Bundesamt
für Sicherheit in der
Informationstechnik

Beschreibung des Beispielunternehmens RECPLAST GmbH

Eine Ergänzung zum Online-Kurs IT-Grundschutz

Änderungshistorie

Version	Datum	Name	Beschreibung
0.9	06.06.2018	Fraunhofer SIT	Finaler Entwurf
1.0	07.08.2018	Fraunhofer SIT	Finale Version

Dieses Dokument ergänzt den Online-Kurs IT-Grundschutz und enthält die Darstellungen, Tabellen und Erläuterungen zu dem fiktiven Unternehmen RECPLAST GmbH, das in dem Kurs als Beispiel zur Veranschaulichung der IT-Grundschutz-Methodik verwendet wird.

Grundlage sind die BSI-Standards 200-1/-2/3 sowie das IT-Grundschutz-Kompendium 2018 (erschienen im Februar).

Der Online-Kurs IT-Grundschutz wurde im Auftrag des Bundesamts für Sicherheit in der Informationstechnik vom Fraunhofer-Institut für Sichere Informationstechnologie SIT, Bereich Security Management SMA, Sankt Augustin angefertigt.
Internet: www.sit.fraunhofer.de.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5369
E-Mail: grundschutz@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Das Beispielunternehmen RECPLAST GmbH

In diesem Dokument werden die einzelnen Schritte bei der Variante „Standard-Absicherung“ der IT-Grundschutz-Methodik veranschaulicht und es wird gezeigt, wie das IT-Grundschutz-Kompendium die Entwicklung eines Sicherheitskonzepts unterstützt.

Als Beispiel dient ein fiktives Unternehmen mittlerer Größe, die RECPLAST GmbH. Sie produziert und vertreibt etwa 400 unterschiedliche aus Recyclingmaterialien gefertigte Kunststoffprodukte, zum Beispiel Bauelemente wie Rund- und Brettprofile, Zäune, Blumenkübel oder Abfallbehälter – teils in größeren Serien für Endkunden, teils spezifisch für einzelne Geschäftskunden. Auftragsvolumen, Häufigkeit der Aufträge und die Kunden variieren: Es gibt einige wenige Stamm- und Großkunden und zahlreiche Einzelkunden. Der jährliche Gesamtumsatz des Unternehmens beläuft sich auf ca. 50 Millionen Euro bei einem Gewinn von etwa einer Million Euro.

Der Darstellung liegt die Edition 2018 des IT-Grundschutz-Kompendiums zugrunde.

1.1 Organisatorische Gliederung

Die organisatorische Gliederung der RECPLAST GmbH gibt das in Abbildung 1 dargestellte Organigramm wieder:

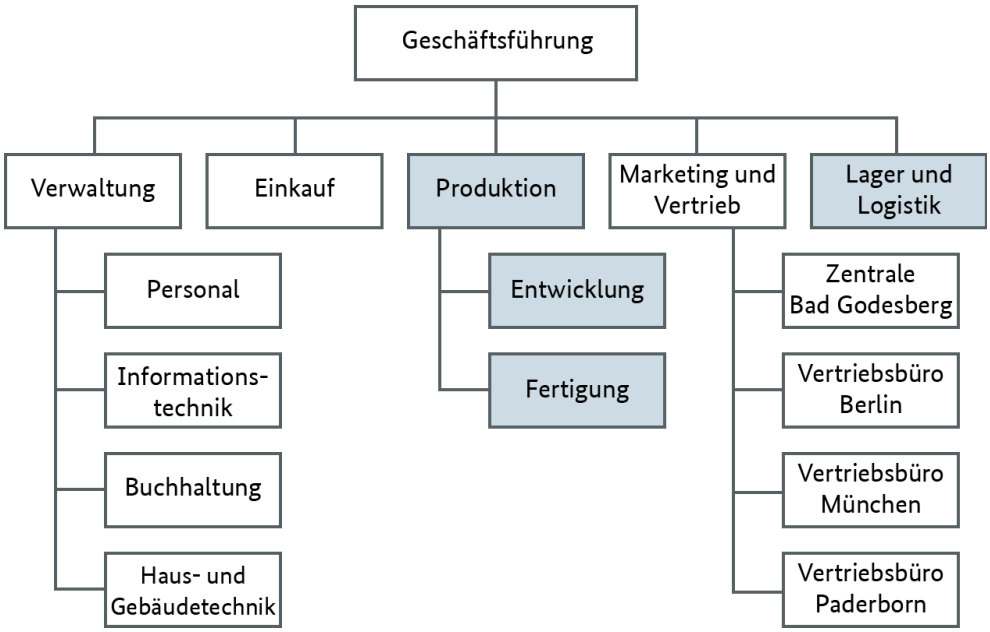

Abbildung 1: Organigramm der RECPLAST GmbH

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, Marketing und Vertrieb ein neues Gebäude in Bad Godesberg bezogen, während Produktion, Material- und Auslieferungslager (im Organigramm grau hinterlegt) am ursprünglichen Firmensitz im Stadtteil Beuel verblieben sind. Zusätzlich gibt es Vertriebsbüros in Berlin, München und Paderborn. Das Unternehmen beschäftigt insgesamt rund 500 Mitarbeiter, von denen 175 in der Verwaltung in Bad Godesberg, 310 in Produktion und Lager in Beuel und jeweils drei Mitarbeiter in den Vertriebsbüros in Berlin, München und Paderborn tätig sind.

1.2 Informationstechnik

Am Standort **Bad Godesberg** ist im Zuge des Umzugs ein zentral administriertes Windows-Netz mit insgesamt 145 angeschlossenen Arbeitsplätzen eingerichtet worden. Die Arbeitsplatzrechner sind einheitlich mit dem Betriebssystem Windows 10, üblichen Büro-Anwendungen (Standardsoftware für Textverarbeitung, Tabellenkalkulation und Präsentationen) und Client-Software zur E-Mail-Nutzung ausgestattet. Zusätzlich ist je nach Aufgabengebiet auf verschiedenen Rechnern Spezialsoftware installiert.

Im Netz des Standorts Bad Godesberg werden insgesamt sechs Server für folgende Zwecke eingesetzt:

- Ein Server dient als Domänen-Controller,
- zwei weitere Server dienen der Dateiablage und als Druckserver,
- ein Server dient als Datenbankserver für die Personal- und Finanzdaten,
- ein weiterer Datenbankserver dient der Kunden- und Auftragsbearbeitung und
- der fünfte Server dient als Kommunikations-Server (Mail-Server, Termin- und Adressverwaltung).

Domänen-Controller, Datei- und Druckserver sind als virtuelle Systeme auf einem Virtualisierungsserver realisiert.

Der **Standort Bonn-Beuel** ist mit zwei weiteren Servern und 70 Arbeitsplatzrechnern über eine angemietete Standleitung in das Firmennetz eingebunden. Ein Server virtualisiert einen zusätzlichen Domänen-Controller sowie je einen Datei- und Druckserver für diesen Standort. Der zweite Server dient der Produktionssteuerung und -überwachung. Die Arbeitsplatzrechner in Beuel haben die gleiche Grundausstattung wie die Rechner in der Verwaltung in Bad Godesberg. Zusätzlich ist auf mehreren PCs CAD/CAM-Software (CAD/CAM = Computer Aided Design/Computer Aided Manufacturing) installiert.

Die Produktion erfolgt durch zwei leistungsfähige speicherprogrammierbare Maschinen, die über den Server zur Produktionssteuerung kontrolliert und konfiguriert werden. Die Programme und Konfigurationen werden in der Entwicklungsabteilung erstellt.

Die **Vertriebsbüros** sind jeweils mit einem PC ausgestattet (Betriebssystem ist ebenfalls Windows 10) und über DSL an das Internet angebunden. Der Zugriff auf das Unternehmensnetz erfolgt bei Bedarf mittels Authentisierung und VPN.

Das **Unternehmensnetz** ist über DSL an das Internet angebunden. Der Internet-Zugang ist über eine Firewall und einen Router mit Paketfilter abgesichert. Alle Client-Rechner haben Zugang zum Internet (für Internet und E-Mail). Die Webseite des Unternehmens wird auf einem Webserver des Providers vorgehalten.

An weiterer Informationstechnik sind zu berücksichtigen:

- Telekommunikationsanlagen in Bad Godesberg und Beuel,
- Alarmanlagen zur Sicherung der Gebäude in Bad Godesberg und Beuel,
- insgesamt acht Faxgeräte (davon vier in Bad Godesberg, je eins in den Vertriebsbüros und eins in Beuel) sowie
- 70 Laptops (45 in Bad Godesberg, je drei in den Vertriebsbüros und 16 in Beuel), die bei Bedarf in das Netz eingebunden werden können, von entfernten Standorten aus über VPN.

Für den reibungslosen Betrieb der Informationstechnik an allen Standorten ist die zentrale IT-Abteilung in Bad Godesberg verantwortlich.

Eine Anweisung regelt den Umgang mit der betrieblichen Informationstechnik, diese darf ausschließlich für Firmenzwecke genutzt werden und das Einbringen von privater Hard- und Software ist untersagt.

2 Sicherheitsmanagement

In diesem Abschnitt werden am Beispiel der RECPLAST GmbH einige Grundelemente eines Managementsystems für Informationssicherheit dargestellt. Der Schwerpunkt liegt auf der Initialisierung des Sicherheitsprozesses und dabei insbesondere auf dem Aufbau einer Organisationsstruktur und der Entwicklung einer Leitlinie zur Informationssicherheit.

Umfassende Informationen zu den behandelten Themen und weiteren Aspekten, die beim Aufbau eines Informationssicherheitsmanagementsystems zu berücksichtigen sind, finden Sie in folgenden Dokumenten:

- BSI-Standard 200-1: *Managementsysteme für Informationssicherheit (ISMS)*,
- BSI-Standard 200-2: *IT-Grundschutz-Methodik*, insbesondere Kapitel 3 und 4, sowie
- IT-Grundschutz-Kompendium, Baustein ISMS.1 *Sicherheitsmanagement* und zugehörige Umsetzungshinweise.

2.1 Organisationsstruktur und Verantwortlichkeiten

Die Geschäftsführung der RECPLAST GmbH beabsichtigt, ein Sicherheitskonzept ausarbeiten zu lassen, das in allen Unternehmensbereichen umgesetzt werden soll. Dazu müssen die vorhandenen Grundsätze und Richtlinien zur Informationssicherheit überprüft und angepasst werden.

In einem ersten Schritt wird ein **Informationssicherheitsbeauftragter** (ISB) ernannt, der die zugehörigen Arbeiten koordinieren soll. Da diese Aufgabe umfangreiche IT-Kenntnisse erfordert, wird hierfür ein Mitarbeiter der Abteilung „Informationstechnik“ bestimmt, in seinen Aufgaben aber gleichzeitig der Geschäftsführung unterstellt. Zusätzlich ernennt diese einen **ICS-Informationssicherheitsbeauftragten** (ICS-ISB), der Sicherheitsanforderungen und -maßnahmen für den Produktionsbereich entwickeln und kontrollieren soll. Danach wird ein zeitlich befristetes Projekt „Sicherheitskonzept“ eingerichtet, das folgende Ergebnisse erzielen soll:

1. Vorschläge und Entscheidungsvorlage für eine Leitlinie zur Informationssicherheit,
2. einen Vorschlag für ein Sicherheitskonzept und einen zugehörigen Realisierungsplan,
3. Vorschläge für Maßnahmen zur Aufrechterhaltung der Informationssicherheit,
4. Dokumentation aller Entscheidungsvorlagen, Entscheidungen und der umgesetzten Maßnahmen des Informationssicherheitsprozesses.

Da der ISB die Geschäftsprozesse nicht im Detail kennt, wird ein IS-Management-Team gebildet, das den ISB und den ICS-ISB bei der Erstellung der Leitlinie und dem Sicherheitskonzept unterstützt. Ihm gehören der Datenschutzbeauftragte, der Leiter des kaufmännischen Bereichs und der Rechtsabteilung und, um Kundenanforderungen einzubeziehen, ein Mitarbeiter des Vertriebs an. So sind alle Geschäftsbereiche vertreten und können weitere Informationen über die Betriebsabläufe und externe Anforderungen einholen.

Das Projekt wird dem Betriebsrat vorgestellt, der regelmäßig über Zwischenergebnisse informiert wird. Auch die Mitarbeiter werden in einer Betriebsversammlung mit dem Projekt und seinen Zielen bekannt gemacht.

2.2 Entwicklung der Leitlinie zur Informationssicherheit

Die zuständige Projektgruppe erarbeitet idealerweise in zwei halbtägigen Sitzungen einen ersten Entwurf für eine Leitlinie. Dieser wird mit der Geschäftsführung abgestimmt und in einer weiteren Sitzung den Abteilungsleitungen und dem Betriebsrat vorgestellt. Die Diskussion zu dem anzustrebenden Sicherheitsniveau sowie den vorgesehenen organisatorischen Regelungen führt in der Regel nur zu

geringfügigen Änderungen, denen alle Beteiligten zustimmen. Die verabschiedete Leitlinie wird von der Geschäftsführung unterschrieben und auf einer Betriebsversammlung vorgestellt. Sie verdeutlicht den Stellenwert der Informationssicherheit für das Unternehmen und erläutert die Ziele und daraus abgeleiteten Maßnahmen der Leitlinie. Die in der Leitlinie formulierten Regelungen sind ab dem Zeitpunkt ihres Inkrafttretens verbindlich.

Jeder Mitarbeiter erhält eine schriftliche Ausfertigung des Dokuments. Die Geschäftsführung kündigt zudem an, die Belegschaft künftig verstärkt für Informationssicherheit zu sensibilisieren. In Schulungen soll das Wissen über mögliche Gefährdungen und zweckmäßige Gegenmaßnahmen gefördert und der sichere Umgang mit Informationen und Informationstechnik eingeübt werden.

2.3 Inhalt der Leitlinie zur Informationssicherheit

Stellenwert der Informationssicherheit und Bedeutung dieser Leitlinie

Der Erfolg der RECPLAST GmbH hängt in besonderem Maße davon ab, dass die Geschäftsinformationen aktuell und unverfälscht sind und bei Bedarf mit der gebotenen Vertraulichkeit behandelt werden.

Informationstechnik ist in allen Geschäftsbereichen eine wichtige Ressource. Sie wird auch immer wichtiger in den Beziehungen zu Kunden, Zulieferern, Partnerunternehmen, der öffentlichen Verwaltung und anderen Institutionen. Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind daher ein wesentlicher Eckpfeiler des Unternehmenserfolges.

Mit der Leitlinie erkennt die Geschäftsführung ausdrücklich an, dass die Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit der geschäftskritischen Informationen eine kontinuierlich zu verfolgende Aufgabe ist und geeignete organisatorische Grundlagen erfordert.

Die Leitlinie wird durch ein alle Unternehmensbereiche umfassendes Sicherheitskonzept ergänzt. Bei der Entwicklung dieses Konzepts stützt sich die RECPLAST GmbH auf die IT-Grundschutz-Methodik und die Vorgaben im IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik. Regelmäßige Überprüfungen sollen dafür sorgen, dass Leitlinie und das Sicherheitskonzept angemessen und aktuell bleiben.

Sicherheitsniveau und Ziele

Insbesondere für auftragsbezogene Entscheidungen und Investitionen sind aktuelle und korrekte Informationen unabdingbar. Ausfälle der Informationstechnik, die zu spürbaren Beeinträchtigungen bei der Abwicklung von Aufträgen, in der internen Kommunikation oder in den Beziehungen mit Kunden und Geschäftspartnern führen, sind nicht vertretbar.

Die Geschäftsführung der RECPLAST GmbH hat entschieden, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Grundlage für diese Entscheidung war eine Gefährdungsabschätzung über die Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit. Dies bedeutet im Einzelnen:

1. Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Beschäftigten die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur Informationssicherheit können hierbei unterstützen.
2. Vertraulichkeit und Integrität der für das Unternehmen wichtigen Informationen sind zu schützen, unabhängig davon in welcher Form sie vorliegen. Auch im Umgang mit elektronischen Dokumenten und Informationen ist daher Geheimhaltungsanweisungen strikt Folge zu leisten.

3. Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für das Unternehmen relevanten Gesetze, Vorschriften und vertragliche Verpflichtungen eingehalten werden.
4. Die Informationstechnik muss so betrieben werden, dass Geschäftsinformationen bei Bedarf hinreichend schnell verfügbar sind. Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag bei der Abwicklung von Aufträgen oder anderen wichtigen Geschäftsvorhaben führen, sind nicht tolerierbar.
5. Durch fahrlässigen Umgang mit Informationen verursachte finanzielle Schäden und ein negatives Image für das Unternehmen müssen verhindert werden. Der Zugriff auf und der Zugang zu allen wichtigen Informationen im Unternehmen werden daher strikt geregelt und kontrolliert.

Verantwortlichkeiten

Die **Geschäftsführung** hat die Gesamtverantwortung für die Informationssicherheit im Unternehmen, den Sicherheitsprozess und die zugehörigen Maßnahmen.

Für die Koordination und Überwachung aller auf Informationssicherheit bezogenen Aktivitäten wird von der Geschäftsführung die Stabsstelle eines **Informationssicherheitsbeauftragten** geschaffen. Der zuständige Mitarbeiter ist gleichzeitig zentraler Ansprechpartner für alle Fragen rund um das Thema Informationssicherheit und der Geschäftsführung berichtspflichtig.

Informationstechnik wird auch im Kernprozess der Firma, der Fertigung, immer wichtiger. Für die spezifischen Fragestellungen zur Sicherheit der Produktionssysteme und deren Steuerung wird daher mit dem **ICS-Sicherheitsbeauftragten** eine eigene Stelle geschaffen, die eng mit dem Informationssicherheitsbeauftragten zusammenarbeitet.

Informationssicherheitsbeauftragter und ICS-Sicherheitsbeauftragter bilden gemeinsam mit weiteren von der Geschäftsführung benannten Mitarbeitern ein **IS-Management-Team**, das für die Aufrechterhaltung und Weiterentwicklung der organisatorischen und technischen Sicherheitsmaßnahmen im Unternehmen zuständig ist.

