde liegt, ergibt sich ein hoher Schutzbedarf (Maximumprinzip).
		Verfügbarkeit	hoch	Aufgrund der Anwendungen A3 und A4, denen diese Datenbank zugrunde liegt, ergibt sich ein hoher Schutzbedarf (Maximumprinzip).

Anwendung		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
A6	Entwurf von Formteilen	Vertraulichkeit	hoch	Die Formteile für Erzeugnisse, die noch nicht auf den Markt gebracht sind, können zum Ziel von Wirtschaftsspionage werden. Der Verlust von Wettbewerbsvorteilen droht.
		Integrität	hoch	Ungewollte Veränderungen werden unter Umständen nur sehr spät erkannt und können einen hohen wirtschaftlichen Schaden bewirken.
		Verfügbarkeit	hoch	In Einzelfällen wird bei wichtigen Kunden sehr zeitnah zum Auftragseingang produziert. Dies ist nur möglich wenn die benötigten Formteile für die Fertigungsanlagen auch kurzfristig hergestellt werden können. Da ansonsten der Verlust von Kunden und größere Umsatzausfälle drohen, wird der Verfügbarkeitsbedarf als hoch bewertet, auch wenn in der Regel eine solch hohe Verfügbarkeit nicht gewährleistet werden muss..
A7	Entwicklung	Vertraulichkeit	hoch	Sowohl bei der Entwicklung neuer Produkte als auch bei der von Fertigungsverfahren gibt es Firmengeheimnisse, die vor der Konkurrenz zu schützen sind.
		Integrität	hoch	Die Entwicklungsergebnisse erfordern zum Teil einen hohen Aufwand. Verletzungen der Integrität können daher einen hohen finanziellen Schaden hervorrufen.
		Verfügbarkeit	normal	Eintägige Unterbrechungen haben keine größeren Schäden zur Folge.
A8	Standard-Büroanwendungen	Vertraulichkeit	normal	Zwar werden auch vertrauliche Dokumente mit Hilfe der eingesetzten Software erzeugt, die Anwendungen selber haben jedoch keinen höheren Vertraulichkeitsbedarf
		Integrität	normal	Fehler können leicht behoben werden und bewirken keine größeren Schäden.
		Verfügbarkeit	normal	Bei Ausfall eines PCs kann problemlos auf ein anderes Gerät ausgewichen werden.

Anwendung		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
A9	E-Mail	Vertraulichkeit	hoch	Es gibt zwar eine Betriebsvereinbarung, gemäß der es untersagt ist, vertrauliche Daten unverschlüsselt zu versenden. Dies kann jedoch bei extern eingehender E-Mail nicht kontrolliert werden. Daher ist der Schutzbedarf als hoch zu bewerten.
		Integrität	hoch	Kundenanfragen oder Bestellungen müssen vor Verfälschungen geschützt werden.
		Verfügbarkeit	hoch	Sowohl die interne Kommunikation als auch ein großer Teil der Kommunikation mit Kunden erfolgt über E-Mail. Ein Ausfall führt zu hohem Ansehensverlust und evtl. zum Verlust von Bestellungen. Ein Ausfall ist daher höchstens für 24 Stunden akzeptabel.
A10	Internet-Recherche	Vertraulichkeit	hoch	Die Verbindungsdaten unterliegen dem betrieblichen Datenschutz. Gemäß Betriebsvereinbarung darf nur zu ausgewiesenen Zwecken und von dazu befugten Personen auf diese Daten zugegriffen werden.
		Integrität	normal	Fehlerhafte Daten können in der Regel leicht erkannt werden.
		Verfügbarkeit	normal	Ein mehr als 24-stündiger Ausfall der Möglichkeit zur Internet-Recherche kann ist für die Abteilungen am Standort Bonn-Beuel tragbar.

Tabelle 9: Dokumentation des Schutzbedarfs der Anwendungen bei der RECPLAST GmbH (Legende: A = Anwendung)

Schutzbedarf der IT-Systeme

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
S1	Server ERP	Vertraulichkeit	hoch	Anwendung des Maximumprinzips (höchster Schutzbedarf der Anwendungen A3 und A4)
		Integrität	hoch	Anwendung des Maximumprinzips (höchster Schutzbedarf der Anwendungen A3 und A4)
		Verfügbarkeit	hoch	Anwendung des Maximumprinzips (höchster Schutzbedarf der Anwendungen A3 und A4)
S2	Datei- und Druckserver	Vertraulichkeit	normal	Zwar hat die Anwendung A3 einen höheren Bedarf an Vertraulichkeit, jedoch dient das IT-System hier lediglich dem Drucken (Verteilungseffekt).
		Integrität	normal	Zwar hat die Anwendung A3 einen höheren Bedarf an Integrität, jedoch dient das IT-System hier lediglich dem Drucken (Verteilungseffekt).
		Verfügbarkeit	normal	Zwar hat die Anwendung A3 einen höheren Bedarf an Verfügbarkeit, jedoch dient das IT-System hier lediglich dem Drucken (Verteilungseffekt).
C1	Büro-PCs	Vertraulichkeit	hoch	Alle PCs in den Räumen der Produktionsleitung und der Lagerverwaltung ermöglichen den Zugriff auf die Komponenten des ERP-Systems, wenn auch mit unterschiedlichen Benutzerberechtigungen. Der Schutzbedarf bezüglich Vertraulichkeit ergibt sich folglich aus dem Maximumprinzip.
		Integrität	hoch	Alle PCs in den Räumen der Produktionsleitung und der Lagerverwaltung ermöglichen den Zugriff auf die Komponenten des ERP-Systems, wenn auch mit unterschiedlichen Benutzerberechtigungen. Der Schutzbedarf bezüglich Integrität ergibt sich folglich aus dem Maximumprinzip.

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
		Verfügbarkeit	normal	Alle PCs in den Räumen der Produktionsleitung und der Lagerverwaltung ermöglichen den Zugriff auf die Komponenten des ERP-Systems, wenn auch mit unterschiedlichen Benutzerberechtigungen. Der Schutzbedarf bezüglich Verfügbarkeit ergibt sich folglich aus dem Verteilungsprinzip. Beim Ausfall eines PCs kann auf einen zweiten zurückgegriffen werden.
C2	PCs Lager	Vertraulichkeit	hoch	Die Rechner sind zwar so konfiguriert, dass sie lediglich den Zugriff auf die Lagerverwaltungskomponente des ERP-Systems gewähren. Der Schutzbedarf ergibt sich jedoch nicht nur aus dem der unterstützten Software, sondern auch daraus, dass Fehler in der Konfiguration des Geräts unter Umständen den Zugang zu anderen IT-Systemen im Netz ermöglichen können.
		Integrität	hoch	Die Rechner sind zwar so konfiguriert, dass sie lediglich den Zugriff auf die Lagerverwaltungskomponente des ERP-Systems gewähren. Der Schutzbedarf ergibt sich jedoch nicht nur aus dem der unterstützten Software, sondern auch daraus, dass Fehler in der Konfiguration des Geräts unter Umständen den Zugang zu anderen Anwendungen im Netz ermöglichen können.
		Verfügbarkeit	normal	Ein höherer Bedarf ist für die unterstützte Anwendung (A4) nicht notwendig. Bei Ausfall eines Rechners kann zudem relativ problemlos auf einen zweiten Rechner ausgewichen werden.
C3	PC Steuerung und Kontrolle Recyclinganlage	Vertraulichkeit	normal	Der Schutzbedarf ergibt sich aus Anwendung A1.
		Integrität	hoch	Der Schutzbedarf ergibt sich aus Anwendung A1.
		Verfügbarkeit	normal	Der Schutzbedarf ergibt sich aus Anwendung A1.