Für alle Informationen, Geschäftsprozesse sowie die unterstützenden informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (**Informations-, Prozess- und Systemeigentümer**) benannt. Diese sind dafür zuständig, die geschäftliche Bedeutung von Informationen und Technik einzuschätzen und darauf zu achten, dass die Mitarbeiter dieser Bedeutung entsprechend handeln. Sie verwalten Zugriffsrechte und Autorisierungen in ihrem Zuständigkeitsbereich und sind gegenüber der Leitung rechenschaftspflichtig. Sie sind auch dafür verantwortlich, externen Dienstleistern und Kooperationspartnern die Vorgaben der RECPLAST GmbH zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

Jeder **Mitarbeiter** soll dazu beitragen, Sicherheitsvorfälle und Verletzungen der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen zu vermeiden. Erkannte Fehler sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

Geltung und Folgen von Zuwiderhandlungen

Diese Leitlinie zur Informationssicherheit gilt für die gesamte RECPLAST GmbH. Jede Mitarbeiterin und jeder Mitarbeiter ist daher angehalten, sicherheitsbewusst mit betrieblich wichtigen Informationen und der Informationstechnik umzugehen und verbindliche Sicherheitsregeln zu befolgen.

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Kunden schädigen oder den Ruf des Unternehmens gefährden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

3 Strukturanalyse

Grundlage eines jeden Sicherheitskonzepts ist eine genaue Kenntnis der im betrachteten Informationsverbund vorhandenen Informationen, ihres Stellenwertes für Geschäftsprozesse und Anwendungen sowie der organisatorischen und technischen Rahmenbedingungen, in denen sie verwendet und verarbeitet werden. Bei der Strukturanalyse geht es darum, die dazu erforderlichen Informationen zusammenzustellen und so aufzubereiten, dass sie die weiteren Schritte der IT-Grundschutz-Methodik unterstützen. Ein sinnvoller Ausgangspunkt für die Strukturanalyse sind die Geschäftsprozesse einer Institution. Es ist danach zu fragen, welche Anwendungen und Informationen jeweils wichtig für einzelne Geschäftsprozesse sind. Anschließend können die technischen Systeme und Infrastrukturkomponenten ermittelt und den Anwendungen zugeordnet werden. Zur Strukturanalyse gehören folglich die folgenden Teilschritte:

1. Erfassung der zum Geltungsbereich gehörigen Geschäftsprozesse, Anwendungen und Informationen,
2. Netzplanerhebung,
3. Erfassung der IT-Systeme sowie
4. Erfassung der Räume.

Bei allen Schritten können der Umfang und die Komplexität der erhobenen Informationen durch die Bildung angemessener Gruppen reduziert werden.

Weitere Informationen zur Strukturanalyse finden Sie in Kapitel 8.1 des BSI-Standards 200-2.

3.1 Erfassung der Geschäftsprozesse, Anwendungen und Informationen

Das Organigramm in Abbildung 1 auf Seite 5 veranschaulicht die organisatorische Gliederung der RECPLAST GmbH.

Jeder Abteilung lassen sich verschiedene Geschäftsprozesse zuordnen, beispielsweise

- Einkauf: Prozesse wie Produktrecherche und Bestellung,
- Informationstechnik: Prozesse wie die zum Betrieb von Servern und Clients, Benutzer-Service, Druckservice oder Netzadministration,
- Personalabteilung: Prozesse wie Einstellung, Gehaltszahlung und Fortbildung sowie
- Fertigung der Produktionsabteilung: die beiden Prozesse zur Umwandlung der Altkunststoffe in wiederverwertbare Regranulate sowie zur Herstellung der neuen Produkte aus diesem Rohmaterialien.

Viele dieser Prozesse können weiter untergliedert werden, beispielsweise die Server-Administration in die Teilprozesse Verwaltung von Mail-, Datei- und Datenbankservern, zu denen jeweils Aktivitäten wie Patch-Management, Datensicherung, Konfiguration oder Dokumentation gehören.

Die folgende Tabelle enthält einen Ausschnitt mit den wichtigsten Geschäftsprozessen (GP). Hinter dem Kürzel „GP“ folgt eine Prozessnummer, 001 bis 009 sind Hauptprozesse. In der kurzen Beschreibung wird angegeben, ob es sich um einen Kern- oder unterstützenden Prozess handelt, und welche Informationen verarbeitet werden. Die für einen Prozess benötigten Anwendungen werden in Tabelle 3 zugeordnet.

Bezeichnung	Name und Beschreibung des Prozesses	Prozess-Verantwortlicher	Mitarbeiter
GP001	**Produktion (Kerngeschäft):** Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis zur Einlagerung des produzierten Materials. Hierzu gehören innerhalb der Produktion die internen Transportwege, die Produktion und Fertigung der verschiedenen Komponenten und das Verpacken der Teile. Es werden alle Informationen über Aufträge, Lagerbestände und Stücklisten verarbeitet.	Leiter Produktion	Alle Mitarbeiter
GP002	**Angebotswesen (unterstützender Prozess):** In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im Regelfall werden Kundenanfragen formlos per E-Mail oder Fax geschickt. Die Angebote werden elektronisch erfasst und ein schriftliches Angebot per Post an den Kunden versendet. Im Angebotswesen werden Kundendaten, Lagerbestände, Anfragen und Angebote bearbeitet.	Leiter Angebotswesen	Vertrieb
GP003	**Auftragsabwicklung (Kerngeschäft):** Kunden schicken die Bestellungen im Regelfall per Fax oder E-Mail. Alle Belege müssen ausgedruckt und elektronisch erfasst werden. Eine Auftragsbestätigung erhält der Kunde nur, wenn er dies ausdrücklich wünscht oder der Produktionsprozess von der üblichen Produktionszeit abweicht. Die Auftragsabwicklung verwendet Kundendaten, Lagerbestände, Aufträge und Bestellungen.	Leiter Auftrags-abwicklung	Vertrieb
GP004	**Einkauf (unterstützender Prozess):** In der Einkaufsabteilung werden alle erforderlichen Artikel bestellt, die nicht für den Produktionsprozess erforderlich sind. In dieser Abteilung werden externe Projekte verhandelt, IT-Verträge gestaltet und Verbrauchsmaterial im organisatorischen Umfeld (Papier, Toner etc.) beschafft. Die verwendeten Informationen sind Lagerbestände, Bedarfsmeldungen und Informationen über Lieferanten.	Leiter Einkauf	Einkauf
GP005	**Disposition (Kerngeschäft):** In der Disposition werden alle für die Produktion benötigten Materialien (Kunststoffe, Schrauben, Tüten, etc.) beschafft. Hierzu liegen normalerweise Rahmenverträge vor. Geplant wird in diesem Umfeld anhand von Jahresplanmengen und verschiedenen Bestellwerten.	Leiter Disposition	Disposition, Produktion
GP006	**Personalverwaltung (unterstützender Prozess):** In dieser Abteilung werden alle Aufgaben bearbeitet, die zur administrativen Abwicklung des Personalwesens erforderlich sind. Die dazu genutzten Daten sind personenbezogen.	Leiter Personal-abteilung	Personalabteilung, Geschäftsführung
GP006a	**Gehaltszahlung (unterstützender Prozess):** Teilprozess von GP006. In der Personalabteilung wird insbesondere die monatliche Gehaltszahlung vorbereitet und durchgeführt. Die dazu genutzten Daten sind personenbezogen.	Leiter Personal-abteilung	Personalabteilung
GP006b	**Neueinstellung (unterstützender Prozess):** Teilprozess von GP006. Die Abteilung ist auch an der Neueinstellung von Mitarbeitern beteiligt. Es fallen Informationen an, die dem Datenschutz unterliegen.	Leiter Personal-abteilung	Geschäftsführung, Personalabteilung
GP007	**IT-Betrieb (unterstützender Prozess):** Die IT-Abteilung sorgt für den störungsfreien Betrieb der IT-Infrastruktur der Server, Clients und Netze. Beim Betrieb der Produktions-IT wird sie von Mitarbeitern der Produktionsabteilung unterstützt. Es wird mit Konfigurationsdaten der IT-Systeme gearbeitet.	Leiter IT-Abteilung	IT-Abteilung

Bezeichnung	Name und Beschreibung des Prozesses	Prozess-Verantwortlicher	Mitarbeiter
GP071	**Betrieb Server (unterstützender Prozess):** Teilprozess von GP007. Dieser Prozess umfasst Beschaffung, Installation, Konfiguration und Pflege der erforderlichen Hard- und Software sowie die Beratung der Nutzer. Dazu wird mit Konfigurationsdaten der Systeme gearbeitet.	Leiter IT-Abteilung	IT-Abteilung
GP072	**Betrieb Clients: (unterstützender Prozess):** Teilprozess von GP007. Dieser Prozess umfasst Beschaffung, Installation, Konfiguration und Pflege der erforderlichen Hard- und Software sowie die Beratung der Nutzer. Dazu wird mit Konfigurationsdaten der Systeme gearbeitet.	Leiter IT-Abteilung	IT-Abteilung
GP073	**Betrieb Netze (unterstützender Prozess):** Teilprozess von GP007. Der Prozess umfasst Beschaffung, Installation, Konfiguration und Pflege der aktiven Komponenten sowie – gemeinsam mit der Abteilung Haustechnik – Verlegung und Wartung der Übertragungsleitungen. Dazu wird mit Konfigurationsdaten der Netzkomponenten gearbeitet.	Leiter IT-Abteilung	IT-Abteilung
GP074	**Betrieb Produktions-IT (unterstützender Prozess):** Teilprozess von GP007. In diesem Prozess werden Beschaffung, Installation und Betrieb der IT-Systeme durchgeführt, die für Überwachung und Steuerung der Produktion erforderlich sind. Verantwortlich ist der Leiter der Produktionsabteilung unter Mitwirkung der IT-Abteilung. Es wird mit Konfigurationsdaten der Systeme und Produktionsdaten gearbeitet.	Leiter Produktion	IT-Abteilung

Tabelle 1: Geschäftsprozesse der RECPLAST GmbH

Bei der Erhebung der Anwendungen werden die wichtigsten Anwendungen einer Institution erfasst, also diejenigen,

- deren Daten, Informationen und Programme den höchsten Bedarf an Geheimhaltung (Vertraulichkeit) haben,
- deren Daten, Informationen und Programme den höchsten Bedarf an Korrektheit und Unverfälschtheit (Integrität) haben oder
- welche die kürzeste tolerierbare Ausfallzeit (höchster Bedarf an Verfügbarkeit) haben.

Eine vollständige Übersicht aller Anwendungen, die im Zusammenhang mit den oben genannten Prozessen bedeutsam sind, wäre zu umfangreich für diesen Kurs. Die nachfolgende Tabelle enthält daher nur einen Ausschnitt.

Bezeichnung	Name und Beschreibung der Anwendung	Anzahl	Benutzer	Verantwortlich/ Administrator
A001	**Textverarbeitung, Präsentation, Tabellenkalkulation:** Alle geschäftlichen Informationen werden in einem Office-Produkt verarbeitet, Geschäftsbriefe, Analysen oder Präsentationen.	290	Alle Mitarbeiter	IT-Betrieb
A002	**Lotus Notes:** Diese Anwendung wird von allen Mitarbeitern für die Bearbeitung von Mailnachrichten, Terminen und Kontakten genutzt.	290	Alle Mitarbeiter	IT-Betrieb
A003	**Internet-Recherche**	290	Alle Mitarbeiter	IT-Betrieb
A004	**Prozessleitsystem:** zur Steuerung der SPS-Systeme	1	Produktion	Leiter Produktion
A005	**Entwicklungssystem:** zur Entwicklung von SPS-Programmierungen	75	Entwicklung	Leiter Produktion

Bezeichnung	Name und Beschreibung der Anwendung	Anzahl	Benutzer	Verantwortlich/ Administrator
A006	**Personaldatenverarbeitung**	17	Personal-abteilung	Personal-abteilung
A007	**Reisekostenabrechnung**	17	Personal-abteilung	Personal-abteilung
A008	**Finanzbuchhaltung**	32	Buchhaltung	Buchhaltung
A009	**Auftrags- und Kundenverwaltung**	55	Marketing/ Vertrieb	Marketing/ Vertrieb
A010	**Active Directory** Zu allen Benutzern der IT-Systeme werden Informationen zu Gruppenzugehörigkeit, Rechten und Authentisierungsmerkmalen verarbeitet und gespeichert. Diese Anwendung ist über beide Domain Controller verfügbar.	2	Alle Mitarbeiter	IT-Abteilung
A011	**Systemmanagement**	35	IT-Abteilung	IT-Abteilung
A012	**Zentrale Dokumentenverwaltung**	2	Alle Mitarbeiter	IT-Abteilung
A013	**Druckservice Bad Godesberg** Über diesen Dienst können alle Mitarbeiter in Bad Godesberg die dortigen Drucker benutzen. Er ist auf dem Druckserver in Bad Godesberg verfügbar, kann aber bei Bedarf auch auf dem Druckserver in Beuel gestartet werden.	1	Alle Abteilungen in Bad Godesberg	IT-Abteilung
A014	**Druckservice Beuel** Über diesen Dienst können alle Mitarbeiter in Beuel die dortigen Drucker benutzen. Er ist auf dem Druckserver in Beuel verfügbar, kann aber bei Bedarf auch auf dem Druckserver in Bad Godesberg gestartet werden.	1	Alle Abteilungen in Beuel	IT-Abteilung
A015	**Firewall** Die Anwendung steuert die Kommunikation zwischen dem Firmennetz und dem Internet und ermöglicht die verschlüsselte Kommunikation der Vertriebsbüros über VPN-Tunnel.	1	Alle Mitarbeiter	IT-Abteilung
A016	**TK-Vermittlung** Über die beiden miteinander gekoppelten TK-Anlagen in Bad Godesberg und Beuel werden ein- und ausgehende Telefongespräche und Fax-Nachrichten vermittelt und ein Telefonverzeichnis gepflegt.	2	Alle Mitarbeiter	IT-Abteilung

Tabelle 2: Anwendungen der RECPLAST GmbH

Der Zusammenhang zwischen Geschäftsprozessen und Anwendungen wird durch eine Zuordnungstabelle dargestellt – nachfolgend nur ein Ausschnitt für die Hauptgeschäftsprozesse:

Geschäftsprozess	Anwendung									
	A001	A002	A003	A004	A005	A006	A007	A008	A009	A010
GP001	X			X	X				X	X
GP002	X	X	X	X					X	X
GP003	X	X		X				X	X	X
GP004	X	X	X					X		X
GP005	X	X	X	X				X	X	X

Tabelle 3: Zuordnung der Anwendungen zu Geschäftsprozessen

3.2 Erhebung des Netzplans

Bei der RECPLAST GmbH dient ein Netzplan als Ausgangspunkt für die Erhebung der technischen Systeme im Rahmen der Strukturanalyse. Abbildung 2 zeigt eine grobe und Abbildung 3 eine detaillierte Darstellung dieses Dokuments.

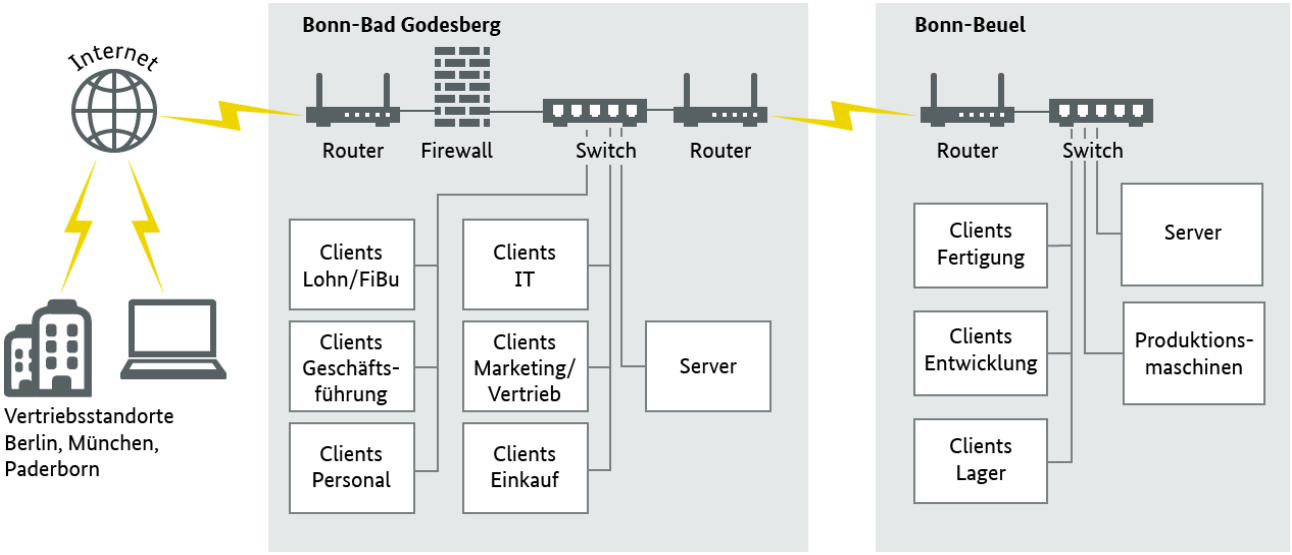

Abbildung 2: Netzplan der RECPLAST GmbH – Übersicht

In beiden Netzplänen sind die IT-Komponenten zu Gruppen zusammengefasst, soweit dies sinnvoll ist. Grundsätzlich ist eine solche „Bereinigung“ des Netzplans immer dann zulässig, wenn die zusammengefassten Komponenten

- vom gleichen Typ sind,
- gleich oder nahezu gleich konfiguriert sind,
- gleich oder nahezu gleich in das Netz eingebunden sind,
- den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen,
- ähnliche Anwendungen bedienen **und**
- den gleichen Schutzbedarf haben.

Die folgenden Beispiele veranschaulichen, wie diese Kriterien angewendet werden können:

- Die Clients der Abteilungen „Fertigung“ und „Lager“ wurden zusammengefasst, da sie grundsätzlich gleich ausgestattet sind und mit ihnen auf weitgehend identische Datenbestände zugegriffen werden kann.
- Die drei Vertriebsbüros zeichnen sich durch eine einheitliche Ausstattung, übereinstimmende Aufgaben und Regelungen sowie eine identische Zugangsmöglichkeit zum Firmennetz aus. Sie lassen sich in gewisser Weise mit häuslichen Telearbeitsplätzen vergleichen. Sie wurden deswegen zu einer Gruppe zusammengefasst.
- Die nicht vernetzten Komponenten TK-Anlagen und Faxgeräte wurden standortübergreifend zu jeweils einer Gruppe zusammengefasst, da für den Umgang mit diesen Geräten übereinstimmende organisatorische Regelungen gelten.