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
C4	PC Steuerung und Kontrolle Fertigungsanlagen	Vertraulichkeit	hoch	Der Schutzbedarf ergibt sich aus Anwendung A1.
		Integrität	hoch	Der Schutzbedarf ergibt sich aus Anwendung A1.
		Verfügbarkeit	hoch	Der Schutzbedarf ergibt sich aus Anwendung A1.
C5	PCs Gabelstapler	Vertraulichkeit	normal	Der Schutzbedarf ergibt sich aus Anwendung A4.
		Integrität	normal	Der Schutzbedarf ergibt sich aus Anwendung A4.
		Verfügbarkeit	normal	Der Schutzbedarf ergibt sich aus Anwendung A4.
C6	Laptop Prod.-Leitung	Vertraulichkeit	hoch	Der Rechner wird hauptsächlich für Präsentationen eingesetzt, daneben als Arbeitsgerät bei Geschäftsreisen. Zumindest vorübergehend kann daher auch vertrauliche Korrespondenz auf dem Laptop gespeichert sein.
		Integrität	normal	Fehler können leicht erkannt und behoben werden.
		Verfügbarkeit	normal	Zur Not kann von der zentralen IT-Abteilung in Bad Godesberg zügig ein Ersatzgerät bereitgestellt werden.
C7	PCs Entwicklung	Vertraulichkeit	hoch	Gemäß Maximumprinzip aus den unterstützten Anwendungen A6 und A7 abgeleitet.
		Integrität	hoch	Gemäß Maximumprinzip aus den unterstützten Anwendungen A6 und A7 abgeleitet.
		Verfügbarkeit	normal	Bei Ausfall eines PCs kann auf einem anderen Rechner weitergearbeitet werden.
N1	WLAN Access Point	Vertraulichkeit	hoch	Zwar hat Anwendung A4 (Lagerverwaltung) keinen hohen Schutzbedarf bezüglich Vertraulichkeit, jedoch kann der Access Point dazu missbraucht werden, in das interne Netz des Unternehmens einzudringen. Die Konfigurationsdaten des Geräts müssen nach außen hin verborgen bleiben.

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
		Integrität	hoch	Zwar hat die Anwendung A4 (Lagerverwaltung) keinen hohen Schutzbedarf bezüglich Integrität, jedoch kann der Access Point dazu missbraucht werden, in das interne Netz des Unternehmens einzudringen.
		Verfügbarkeit	normal	Ein Ausfall des IT-Systems hätte keine weitergehenden Folgen. Von daher ergibt sich der Verfügbarkeitsbedarf lediglich aus dem der unterstützten Anwendung A4.
N2	Switch	Vertraulichkeit	hoch	Wegen der andernfalls gegebenen Missbrauchs-möglichkeiten dürfen die Konfigurations- und Zugangsdaten zum Switch nur Befugten bekannt sein.
		Integrität	hoch	Wegen der andernfalls gegebenen Missbrauchs-möglichkeiten dürfen die Konfigurations- und Zugangsdaten zum Switch nicht verfälscht werden.
		Verfügbarkeit	hoch	Das IT-System ist eine wesentliche Grundlage für funktionierende Kommunika-tionsbeziehungen. Ausfälle des Geräts müssen daher rasch behoben werden können.
N3	Router	Vertraulichkeit	hoch	Wegen der andernfalls gegebenen Missbrauchs-möglichkeiten dürfen die Konfigurations- und Zugangsdaten zum Router nur Befugten bekannt sein.
		Integrität	hoch	Wegen der andernfalls gegebenen Missbrauchs-möglichkeiten dürfen die Konfigurations- und Zugangsdaten zum Router nicht verfälscht werden.
		Verfügbarkeit	normal	Das IT-System ist zwar eine wesentliche Grundlage für funktionierende Kommunika-tionsbeziehungen. Ausfälle des Geräts können jedoch rasch behoben werden, notfalls durch ein Ersatz-System.

Tabelle 10: Dokumentation des Schutzbedarfs der IT-Systeme bei der RECPLAST GmbH (Legende: S = Server; C = Client; N = Netzkopplungskomponente)

Kritische Kommunikationsverbindungen

	Kritisch aufgrund				
Verbindung	**Außen-verbindung**	**hohe Ver-traulichkeit**	**hohe Integri-tät**	**hohe Ver-fügbarkeit**	**keine Über-tragung**
N3 – LAN BG.	X				
N1 – WLAN	X				
N2 – C7		X			
N2 – N3		X	X	X	
S1 – N2		X	X	X	

Tabelle 11: Kritische Kommunikationsverbindungen bei der RECPLAST GmbH

Erläuterungen:

- Als kritisch ist eine Kommunikationsverbindung zwischen zwei IT-Systemen immer dann zu betrachten, wenn
  - diese eine Außenverbindung darstellt,
  - die übertragenen Informationen einen hohen Schutzbedarf bezüglich Vertraulichkeit, Integrität oder Verfügbarkeit haben oder aber
  - auf ihr Informationen auf keinen Fall übertragen werden dürfen.
- Kritische Kommunikationsverbindungen können dokumentiert werden, indem sie im Netzplan als solche markiert sowie – wie vorstehend – tabellarisch zusammengestellt werden.
- Die angemietete Standleitung zwischen den beiden Standorten der RECPLAST GmbH steht nicht unter Kontrolle des Unternehmens und ist deswegen als Außenverbindung zu betrachten. Zum Sicherheit von Standleitungen siehe auch die Studie [STL].
- Auch ein WLAN sollte aufgrund der fehlenden physischen Schutzmechanismen als Außenverbindung behandelt werden.

Schutzbedarf der Räume

Raum		**IT/Informationen**	**Schutzbedarf**		
Bezeich-nung	**Art**	**IT-Systeme/ Datenträger**	**Vertrau-lichkeit**	**Integrität**	**Verfüg-barkeit**
R 4.01	Besprechungsraum	Möglichkeit zum An-schluss von Laptops etc. an das Netz	hoch	normal	normal
R 3.01 bis 3.03; R 4.11 bis 4.14	Büroräume	C1 Büro-PCs; Faxgerät in Raum 4.11	hoch	normal	normal
R 4.08 bis 4.10	Büroräume	C7 PCs Entwicklung	hoch	normal	normal

Raum		IT/Informationen	Schutzbedarf		
Bezeich-nung	**Art**	**IT-Systeme/ Datenträger**	**Vertrau-lichkeit**	**Integrität**	**Verfüg-barkeit**
R 4.07	Serverraum	Server S1 und S2, Access Point N1, Switch N2, Router N3, TK-Anlage	hoch	hoch	hoch
Halle 1 (offener Bereich)	Lagerhalle	RFID-Chips zur Kennzeichnung der Lagerpositionen	hoch	hoch	normal
Halle 2 (offener Bereich)	Produktionshalle	C3 PC Steuerung und Kontrolle Recyclinganlage	normal	hoch	normal
Halle 3 (offener Bereich)	Lagerhalle	RFID-Chips zur Kennzeichnung der Lagerpositionen 1 PC Lager	hoch	hoch	normal
Halle 4 (offener Bereich)	Produktionshalle	C4 PC Steuerung und Kontrolle Spritzgussanlagen	hoch	hoch	hoch
Halle 5 (offener Bereich)	Lagerhalle	RFID-Chips zur Kennzeichnung der Lagerpositionen 1 PC Lager	hoch	hoch	normal

Tabelle 12: Räume des betrachteten Informationsverbunds (Legende: R = Raum)

B.3 Dokumentation der Modellierung

Bausteine der Schicht 1: Übergreifende Aspekte

Nr.	Titel	Zielobjekt/ Zielgruppe	Hinweise
B 1.0	Sicherheitsmanagement	gesamter Informations-verbund	Die Regelungen des Bausteins gelten für das gesamte Unternehmen, also auch für die Betriebsstätte in Bonn-Beuel.
B 1.1	Organisation	gesamter Informations-verbund	Die Regelungen des Bausteins gelten für das gesamte Unternehmen, also auch für die Betriebsstätte in Bonn-Beuel.
B 1.2	Personal	gesamter Informations-verbund	Die Regelungen des Bausteins gelten für das gesamte Unternehmen, also auch für die Betriebsstätte in Bonn-Beuel.
B 1.3	Notfall-Vorsorgekonzept	gesamter Informations-verbund	Ein unternehmensweites Notfall-Vorsorgekonzept soll entwickelt werden. Dabei soll ein besonderes Augenmerk auf den Standort in Bonn-Beuel gelegt werden, da die dort angesiedelten wertschöpfenden Prozesse besonders wichtig für das Unternehmen sind.
B 1.4	Datensicherungskonzept	gesamter Informations-verbund	Der Standort Bonn-Beuel ist in das Datensicherungskonzept des Unternehmens einbezogen.
B 1.5	Datenschutz	gesamter Informations-verbund	Datenschutz ist für das gesamte Unternehmen geregelt.
B 1.6	Computer-Virenschutzkonzept	gesamter Informations-verbund	Es gibt unternehmensweite Konzepte. In diesen ist jedoch der Schutz der PCs, die zur Produktionssteuerung eingesetzt sind, nicht berücksichtigt.
B 1.7	Kryptokonzept	gesamter Informations-verbund	Bei der Schutzbedarfs-feststellung wurde eine Reihe von Zielobjekten identifiziert, die einen hohen Bedarf an Vertraulichkeit haben. Derzeit existiert kein unternehmens-weites Kryptokonzept. Es wird erwogen, ein solches unter Berücksichtigung der Ergebnisse des Basis-Sicherheitschecks anzufertigen.

Nr.	Titel	Zielobjekt/ Zielgruppe	Hinweise
B 1.8	Behandlung von Sicherheitsvorfällen	gesamter Informations-verbund	Derzeit existiert dazu kein umfassendes Konzept. Beim Basis-Sicherheitscheck soll insbesondere darauf geachtet werden, inwieweit vorhandene Ansätze zu einem solchen ausgebaut werden können.
B 1.9	Hard- und Software-Management	gesamter Informations-verbund	Hierzu gibt es unternehmens-weite Regelungen. Diese sind aber sehr an den Bedingungen für IT im Büro ausgerichtet. Es wird angestrebt, die IT in der Produktion stärker zu berück-sichtigen.
B 1.10	Standardsoftware	gesamter Informations-verbund	Die vorhandene unternehmens-weit gültige Regelung zum Einsatz von Standardsoftware soll überprüft werden.
B 1.12	Archivierung	gesamter Informations-verbund	Es soll insbesondere darauf geachtet werden, ob das vorhandene Archivierungs-konzept die zu archivierenden Informationen des Produktions-bereichs berücksichtigt.
B 1.13	IT-Sicherheitssensibilisierung und Schulung	gesamter Informations-verbund	Ein unternehmensweites Konzept wird angestrebt.
B 1.14	Patch- und Änderungsmanagement	gesamter Informations-verbund	Ein unternehmensweites Konzept wird angestrebt.

Tabelle 13: Bausteinzuordnung für die übergreifenden Aspekte bei der RECPLAST GmbH

Erläuterungen:

- Es ist zweckmäßig, bei der tabellarischen Dokumentation der Modellierung eine eigene Spalte für die Ansprechpartner beim Basis-Sicherheitscheck vorzusehen. Aus Platzgründen wird in dieser und den folgenden Tabellen darauf verzichtet.
- Für die Bausteine der Schicht 1 wurden bei der RECPLAST GmbH unterschiedliche Ansprechpartner ausgewählt:
  - für den Baustein B 1.2 *Personal* ein Mitarbeiter der Personalabteilung,
  - für andere eher organisatorisch ausgerichtete Bausteine ein Mitarbeiter aus der Leitungsebene des Unternehmens,
  - für die eher technisch ausgerichteten Bausteine die im Verwaltungsstandort in Bad Godesberg angesiedelt Netz- und Systemadministration.

- Der Baustein B 1.11 *Outsourcing* wurde nicht in das IT-Grundschutz-Modell aufgenommen, weil keine relevanten Teilprozesse des Informationsverbunds zu externen Dienstleistern ausgelagert sind oder ausgelagert werden sollen.

Bausteine der Schicht 2: Infrastruktur

Nr.	Titel	Zielobjekt/ Zielgruppe	Hinweise
B 2.1	Gebäude	Hallen 1 bis 5	Die fünf Hallen bilden einen zusammenhängenden Komplex und werden daher als ein Gebäude betrachtet.
B 2.2	Elektrotechnische Verkabelung	Hallen 1 bis 5	Insbesondere soll darauf geachtet werden, ob die elektrotechnische Verkabelung den Umgebungsbedingungen in den Produktions- und Lagerhallen gerecht wird.
B 2.3	Büroraum	Büroräume Fertigung und Lager R 3.01 bis 3.03; R 4.11 bis 4.14	Aufgrund ihrer geringen Anzahl werden alle Räume geprüft, nicht nur eine Stichprobe.
		Büroräume Entwicklung R 4.08 bis 4.10	Die Räume der Entwicklungs-abteilung haben einen höheren Schutzbedarf und werden daher gesondert betrachtet.
B 2.4	Serverraum	Serverraum R 4.07	Aufgrund ihrer geringen Anzahl beherbergt der Raum auch die am Standort vorhandenen Server
B 2.10	Mobiler Arbeitsplatz	C6 Laptop Prod.-Leitung	Das IT-System wird an wechselnden Orten genutzt.
B 2.11	Besprechungs-, Veranstaltungs- und Schulungsräume	Besprechungsraum R 4.01	Der Raum wird von einem wechselnden Personenkreis benutzt, insbesondere auch von Geschäftspartnern, Kunden und anderen Besuchern.
B 2.12	IT-Verkabelung	Hallen 1 bis 5	Insbesondere soll darauf geachtet werden, ob die IT-Verkabelung den Umgebungsbedingungen in den Produktions- und Lagerhallen gerecht wird.