Folgende Clients sollten **nicht zusammengefasst** werden:

- Bei den Rechnern der **Geschäftsführung** ist von einem höheren Schutzbedarf auszugehen (z. B. könnte auf ihnen besonders vertrauliche Korrespondenz gespeichert sein).
- Die höhere Vertraulichkeit der Daten ist auch ein Grund dafür, die Rechner der **Entwicklungsabteilung** gesondert zu erfassen. Auf ihnen befinden sich Konstruktionspläne und unter Umständen kundenspezifische Entwicklungen und Verfahrensbeschreibungen, die z. B. vor Wirtschaftsspionage und damit möglichen gravierenden wirtschaftlichen Folgen für die Firma zu schützen sind.
- Eine hohe Vertraulichkeit besitzen auch die Informationen, die in der **Personalabteilung** bearbeitet werden, sowie diejenigen aus der **Finanz- und Lohnbuchhaltung**.
- Auf Rechnern der **IT-Administratoren** laufen Anwendungen, die für die Verwaltung des Netzes erforderlich sind. Von daher verlangen auch diese Rechner eine besondere Aufmerksamkeit und werden nicht mit anderen zusammengefasst.

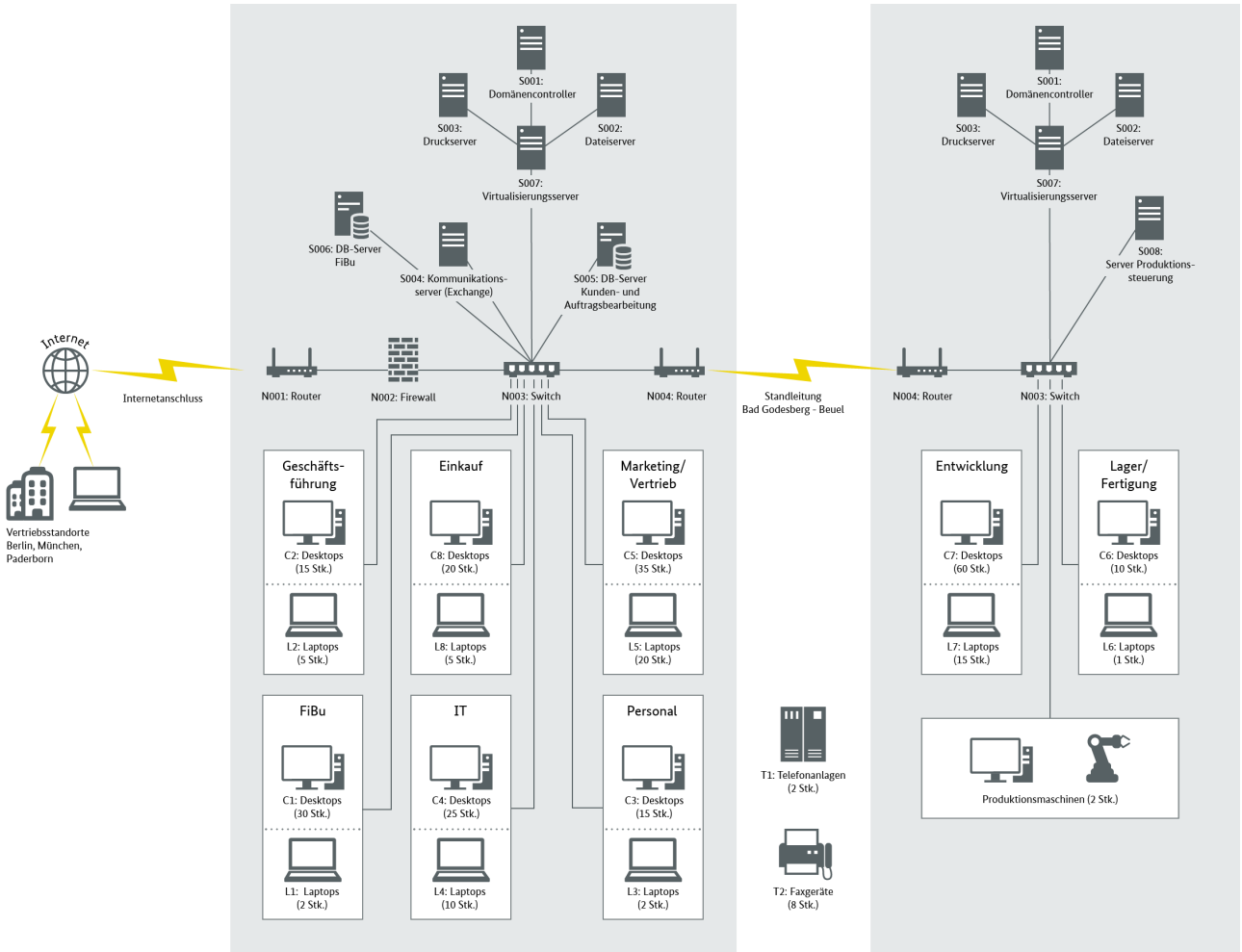

Abbildung 3: Netzplan der RECPLAST GmbH - Detaildarstellung

3.3 Erhebung der IT-Systeme

Bei der Erhebung der IT-Systeme geht es darum, die vorhandenen und geplanten IT-Systeme und die sie jeweils charakterisierenden Angaben zusammenzustellen. Dazu zählen:

- alle im Netz vorhandenen Computer (Clients und Server), Gruppen von Computern und aktiven Netzkomponenten, Netzdrucker, aber auch
- nicht vernetzte Computer (wie Internet PCs) und
- Telekommunikationskomponenten (wie TK-Anlagen, Faxgeräte, Mobiltelefone und Anrufbeantworter).

Die Erhebung der IT-Systeme bei der RECPLAST GmbH ergab die nachfolgend zusammengestellten Übersichten.

In den Tabellen sind die IT-Systeme jeweils durchnummeriert. Ein vorangestellter Buchstabe kennzeichnet ihren Typ: S = Server, C = Arbeitsplatzrechner (Client), L = Laptop, N = Netzkomponente, T = Telekommunikationskomponente, I = ICS-Systeme, O = Anderes.

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
S001	Domänen-Controller (virtualisiert)	Windows Server 2012	Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration
S002	Dateiserver (virtualisiert)	Windows Server 2012	Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration
S003	Druckserver (virtualisiert)	Windows Server 2012	Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration
S004	Kommunikationsserver	Windows Server 2012 mit Exchange	Bad Godesberg R. 1.02 (Serverraum)	1	Alle IT-Benutzer/ IT-Administration
S005	DB-Server der Kunden- und Auftragsbearbeitung	Windows Server 2012	Bad Godesberg, R. 1.02 (Serverraum)	1	Marketing und Vertrieb, Fertigung, Lager/ IT-Administration
S006	DB-Server der Finanzbuchhaltung	Windows Server 2012	Bad Godesberg, R. 1.02 (Serverraum)	1	Mitarbeiter der Finanzbuchhaltung/ IT-Administration
S007	Virtualisierungsserver	Linux	Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Administratoren/ IT-Administration
S008	Server für Produktionssteuerung	Linux	Beuel, R. 2.01 (Serverraum)	1	Mitarbeiter der Produktion/ IT-Administration

Tabelle 4: Übersicht zu den Servern der RECPLAST GmbH

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
I001	Speicherprogrammierbare Produktionsmaschinen (SPS)	SPS	Bad Godesberg, (Werkhalle)	2	Produktion/ IT-Administration
S200	Alarmanlagen für Gebäude in Bad Godesberg und Beuel		Bad Godesberg, Beuel	2	Haustechnik

Tabelle 5: Übersicht zu industriellen Steuerungen und sonstigen IT-Systemen der RECPLAST GmbH

In der folgenden Tabelle sind Anwendungen und Server einander zugeordnet. Ein „X“ bedeutet, dass die Ausführung einer Anwendung von dem betreffenden Server abhängt.

Nr.	Beschreibung	S001	S002	S003	S004	S005	S006	S007	S008
A001	Office-Anwendungen		X					X	
A002	E-Mail und Terminkalender	X			X			X	
A003	Internet-Recherche		X					X	
A004	Prozessleitsystem								X
A005	Entwicklungssystem		X					X	
A006	Personaldatenverarbeitung	X						X	
A007	Reisekostenabrechnung		X				X	X	
A008	Finanzbuchhaltung		X				X	X	
A009	Auftrags- und Kundenverwaltung		X			X	X	X	
A010	Active Directory	X						X	
A011	Systemmanagement	X						X	
A012	Zentrale Dokumentenverwaltung		X					X	
A013	Druckservice Bad Godesberg			X				X	
A014	Druckservice Beuel			X				X	
A015	Application Gateway								
A016	TK-Vermittlung								

Tabelle 6: Verknüpfungen zwischen Anwendungen und Servern

Als Clients werden alle Einzelplatz-PCs erfasst. Die Unterscheidung zwischen ortsfesten Desktoprechnern und Laptops ist erforderlich, da für mobile Systeme zusätzliche Sicherheitsanforderungen bestehen.

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
C1	Desktops der Finanzbuchhaltung	Windows 10	BG, R. 2.10 – 2.12	30	Mitarbeiter in der Finanzbuchhaltung IT-Administration
C2	Desktops der Geschäftsführung	Windows 10	BG, R. 1.10 – 1.13	15	Geschäftsführung/ IT-Administration
C3	Desktops der Personalabteilung	Windows 10	BG, R. 1.07 – 1.09	15	Mitarbeiter der Personalabteilung/ IT-Administration
C4	Desktops der Informationstechnik	Windows 10	BG, R. 1.03 – 1.06	25	Mitarbeiter IT/ IT-Administration

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
C5	Desktops Marketing & Vertrieb	Windows 10	BG, R. 2.03 – 2.09	35	Marketing und Vertrieb/ IT-Administration
C6	Desktops von Fertigung und Lager	Windows 10	Beuel, R. 2.10 – 2.13	10	Mitarbeiter Fertigung und Lager/IT-Administration
C7	Desktops der Entwicklungsabteilung	Windows 10	Beuel, R. 2.14 – 2.20	60	Entwicklung/ IT-Administration
C8	Desktops der Einkaufsabteilung	Windows 10	BG, R. 2.13 – 2.17	20	Mitarbeiter des Einkaufs/ IT-Administration
C9	Laptops in den Vertriebsbüros	Windows 10	Vertriebsbüros (Berlin, Paderborn, München)	9	Mitarbeiter in den Vertriebsbüros / IT-Administration
L1	Laptops der Finanzbuchhaltung	Windows 10	BG, R. 2.10 – 2.12	2	Mitarbeiter in der Finanzbuchhaltung IT-Administration
L2	Laptops der Geschäftsführung	Windows 10	BG, R. 1.10 – 1.13	5	Geschäftsführung/ IT-Administration
L3	Laptops der Personalabteilung	Windows 10	BG, R. 1.07 – 1.09	2	Mitarbeiter der Personalabteilung/ IT-Administration
L4	Laptops der Informationstechnik	Windows 10	BG, R. 1.03 – 1.06	10	Mitarbeiter IT/ IT-Administration
L5	Laptops Marketing & Vertrieb	Windows 10	BG, R. 2.03 – 2.09	20	Marketing und Vertrieb/ IT-Administration
L6	Laptops von Fertigung und Lager	Windows 10	Beuel, R. 2.10 – 2.13	1	Mitarbeiter Fertigung und Lager/IT-Administration
L7	Laptops der Entwicklungsabteilung	Windows 10	Beuel, R. 2.14 – 2.20	15	Entwicklung/ IT-Administration
L8	Laptops der Einkaufsabteilung	Windows 10	BG, R. 2.13 – 2.17	5	Mitarbeiter des Einkaufs/ IT-Administration
L9	Laptops in den Vertriebsbüros	Windows 10	Vertriebsbüros (Berlin, Paderborn, München)	9	Mitarbeiter in den Vertriebsbüros / IT-Administration

Tabelle 7: Übersicht zu den Clients der RECPLAST GmbH

In der folgenden Tabelle sind Anwendungen und Clients (Arbeitsplatzrechner) einander zugeordnet. Ein „X“ bedeutet, dass die Ausführung einer Anwendung von dem betreffenden Client abhängt. Die Zuordnung gilt in gleicher Weise für die entsprechenden Laptops L1 bis L9.

Nr.	Beschreibung	C1	C2	C3	C4	C5	C6	C7	C8	C9
A001	Office-Anwendungen	X	X	X	X	X	X	X	X	X
A002	E-Mail und Terminkalender	X	X	X	X	X	X	X	X	X
A003	Internet-Recherche	X	X	X	X	X			X	X
A004	Prozessleitsystem						X	X		
A005	Entwicklungssystem						X	X		
A006	Personaldatenverarbeitung		X	X						
A007	Reisekostenabrechnung			X						
A008	Finanzbuchhaltung	X	X							

Nr.	Beschreibung	C1	C2	C3	C4	C5	C6	C7	C8	C9
A009	Auftrags- und Kundenverwaltung	X	X			X	X		X	X
A010	Active Directory	X	X	X	X	X	X	X	X	X
A011	Systemmanagement				X		X			
A012	Zentrale Dokumentenverwaltung	X	X	X	X	X	X	X	X	X
A013	Druckservice BG	X	X	X	X	X			X	
A014	Druckservice Beuel						X	X		
A015	Application Gateway	X	X	X	X	X	X	X	X	X
A016	TK-Vermittlung									

Tabelle 8: Verknüpfungen zwischen Anwendungen und Clients

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
N1	Router zum Internet	DSL-Router	Bad Godesberg, R. 1.02 (Serverraum)	1	Alle IT-Benutzer/ IT-Administration
N2	Firewall		Bad Godesberg, R. 1.02 (Serverraum)	1	Alle IT-Benutzer/ IT-Administration
N3	Zentrale Switche in Bad Godesberg und Beuel		Bad Godesberg, R. 1.02 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration
			Beuel, R. 2.01 (Serverraum)		
N4	Router zur Verbindung der Standorte Bad Godesberg und Beuel		Bad Godesberg, R. 1.02 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration
			Beuel, R. 2.01 (Serverraum)		
T1	Telefonanlagen Bad Godesberg und Beuel	TK-Anlage	Bad Godesberg, R. 1.01	2	Alle Mitarbeiter/ IT-Administration
			Beuel, R. 2.02		
T3	Faxgeräte		4 in Bad Godesberg, je 1 in Beuel und in den Vertriebsbüros	8	Alle Mitarbeiter

Tabelle 9: Übersicht zu den Netz- und Telekommunikationskomponenten bei der RECPLAST GmbH

In der folgenden Tabelle sind Anwendungen sowie Netz- und Telekommunikationskomponenten einander zugeordnet. Ein „X“ bedeutet, dass die Ausführung einer Anwendung von der betreffenden Komponente abhängt.

Nr.	Beschreibung	N1	N2	N3	N4	T1	T2
A001	Office-Anwendungen			X	X		
A002	E-Mail und Terminkalender	X	X	X	X		
A003	Internet-Recherche	X	X	X	X		
A004	Prozessleitsystem			X	X		
A005	Entwicklungssystem			X	X		
A006	Personaldatenverarbeitung			X			
A007	Reisekostenabrechnung			X			

Nr.	Beschreibung	N1	N2	N3	N4	T1	T2
A008	Finanzbuchhaltung			X			
A009	Auftrags- und Kundenverwaltung			X			
A010	Active Directory			X	X		
A011	Systemmanagement			X	X		
A012	Zentrale Dokumentenverwaltung			X	X		
A013	Druckservice BG			X			
A014	Druckservice Beuel			X	X		
A015	Application Gateway		X				
A016	TK-Vermittlung					X	

Tabelle 10: Verknüpfungen zwischen Anwendungen und Netz- und Telekommunikationskomponenten

3.4 Erhebung der räumlichen Gegebenheiten

Bei der Strukturanalyse wurden die in der folgenden Tabelle aufgeführten Gebäude und Räume erfasst. Die Dokumentation enthält auch Angaben zu den in einem Raum befindlichen IT-Komponenten:

Gebäude/Raum				IT-Komponenten
Kürzel	Bezeichnung	Art	Lokation	IT-Systeme
GB1	Verwaltungsgebäude	Gebäude	Bonn-Bad Godesberg	
GB2	Produktionsgebäude	Gebäude	Bonn-Beuel	
R001	Technikraum Bad Godesberg (BG, R. 1.01)	Technikraum	GB1	T1
R002	Serverraum Bad Godesberg (BG, R. 1.02)	Serverraum	GB1	S001 bis S007 N1 bis N4
R003	Büros IT-Abteilung (BG, R. 1.03 – 1.06)	Büroräume	GB1	C4, L4
R004	Büros Personalabteilung (BG, R. 1.07 – 1.09)	Büroräume	GB1	C3, L3
R005	Büros Geschäftsführung (BG, R. 1.10 – 1.13)	Büroräume	GB1	C2, L2
R006	Büros Marketing/Vertrieb (BG, R. 2.03 – 2.09)	Büroräume	GB1	C5, L5, T2
R007	Büros Lohn/Fibu (BG, R. 2.10 – 2.12)	Büroräume	GB1	C1, L1
R008	Büros Einkauf (BG, R. 2.13 – 2.17)	Büroräume	GB1	C8, L8, T2
R009	Serverraum-Beuel (Beuel, R. 2.01)	Serverraum	GB2	S001 bis S003, S007, S008, N3, N4
R010	Technikraum Beuel (Beuel, R. 2.02)	Technikraum	GB2	T1

Gebäude/Raum				IT-Komponenten
Kürzel	**Bezeichnung**	**Art**	**Lokation**	**IT-Systeme**
R011	Büros Fertigung/Lager (Beuel, R. 2.10 – 2.13)	Büroräume	GB2	C6, L6, T2
R012	Büros Entwicklungsabteilung (Beuel, R. 2.14 – 2.20)	Büroräume	GB2	C7, L7
R013	Produktionshalle Beuel	Werkhalle	GB2	I001, I002
R014	Vertriebsbüros (3 Standorte)	Häuslicher Arbeitsplatz	Berlin, Paderborn, München	C9, L9, T2
R015	Außendienst	Mobiler Arbeitsplatz	Mitarbeiter aller Standorte (mit Laptops)	L1 bis L9

Tabelle 11: Übersicht zu den erfassten Gebäuden und Räumen der RECPLAST GmbH

4 Schutzbedarfsfeststellung

Wie viel Schutz benötigen Informationen, Anwendungen und die zugehörigen technischen Systeme und Infrastruktur-Komponenten? Wie lässt sich der Schutzbedarf nachvollziehbar begründen? Welche Komponenten benötigen mehr Sicherheit, wann genügen elementare Schutzmaßnahmen?