Tabelle 14: Bausteinzuordnung für die Infrastruktur der RECPLAST GmbH

Erläuterungen:

- Der Ansprechpartner für die Bausteine dieser Schicht stammt aus dem Bereich der Gebäudetechnik. Bei Bedarf sollen zu Einzelfragen Mitarbeiter der IT-Administration hinzugezogen werden.

- Es wird im Rahmen einer ergänzenden Sicherheitsanalyse geprüft, ob ein eigener Baustein zu den Fertigungs- und Lagerhallen erforderlich ist.

Bausteine der Schicht 3: IT-Systeme

Nr.	Titel	Zielobjekt/ Zielgruppe	Hinweise
B 3.101	Allgemeiner Server	S1 Server ERP	Die Server S1 und S2 unterscheiden sich in Einsatzzweck und Schutzbedarf. Daher sind sie gesondert zu prüfen.
		S2 Datei- und Druckserver	
B 3.108	Windows Server 2003	S1 Server ERP	
		S2 Datei- und Druckserver	
B 3.201	Allgemeiner Client	C1 Büro PCs	
		C2 PCs Lager	
		C3 PC Steuerung und Kontrolle Recyclinganlage	Wegen seines Schutzbedarfs und der besonderen Einsatzumgebung wird auf diesen PC zusätzlich in der ergänzenden Sicherheitsanalyse eingegangen.
		C4 PC Steuerung und Kontrolle Spritzgussanlagen	Wegen seines Schutzbedarfs und der besonderen Einsatzumgebung wird auf diesen PC zusätzlich in der ergänzenden Sicherheitsanalyse eingegangen.
		C5 PCs Gabelstapler	Wegen ihrer besonderen Einsatzumgebung und weil ein betriebssystemspezifischer Baustein fehlt, wird auf diese IT-Systeme zusätzlich in der ergänzenden Sicherheitsanalyse eingegangen.
		C6 Laptop Produktionsleitung	
		C7 PCs Entwicklung	Wegen des besonderen Schutzbedarfs wird auf diese IT-Systeme zusätzlich in der ergänzenden Sicherheitsanalyse eingegangen.
B 3.203	Laptop	C6 Laptop Produktionsleitung	
B 3.205	Client unter Windows NT	C4 PC Steuerung und Kontrolle Spritzgussanlagen	
B 3.206	Client unter Windows 95	C3 PC Steuerung und Kontrolle Recyclinganlage	Der Baustein ist auch auf PCs mit der Nachfolgeversion Windows 98 anzuwenden.

Nr.	Titel	Zielobjekt/ Zielgruppe	Hinweise
B 3.209	Client unter Windows XP	C1 Büro-PCs	
		C2 PCs Lager	
		C6 Laptop Produktionsleitung	
		C7 PCs Entwicklung	
B 3.302	Router und Switches	N2 Switch	Aufgrund ihrer unterschiedlichen Funktion sind die beiden Netzkopplungselemente N2 und N3 gesondert zu prüfen.
		N3 Router	

Tabelle 15: Bausteinzuordnung für die IT-Systeme der RECPLAST GmbH

Erläuterungen:

- Ansprechpartner für alle Bausteine ist die im Verwaltungsstandort in Bad Godesberg angesiedelt Netz- und Systemadministration.
- Sicherheitsmaßnahmen für den Access Point N1 sind im Bausteins B 4.6 *WLAN* enthalten.

Bausteine der Schicht 4: Netze

Nr.	Titel	Zielobjekt/ Zielgruppe	Hinweise
B 4.1	Heterogene Netze	Gesamtes Netz in Bonn-Beuel	Der Baustein wird auf das gesamte Netz in Bonn-Beuel angewendet, da dieses nicht in Teilnetze gegliedert ist.
B 4.2	Netz- und Systemmanagement	Gesamtes Netz in Bonn-Beuel	Das Netz wird zentral von der Netzadministration in Bad Godesberg verwaltet. Beim Basis-Sicherheitscheck ist darauf zu achten, dass die in diesem Zusammenhang getroffenen Entscheidungen den Bedingungen in Bonn-Beuel gerecht werden.
B 4.4	Remote Access	Fernwartung der Recyclinganlage (IT-System C3)	Die Wartung erfolgt über eine Einwählverbindung und VPN. Der Fernwartungszugang wird sowohl von den Herstellerfirmen als auch der unternehmenseigenen IT-Administration benutzt.
		Fernwartung der Spritzgussanlagen (IT-System C4)	Die Wartung erfolgt über eine Einwählverbindung und VPN. Der Fernwartungszugang wird sowohl von den Herstellerfirmen als auch der unternehmenseigenen IT-Administration benutzt.

Nr.	Titel	Zielobjekt/ Zielgruppe	Hinweise
		C6 Laptop der Prod.-Leitung (IT-System)	Gelegentlich wird mit Hilfe des Laptops und VPN-Software von externen Standorten aus auf das Firmennetz zugegriffen.
B 4.6	WLAN	Über den Access Point N1 aufgebautes Funknetz	Über diesen Baustein erfolgt auch die Absicherung des Access Points N1

Tabelle 16: Bausteinzuordnung für die Kommunikationsverbindungen der RECPLAST GmbH

Erläuterungen:

- Ansprechpartner für alle Bausteine ist die im Verwaltungsstandort in Bad Godesberg angesiedelt Netz- und Systemadministration.
- Der Baustein B 4.3 *Modem* wird nicht angewendet. Zwar verfügen die Recycling-Anlage und die Anlagen zur Herstellung der Kunststofferzeugnisse über Modems, diese sind aber nicht an das Telefonnetz angeschlossen und damit deaktiviert. Der Baustein wäre erst dann relevant, wenn diese Kommunikationsschnittstellen wieder in Betrieb genommen würden.
- In allen anderen IT-Systemen sind keine Modems eingebaut, auch nicht in den Laptop der Produktionsleitung (IT-System C6).

Bausteine der Schicht 5: Anwendungen

Nr.	Titel	Zielobjekt/ Zielgruppe	Hinweise
B 5.3	E-Mail	A8 E-Mail	Als E-Mail-Software sind Exchange 2007 und Outlook 2003-Clients im Einsatz
B 5.7	Datenbanken	A5 ERP-Datenbank	Die Anwendungen A3 und A4 beruhen auf dieser Datenbank.
B 5.8	Telearbeit	C6 Laptop Produktionsleitung	Der Baustein ist relevant, weil dieses IT-System gelegentlich auch im privaten häuslichen Umfeld benutzt wird.
B 5.12	Exchange 2000 / Outlook 2000	A8 E-Mail	Für die im Unternehmen eingesetzte Version dieser Software gibt es keinen eigenen Baustein. Daher wird ersatzweise der Baustein B 5.12 hinzugezogen. Ob weitergehender Analysebedarf besteht, ist noch zu prüfen.
B 5.14	Mobile Datenträger	Gesamter Informationsverbund	Mobile Datenträger sind für unterschiedliche Zwecke im Einsatz; eine einheitliche Regelung für das gesamte Unternehmen wird angestrebt.

Tabelle 17: Bausteinzuordnung für die Anwendungen der RECPLAST GmbH

Erläuterungen:

- Die Ansprechpartner für die jeweiligen Bausteine und Zielobjekte ergeben sich aus den technischen und fachlichen Verantwortlichkeiten für die einzelnen Anwendungen.
- Für die Anwendungen A1 „Steuerung Recyclinganlage“ und A2 „Steuerung Spritzgussanlagen“ gibt es keinen passenden Baustein in den [GSK]. Auf beide Anwendungen wird daher in einer ergänzenden Sicherheitsanalyse eingegangen.
- Für einige Anwendungen gibt es zwar keinen unmittelbar passenden Baustein. Weil die Sicherheitsanforderungen der Zielobjekte jedoch hinreichend durch Maßnahmen in anderen Bausteinen erfüllt werden, besteht kein zusätzlicher Analysebedarf. Dies gilt für die Anwendungen:
  - A6 „Entwurf von Formteilen“ und A7 „Entwicklung“, für die übliche CAD/CAM-Werkzeuge und andere Software-Tools eingesetzt werden,
  - A8 „Standard-Büroanwendungen“
    ebenfalls mit dem Baustein B 1.10 *Standardsoftware* sowie
  - A10 „Internet-Recherche“
    (relevant ist beispielsweise Maßnahme M 4.5 *Sicherheit von WWW-Browsern* in Baustein B 3.201 *Allgemeiner Client*).
- Bei anderen Anwendungen können vorhandene Bausteine in mehr oder weniger großem Umfang und gegebenenfalls modifiziert für die Modellierung herangezogen werden:
  - Wie in der Tabelle angemerkt, kann die eingesetzte E-Mail-Software zumindest teilweise mit Hilfe des Bausteins B 5.12 *Exchange 2000 / Outlook 2000* modelliert werden.
  - Die bei der RECPLAST GmbH eingesetzte ERP-Software ist zwar kein Produkt des Herstellers SAP. Aufgrund ähnlicher Funktionen wird überlegt, den B 5.13 *SAP System* als Vorlage für einen neu anzulegenden benutzerdefinierten Baustein zur Modellierung der Anwendungen A3 „Produktionsplanung und Steuerung“ und A4 „Lagerverwaltung“ zu verwenden.

B.4 Dokumentation des Basis-Sicherheitschecks

Als Beispiel für die Dokumentation des Basis-Sicherheitschecks dient nachfolgend das ausgefüllte Erhebungsformular für den Baustein B 3.201 *Allgemeiner Client* für das Zielobjekt C4, den PC zur Steuerung und Kontrolle der Spritzgussanlagen.

Baustein: B 3.201 *Allgemeiner Client* Zielobjekt: C4 „PC Steuerung und Kontrolle Spritzgussanlagen“					
Maßnahme	**Umsetzungsstand**				
Nr. (Siegel) Bezeichnung	**entbehrlich**	**ja**	**teilweise**	**nein**	**Bemerkungen/ Begründung für Nicht-Umsetzung**
M 2.23 (Z) *Herausgabe einer PC-Richtlinie*		X			Es gibt Verfahrensanweisungen zur Benutzung des IT-Systems, deren Kenntnisnahme die berechtigten Benutzer bestätigen müssen.
M 2.25 (A) *Dokumentation der Systemkonfiguration*		X			Die Dokumentation kann bei der IT-Administration eingesehen werden.
M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*				X	Die Wartung des Systems liegt in der Verantwortung des Anlagenherstellers. Sofern überhaupt vorhanden, werden Patches nur verzögert und wenn die Erfordernisse der Produktion es zulassen eingespielt.
M 2.321 (A) *Planung des Einsatzes von Client-Server-Netzen*		X			Bei der Beschaffung des Systems gab es ein entsprechendes Planungsdokument.
M 2.322 (A) *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz*			X		Das Planungsdokument, das vor der Beschaffung des IT-Systems angefertigt wurde, enthielt auch Sicherheitsrichtlinien. Diese sind allerdings nicht mehr auf dem neuesten Stand.
M 2.323 (A) *Geregelte Außerbetriebnahme eines Clients*		X			Der Sachverhalt ist hinreichend geregelt.
M 3.18 (A) *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*				X	Die Umsetzung ist für dieses IT-System nicht zweckmäßig.
M 4.2 (A) *Bildschirmsperre*				X	Die Umsetzung ist für dieses IT-System nicht zweckmäßig.
M 4.3 (A) *Regelmäßiger Einsatz eines Anti-Viren-Programms*				X	Lokaler Virenschutz verträgt sich nicht mit der Funktionalität des IT-Systems.
M 4.4 (C) *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*					Mit technischen Mitteln und durch entsprechende Regelungen wurde dafür gesorgt, dass die vorhandenen Laufwerke nur von dazu Befugten benutzt werden können.
M 4.40 (A) *Verhinderung der unautorisierten Nutzung des Rechnermikrofons*	X				Am IT-System ist kein Mikrofon vorhanden.
M 4.41 (C) *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*				X	Zusätzliche Sicherheitsprodukte gefährden das Funktionieren der Anlagensteuerung und -kontrolle.
M 4.93 (B) *Regelmäßige Integritätsprüfung*				X	Rechner ist quasi im Dauereinsatz. Die Umsetzung der Maßnahme ist nicht möglich.

Baustein: B 3.201 *Allgemeiner Client* Zielobjekt: C4 „PC Steuerung und Kontrolle Spritzgussanlagen“					
Maßnahme	**Umsetzungsstand**				
Nr. (Siegel) Bezeichnung	**entbehrlich**	**ja**	**teilweise**	**nein**	**Bemerkungen/ Begründung für Nicht-Umsetzung**
M 4.200 (Z) *Umgang mit USB-Speichermedien*	X				Das Gerät hat keine USB-Schnittstelle
M 4.237 (A) *Sichere Grundkonfiguration eines IT-Systems*				X	Bewertung resultiert aus Mängeln wie fehlender Virenschutz und dem alten, mit Sicherheitslücken behafteten Betriebssystem
M 4.238 (A) *Einsatz eines lokalen Paketfilters*				X	Ein solcher Filter könnte die Funktionalität des IT-Systems gefährden.
M 4.241 (A) *Sicherer Betrieb von Clients*		X			Die Wartungszugänge sind gesichert. Konfigurationsänderungen erfolgen erst, nachdem sie zuvor (beim Hersteller) getestet wurden, alle Änderungen werden dokumentiert.
M 4.242 (Z) *Einrichten einer Referenzinstallation für Clients*	X				Es handelt sich um ein spezielles IT-System.
M 5.37 (B) *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz*		X			Entsprechende Funktionen sind deaktiviert.
M 5.45 (B) *Sicherheit von WWW-Browsern*			X		Zur Ausrüstung des IT-Systems gehört auch ein (veralteter) Webbrowser
M 6.24 (A) *Erstellen eines Notfall-Bootmediums*		X			Eine Notfall-CD ist vorhanden.
M 6.32 (A) *Regelmäßige Datensicherung*		X			Soweit auf diesem IT-System Informationen zu sichern sind, werden sie lokal gesichert.