Ziel der Schutzbedarfsfeststellung ist es, diese Fragen zu klären und damit die Auswahl der **angemessenen Sicherheitsmaßnahmen** für Geschäftsprozesse, Informationen, Anwendungen, IT-Systeme, Räume und Kommunikationsverbindungen zu unterstützen.

Zur Schutzbedarfsfeststellung gehören die folgenden Aktivitäten:

1. die auf eine Institution zugeschnittene Definition von Schutzbedarfskategorien (z. B. „normal“, „hoch“, „sehr hoch“),
2. die Feststellung des Schutzbedarfs der in der Strukturanalyse erfassten Anwendungen mit Hilfe dieser Kategorien,
3. die Ableitung des Schutzbedarfs der IT-Systeme aus dem Schutzbedarf der Anwendungen,
4. daraus abgeleitet die Feststellung des Schutzbedarfs der Kommunikationsverbindungen und der räumlichen Gegebenheiten sowie
5. die Dokumentation und Auswertung der vorgenommenen Einschätzungen.

Weitere Informationen zur Schutzbedarfsfeststellung finden Sie in BSI-Standard 200-2, Kapitel 8.2.

4.1 Anpassung der Schutzbedarfskategorien

Bei der RECPLAST GmbH wurden die Schutzbedarfskategorien vom einberufenen Sicherheitsmanagement-Team folgendermaßen definiert und mit der Geschäftsführung abgestimmt:

Schutzbedarfskategorie normal:

Ein möglicher Schaden hätte begrenzte, überschaubare Auswirkungen auf die RECPLAST GmbH:

- Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen allenfalls geringfügige juristische Konsequenzen oder Konventionalstrafen.
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten nur geringfügige Auswirkungen auf die davon Betroffenen und würden von diesen toleriert.
- Die persönliche Unversehrtheit wird nicht beeinträchtigt.
- Die Abläufe bei der RECPLAST GmbH werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.
- Es droht kein Ansehensverlust bei Kunden und Geschäftspartnern.
- Der mögliche finanzielle Schaden liegt unter 50.000 Euro.

Schutzbedarfskategorie hoch:

Ein möglicher Schaden hätte beträchtliche Auswirkungen auf die RECPLAST GmbH:

- Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen schwerwiegende juristische Konsequenzen oder hohe Konventionalstrafen.
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten beträchtliche Auswirkungen auf die davon Betroffenen und würden von diesen nicht toleriert werden.

- Die persönliche Unversehrtheit wird beeinträchtigt, allerdings nicht mit dauerhaften Folgen.
- Die Abläufe bei der RECPLAST GmbH werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.
- Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird erheblich beeinträchtigt.
- Der mögliche finanzielle Schaden liegt zwischen 50.000 und 500.000 Euro.

Schutzbedarfskategorie sehr hoch:

- Ein möglicher Schaden hätte katastrophale Auswirkungen:
- Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen juristische Konsequenzen oder Konventionalstrafen, die die Existenz des Unternehmens gefährden.
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten ruinöse Auswirkungen auf die gesellschaftliche oder wirtschaftliche Stellung der davon Betroffenen.
- Die persönliche Unversehrtheit wird sehr stark und mit bleibenden Folgen beeinträchtigt.
- Die Abläufe bei der RECPLAST GmbH werden so stark beeinträchtigt, dass Ausfallzeiten, die über zwei Stunden hinausgehen, nicht toleriert werden können.
- Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird grundlegend und nachhaltig beschädigt.
- Der mögliche finanzielle Schaden liegt über 500.000 Euro.

4.2 Schutzbedarfsfeststellung für Anwendungen

Zunächst ist der Schutzbedarf der bei der Strukturanalyse erfassten Anwendungen festzustellen. Dies bedeutet, dass für jede Anwendung mit Hilfe der zuvor festgelegten Kategorien bestimmt werden muss, wie groß ihr Bedarf an Vertraulichkeit, Integrität und Verfügbarkeit ist. Die folgende Tabelle zeigt die Ergebnisse dieser Aktivität bei der RECPLAST GmbH.

Anwendung		**Schutzbedarfsfeststellung**		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
A001	Office-Anwendungen	Vertraulichkeit	normal	Zwar werden unter Umständen auch vertrauliche Dokumente mit den Anwendungen angefertigt, die Anwendung selber hat dadurch jedoch noch keinen hohen Schutzbedarf bezüglich Vertraulichkeit.
		Integrität	normal	Fehlerhafte Daten können leicht erkannt und korrigiert werden. Es sind keine finanziellen Schäden zu erwarten.
		Verfügbarkeit	normal	Der Ausfall auf einem Client ist bis zu einer Woche hinnehmbar. Ersatzweise kann auf einem Laptop weitergearbeitet werden.
A002	Lotus Notes	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.

Anwendung		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
		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.
A003	Internet-Recherche	Vertraulichkeit	normal	Es werden keine vertraulichen Daten verarbeitet.
		Integrität	normal	Fehlerhafte Daten werden in der Regel leicht erkannt.
		Verfügbarkeit	**hoch**	Die Recherche im Internet ist für einige Abteilungen wichtig (insbesondere für die Einkaufsabteilung). Ein Ausfall ist höchstens 24 Stunden hinnehmbar.
A004	Prozessleitsystem	Vertraulichkeit	**hoch**	Die eingesetzten Prozesse und Verfahren sind Objekte der Wirtschaftsspionage.
		Integrität	**hoch**	Verfälschte Informationen führen zur Störungen, können aber nach kurzer Unterbrechung der Produktion aus der Datensicherung korrigiert werden.
		Verfügbarkeit	**Sehr hoch**	Ein Stillstand der Produktion durch Ausfall des Systems kann höchstens für 2 Stunden toleriert werden.
A005	Entwicklungssystem	Vertraulichkeit	**Sehr hoch**	Die hier entwickelten Verfahren und Abläufe können Ziel von Wirtschaftsspionage sein und patentrechtliche Bedeutung haben.
		Integrität	**hoch**	Manipulationen an den Ergebnissen können später zu Störungen im Betrieb führen.
		Verfügbarkeit	normal	Da die Entwicklungsergebnisse noch nicht produktiv sind, sind Ausfälle von mehreren Tagen hinnehmbar.
A006	Personaldatenverarbeitung	Vertraulichkeit	**hoch**	Personaldaten sind besonders schutzbedürftige Daten, deren Missbrauch die Betroffenen erheblich beeinträchtigen kann.
		Integrität	normal	Fehler werden rasch erkannt und können entweder aus der Datensicherung eingespielt oder durch manuelle Eingabe korrigiert werden.
		Verfügbarkeit	normal	Ausfälle bis zu einer Woche können mit manuellen Verfahren überbrückt werden.
A007	Reisekostenabrechnung	Vertraulichkeit	**hoch**	Auch Reisekostendaten sind personenbezogene Daten und damit schützenswert.
		Integrität	normal	Fehler werden rasch erkannt und können nachträglich korrigiert werden.
		Verfügbarkeit	normal	Ausfälle können mittels manueller Verfahren überbrückt werden.
A008	Finanzbuchhaltung	Vertraulichkeit	**hoch**	Wenn vertrauliche Finanzdaten des Unternehmens Unbefugten zugänglich werden, kann dies hohe finanzielle Schäden und Ansehensverluste bewirken.
		Integrität	**hoch**	Alle Finanzdispositionen setzen korrekte Daten voraus. Bei falschen Daten sind finanzielle Schäden über 50.000 EURO möglich.
		Verfügbarkeit	normal	Ein Ausfall bis zu drei Tagen kann (mit zumutbarem Mehraufwand) manuell überbrückt werden.

Anwendung		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
A009	Auftrags- und Kundenverwaltung	Vertraulichkeit	**hoch**	Es werden vertrauliche Daten (z. B. besondere Kundenkonditionen) verarbeitet, deren Missbrauch dem Unternehmen großen Schaden zufügen kann
		Integrität	**hoch**	Falls Mengen- oder Preisangaben verändert werden, kann dem Unternehmen großer Schaden entstehen, der leicht bis 500.000 Euro gehen und zu großem Ansehensverlust führt.
		Verfügbarkeit	**hoch**	Da mit dieser Anwendung alle Funktionen vom Einkauf über die Bestellabwicklung und das Schreiben der Lieferscheine, bis hin zum Lagerbestand abgedeckt werden, kann ein Ausfall höchstens bis zu 24 Stunden manuell überbrückt werden.
A010	Active Directory	Vertraulichkeit	normal	Passwörter sind ausschließlich verschlüsselt gespeichert und damit praktisch nicht zugänglich.
		Integrität	**hoch**	Der hohe Schutzbedarf ergibt sich daraus, dass sich alle Mitarbeiter hierüber identifizieren und ihre Rollen und Rechte im AD verwaltet werden.
		Verfügbarkeit	**sehr hoch**	Bei Ausfall dieser Anwendung sind keine Identifizierung, keine Vergabe von Rechten und damit keine Ausführung von IT-Verfahren möglich. Ein Ausfall ist von mehr als 2 Stunden ist nicht tolerabel.
A011	Systemmanagement	Vertraulichkeit	normal	Es werden keine vertraulichen Daten erzeugt oder gespeichert.
		Integrität	**hoch**	Fehler in den Konfigurationsdateien können alle Rechner und insbesondere die Sicherheitseinstellungen betreffen.
		Verfügbarkeit	normal	Bei Ausfall der Anwendung können Administration und Konfiguration an den einzelnen Rechnern durchgeführt werden. Ein Ausfall ist daher kurzzeitig vertretbar.
A012	Zentrale Dokumentenverwaltung	Vertraulichkeit	normal	Die Dokumentenvorlage und auch die hier gespeicherten Dokumente sind nicht vertraulich.
		Integrität	normal	Fehler werden in der Regel schnell erkannt und können nachträglich bereinigt werden.
		Verfügbarkeit	**hoch**	Bei Ausfall der Anwendung können die Arbeitsabläufe in größerem Umfang gestört werden, da unter Umständen nicht mehr auf wichtige Dokumente zugegriffen werden kann.
A013	Druckservice für den Standort Bad Godesberg	Vertraulichkeit	normal	Es werden keine vertraulichen Daten verarbeitet. Abteilungen, die vertrauliche oder personenbezogene Daten ausdrucken, sind mit Arbeitsplatzdruckern ausgestattet.
		Integrität	normal	Wenn Daten fehlerhaft ausgedruckt werden, kann dies leicht festgestellt werden.
		Verfügbarkeit	normal	Da an wichtigen Arbeitsplätzen lokale Drucker vorhanden sind, kann ein Ausfall bis zu drei Tagen hingenommen werden.
A014	Druckservice für den Standort Beuel	Vertraulichkeit	normal	Es werden in der Hauptsache Lieferscheine und Lagerbestände gedruckt, die keine vertraulichen Angaben enthalten.
		Integrität	normal	Falsch ausgedruckte Daten werden leicht erkannt und können korrigiert werden.
		Verfügbarkeit	normal	Da noch ein weiterer Arbeitsplatzdrucker vorhanden ist, können Daten bei Ausfall der Anwendung darüber ausgedruckt werden.
A015	Application Gateway	Vertraulichkeit	normal	Über das System werden keine vertraulichen Daten geleitet.

Anwendung		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
		Integrität	**hoch**	An die Integrität der Konfigurations- und Betriebssystem-dateien sind hohe Anforderungen zu stellen, um Netzeinbrüche auszuschließen.
		Verfügbarkeit	**hoch**	E-Mail und Internet-Recherche sind wesentliche Bestandteile der Tätigkeit der Fachabteilungen. Ein Ausfall der Anwendung ist für maximal 24 Stunden tolerabel.
A016	TK-Vermittlung	Vertraulichkeit	normal	Die Betroffenen werden nur unerheblich beeinträchtigt, wenn die Daten bekannt werden.
		Integrität	normal	Fehler in der Konfigurationsdatei können leicht erkannt und korrigiert werden. Evtl. Schäden aufgrund fehlerhafter Gebührenerfassung liegen unter 500 Euro.
		Verfügbarkeit	**hoch**	Die TK-Anlage ist ein wesentliches Kommunikationsmittel mit den Kunden. Ein Ausfall würde die Arbeitsabläufe wesentlich beeinträchtigen und zu einem wesentlichen Ansehensverlust führen.

Tabelle 12: Schutzbedarfsfeststellung der Anwendungen

4.3 Schutzbedarfsfeststellung für IT-Systeme

Der Schutzbedarf eines IT-Systems hängt im Wesentlichen von dem Schutzbedarf der Anwendungen ab, für deren Ausführung es benötigt wird. Dieser Schutzbedarf vererbt sich auf den Schutzbedarf des IT-Systems. Bei der Vererbung lassen sich folgende Fälle unterscheiden:

- In vielen Fällen lässt sich der höchste Schutzbedarf aller Anwendungen, die das IT-System benötigen, übernehmen (**Maximumprinzip**).
- Der Schutzbedarf des IT-Systems kann höher sein als der Schutzbedarf der einzelnen Anwendungen (**Kumulationseffekt**). Dies ist beispielsweise der Fall, wenn auf einem Server mehrere Anwendungen mit normalem Schutzbedarf in Betrieb sind. Der Ausfall einer dieser Anwendungen könnte überbrückt werden. Wenn aber alle Anwendungen gleichzeitig ausfallen würden, dann kann ein hoher Schaden entstehen.
- Der Schutzbedarf kann niedriger sein als der Schutzbedarf der zugeordneten Anwendungen, wenn eine Anwendung mit hohem Schutzbedarf auf mehrere Systeme verteilt ist, und auf dem betreffenden IT-System nur weniger wichtige Teile dieser Anwendung ausgeführt werden (**Verteilungseffekt**). Bei Anwendungen, die personenbezogene Daten verarbeiten, sind z. B. Komponenten weniger kritisch, in denen die Daten nur in pseudonymisierter Form verwendet werden.

Auch der Schutzbedarf für die IT-Systeme sollte für jeden der drei Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit) festgelegt und anschließend (z. B. tabellarisch) dokumentiert werden.

Die folgenden Tabellen enthalten die Schutzbedarfsfeststellung für die Server, Clients, Netz- und Telekommunikationskomponenten der RECPLAST GmbH.

IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
S001	Domänen-Controller (virtualisiert)	Vertraulichkeit	normal	Maximumprinzip gemäß Anwendung A010 (Active Directory)
		Integrität	**hoch**	Maximumprinzip gemäß Anwendung A010 (Active Directory)
		Verfügbarkeit	normal	Gemäß Anwendung A010 (Active Directory) ist der Schutzbedarf hoch. Da jedoch an beiden Standorten Domänencontroller stehen, ist eine Anmeldung auch über den Rechner am anderen Standort möglich. Ein Ausfall bis zu drei Tagen ist hinnehmbar (Verteilungseffekt).
S002	Dateiserver (virtualisiert)	Vertraulichkeit	normal	Maximumprinzip gemäß der Anwendung A012 (Zentrale Dokumentenverwaltung)
		Integrität	normal	Maximumprinzip gemäß der Anwendung A012 (Zentrale Dokumentenverwaltung)
		Verfügbarkeit	**hoch**	Maximumprinzip gemäß der Anwendung A012 (Zentrale Dokumentenverwaltung)
S003	Druckserver (virtualisiert)	Vertraulichkeit	normal	Maximumprinzip gemäß Anwendungen A013 bzw. A014 (Druckservices)
		Integrität	normal	Maximumprinzip gemäß Anwendungen A013 bzw. A014 (Druckservices)
		Verfügbarkeit	normal	Maximumprinzip gemäß Anwendungen A013 bzw. A014 (Druckservices)
S004	Kommunikationsserver	Vertraulichkeit	**hoch**	Maximumprinzip gemäß Anwendung A002 (E-Mail)
		Integrität	**hoch**	Maximumprinzip gemäß Anwendung A002 (E-Mail)
		Verfügbarkeit	**hoch**	Maximumprinzip gemäß Anwendung A002 (E-Mail)
S005	Server für Kunden- und Auftrags-bearbeitung	Vertraulichkeit	**hoch**	Maximumprinzip: Die Standardanwendung „Auftrags- und Kundenverwaltung“ (A009) hat hohen Schutzbedarf.
		Integrität	**hoch**	Maximumprinzip: Die Standardanwendung „Auftrags- und Kundenverwaltung“ (A009) hat hohen Schutzbedarf.
		Verfügbarkeit	**hoch**	Maximumprinzip: Die Standardanwendung „Auftrags- und Kundenverwaltung“ (A009) hat hohen Schutzbedarf.
S006	DB-Server Finanzbuchhaltung	Vertraulichkeit	**hoch**	Maximumprinzip gemäß der verknüpften Anwendungen A006 (Personaldatenverarbeitung), A007 (Reisekostenabrechnung) und A008 (Finanzbuchhaltung)
		Integrität	**hoch**	Maximumprinzip gemäß der verknüpften Anwendungen A006 (Personaldatenverarbeitung), A007 (Reisekostenabrechnung) und A008 (Finanzbuchhaltung)
		Verfügbarkeit	normal	Ausfälle können mittels manueller Verfahren überbrückt werden.

IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
S007	Virtualisierungsserver	Vertraulichkeit	**hoch**	*Maximumprinzip*: Der Domain Controller beinhaltet das Active Directory und damit die Anmeldeinformationen aller Mitarbeiter.
		Integrität	**hoch**	*Maximumprinzip*: Der Dateiserver verwaltet Dateien, deren Korrektheit für den Geschäftsbetrieb sichergestellt sein muss.
		Verfügbarkeit	**hoch**	*Kumulationseffekt*: Sowohl der Domain Controller als auch der Dateiserver haben jeder hohe Verfügbarkeitsanforderungen. Daraus ergibt sich für den Virtualisierungsserver ein sehr hoher Schutzbedarf. Alle virtualisierten Systeme können aber innerhalb kurzer Zeit auf dem anderen Virtualisierungsserver zur Verfügung gestellt werden. Durch diesen *Verteilungseffekt* reduziert sich der Schutzbedarf auf ein nur noch hohes Niveau.
S008	Server für Produktionssteuerung	Vertraulichkeit	**hoch**	Maximumprinzip gemäß Anwendung A004 Prozessleitsystem
		Integrität	**hoch**	Maximumprinzip gemäß Anwendung A004 Prozessleitsystem
		Verfügbarkeit	**Sehr hoch**	Maximumprinzip gemäß Anwendung A004 Prozessleitsystem

Tabelle 13: Schutzbedarf der Server

Für die nachfolgende Übersicht zur Schutzbedarfsfeststellung für die Clients gilt folgende **Vorbemerkung:** Die Anwendung A002 „E-Mail“ hat in allen drei Grundwerten einen hohen Schutzbedarf, dieser vererbt sich wie dargestellt gemäß Maximumprinzip auch auf den zuständigen Kommunikationsserver S004, nicht jedoch vollständig auf die Clients. Zwar ist auf allen ein E-Mail-Client installiert, die zugehörigen Postfächer befinden sich jedoch auf dem Server S004, so dass das Verteilungsprinzip wirksam wird und der hohe Schutzbedarf der Anwendung „E-Mail“ sich zwar hinsichtlich der Vertraulichkeit auf den Schutzbedarf der Clients auswirkt, nicht aber hinsichtlich Integrität und Verfügbarkeit.

IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
C1, L1	Clients in der Finanzbuchhaltung	Vertraulichkeit	hoch	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A008 (Finanzbuchhaltung)
		Integrität	hoch	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A008 (Finanzbuchhaltung)
		Verfügbarkeit	normal	Bei Ausfall eines Clients kann die Aufgabe an einem anderen Client wahrgenommen werden oder kurzfristig ein Laptop zur Verfügung gestellt werden.
C2, L2	Clients der Geschäftsführung	Vertraulichkeit	**hoch**	Es werden personenbezogene Daten und vertrauliche Korrespondenz bearbeitet. Maximumprinzip von Anwendungen A001 und A006
		Integrität	normal	Integritätsverletzungen der Informationen, die auf den IT-Systemen gespeichert werden, können leicht erkannt und behoben werden.
		Verfügbarkeit	normal	Der Ausfall eines Rechners kann bis zu drei Tagen toleriert werden. Ein Laptop steht als Reserve bereit.

IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
C3, L3	Clients in der Personalabteilung	Vertraulichkeit	**hoch**	Es werden personenbezogene Daten verarbeitet.
		Integrität	normal	Integritätsverletzungen der Informationen, die auf den IT-Systemen gespeichert werden, können leicht erkannt und behoben werden.
		Verfügbarkeit	normal	Ein Ausfall bis zu drei Tagen kann toleriert werden. Ein Laptop steht als Ersatz zur Verfügung.
C4, L4	Clients in der Informationstechnik	Vertraulichkeit	normal	Es werden keine personenbezogenen Daten verarbeitet. Auf den System- und Netzmanagement-Server kann nur mit Passwort zugegriffen werden.
		Integrität	normal	Integritätsverletzungen der Informationen, die auf den IT-Systemen gespeichert werden, können leicht erkannt und behoben werden.
		Verfügbarkeit	normal	Bei Ausfall eines PCs kann kurzfristig ein Laptop zur Verfügung gestellt werden.
C5, L5	Clients Marketing und Vertrieb	Vertraulichkeit	**hoch**	Maximumprinzip gemäß der verknüpften Anwendungen z. B. A009 (Auftrags- und Kundenverwaltung) und A002 (E-Mail)
		Integrität	**hoch**	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A009 (Auftrags- und Kundenverwaltung) und A002 (E-Mail)
		Verfügbarkeit	normal	Bei Ausfall eines Clients kann die Aufgabe an einem anderen Client wahrgenommen oder ein Laptop zur Verfügung gestellt werden.
C6, L6	Clients Fertigung und Lager	Vertraulichkeit	**hoch**	Da auch auf Kundendaten zugegriffen wird, ist die Vertraulichkeit als hoch zu bewerten.
		Integrität	normal	Integritätsverletzungen der Informationen, die auf den IT-Systemen gespeichert werden, können leicht erkannt und behoben werden.
		Verfügbarkeit	normal	Bei Ausfall eines Clients kann die Aufgabe an einem anderen Client wahrgenommen werden oder kurzfristig ein Laptop zur Verfügung gestellt werden.
C7, L7	Clients in Entwicklungsabteilung	Vertraulichkeit	**sehr hoch**	Auf den Rechnern befinden sich Konstruktionspläne und unter Umständen kundenspezifische Entwicklungen und Verfahrensbeschreibungen, die z. B. vor Wirtschaftsspionage und damit möglichen gravierenden wirtschaftlichen Folgen für die Firma zu schützen sind.
		Integrität	normal	Fehler werden in der Regel schnell und leicht erkannt.
		Verfügbarkeit	normal	Bei Ausfall eines Rechners kann auf den anderen Rechnern weitergearbeitet werden. Ein Laptop kann als Ersatzrechner zur Verfügung gestellt werden.
C8, L8	Clients der Einkaufsabteilung	Vertraulichkeit	normal	Es werden keine vertraulichen oder personenbezogenen Daten verarbeitet.
		Integrität	normal	Fehler werden in der Regel schnell und leicht erkannt.
		Verfügbarkeit	normal	Bei Ausfall eines Rechners kann auf den anderen Rechnern weitergearbeitet werden.

IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
C9, L9	Clients in Vertriebsbüros	Vertraulichkeit	**hoch**	Da auch auf Kundendaten zugegriffen wird, ist die Vertraulichkeit als hoch zu bewerten.
		Integrität	**hoch**	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A009 (Auftrags- und Kundenverwaltung) und A002 (E-Mail)
		Verfügbarkeit	normal	Bei Ausfall des Rechners kann ersatzweise mit dem Laptop gearbeitet werden. Ein Ausfall bis zu 8 Tagen erscheint tolerierbar.

Tabelle 14: Schutzbedarf der Clients

Nachfolgend die Übersicht zum Schutzbedarf der Netz- und Telekommunikationskomponenten:

IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
N1	Router zum Internet	Vertraulichkeit	normal	Es werden keine vertraulichen Daten übermittelt. Vertrauliche E-Mails werden vorher verschlüsselt.
		Integrität	**hoch**	Durch Fehler in der Konfiguration können Sicherheitseinstellungen beeinträchtigt werden und E-Mails an einen falschen Adressaten weitergeleitet werden.
		Verfügbarkeit	**hoch**	Maximumprinzip gemäß der verknüpften Anwendungen A002 (E-Mail und A003 (Internet-Recherche)
N2	Firewall	Vertraulichkeit	normal	Es laufen keine vertraulichen Daten unverschlüsselt über die Firewall.
		Integrität	**hoch**	Von der korrekten Konfiguration hängt die Sicherheit des internen Netzes und aller angeschlossenen IT-Systeme ab.
		Verfügbarkeit	**hoch**	Bei Ausfall muss die gesamte Verbindung zum Internet, einschließlich E-Mail unterbrochen werden. Dies ist nur bis zu 24 Stunden tolerabel.
N3	Zentrale Switche	Vertraulichkeit	**hoch**	Über dieses System fließen vertrauliche Daten, z.B. zur Ablage auf dem Dateiserver.
		Integrität	normal	Fehler in den übertragenen Daten werden leicht erkannt und korrigiert.
		Verfügbarkeit	**hoch**	Bei einem Ausfall des Switches ist ein IT-gestütztes Arbeiten nicht mehr möglich, da kein Zugriff zu den Servern mit den Daten besteht. Ein Ausfall ist höchstens 3 Stunden tolerierbar.
N4	Router zur Verbindung der Standorte	Vertraulichkeit	**hoch**	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A002 (E-Mail)
		Integrität	normal	Bei Fehlern in der Konfigurationsdatei ist die gesamte interne Kommunikation gestört. Diese Fehler können aber leicht erkannt und korrigiert werden.
		Verfügbarkeit	**hoch**	Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A002 (E-Mail). Ein Ausfall ist höchstens für 24 Stunden tolerabel.
T1	TK-Anlagen	Vertraulichkeit	normal	Maximumprinzip gemäß Anwendung A016
		Integrität	normal	Maximumprinzip gemäß Anwendung A016
		Verfügbarkeit	hoch	Maximumprinzip gemäß Anwendung A016

IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
T3	Faxgeräte	Vertraulichkeit	hoch	Es wird unter Umständen vertrauliche Korrespondenz übermittelt.
		Integrität	normal	Fehler würden zu Rückfragen führen und durch erneute Übermittlung behoben.
		Verfügbarkeit	normal	Bei Ausfall eines Faxgeräts stehen weitere Faxgeräte zur Verfügung. Ein Ausfall eines Geräts führt nur zu minimalen Einschränkungen.

Tabelle 15: Schutzbedarf der Netz- und Telekommunikationskomponenten

4.4 Schutzbedarfsfeststellung für Kommunikationsverbindungen

Im nächsten Arbeitsschritt geht es darum, den Schutzbedarf für die Kommunikationsverbindungen festzustellen. Es gibt Verbindungen, die gefährdeter sind als andere und durch doppelte Auslegung oder besondere Maßnahmen gegen Angriffe von außen oder innen geschützt werden müssen.

Als **kritische Verbindungen** gelten:

- Verbindungen, die aus dem Unternehmen **in ein öffentliches Netz** (z. B. Telefonnetz, Internet) oder über ein öffentliches Gelände reichen. Über solche Verbindungen können Schadprogramme in das Unternehmensnetz eingeschleust werden, Unternehmens-Server angegriffen werden oder Mitarbeiter vertrauliche Daten an Unbefugte weiterleiten.
- Verbindungen, über die besonders **schützenswerte Informationen** übertragen werden. Mögliche Gefährdungen sind Abhören, vorsätzliche Manipulation und betrügerischer Missbrauch. Der Ausfall solcher Verbindungen ist für Anwendungen, für die eine hohe Verfügbarkeit erforderlich ist, besonders kritisch.
- Verbindungen, über die **vertrauliche Informationen** nicht übertragen werden dürfen. Personaldaten dürfen zum Beispiel nur von Mitarbeitern der Personalabteilung und der Geschäftsführung eingesehen und bearbeitet werden. Daher muss verhindert werden, dass diese Daten bei ihrer Übertragung von unbefugten Mitarbeitern eingesehen werden können.

Diese kritischen Verbindungen werden zunächst analog zur Strukturanalyse tabellarisch erfasst:

Nr.	Beschreibung der Verbindung	Bemerkung
K001	Internetanschluss Bonn-Bad Godesberg	Außenanschluss der RECPLAST GmbH an das Internet. Gleichzeitig Teil der Verbindung zu den Vertriebsbüros und den mobilen Clients.
K002	Standleitung Bad Godesberg – Beuel	Standleitung für die Verbindung der beiden Bonner Standorte. Sie führt über öffentliches Gelände.
K003	Verbindungen zwischen Netzkomponenten innerhalb der RECPLAST GmbH	Es werden unter Umständen Informationen mit hohem Schutzbedarf übertragen.
K004	Verbindungen zwischen Switches und Servern	Es werden unter Umständen Informationen mit hohem Schutzbedarf übertragen.
K005	Verbindungen zwischen Switches und Clients	Es werden unter Umständen Informationen mit hohem Schutzbedarf übertragen.
K006	Verbindungen zwischen Switches und Produktionsmaschinen	Es werden Informationen mit hohem Schutzbedarf übertragen.
K007	Internetanschlüsse der Vertriebsbüros	Verbindung zur RECPLAST GmbH über ein öffentliches Netz
K008	Mobile Internetanschlüsse der Laptops	Verbindung zur RECPLAST GmbH über ein öffentliches Netz

Tabelle 16: Kritische Verbindungen

Für jede dieser Verbindungen wird anhand der darüber übertragenen Informationen der Schutzbedarf für die drei Grundwerte bestimmt.

Verbindung		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
K001	Internetanschluss Bad Godesberg	Vertraulichkeit	**hoch**	Abgefangene E-Mails könnten an den Wettbewerb gelangen.
		Integrität	**hoch**	Ein Großteil der Kommunikation erfolgt über das Internet. Gefälschte Informationen können z.B. den Ruf schädigen.
		Verfügbarkeit	**hoch**	Ohne diese Außenverbindung kann keine Kommunikation mehr stattfinden.
K002	Standleitung BG-Beuel	Vertraulichkeit	**hoch**	Firmeninterne Informationen müssen vertraulich übertragen werden.
		Integrität	normal	Die Standleitung wurde durch die Administratoren abgesichert, Informationen können nur mit hohem Aufwand manipuliert werden.
		Verfügbarkeit	**hoch**	Ohne die Anbindung können keine Produktionsaufträge bearbeitet werden.
K003	Verbindungen zwischen Netzkomponenten	Vertraulichkeit	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten eingesehen werden.
		Integrität	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten verändert werden.
		Verfügbarkeit	**hoch**	Wenn eine interne Verbindung ausfällt, sind die Netzkomponenten nicht mehr erreichbar und der interne Datenfluss ist nicht mehr möglich.
K004	Verbindungen zwischen Switches und Servern	Vertraulichkeit	**hoch**	Maximumprinzip: Von Clients der Personalabteilung werden personenbezogene Informationen auf dem Datei- und einem Datenbankserver abgelegt.
		Integrität	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten verändert werden.
		Verfügbarkeit	**hoch**	Maximumprinzip: Ohne den DB-Server für Kunden- und Auftragsbearbeitung und den Server zur Produktionssteuerung ist keine Produktion möglich. Das kann maximal 24 Stunden toleriert werden.
K005	Verbindungen zwischen Switches und Clients	Vertraulichkeit	**hoch**	Maximumprinzip: Von Clients der Personalabteilung werden personenbezogene Informationen auf dem Datei- und einem Datenbankserver abgelegt.
		Integrität	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten verändert werden.
		Verfügbarkeit	**hoch**	Ohne die Anbindung können keine Produktionsaufträge bearbeitet werden.
K006	Verbindungen zwischen Switches und Produktionsmaschinen	Vertraulichkeit	normal	Informationen auf internen Verbindungen können nicht von Dritten eingesehen werden.
		Integrität	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten verändert werden.
		Verfügbarkeit	**sehr hoch**	Ein Stillstand der Produktion durch Ausfall dieser Verbindungen kann höchstens für 2 Stunden toleriert werden.

Verbindung		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
K007	Internetanschlüsse der Vertriebsbüros	Vertraulichkeit	**hoch**	Firmeninterne Informationen müssen vertraulich übertragen werden.
		Integrität	normal	Gefälschte Informationen können bemerkt und korrigiert werden.
		Verfügbarkeit	normal	Die Kommunikation kann vorübergehend über andere Medien erfolgen.
K008	Mobile Internetanschlüsse der Laptops	Vertraulichkeit	**hoch**	Firmeninterne Informationen müssen vertraulich übertragen werden.
		Integrität	normal	Gefälschte Informationen können bemerkt und korrigiert werden.
		Verfügbarkeit	normal	Die Kommunikation kann vorübergehend über andere Medien erfolgen.

Tabelle 17: Schutzbedarf der Kommunikationsverbindungen

4.5 Schutzbedarfsfeststellung für Räumlichkeiten

Bei der Schutzbedarfsfeststellung für Räume werden alle Räume und Liegenschaften betrachtet, die zuvor in der Strukturanalyse identifiziert wurden und die für die Informationen, Geschäftsprozesse, Anwendungen und IT-Systeme des betrachteten Informationsverbundes relevant sind.

Auch hier sind wieder Vererbungsprinzipien zu berücksichtigen. Der Schutzbedarf eines Raums bemisst sich nach dem Schutzbedarf der IT-Systeme, die sich in ihm befinden, sowie der Informationen und Datenträger, die in ihm verarbeitet und gelagert werden. Folglich kann in den meisten Fällen wieder das Maximumprinzip angewendet werden (vergleichbar der Schutzbedarfsfeststellung der IT-Systeme). Unter Umständen ergibt sich aus der Vielzahl an Objekten, die sich in einem Raum befinden, jedoch ein höherer Schutzbedarf in einem Grundwert als für jedes einzelne Objekt (Kumulationseffekt). Dies kann z. B. für Räume gelten, in denen sich gespiegelte Server mit jeweils normalen Verfügbarkeitsanforderungen befinden – bei Ausfall eines Servers gibt es ja noch einen zweiten, während von einem „Ausfall“ des Raums (zum Beispiel aufgrund eines Brandes) beide Server betroffen sind.

Die folgende Tabelle zeigt das Ergebnis der Schutzbedarfsfeststellung für die IT-genutzten Räume bei der RECPLAST GmbH. Der Schutzbedarf der Räume wird meistens nach dem jeweils höchsten Schutzbedarf der darin befindlichen IT-Systeme (Maximumprinzip) festgelegt. Eine Ausnahme bildet der Schutzbedarf des Produktionsgebäudes, dessen Verfügbarkeitsbedarf aufgrund von Kumulationseffekten als sehr hoch bewertet wurde – bei einem Verlust dieses Gebäudes wäre keine Produktion mehr möglich und damit der wesentliche Geschäftszweck des Unternehmens.