Tabelle 18: Dokumentation der ergänzenden Sicherheitsanalyse (Auszug)

Erläuterungen:

- Eine reale Dokumentation sollte um Angaben zu dem Befragungszeitpunkt, den Befragten und den Befragern ergänzt werden.
- Die einer Maßnahme vorangestellten Buchstaben zur **Siegelstufe** weisen auf die Wichtigkeit einer Maßnahme hin: Ein **„A“** kennzeichnet vorrangig umzusetzende Maßnahmen, ein **„B“** Maßnahmen, deren Realisierung zügig anzustreben ist, ein **„C“** solche, die zusätzlich für die Erlangung eines ISO 27001-Zertifikats auf Basis von IT-Grundschutz umzusetzen sind. Maßnahmen, die mit einem **„Z“** versehen sind, stellen Ergänzungen dar, die vor allem bei höheren Sicherheitsanforderungen hilfreich sein können. Verschiedene Bausteine enthalten mit **„W“** gekennzeichnete Maßnahmen. Diese dienen der Vermittlung von Grundlagen und Kenntnissen, die für das Verständnis und die Umsetzung der Maßnahmen hilfreich sind.

B.5 Dokumentation der ergänzenden Sicherheitsanalyse

Zielobjekt	Entscheidung (mit Begründung)
A1 „Steuerung Recyclinganlage“, C3 „PC Steuerung und Kontrolle Recyclinganlage“	Die Anwendung hat einen hohen Schutzbedarf bezüglich Integrität. Die Sicherheit der Anwendung hängt von drei Faktoren ab: der sachgerechten Bedienung, der Zuverlässigkeit der technischen Systeme und der Sicherheit des zugehörigen Leitrechners C3. Zur sicheren Benutzung wurde das betroffene Personal umfassend geschult, auf die Zuverlässigkeit der technischen Systeme wurde bei der Beschaffung der Anlage geachtet; hier hat zudem der Hersteller Haftungsverpflichtungen. Eine Risikoanalyse wurde daher zwar nicht für die Anwendung an sich, wohl aber für den zugehörigen Leitrechner C3 erwogen, bei dem der Basis-Sicherheitscheck zudem ergeben hat, dass wichtige Sicherheitsmaßnahmen nicht umgesetzt sind, bzw. nicht umgesetzt werden können. Eine Risikoanalyse für den Leitrechner C4 (einschließlich der zugehörigen Zielobjekte) wird jedoch vorgezogen, da dieser eine vergleichbare Problemlage aufweist und einen noch höheren Schutzbedarf hat. Es wird davon ausgegangen, dass die Ergebnisse dieser Risikoanalyse auf die Anwendung A1 und den Client C3 übertragen werden können.
A2 „Steuerung Spritzgussanlagen“, C4 PC „Steuerung und Kontrolle Spritzgussanlagen“	Die Anwendung und der zugehörige Leitrechner C4 haben einen hohen Schutzbedarf in allen drei Grundwerten. Weil außerdem der Basis-Sicherheitscheck ergeben hat, dass auf dem zugehörigen Leitrechner C4 wichtige Sicherheitsmaßnahmen nicht umgesetzt sind, bzw. nicht umgesetzt werden können, wird in Anbetracht der zentralen Bedeutung dieses IT-Systems für das Unternehmen beschlossen, dieses einer Risikoanalyse zu unterziehen. Diese Analyse wird insbesondere auch die Kommunikationsverbindung zu diesem IT-System einbeziehen.
A4 „Lagerverwaltung“	Diese Anwendung verwendet mit RFID zwar eine Technik, für die es derzeit in den IT-Grundschutz-Katalogen noch keinen entsprechenden Baustein gibt. Da die Anwendung aber keinen hohen Schutzbedarf hat und weil das Missbrauchsrisiko derzeit ebenfalls nicht als hoch angesehen wird, wird auf eine Risikoanalyse verzichtet. Es wird jedoch entschieden, in der nächsten Zeit die Publikationen und Meldungen zu den Risiken von RFID genau zu verfolgen.
S1 „Server ERP“	Der Server hat in allen drei Grundwerten einen hohen Schutzbedarf, der sich aus der Bedeutung des ERP-Systems für das Unternehmen ableitet. Für den Schutz von Integrität und Vertraulichkeit der Informationen werden die verwendeten kryptographischen Mechanismen des Datenbanksystems jedoch als hinreichend sicher angesehen. Innerhalb von einem Tag kann ein Ersatzsystem gestellt werden, so dass auch die Verfügbarkeit hinreichend gesichert ist. Auf eine Risikoanalyse wird daher verzichtet.

Zielobjekt	Entscheidung (mit Begründung)
C1 „Büro-PCs“	Auf den PCs werden neben anderen auch Informationen verarbeitet und gespeichert, deren Vertraulichkeit und Integrität in hohem Maße zu schützen sind. Es wurde beschlossen, für solche Informationen ein unternehmensweites Verschlüsselungskonzept zu entwickeln. In diesem Rahmen sollen auch Software zur verschlüsselten Ablage von Informationen beschafft und Richtlinien zu deren Anwendung entwickelt werden. Eine Risikoanalyse wird daher nicht für erforderlich gehalten.
Hallen 2 bis 5	Die Hallen haben aufgrund der in ihr befindlichen IT-Systeme einen hohen Schutzbedarf in mindestens einem Grundwert. Auf eine Risikoanalyse wird jedoch verzichtet, da die Umsetzung der gebäudespezifischen Sicherheitsmaßnahmen, insbesondere auch der Regelungen zum Zugangs- und Zugriffsschutz als ausreichend angesehen wird. Aus diesen Gründen wird auch darauf verzichtet, einen eigenen benutzerdefinierten Baustein Lagerhalle zu verfassen. Diese Entscheidung gilt sowohl für die Lagerhallen (Hallen 3 und 5) als auch für die Produktionshallen (Hallen 2 und 4).

Tabelle 19: Dokumentation der ergänzenden Sicherheitsanalyse (Auszug)

Erläuterungen:

- Die Tabelle listet Management-Entscheidungen dazu auf, ob eine Risikoanalyse für ein Zielobjekt durchgeführt wird oder nicht. Die Begründungen stellen keine allgemein gültigen Empfehlungen dar. Für reale Unternehmen können in vergleichbaren Fällen andere Entscheidungen (und Begründungen) zweckmäßiger sein.