Gebäude/Raum				IT/ Informationen	Schutzbedarf		
Kürzel	**Bezeichnung**	**Art**	**Lokation**	**IT-Systeme**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
GB1	Verwaltungsgebäude	Gebäude	Bad Godesberg	alle in R1 bis R8	hoch	hoch	hoch
GB2	Produktionsgebäude	Gebäude	Beuel	alle in R9 bis R14	sehr hoch	hoch	sehr hoch
R1	Technikraum Bad Godesberg (BG, R. 1.01)	Technikraum	GB1	T1	normal	normal	hoch

Gebäude/Raum				IT/ Informationen	Schutzbedarf		
Kürzel	**Bezeichnung**	**Art**	**Lokation**	**IT-Systeme**	**Vertraulich-keit**	**Integrität**	**Verfügbarkeit**
R2	Serverraum Bad Godesberg (BG, R. 1.02)	Serverraum	GB1	S001 bis S007 N1 bis N4	hoch	hoch	hoch
R3	Büros IT-Abteilung (BG, R. 1.03 – 1.06)	Büroräume	GB1	C4, L4	normal	normal	normal
R4	Büros Personal-abteilung (BG, R. 1.07 – 1.09)	Büroräume	GB1	C3, L3	hoch	normal	normal
R5	Büros Geschäfts-führung (BG, R. 1.10 – 1.13)	Büroräume	GB1	C2, L2	hoch	normal	normal
R6	Büros Marketing/ Vertrieb (BG, R. 2.03 – 2.09)	Büroräume	GB1	C5, L5, einige Räume mit Faxgeräten	hoch	hoch	normal
R7	Büros Lohn/Fibu (BG, R. 2.10 – 2.12)	Büroräume	GB1	C1, L1	hoch	hoch	normal
R8	Büros Einkauf (BG, R. 2.13 – 2.17)	Büroräume	GB1	C8, L8, einige Räume mit Faxgeräten T2	hoch	hoch	normal
R9	Serverraum Beuel (Beuel, R. 2.01)	Serverraum	GB2	S001-S003, S007, S008, N3, N4	hoch	hoch	hoch
R10	Technikraum Beuel (Beuel, R. 2.02)	Technikraum	GB2	T2	normal	normal	hoch
R11	Büros Fertigung/Lager (Beuel, R. 2.10 – 2.13	Büroräume	GB2	C6, L6, ein Raum mit Faxgerät T2	hoch	normal	normal
R12	Büros Entwicklungs-abteilung (Beuel, R. 2.14 – 2.20)	Büroräume	GB2	C7, L7	sehr hoch	normal	normal
R13	Vertriebsbüros	Häuslicher Arbeitsplatz	Berlin, Hamburg, München	C9, L9, T2	hoch	hoch	normal
R14	Außendienst	Mobiler Arbeitsplatz	Alle Standorte	L1 bis L9	hoch	hoch	normal

Tabelle 18: Schutzbedarf der Räume

5 Modellierung

Ziel der Modellierung gemäß IT-Grundschutz ist es, IT-Grundschutz-Bausteine festzulegen, die auf die ausgewählten Zielobjekte des betrachteten Informationsverbundes anzuwenden sind. Das Ergebnis ist ein **IT-Grundschutzmodell**, das je nach Umsetzungsstand als Entwicklungskonzept oder, wie nachfolgend für die RECPLAST GmbH dargestellt, als Prüfplan verwendet werden kann.

Die folgende Tabelle zeigt anhand ausgewählter Bausteine das Ergebnis der IT-Grundschutz-Modellierung für die RECPLAST GmbH. Zielobjekte, die nicht mit einer Kennzeichnung angegeben sind, wurden in der Strukturanalyse für dieses Beispiel nicht erfasst, um die Darstellung überschaubar zu halten.

Weitere Informationen zur Modellierung gemäß IT-Grundschutz finden Sie in Kapitel 8.3, *Modellierung eines Informationsverbunds,* des BSI-Standards 200-2 und in Kapitel 2, *Schichtenmodell und Modellierung*, des IT-Grundschutz-Kompendiums.

Baustein	Zielobjekte	Begründung	Ansprechpartner
Schicht ISMS: Sicherheitsmanagement			
ISMS.1 Sicherheitsmanagement	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	ISB
Schicht ORP: Organisation und Personal			
ORP.1 Organisation	Informationsverbund	In der RECPLAST GmbH gelten einheitliche Rahmenbedingungen für die Anwendung des Bausteins.	
ORP.2 Personal	Informationsverbund	In der RECPLAST GmbH gelten einheitliche Rahmenbedingungen für die Anwendung des Bausteins.	
ORP.3 Sensibilisierung und Schulung	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
ORP.4 Identitäts- und Berechtigungsmanagement	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
ORP.5 Compliance Management (Anforderungsmanagement)	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
Schicht CON: Konzeption und Vorgehensweisen			
CON.1 Kryptokonzept	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
CON.2 Datenschutz	Informationsverbund	Die RECPLAST GmbH verarbeitet auch personenbezogene Daten	
CON.3 Datensicherungskonzept	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
CON.4 Auswahl und Einsatz von Standardsoftware	Informationsverbund	Der Umgang mit Standardsoftware ist in der RECPLAST GmbH einheitlich geregelt.	
CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen	Informationsverbund	Insbesondere die Prozesse im Fertigungsbereich werden durch Spezialsoftware unterstützt.	
CON.6 Löschen und Vernichten	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
CON.7 Informationssicherheit auf Auslandsreisen	Informationsverbund	Die RECPLAST GmbH ist auch international tätig.	

Baustein	Zielobjekte	Begründung	Ansprechpartner
Schicht OPS: Betrieb			
OPS.1.1.2 Ordnungsgemäße IT-Administration	Informationsverbund	Die RECPLAST GmbH administriert ihre IT selber.	
OPS.1.1.3 Patch- und Änderungsmanagement	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
OPS.1.1.4 Schutz vor Schadprogrammen	Informationsverbund	Der Baustein wird auf alle IT-Systeme im Informationsverbund angewendet.	
OPS.1.1.5 Protokollierung	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
OPS.1.1.6 Software-Tests und -Freigaben	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
OPS.1.2.2 Archivierung	Informationsverbund	Relevant, weil gesetzliche Aufbewahrungsfristen (z. B. für Finanzbehörden) einzuhalten sind	
OPS.1.2.3 Informations- und Datenträgeraustausch	Alle Anwendungen, die Datenträger (z.B. USB-Sticks) nutzen können.	Datenträgeraustausch mit Externen ist nicht vorgesehen, aber auch intern existieren Bedrohungen durch Schad-software oder Informationsabfluss.	
OPS.1.2.4 Telearbeit	Nicht relevant	Arbeiten im häuslichen Umfeld sind nicht vorgesehen.	
OPS.2.1 Outsourcing für Kunden	Nicht relevant	Entsprechende Dienstleistungen werden nicht erbracht.	
OPS.2.4 Fernwartung	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
OPS.3.1 Outsourcing für Dienstleister	Nicht relevant	Entsprechende Dienstleistungen werden nicht genutzt.	
Schicht DER: Detektion und Reaktion			
DER.1 Detektion von sicherheitsrelevanten Ereignissen	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
DER.2.1 Behandlung von Sicherheitsvorfällen	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
DER.2.2 Vorsorge für die IT-Forensik	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
DER.3.1 Audits und Revisionen	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
DER.3.2 IS-Revision für Bundesbehörden	Nicht relevant	Kein verpflichtendes Verfahren für privatwirtschaftliche Unternehmen	
DER.4 Notfallmanagement	Informationsverbund	Gemäß Kapitel 2.2 des IT-Grundschutz-Kompendiums	
Schicht APP: Anwendungen			
APP.1.1 Office-Produkte	A001	Office ist auf allen Clients installiert	IT-Betrieb
APP.1.2 Web-Browser	A003	Auf allen Clients ist ein Web-Browser installiert	IT-Betrieb
APP.2.1 Allgemeiner Verzeichnisdienst	A010	Es wird eine Windows-Domäne genutzt.	
APP.2.2 Active Directory	A010	Es wird eine Windows-Domäne genutzt.	IT-Betrieb
APP.3.1 Webanwendungen	Nicht relevant	Es werden keine Webanwendungen eingesetzt.	

Baustein	Zielobjekte	Begründung	Ansprechpartner
APP.3.2 Webserver	Nicht relevant	Der einfache Webauftritt der RECPLAST GmbH wird auf einem Server des Providers gehostet.	
APP.3.3 Fileserver	A012	Die zentrale Dokumentenverwaltung ist mittels eines Fileservers realisiert.	IT-Betrieb
APP.3.4 Samba	A004	Auf dem Server für Produktionssteuerung gibt es Samba-Freigaben	IT-Betrieb
APP.3.6 DNS-Server	Nicht relevant	Der DNS-Server des Providers wird genutzt.	
APP.4.3 Relationale Datenbanksysteme	A007, A008, A009	Für Personaldatenverarbeitung, Finanzbuchhaltung und Auftrags- und Kundenverwaltung werden DB-Server eingesetzt.	IT-Betrieb
APP.5.1 Allgemeine Groupware	A002	Auf allen Clients wird der Lotus Notes-Client genutzt.	IT-Betrieb
APP.5.2 Microsoft Exchange und Outlook	A002		IT-Betrieb
Schicht SYS: IT-Systeme			
SYS.1.1 Allgemeiner Server	S001 bis S008		
SYS.1.2.2 Windows Server 2012	S001 bis S006		IT-Betrieb
SYS.1.3 Server unter Unix	S007, S008		IT-Betrieb
SYS.1.5 Virtualisierung	S007		IT-Betrieb
SYS.1.8 Speicherlösungen	Nicht relevant	Es werden keine separaten Speicherlösungen betrieben.	
SYS.2.1 Allgemeiner Client	C1 bis C9, L1 bis L9		
SYS.2.2.2 Clients unter Windows 8.1	Nicht relevant	Wird nicht mehr eingesetzt	
SYS.2.2.3 Clients unter Windows 10	C1 bis C9, L1 bis L9		IT-Betrieb
SYS.2.3 Clients unter Unix	Nicht relevant	Wird nicht eingesetzt	
SYS.3.1 Laptops	L1 bis L9		IT-Betrieb
SYS.3.2.1 Allgemeine Smartphones und Tablets	Nicht relevant	Dienstliche Smartphones oder Tablets werden nicht genutzt, Nutzung privater Geräte ist verboten.	
SYS.3.2.2 Mobile Device Management (MDM)	Nicht relevant	Dienstliche Smartphones oder Tablets werden nicht genutzt, Nutzung privater Geräte ist verboten.	
SYS.3.2.3 iOS (for Enterprise)	Nicht relevant	Dienstliche Smartphones oder Tablets werden nicht genutzt, Nutzung privater Geräte ist verboten.	
SYS.3.2.4 Android	Nicht relevant	Dienstliche Smartphones oder Tablets werden nicht genutzt, Nutzung privater Geräte ist verboten.	
SYS.3.4 Mobile Datenträger	Alle USB-Sticks		
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	Alle Drucker und Kopierer		
SYS.4.4 Allgemeines IoT-Gerät	Nicht relevant	Kein IoT-Gerät im Einsatz	

Baustein	Zielobjekte	Begründung	Ansprechpartner
Schicht IND: Industrielle IT			
IND.1 Betriebs- und Steuerungstechnik	I001, S008		
IND.2.1 Allgemeine ICS-Komponente	I001		
IND.2.2 Speicherprogrammierbare Steuerung (SPS)	I001		Leiter Produktion
IND.2.3 Sensoren und Aktoren	I001		
IND.2.4 Maschine	I001		
Schicht NET: Netze und Kommunikation			
NET.1.1 Netzarchitektur und -design	Gesamtnetz		IT-Betrieb
NET.1.2 Netzmanagement	Nicht relevant	Ein Netzmanagementsystem wird noch nicht eingesetzt	
NET.2.1 WLAN-Betrieb	Nicht relevant	WLAN wird nicht eingesetzt	
NET.2.2 WLAN-Nutzung	Nicht relevant	WLAN wird nicht eingesetzt	
NET.3.1 Router und Switches	N001, N003, N004		IT-Betrieb
NET.3.2 Firewall	N002		IT-Betrieb
NET.3.3 VPN	K007, K008	VPN wird in den Vertriebsbüros und auf den Laptops verwendet.	IT-Betrieb
Schicht INF: Infrastruktur			
INF.1 Allgemeines Gebäude	GB1, GB2	Die Gebäude an beiden Standorten werden gesondert betrachtet.	Haustechnik
INF.2 Rechenzentrum sowie Serverraum	R002, R009	Beide Serverräume werden gesondert betrachtet.	IT-Betrieb
INF.3 Elektrotechnische Verkabelung	GB1, GB2, R002, R009	Der Baustein wird auf beide Gebäude und auch auf beide Serverräume angewendet, da deren Elektroinstallation Besonderheiten aufweist.	Haustechnik
INF.4 IT-Verkabelung	GB1, GB2, R002, R009	Der Baustein wird auf beide Gebäude und auch auf beide Serverräume angewendet, da deren Elektroinstallation Besonderheiten aufweist.	Haustechnik
INF.7 Büroarbeitsplatz	R003 bis R008, R011, R012	Der Baustein wird auf jede Gruppe von Büroräumen gesondert angewendet.	
INF.8 Häuslicher Arbeitsplatz	R014	Die Vertriebsbüros werden wie Home Offices behandelt.	
INF.9 Mobiler Arbeitsplatz	R015		
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume	Nicht relevant		

Tabelle 19: Modellierung für den Informationsverbund der RECPLAST GmbH

6 IT-Grundschutz-Check

In einem ersten IT-Grundschutz-Check wird – vor der Durchführung von Risikoanalyse – ermittelt, ob und inwieweit die Basis- und Standard-Anforderungen der relevanten Bausteine des IT-Grundschutz-Kompendiums für die einzelnen Zielobjekte eines Informationsverbundes erfüllt sind. Die nachfolgenden Tabellen veranschaulichen die Dokumentation einer solchen Überprüfung für die RECPLAST GmbH am Beispiel von folgenden Zielobjekten und Bausteinen:

- Zielobjekt gesamter Informationsverbund
  - ISMS.1 *Sicherheitsmanagement*
  - ORP.2 *Personal*
  - CON.3 *Datensicherungskonzept*
- Zielobjekt Server S007
  - SYS.1.1 *Allgemeiner Server*
  - SYS.1.5 *Virtualisierung*
- Zielobjekt *Serverraum*
  - *INF.2 Rechenzentrum sowie Serverraum*

Anforderungen für den höheren Schutzbedarf werden in einem zweiten IT-Grundschutz-Check geprüft, sofern das Sicherheitskonzept aufgrund der Entscheidungen zur Risikobehandlung durch neue oder geänderte Maßnahmen ergänzt wurde.

Die nachfolgenden Übersichten enthalten auch Hinweise zu den Verantwortlichkeiten für den einzelnen Baustein sowie auch für Anforderungen. Zusätzlich zu den genannten Verantwortlichkeiten gilt, dass in der Regel der Informationssicherheitsbeauftragte (ISB) bei strategischen Entscheidungen einzubeziehen ist. Dieser ist außerdem dafür verantwortlich, dass alle Anforderungen gemäß des festlegten Sicherheitskonzepts erfüllt und überprüft werden.

Zur Dokumentation des IT-Grundschutz-Checks gehören auch Informationen zum Überprüfungsprozess (z. B. Befrager, Befragte, Zeitpunkt der Befragung). Auf die Angabe dieser Metadaten wird nachfolgend verzichtet, sie ist gleichwohl bei IT-Grundschutz-Checks in der Praxis unabdingbar.

6.1 ISMS.1 *Sicherheitsmanagement*

Im Folgenden werden die Ergebnisse des IT-Grundschutz-Checks für die Basis- und Standard-Anforderungen des Bausteins ISMS.1 *Sicherheitsmanagement* dargestellt. Zielobjekt ist der gesamte Informationsverbund.

Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Anforderung [Verantwortung]	Status	Umsetzung
ISMS.1.A1 *Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene* [Institutionsleitung]	erfüllt	Die Geschäftsführung hat die Erstellung der Leitlinie initiiert. Die Leitlinie wurde von der Geschäftsführung unterzeichnet. Die Geschäftsführung hat die gesamte Verantwortung für das Thema Informationssicherheit übernommen und delegiert an den ISB die Umsetzung der geforderten Maßnahmen. Einmal monatlich erhält die Geschäftsführung einen Management-Report, kontrolliert den Umsetzungsstand der Maßnahmen, initiiert bei Bedarf weitere Maßnahmen und bewilligt das entsprechende Budget.