B.6 Dokumentation der Risikoanalyse

Schritt 1: Gefährdungsübersicht

Zielobjekt: C4 PC Steuerung und Kontrolle Spritzgussanlagen	
Vertraulichkeit:	hoch
Integrität:	hoch
Verfügbarkeit:	hoch
G 1.1	*Personalausfall*
G 1.2	*Ausfall des IT-Systems*
G 2.1	*Fehlende oder unzureichende Regelungen*
G 2.2	*Unzureichende Kenntnis über Regelungen*
G 2.4	*Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen*
G 2.6	*Unbefugter Zutritt zu schutzbedürftigen Räumen*
G 2.7	*Unerlaubte Ausübung von Rechten*
G 2.22	*Fehlende Auswertung von Protokolldaten*

G 2.31	*Unzureichender Schutz des Windows NT-Einsatzes*
G 2.37	*Unkontrollierter Aufbau von Kommunikationsverbindungen*
G 2.67	*Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten*
G 3.1	*Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer*
G 3.2	*Fahrlässige Zerstörung von Gerät oder Daten*
G 3.3	*Nichtbeachtung von IT-Sicherheitsmaßnahmen*
G 3.5	*Unbeabsichtigte Leitungsbeschädigung*
G 3.6	*Gefährdung durch Reinigungs- oder Fremdpersonal*
G 3.8	*Fehlerhafte Nutzung des IT-Systems*
G 3.9	*Fehlerhafte Administration des IT-Systems*
G 3.44	*Sorglosigkeit im Umgang mit Informationen*
G 4.1	*Ausfall der Stromversorgung*
G 4.10	*Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
G 4.22	*Software-Schwachstellen oder Fehler*
G 5.1	*Manipulation/Zerstörung von IT-Geräten oder Zubehör*
G 5.2	*Manipulation an Daten oder Software*
G 5.4	*Diebstahl*
G 5.7	*Abhören von Leitungen*
G 5.20	*Missbrauch von Administratorrechten*
G 5.21	*Trojanische Pferde*
G 5.23	*Computer-Viren*

Tabelle 20: Gefährdungsübersicht (Auszug)

Erläuterungen

- Diese Zusammenstellung berücksichtigt sowohl die Gefährdungen, die in den direkt auf das Zielobjekt anzuwendenden Bausteinen B 3.201 *Allgemeiner Client* und B 3.205 *Client unter Windows NT* referenziert werden, als auch solche aus relevanten übergeordneten Bausteinen (beispielsweise B 1.9 *Hard- und Software-Management*).
- Doppelte und offensichtlich im konkreten Anwendungsfall nicht relevante Gefährdungen wurden gestrichen.
- Die Tabelle enthält wegen der besseren Übersichtlichkeit lediglich eine Auswahl der verbleibenden Gefährdungen.

Schritt 2: Ermittlung zusätzlicher Gefährdungen

Zielobjekt: C4 PC Steuerung und Kontrolle Spritzgussanlagen	
Vertraulichkeit:	hoch
Integrität:	hoch
Verfügbarkeit:	hoch
G 2.70	*Manipulation durch Familienangehörige und Besucher*
	Diese Gefährdung aus den Grundschutzkatalogen ist in der Modellierung für das betrachtete Zielobjekt nicht berücksichtigt. Sie wurde aufgenommen, weil Familienangehörige und Besucher relativ häufig in der Fertigungshalle anwesend sind.
G 2.B1	*Beschädigung von Informationstechnik im Fertigungsbereich*
	Der Client C4 wird im Fertigungsbereich des Unternehmens betrieben und ist deshalb besonderen physischen Gefahren ausgesetzt, beispielsweise durch Staub, Erschütterung oder hohe Luftfeuchtigkeit.
G 3.B1	*Unzulässiges Einspielen eines Patches*
	Eine versehentlich eingespielte Software-Aktualisierung, beispielsweise durch einen mit den betrieblichen Gepflogenheiten nicht vertrauten neu eingestellten Administrator, führt zu einem Stillstand der Fertigungsanlage.
G 4.B1	*Mangelnde Verfügbarkeit eines Leitrechners aufgrund von Netzüberlastung*
	Eine außergewöhnlich hohe Netzauslastung schränkt die Verfügbarkeit eines Leitrechners so ein, dass nicht mehr schnell genug auf Störungen reagiert werden kann.
G 5.B1	*Gezielter Hacker-Angriff auf eine Produktionsanlage*
	Aufgrund von Schwachstellen der externen Schnittstellen gelingt es einem Angreifer, Fehlfunktionen bei der Fertigungsanlage auszulösen.
G 5.B2	*Produktionsausfall durch ungezielten Denial-of-Service-Angriff*
	Ein planloser Hackerangriff überlastet das Netz und führt zum Ausfall einer Produktionsanlage.

Tabelle 21: Zusätzliche Gefährdungen (Auszug)

Erläuterungen:

- Gefährdungen, die nicht Bestandteil der [GSK] sind, sind durch ein „B“ als benutzerdefiniert gekennzeichnet.

Schritt 3: Gefährdungsbewertung

Zielobjekt: C4 PC Steuerung und Kontrolle Spritzgussanlagen		
Vertraulichkeit:	hoch	
Integrität:	hoch	
Verfügbarkeit:	hoch	
G 1.1	*Personalausfall*	*OK = N*
	Es kann nicht vollständig ausgeschlossen werden, dass zum Beispiel aufgrund einer Pandemie alle Mitarbeiter ausfallen, die berechtigt und befähigt sind, das IT-System zu benutzen.	
G 2.70	*Manipulation durch Familienangehörige und Besucher*	*OK =N*
	Solche Manipulationen können trotz der geltenden Bestimmung, dass sich Werksfremde nicht unbeaufsichtigt im Werk aufhalten dürfen, nicht ausgeschlossen werden	

G 2.B1	*Beschädigung von Informationstechnik im Fertigungsbereich*	*OK = J*
	Bei dem IT-System handelt es sich um einen hinreichend robusten Industrie-PC.	
G 4.B1	*Mangelnde Verfügbarkeit eines Leitrechners aufgrund von Netzüberlastung*	*OK = N*
	Aufgrund der vorhandenen Netzstruktur ist das Risiko recht groß.	
G 5.B1	*Gezielter Hacker-Angriff auf eine Produktionsanlage*	*OK = N*
	Netzstruktur sowie die Software des IT-Systems erleichtern solche Angriffe	
G 5.B2	*Produktionsausfall durch ungezielten Denial-of-Service-Angriff*	*OK = N*
	Netzstruktur sowie die Software des IT-Systems erleichtern solche Angriffe	

Tabelle 22: Gefährdungsbewertung (Auszug)

Schritt 4: Behandlung der Risiken

Zielobjekt: C4 PC Steuerung und Kontrolle Spritzgussanlagen	
Vertraulichkeit:	hoch
Integrität:	hoch
Verfügbarkeit:	hoch
G 1.1	*Personalausfall*
C	Risiko-Übernahme Im Normalfall reicht die Anzahl an Mitarbeitern aus, die berechtigt und in der Lage sind, das IT-System und die Fertigungsanlagen zu steuern. Der Ausfall einzelner Mitarbeiter kann problemlos kompensiert werden. Um gegen den Ausfall aller Mitarbeiter gerüstet zu sein, wären weitere Einstellungen erforderlich. Dies wird derzeit von der Unternehmensleitung als nicht wirtschaftlich angesehen.
G 2.70	*Manipulation durch Familienangehörige und Besucher*
C	Risiko-Übernahme Der regelmäßige Hinweis auf die Einhaltung der geltenden Regelungen zur Beaufsichtigung von Werksfremden wird als ausreichend erachtet. Solange Dritte sich im Werksgebäude aufhalten dürfen, lässt sich das Risiko nicht vollständig ausschalten.
G 4.B1	*Mangelnde Verfügbarkeit eines Leitrechners aufgrund von Netzüberlastung*
B	Risiko-Vermeidung durch Umstrukturierung Aufgrund der vorhandenen Netzstruktur ist das Risiko recht groß. Eine völlige Trennung des IT-Systems vom Büronetz des Unternehmens wird daher angestrebt. Hierzu wird zwischen Büro-Netz und den Leitrechnern im Produktionsbereich ein Sicherheitsgateway platziert. Für Fernwartung, Software-Update und die durchaus wünschenswerte Möglichkeit Statusinformationen zur Produktion auch von externen Positionen aus abrufen zu können, werden sichere Wege geplant.
G 5.B1	*Gezielter Hacker-Angriff auf eine Produktionsanlage*
B	Risiko-Vermeidung durch Umstrukturierung Die vorhandene Netzstruktur sowie die Software des IT-Systems erleichtern solche Angriffe. Auch dieser Gefährdung wird durch die vorstehend angesprochene Umstrukturierung des Netzes begegnet.
G 5.B2	*Produktionsausfall durch ungezielten Denial-of-Service-Angriff*
B	Risiko-Vermeidung durch Umstrukturierung Begründung: siehe G 5.B1.

Tabelle 23: Behandlung von Risiken (Auszug)

Anhang C: Glossar

Application-Level-Gateway (ALG)

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den ISO-/OSI-Schichten 1 bis 3 wahr. ALGs, auch Sicherheitsproxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog.

Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise bestimmte Protokollbefehle zu filtern.

Basis-Sicherheitscheck

Der Begriff bezeichnet gemäß IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Maßnahmen in einer Organisation bereits umgesetzt sind und welche grundlegenden Sicherheitsmaßnahmen noch fehlen.

Baustein

Der Begriff dient zur Strukturierung von Empfehlungen der IT-Grundschutz-Kataloge. 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.

Business Continuity Management (BCM)

Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Behörde oder eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.

Business Impact Analyse

Analyse zur Ermittlung von potentiellen direkten und indirekten Folgeschäden, die durch das Auftreten eines Notfalls oder einer Krise verursacht werden.

Ergänzende Sicherheitsanalyse

Diese Analyse ist nach IT-Grundschutz erforderlich, wenn Zielobjekte des betrachteten Informationsverbunds einen erhöhten Schutzbedarf haben, nicht geeignet modelliert werden können oder in untypischen Einsatzszenarien betrieben werden. Die Vorgehensweise hierzu ist im BSI-Standard 100-2 "IT-Grundschutz-Vorgehensweise" beschrieben. Die ergänzende Sicherheitsanalyse dient dazu festzustellen, für welche Teile des Informationsverbunds eine Risikoanalyse notwendig ist.

Ethernet

Standardisierte kabelgebundene Netztechnik für lokale Netze.

Enterprise Resource Planning (ERP)

Planung der Ressourcen, die für die verschiedenen Abläufe und Geschäftsprozesse in einem Unternehmen erforderlich sind. Die zugehörigen Aufgaben werden mit Hilfe spezieller ERP-Software unterstützt.

Feldbus

In den 80-er Jahren des letzten Jahrhunderts entwickeltes industrielles Kommunikationssystem, mit dem Messfühler (*Sensoren*) und Antriebsgeräte (*Aktoren*) angesteuert werden können. In den letzten Jahren werden als Alternative zur herkömmlichen Feldbussystemen zunehmend Kommunikationsnetze entwickelt, die auf Ethernet basieren.

Grundwerte der Informationssicherheit

Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellen Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel:

- Authentizität
- Verbindlichkeit
- Zuverlässigkeit
- Nichtabstreitbarkeit

Hotfix

Ein Hotfix (vom englischen *hot* = heiß und *fix* = reparieren) ist kleines Stück Software, dass ein Hersteller als Soforthilfe zur Behebung eines Programmfehlers bereitstellt.

Informationsverbund

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

Informationssicherheit

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 daher umfassender und wird zunehmend verwendet. Da aber in der Literatur noch überwiegend der Begriff "IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

Informationssicherheitsmanagementsystem (IS-Management)

Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Aus den gleichen Gründen, die oben für die Begriffe "Informationssicherheit" und "IT-Sicherheit" genannt sind, wird im IT-Grundschutz noch häufig der Begriff "IT-Sicherheitsmanagement" verwendet.

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff

Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

LAN

(= Local Area Network) Lokales Netz.

Maximumprinzip

Nach dem Maximum-Prinzip bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Geschäftsprozesses, einer Anwendung bzw. eines IT-Systems.

Netzplan

Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen.

Patch

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

Recyclinganlage

Anlage zur werkstofflichen Wiederaufbereitung von Altstoffen. Beim rohstofflichen Recycling von Kunststoffen wird beispielsweise versucht, aus Kunststoffen wieder den Rohstoff (Erdöl) zu gewinnen. Beim werkstofflichen Kunststoffrecycling werden Altkunststoffe sortiert, gereinigt und granuliert. Die erzeugten Granulate werden dann wie in der konventionellen Kunststoffindustrie weiterverarbeitet werden.

Service Pack

Als Service Pack (auf Deutsch: Wartungspaket) bezeichnen verschiedene Softwarehersteller Zusammenstellungen von Patches. Services Packs können sowohl Fehlerkorrekturen als auch funktionale Ergänzungen enthalten.

Sicherheitsgateway

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardware-technischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie 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.

Sicherheitsprozess

Organisatorischer Prozess, der die Umsetzung und Kontrolle von Maßnahmen zur Informationssicherheit zum Ziel hat.

Spritzgussanlage

Vorwiegend in der kunststoffverarbeitenden Industrie zur Erzeugung von Produkten in großer Stückzahlen eingesetzte Anlagen. Beim Kunststoff-Spritzgießen werden zunächst die Ausgangsstoffe (Granulate) in eine formbare Kunststoffmasse umgewandelt und anschließend ein Werkzeug eingespritzt.

Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Vertraulichkeit

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

WLAN

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.

Anhang D: Referenzen

[BSI 100-1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, März 2008, http://www.bsi.bund.de/

[BSI 100-2] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, März 2008, http://www.bsi.bund.de/

[BSI 100-3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, März 2008, http://www.bsi.bund.de/

[BSI 100-4] Notfallmanagement, BSI-Standard 100-4, Version 1.0, http://www.bsi.bund.de/

[GSK] IT-Grundschutz-Kataloge – Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, http://www.bsi.bund.de/gshb

[ISO 24702] ISO/IEC 24702:2006 "Information technology – Generic cabling – Industrial premises"

[ISO 27001] ISO/IEC 27001:2005 "Information technology – Security techniques – Information security management systems requirements specification", ISO/IEC JTC1/SC27

[RFID] TR 03126 Technische Richtlinie für den sicheren RFID-Einsatz, geplante Veröffentlichung Januar 2009, http://www.bsi.bund.de/

[STL] Studie: Sicherheitseigenschaften von Standleitungstechnologien, unterhalb von http://www.bsi.bund.de/gshb/deutsch/hilfmi/doku.htm

[ZERT] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits, BSI, Version 1.2, März 2008, www.bsi.bund.de/gshb/zert