Anforderung [Verantwortung]	Status	Umsetzung
ISMS.1.A2 *Festlegung der Sicherheitsziele und -strategie* [Institutionsleitung]	erfüllt	Die Geschäftsführung hat Ziele sowie eine Strategie für Informationssicherheit festgelegt und dokumentiert.Der Sicherheitsprozess ist an diesen Vorgaben ausgerichtet. Dieser organisatorische Rahmen unterstützt den ordnungsgemäßen und sicheren Umgang mit Informationen in allen Geschäftsprozessen. Die Geschäftsführung hat außerdem veranlasst, dass Aktualität, Angemessenheit und wirksame Umsetzung der Sicherheitsziele und -strategie regelmäßig geprüft werden.
ISMS.1.A3 *Erstellung einer Leitlinie zur Informationssicherheit* [Institutionsleitung]	erfüllt	Die Geschäftsführung hat eine übergeordnete Leitlinie zur Informationssicherheit verabschiedet und den Mitarbeitern und anderen relevanten Stellen bekanntgegeben. In dieser wird der Stellenwert dieser Aufgabe verdeutlicht und werden die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit beschrieben. Die Leitlinie soll alle zwei Jahre überprüft und bei Bedarf aktualisiert werden.
ISMS.1.A4 *Benennung eines Informationssicherheitsbeauftragten* [Institutionsleitung]	erfüllt	Die Geschäftsführung hat einen fachlich qualifizierten Informationssicherheitsbeauftragten (ISB) benannt, der ihr unmittelbar über alle relevanten Fragestellungen zur Informationssicherheit berichtet. Sie hat außerdem durch Richtlinien dafür gesorgt, dass er angemessen in die Prozesse des Unternehmens eingebunden ist und frühzeitig in neue Entwicklungen und Vorhaben eingebunden wird.
ISMS.1.A5 *Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten* [Institutionsleitung]	entbehrlich	Der Informationssicherheitsbeauftragte ist ein Mitarbeiter der RECPLAST GmbH.
ISMS.1.A6 *Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit* [Institutionsleitung]	erfüllt	Neben dem ISB hat die Geschäftsführung weitere Verantwortlichkeiten für Informationssicherheit festgelegt (ICS-ISB, IS-Management-Team) und (z. B. durch die Beschreibung von Meldewegen) in den Unternehmensprozessen verankert.
ISMS.1.A7 *Festlegung von Sicherheitsmaßnahmen*	teilweise erfüllt	Alle Mitarbeiter, die Maßnahmen im Sinne der Informationssicherheit umsetzen, sind verpflichtet, diese zu dokumentieren und dem ISB per E-Mail zuzusenden. Eine Auswertung und ausreichende Dokumentation der umgesetzten Maßnahmen gibt es nicht. Umsetzungszeitpunkt für ausführliche Dokumentation: 30.04.
ISMS.1.A8 *Integration der Mitarbeiter in den Sicherheitsprozess* [Vorgesetzte]	teilweise erfüllt	Zwar gibt es entsprechende Vorgaben an die Vorgesetzten, die Interviews zeigten aber, dass die Mitarbeiter in einigen Fällen nur verzögert und partiell über den Sinn von Sicherheitsmaßnahmen informiert und in deren Handhabung geschult wurden.
ISMS.1.A9 *Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse* [Institutionsleitung]	erfüllt	Die Geschäftsführung hat durch Richtlinien dafür gesorgt, dass der ISB in bestehende, aber auch geplante neue Prozesse eingebunden wird und bei sicherheitsrelevanten Entscheidungen mitwirkt. Dazu gehört auch eine enge Zusammenarbeit mit anderen Sicherheitsverantwortlichen im Unternehmen (z. B. denen für das allgemeine Risikomanagement).
ISMS.1.A10 *Erstellung eines Sicherheitskonzepts*	teilweise erfüllt	Das Unternehmen hat bislang zwar eine Vielzahl an Einzelmaßnahmen zur Informationssicherheit umgesetzt, diese allerdings bislang noch nicht in ein umfassendes Sicherheitskonzept integriert. Allerdings wurde damit begonnen, ein solches Konzept mithilfe der Variante Standard-Absicherung der IT-Grundschutz-Methodik zu entwickeln. Diese Arbeit soll am 1. September abgeschlossen sein.
ISMS.1.A11 *Aufrechterhaltung der Informationssicherheit*	erfüllt	Alle Dokumente und Prozesse werden einmal jährlich einem internen Audit unterzogen. Der ISB hat dafür die entsprechende fachliche Weisungsbefugnis für die Mitarbeiter, in deren Verantwortungsbereich einzelne Dokumente und Prozesse fallen.

Anforderung [Verantwortung]	Status	Umsetzung
ISMS.1.A12 *Management-Berichte zur Informationssicherheit* [Institutionsleitung]	teilweise erfüllt	Zwar lässt sich die Geschäftsführung regelmäßig durch den ISB über den Stand der Informationssicherheit informieren, allerdings geschieht dies eher unstrukturiert. Die Dokumentation der getroffenen Entscheidungen ist daher lückenhaft, auch fehlen Regeln für deren langfristige fälschungssichere Archivierung.
ISMS.1.A13 *Dokumentation des Sicherheitsprozesses*	nicht erfüllt	Es gibt zwar eine Fülle an Dokumenten zur Informationssicherheit, allerdings noch keinen systematischen Prozess, in dem beschrieben ist, wie mit diesen Dokumenten in ihrem Lebenszyklus (von der Erstanlage bis zu deren Archivierung) umzugehen ist. Ebenso wenig gibt es ein Konzept, in dem festgelegt ist, wie für die erforderliche Vertraulichkeit der Dokumentation gesorgt wird.
ISMS.1.A14 *Sensibilisierung zur Informationssicherheit*	teilweise erfüllt	Bislang gab es nur punktuelle Aktivitäten zur Sensibilisierung, allerdings gehört die Entwicklung eines diesbezüglichen Konzepts zu den in der Sicherheitsleitlinie formulierten Zielen. Mit dieser Arbeit wurde zwischenzeitlich begonnen, das Konzept soll am 30. Juni fertiggestellt sein.
ISMS.1.A15 *Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit*	erfüllt	Vor Einführung einer Maßnahme wird diese einer gründlichen Wirtschaftlichkeitsprüfung unterzogen, bei der die erforderlichen Aufwände und der mögliche Sicherheitsgewinn gegeneinander abgewogen werden. In diese Prüfungen werden die jeweils relevanten Mitarbeiter einbezogen.

Tabelle 20: IT-Grundschutz-Check – Baustein ISMS.1 *Sicherheitsmanagement*

6.2 ORP.2 *Personal*

Im Folgenden werden die Ergebnisse des IT-Grundschutz-Checks für die Basis- und Standard-Anforderungen des Bausteins ORP.2 *Personal* aufgeführt. Zielobjekt ist der gesamte Informationsverbund.

Grundsätzlich ist die Personalabteilung für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Anforderung [Verantwortung]	Status	Umsetzung
ORP.2.A1 *Geregelte Einarbeitung neuer Mitarbeiter* [Vorgesetzte]	teilweise erfüllt	Die vorhandenen Regelungen zur Einarbeitung neuer Mitarbeiter berücksichtigen lediglich die Verpflichtung zum vertraulichen Umgang mit Unternehmensinformationen und zur Einhaltung gesetzlichen Verpflichtungen, enthalten aber ansonsten keine weiteren Regelungen zur Informationssicherheit. Eine Überarbeitung ist bis Mai geplant.
ORP.2.A2 *Geregelte Verfahrensweise beim Weggang von Mitarbeitern* [Vorgesetzte, IT-Betrieb]	teilweise erfüllt	Es gibt detaillierte Einzelregelungen hierzu, die in der Regel auch praktiziert werden und deren Einhaltung überwacht wird. Bei der IT-Administration gibt es allerdings noch einen Regelungsbedarf. So wurde bei der Begehung im Rahmen des IT-Grundschutz-Checks einige Benutzer-Accounts entdeckt, die ausgeschiedenen Mitarbeitern zugeordnet sind. Eine Ursache hierfür ist, dass die IT-Administration nur unsystematisch in Personalvorgänge eingebunden wird.
ORP.2.A3 *Vertretungsregelungen* [Vorgesetzte]	erfüllt	Für alle relevanten Teilaufgaben sind Vertretungsregelungen festgelegt.
ORP.2.A4 *Regelungen für den Einsatz von Fremdpersonal*	erfüllt	Fremdpersonal wird nur sporadisch eingesetzt und wird dann beaufsichtigt.
ORP.2.A5 *Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal*	erfüllt	Es gibt eine diesbezügliche Anweisung, die Einhaltung wird geprüft.
ORP.2.A6 *Überprüfung von Kandidaten bei der Auswahl von Personal*	erfüllt	Bei der Auswahl neuer Mitarbeiter wird geprüft, ob sie hinreichend qualifiziert sind und die erforderlichen Fähigkeiten haben.
ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern	erfüllt	Die Vertrauenswürdigkeit von Mitarbeitern wird geprüft. Dabei wird ihr künftiger Aufgabenbereich berücksichtigt.

Anforderung [Verantwortung]	Status	Umsetzung
ORP.2.A8 *Aufgaben und Zuständigkeiten von Mitarbeitern* [Informationssicherheitsbeauftragter (ISB)]	teilweise erfüllt	Die Regelungen hierzu sind unvollständig, eine Ergänzung und Anpassung ist bis Mai geplant (siehe ORP.2.A.1).
ORP.2.A9 *Schulung von Mitarbeitern*	nicht erfüllt	Es gibt noch keine Schulungen zur Informationssicherheit. Ein Konzept wird bis Juli erarbeitet.

Tabelle 21: IT-Grundschutz-Check – Baustein ORP.2 *Personal*

6.3 CON.3 *Datensicherungskonzept*

Im Folgenden werden die Ergebnisse des IT-Grundschutz-Checks für die Basis- und Standard-Anforderungen des Bausteins CON.3 *Datensicherungskonzept* aufgeführt. Zielobjekt ist der gesamte Informationsverbund.

Grundsätzlich ist der Informationssicherheitsbeauftragte für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Anforderung [Verantwortung]	Status	Umsetzung
CON.3.A1 *Erhebung der Einflussfaktoren der Datensicherung* [Fachverantwortliche, IT-Betrieb]	erfüllt	Es gibt ein aktuelles Datensicherungskonzept, bei dem die relevanten Einflussfaktoren (Umfang und Zeitpunkte von Änderungen, Verfügbarkeitsanforderungen etc.) für die unterschiedlichen Anwendungen des Unternehmens berücksichtigt sind
CON.3.A2 *Festlegung der Verfahrensweise für die Datensicherung* [Fachverantwortliche, IT-Betrieb]	erfüllt	Im Datensicherungsverfahren sind Art, Häufigkeit und Zeitpunkte der Datensicherungen sowie die Verantwortlichkeiten festgelegt, außerdem regelt es Art, Transport und Aufbewahrung der Speichermedien.
CON.3.A3 *Ermittlung von rechtlichen Einflussfaktoren auf die Datensicherung*	erfüllt	Rechtliche Anforderungen werden angemessen berücksichtigt.
CON.3.A4 *Erstellung eines Minimaldatensicherungskonzeptes*	erfüllt	Das Datensicherungskonzept beschreibt auch Minimalanforderungen.
CON.3.A5 *Regelmäßige Datensicherung* [IT-Betrieb]	teilweise erfüllt	Die Sicherungen erfolgen regelmäßig, die Sicherungsmedien werden vor unbefugten Zugriffen geschützt. Es wird jedoch nicht ausreichend getestet, ob die Datensicherung auch wie gewünscht funktioniert und gesicherte Daten problemlos zurückgespielt werden können.
CON.3.A6 *Entwicklung eines Datensicherungskonzepts* [Fachverantwortliche, Leiter IT]	erfüllt	Vgl. CON.3.A1 und CON.3.A2
CON.3.A7 Beschaffung eines geeigneten Datensicherungssystems [IT-Betrieb, Leiter IT]	erfüllt	Das eingesetzte Datensicherungssystem entspricht den Vorgaben.
CON.3.A8 *Funktionstests und Überprüfung der Wiederherstellbarkeit* [IT-Betrieb]	nicht erfüllt	Siehe CON.3A5
CON.3.A9 V*oraussetzungen für die Online-Datensicherung* [IT-Betrieb, Leiter IT]	entbehrlich	Verfahren ist nicht im Einsatz.
CON.3.A10 *Verpflichtung der Mitarbeiter zur Datensicherung*	erfüllt	Wird im Datensicherungskonzept berücksichtigt.
CON.3.A11 *Sicherungskopie der eingesetzten Software* [IT-Betrieb]	erfüllt	Hierzu gibt es eine entsprechende Verfahrensbeschreibung für die IT-Administration.
CON.3.A12 *Geeignete Aufbewahrung der Backup-Datenträger* [IT-Betrieb]	erfüllt	Die Backup-Datenträger werden unbefugtem Zugriff geschützt, räumlich von den Quellsystemen getrennt und unter angemessenen klimatischen Bedingungen aufbewahrt.

Tabelle 22: IT-Grundschutz-Check – Baustein CON.3 *Datensicherungskonzept*

6.4 SYS.1.1 *Allgemeiner Server*

Im Folgenden werden die Ergebnisse des IT-Grundschutz-Checks für die Basis- und Standard-Anforderungen des Bausteins SYS.1.1 *Allgemeiner Server* aufgeführt. Zielobjekt ist der Server S007.

Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Anforderung [Verantwortung]	Status	Umsetzung
SYS.1.1.A1 *Geeignete Aufstellung [Haustechnik]*	erfüllt	Der Zutritt zum Server ist geschützt und nur Berechtigten möglich. Der Standort des Servers ist in einem anderen Brandabschnitt als sein Backup-System.
SYS.1.1.A2 *Benutzerauthentisierung*	erfüllt	Benutzer müssen sich mit Passwörtern authentisieren, die den Komplexitätsanforderungen der Passwort-Richtlinie genügen sowie geheim gehalten und regelmäßig gewechselt werden müssen.
SYS.1.1.A3 *Restriktive Rechtevergabe*	erfüllt	Das Prinzip der minimalen Rechte ist gewahrt.
SYS.1.1.A4 *Rollentrennung*	erfüllt	Es gibt je eigene Konten für administrative Aufgaben und normale Benutzeraktivitäten. Die zuständigen Mitarbeiter sind angehalten, diese entsprechend den Erfordernissen zu verwenden.
SYS.1.1.A5 *Schutz der Administrationsschnittstellen*	erfüllt	Die Administration ist nur am IT-System selber möglich.
SYS.1.1.A6 *Deaktivierung nicht benötigter Dienste und Kennungen*	teilweise erfüllt	Die Konfiguration des Servers ist nicht dokumentiert, allerdings ergab ein ausführlicher Vor-Ort-Check keine Mängel.
SYS.1.1.A7 Updates und Patches für Firmware, Betriebssystem und Anwendungen	erfüllt	Der Server wird in angemessener Weise im Konzept des Unternehmens für die Behandlung und Behebung von Schwachstellen berücksichtigt.
SYS.1.1.A8 *Regelmäßige Datensicherung*	erfüllt	Der Server wird im Datensicherungskonzept (siehe CON.3) angemessen berücksichtigt. Die Sicherung erfolgt mithilfe der Snapshot-Funktion der Virtualisierungssoftware.
SYS.1.1.A9 *Einsatz von Viren-Schutzprogrammen*	erfüllt	Regelmäßig aktualisierte Virenschutz-Programme sind in Betrieb.
SYS.1.1.A10 *Protokollierung*	nicht erfüllt	Es gibt keine dokumentierte Vorgehensweise zur Protokollierung auf diesem IT-System, die von Betriebssystem- und Anwendungssoftware standardmäßig vorgesehene Ereignisaufzeichnung wird zwar ausgeführt, aber nicht ausgewertet.
SYS.1.1.A11 *Festlegung einer Sicherheitsrichtlinie für Server*	nicht erfüllt	Eine solche Richtlinie ist derzeit noch nicht vorhanden. Es ist geplant, sie bis Ende Juni anzufertigen.
SYS.1.1.A12 *Planung des Server-Einsatzes*	teilweise erfüllt	Die hierzu vorhandene Dokumentation ist unvollständig, z. B. fehlen Regelungen zu den Benutzerzugriffen und zur Protokollierung.
SYS.1.1.A13 *Beschaffung von Servern*	erfüllt	Vor der Beschaffung wurde eine Liste mit Auswahlkriterien zusammengestellt.
SYS.1.1.A14 *Erstellung eines Benutzer- und Administrationskonzepts*	teilweise erfüllt	Es gibt zwar eine Reihe an Einzelregelungen, aber noch kein integriertes Gesamtkonzept.
SYS.1.1.A15 *Unterbrechungsfreie und stabile Stromversorgung* [Haustechnik]	erfüllt	Alle Server sind an eine ausreichend dimensionierte, angemessen administrierte und regelmäßig geprüfte USV angeschlossen.
SYS.1.1.A16 *Sichere Installation und Grundkonfiguration von Servern*	erfüllt	Bei der nur von dazu berechtigten Personen durchgeführten und sorgfältig protokollierten Installation werden ausschließlich benötigte Dienste aktiviert. Die Software stammt aus vertrauenswürdigen Quellen.
SYS.1.1.A17 *Einsatzfreigabe*	erfüllt	Vor Inbetriebnahme und Netzanbindung eines Servers werden dessen Konfiguration und Funktionalität sorgfältig getestet. Die Freigabe wird dokumentiert.

Anforderung [Verantwortung]	Status	Umsetzung
SYS.1.1.A18 *Verschlüsselung der Kommunikationsverbindungen*	erfüllt	Es wurde geprüft, ob die Verschlüsselung der Verbindungen zweckmäßig ist.
SYS.1.1.A19 *Einrichtung lokaler Paketfilter*	erfüllt	Vorhandene Paketfilter werden so konfiguriert, dass ein- und ausgehende Kommunikation auf erforderliche Partner, Protokolle, Ports und Schnittstellen beschränkt ist.
SYS.1.1.A20 *Beschränkung des Zugangs über Netze*	teilweise erfüllt	Das interne Netz ist nach außen durch ein Sicherheitsgateway geschützt, Server für Dienste im internen Netz befinden sich im selben IP-Subnetz wie die Clients und sind nur durch einen Switch von den Clients getrennt.
SYS.1.1.A21 *Betriebsdokumentation*	teilweise erfüllt	Eine entsprechende Dokumentation ist angelegt, allerdings nicht auf dem aktuellen Stand. Dieser Mangel soll bis Mai behoben werden.
SYS.1.1.A22 *Einbindung in die Notfallplanung*	nicht erfüllt	Derzeit gibt es im Unternehmen noch kein geregeltes Notfallmanagement.
SYS.1.1.A23 *Systemüberwachung*	erfüllt	Die in Betrieb befindlichen Server werden umfassend überwacht. Bei Auffälligkeiten werden die zuständigen Administratoren automatisiert benachrichtigt.
SYS.1.1.A24 *Sicherheitsprüfungen*	teilweise erfüllt	Zwar gibt es Sicherheitsüberprüfungen, diese werden auch dokumentiert. Allerdings ist hierfür kein Zyklus festgelegt.
SYS.1.1.A25 *Geregelte Außerbetriebnahme eines Servers*	erfüllt	Für die Außerbetriebnahme eines Servers gibt es eine Checkliste. Es wird vorab geprüft, ob wichtige Daten vorab zu sichern sind, durch geeignete Verfahren ist sichergestellt, dass die vorhandenen Daten sicher gelöscht werden, und dafür gesorgt, dass auch bei Wegfall des IT-Systems, im Netz benötigte Dienste weiter angeboten werden.

Tabelle 23: IT-Grundschutz-Check – Baustein SYS.1.1 *Allgemeiner Server*

6.5 SYS.1.5 *Virtualisierung*

Im Folgenden werden die Ergebnisse des IT-Grundschutz-Checks für die Basis- und Standard-Anforderungen des Bausteins SYS.1.5 *Virtualisierung* aufgeführt. Zielobjekt ist der Server S007.

Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Anforderung [Verantwortung]	Status	Umsetzung
SYS.1.5.A1 Einspielen von Aktualisierungen und Sicherheitsupdates	erfüllt	Host-Betriebssystem, Management-Software und Hardware-Firmware werden regelmäßig aktualisiert und Sicherheitsupdates zeitnah eingespielt.
SYS.1.5.A2 Sicherer Einsatz virtueller IT-Systeme	erfüllt	Die Administratoren sind mit der Technik vertraut, ihre Zugriffsrechte auf die virtuellen IT-Systeme auf das notwendige Maß begrenzt. Die Systeme sind hinreichend gekapselt und werden überwacht, die Verfügbarkeitsanforderungen werden erfüllt.
SYS.1.5.A3 Sichere Konfiguration virtueller IT-Systeme	erfüllt	Die einzelnen virtuellen IT-Systeme sind den Sicherheitsrichtlinien der Institution entsprechend konfiguriert und geschützt, Zugriffe auf die Virtualisierungsschicht werden ausgeschlossen.
SYS.1.5.A4 Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen	erfüllt	Durch die Konfiguration des Virtualisierungsservers und der virtualisierten IT-Systeme werden keine Sicherheitsmechanismen des Netzes ausgehebelt oder geltende Sicherheitsrichtlinien der Institution verletzt.
SYS.1.5.A5 Schutz der Administrationsschnittstellen	erfüllt	Die Administration des Managementsystems ist nur am Gerät selber möglich.

Anforderung [Verantwortung]	Status	Umsetzung
SYS.1.5.A6 Protokollierung in der virtuellen Infrastruktur	nicht erfüllt	Die vorhandenen Protokollierungen folgen keinem Konzept, die Protokolle werden allenfalls unsystematisch ausgewertet.
SYS.1.5.A7 Zeitsynchronisation in virtuellen IT-Systemen	erfüllt	Die Systemzeiten werden über einen Zeitserver regelmäßig synchronisiert.
SYS.1.5.A8 Planung einer virtuellen Infrastruktur [Leiter IT, Leiter Netze]	erfüllt	Der Virtualisierungsserver wurde detailliert geplant und wird seitdem qualifiziert administriert.
SYS.1.5.A9 Netzplanung für virtuelle Infrastrukturen [Leiter IT, Leiter Netze]	nicht erfüllt	Es sind keine dokumentierten Planungen hinsichtlich des Netzes vorhanden.
SYS.1.5.A10 Einführung von Verwaltungsprozessen für virtuelle IT-Systeme [Leiter IT]	teilweise erfüllt	Es gibt Verfahrensanweisungen für die einzelnen Phasen im Lebenszyklus des Virtualisierungsservers und der zugehörigen virtuellen IT-Systeme. Es gibt allerdings keine gesonderte Test- und Entwicklungsumgebung für virtuelle IT-Systeme.
SYS.1.5.A11 Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz	entbehrlich	Die Administration der Virtualisierungsschicht ist nur lokal am Gerät möglich.
SYS.1.5.A12 Rechte- und Rollenkonzept für die Administration einer virtuellen Infrastruktur	erfüllt	Es gibt ein dokumentiertes Rollenkonzept.
SYS.1.5.A13 Auswahl geeigneter Hardware für Virtualisierungsumgebungen	erfüllt	Bei Beschaffung wurde auch ein hinreichend langer Supportzeitraum des Herstellers berücksichtigt.
SYS.1.5.A14 Einheitliche Konfigurationsstandards für virtuelle IT-Systeme [Leiter IT]	erfüllt	Entsprechende Standards sind definiert und dokumentiert.
SYS.1.5.A15 Betrieb von Gast-Betriebssystemen mit unterschiedlichem Schutzbedarf	erfüllt	Die virtuellen IT-Systeme sind ausreichend gekapselt und voneinander isoliert.
SYS.1.5.A16 Kapselung der virtuellen Maschinen	erfüllt	Die Funktionen „Kopieren" und „Einfügen" von Informationen zwischen virtuellen Maschinen sind deaktiviert.
SYS.1.5.A17 Überwachung des Betriebszustands und der Konfiguration der virtuellen Infrastruktur	teilweise erfüllt	Trotz vorhandener Überwachung werden die Konfigurationsdateien der virtuellen IT-Systeme allenfalls sporadisch auf unautorisierte Änderungen überprüft.
SYS.1.5.A18 Schulung der Administratoren virtueller Umgebungen [Vorgesetzte, Leiter IT, Leiter Netze]	erfüllt	Alle Administratoren sind geschult.
SYS.1.5.A19 Regelmäßige Audits der Virtualisierungsinfrastruktur	nicht erfüllt	Es gibt keine regelmäßigen Audits.

Tabelle 24: IT-Grundschutz-Check – Baustein SYS.1.5 *Virtualisierung*

6.6 INF.2 *Rechenzentrum sowie Serverraum*

Im Folgenden werden die Ergebnisse des IT-Grundschutz-Checks für die Basis- und Standard-Anforderungen des Bausteins INF.2 *Rechenzentren sowie Serverraum* aufgeführt. Grundsätzlich ist der Leiter IT dafür zuständig, die Anforderungen zu erfüllen. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt.

Anforderung [Verantwortung]	Status	Umsetzung
INF.2.A1 Festlegung von Anforderungen [Planer, IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Haustechnik]	nicht erfüllt	Ein ansonsten nicht benötigter Raum wurde zum Serverraum umgebaut, ohne dass hierfür vertiefte konzeptionelle Überlegungen angestellt und dokumentiert wurden.

Anforderung [Verantwortung]	Status	Umsetzung
INF.2.A2 Bildung von Brandabschnitten [Planer]	nicht erfüllt	Der Serverraum bildet keinen eigenen, sondern einen gemeinsamen Brandabschnitt mit anderen kritischen Bereichen des Unternehmens.
INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung [Haustechnik]	erfüllt	Die IT-Systeme verfügen über eine ausreichend dimensionierte USV, die dem Stand der Technik entspricht, sodass bei plötzlichem Stromausfall ein geordnetes Herunterfahren möglich ist und Datenverluste vermieden werden können. Die vom Hersteller vorgegebenen Wartungsintervalle werden eingehalten.
INF.2.A4 Notabschaltung der Stromversorgung [Haustechnik]	erfüllt	Ein gegen versehentliches Betätigen gut geschützter Not-Aus-Schalter ist installiert.
INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit [Haustechnik]	erfüllt	Eine geeignete Klimaanlage ist im Einsatz – siehe auch INF.2.A16.
INF.2.A6 Zutrittskontrolle [IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Haustechnik]	erfüllt	Für den Serverraum gelten strikte Zutrittsregelungen, nur wenige Berechtigte haben einen Schlüssel. Andere Personen dürfen sich nur unter Aufsicht im Raum aufhalten. Ihre Anwesenheit wird in einem Besucherbuch dokumentiert.
INF.2.A7 Verschließen und Sichern [Mitarbeiter, Haustechnik]	erfüllt	Der Serverraum ist verschlossen, nur Berechtigte haben einen Schlüssel. Es sind zwar Fenster vorhanden, die aber ebenfalls verschlossen gehalten werden und zusätzlich durch ein Metallgitter geschützt sind.
INF.2.A8 Einsatz einer Brandmeldeanlage [Planer]	teilweise erfüllt	Eine Brandmeldeanlage ist installiert. Da im Raum umfangreiche Akten gelagert sind, darunter die Dokumentation der IT-Systeme ist allerdings die Brandlast unnötigerweise erheblich erhöht.
INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage [Planer]	erfüllt	Die vorhandene Anlage wird regelmäßig geprüft und entspricht dem Stand der Technik. Die Mitarbeiter wurden in die Benutzung der Handfeuerlöscher eingewiesen.
INF.2.A10 Inspektion und Wartung der Infrastruktur [IT-Betrieb, Haustechnik, Wartungspersonal]	teilweise erfüllt	Bei der Wartung einzelner Komponenten zeigten sich Mängel – siehe auch INF.2.A13.
INF.2.A11 Automatisierte Überwachung der Infrastruktur [IT-Betrieb, Haustechnik]	nicht erfüllt	Es gibt zwar Alarmierungen für einzelne Komponenten, aber keine durchgängig automatisierte Überwachung der Infrastruktur und auch keine technische Unterstützung hierfür.
INF.2.A12 Entwurf und Umsetzung eines Perimeterschutzes für das Rechenzentrum [Planer, Haustechnik]	erfüllt	Die Maßnahmen zur Gebäudesicherheit sorgen für einen angemessenen Schutz.
INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen [Planer]	nicht erfüllt	Zwar gibt es automatisierte Alarme gegen die Gefahren durch Feuer und ungünstige klimatische Bedingungen, allerdings nur als Einzelmaßnahmen und nicht als Teil eines konsistenten Schutzkonzepts. Die vorhandenen Prozessbeschreibungen zur Behandlung von Alarmen sind veraltet und entsprechen nicht mehr den Gegebenheiten.
INF.2.A14 Einsatz einer Netzersatzanlage [Planer, Haustechnik]	teilweise erfüllt	Das Unternehmen verfügt über eine Netzersatzanlage (NEA), allerdings zeigten sich Mängel bei der Wartung (die hierfür vorgesehenen Intervalle werden nicht eingehalten, Belastungs- und Funktionstests werden nur sporadisch durchgeführt).
INF.2.A15 Überspannungsschutzeinrichtung [Planer, Haustechnik]	erfüllt	Die vorhandenen Vorrichtungen werden zum Überspannungsschutz sind angemessen, gut dokumentiert und werden regelmäßig gewartet.
INF.2.A16 Klimatisierung im Rechenzentrum [Haustechnik]	erfüllt	Eine durch redundante Komponenten hinreichend ausfallsichere Klimaanlage wird betrieben, die bei Überschreitung der Grenzwerte für Temperatur und Feuchtigkeit der Luft einen akustischen Alarm auslöst.
INF.2.A17 Brandfrüherkennung [Planer, Haustechnik]	erfüllt	Eine dem Stand der Technik gemäße Anlage ist vorhanden und wird regelmäßig gewartet.

Anforderung [Verantwortung]	Status	Umsetzung
INF.2.A18 Schutz vor Wasseraustritt [Haustechnik]	nicht erfüllt	In der Decke des Raums befinden sich Versorgungsleitungen für Wasser und die Heizungen. Es gibt keine Vorkehrungen zur Begrenzung der Folgen eines möglichen Wasseraustritts.
INF.2.A19 Durchführung von Funktionstests der technischen Infrastruktur [Haustechnik]	nicht erfüllt	Es gibt keine Vorgaben für die Durchführung regelmäßiger Funktionstests und deren Dokumentation. Der letzte Test liegt zwei Jahre zurück, die Dokumentation hierzu ist lückenhaft.
INF.2.A20 Regelmäßige Aktualisierungen der Infrastruktur- und Baupläne [Planer]	nicht erfüllt	Die vorliegenden Pläne sind nicht aktuell. Prozesse zur regelmäßigen Prüfung und Aktualisierung dieser Dokumente sind nicht dokumentiert.

Tabelle 25: IT-Grundschutz-Check – Baustein INF.2 *Rechenzentrum sowie Serverraum*

7 Risikoanalyse

7.1 Organisatorischer Rahmen

In der RECPLAST GmbH wurde beschlossen, das Risikomanagement gemäß IT-Grundschutz auszurichten und ihre Sicherheitskonzeption gemäß Standard-Absicherung zu entwickeln. Für Objekte mit normalem Schutzbedarf erfolgt die Risikobehandlung mithilfe der Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums. Als Methode für unter Umständen erforderliche Risikoanalysen wurde der BSI-Standard 200-3 festgelegt. In einer Richtlinie zur Behandlung von Risiken wurde ferner formuliert, dass Risiken, die aus der Nichterfüllung von Basis-Anforderungen folgen, nicht akzeptiert werden können. Risiken sollen darüber hinaus unter Betrachtung der Kosten möglicher Maßnahmen und ihres Beitrags zur Risikominimierung behandelt werden.

Die Verantwortlichkeit für die Durchführung der Risikoanalyse obliegt dem ISB, der hierfür spezialisierte Teams bildet. Deren Zusammensetzung hängt vom jeweiligen Sachverhalt ab: Anwendungsverantwortliche wirken bei der Bewertung möglicher Schadensfolgen mit; erfordert die Bewertung der Risiken einen hohen technischen Sachverstand, werden kompetente Mitarbeiter der IT-Abteilung beteiligt.

Die durchgeführten Risikoanalysen werden dokumentiert, die Ergebnisse und die Vorschläge zur Risikobehandlung an die Geschäftsführung berichtet und mit ihr abgestimmt. Aktualität und Angemessenheit der Risikoanalysen sollen jährlich geprüft werden.

7.2 Zielobjekte für Risikoanalyse zusammenstellen

Bei der RECPLAST GmbH wurde aufgrund der Schutzbedarfsfeststellung und der Modellierung eine Reihe von Zielobjekten ermittelt, für die eine Risikoanalyse durchzuführen ist. Dazu gehören unter anderem die folgenden Komponenten:

- die Anwendung A007 *Lotus Notes*, die einen hohen Bedarf an Vertraulichkeit und einen sehr hohen Bedarf an Verfügbarkeit hat,
- die Netzkopplungselemente N001 *Router Internet-Anbindung* und N002 *Firewall Internet-Eingang*, beide wegen der Vertraulichkeit der über sie übertragenen Daten,
- der Virtualisierungsserver S007, der in allen drei Grundwerten aufgrund der auf ihm betriebenen virtuellen Systeme einen hohen Schutzbedarf hat,
- die Alarmanlagen S200 an beiden Standorten in Bonn, deren korrektes Funktionieren als sehr wichtig eingestuft und deren Schutzbedarf bezüglich Integrität und Verfügbarkeit folglich mit „sehr hoch“ bewertet wurde.

Nachfolgend werden die einzelnen Schritte der Risikoanalyse am Beispiel des über beide Standorte hinweg redundant ausgelegten Virtualisierungsservers S007 veranschaulicht.

7.3 Gefährdungsübersicht anlegen

Für den Virtualisierungsserver der RECPLAST GmbH sind die Bausteine SYS.1.1 *Allgemeiner Server*, SYS.1.3 *Server unter Unix* und SYS.1.5 *Virtualisierung* relevant. Darin werden die folgenden Gefährdungen betrachtet (Grundwerte: C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit):

Gefährdung	Betroffene Grundwerte
G 0.8 Ausfall oder Störung der Stromversorgung	A
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	A
G 0.14 Ausspähen von Informationen (Spionage)	C
G 0.15 Abhören	C
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A
G 0.18 Fehlplanung oder fehlende Anpassung	C, I, A
G 0.19 Offenlegung schützenswerter Informationen	C
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	I, A
G 0.21 Manipulation von Hard- oder Software	I, A
G 0.22 Manipulation von Informationen	I
G 0.23 Unbefugtes Eindringen in IT-Systeme	C, I, A
G 0.25 Ausfall von Geräten oder Systemen	A
G 0.26 Fehlfunktion von Geräten oder Systemen	A
G 0.27 Ressourcenmangel	A
G 0.28 Software-Schwachstellen oder -Fehler	C, I, A
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.32 Missbrauch von Berechtigungen	C, I, A
G 0.39 Schadprogramme	C, I, A
G 0.40 Verhinderung von Diensten (Denial of Service)	A
G 0.43 Einspielen von Nachrichten	I
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	C, I, A
G 0.45 Datenverlust	C, A
G 0.46 Integritätsverlust schützenswerter Informationen	I

Tabelle 26: Relevante elementare Gefährdungen für den betrachteten Virtualisierungsserver

7.4 Gefährdungsübersicht ergänzen

Bei der RECPLAST GmbH wurde keine Gefährdung identifiziert, die nicht schon in den oben genannten Bausteinen betrachtet wurde.

7.5 Risiken bewerten

Die Kategorien zur Bewertung von Eintrittshäufigkeiten, Schadensauswirkungen und resultierenden Risiken wurden wie in den folgenden Tabellen dargestellt definiert:

Eintrittshäufigkeit	Beschreibung
selten	Das Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre auftreten.
mittel	Das Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Das Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
Sehr häufig	Das Ereignis tritt mehrmals im Monat ein.

Tabelle 27: Definition der Kategorien für die Bewertung von Eintrittshäufigkeiten

Schadensauswirkungen	Beschreibung
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß annehmen.

Tabelle 28: Definition der Kategorien für die Bewertung von Schadensauswirkungen

Risikokategorie	Definition
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Maßnahmen bieten einen ausreichenden Schutz.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Maßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer großen Wahrscheinlichkeit nicht akzeptiert werden.
Sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer sehr großen Wahrscheinlichkeit nicht akzeptiert werden.

Tabelle 29: Definition der Kategorien für die Bewertung von Risiken

Die folgende Risikomatrix zeigt, wie die Bewertungen von Häufigkeiten und Auswirkungen in die Risikobewertung einfließen:

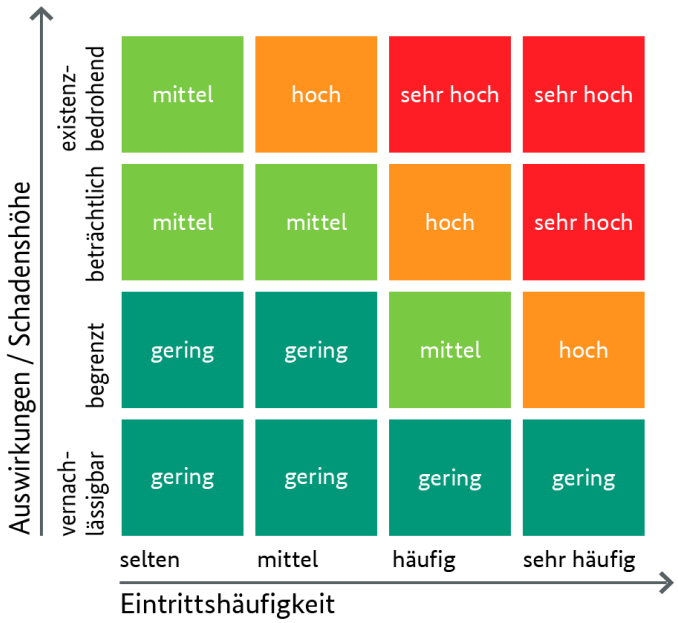

Abbildung 4: Risikomatrix

Mithilfe dieser Risikodefinition wurden die Risiken für die als relevant angesehenen Gefährdungen für den Virtualisierungsserver S007 wie in der folgenden Tabelle dargestellt bewertet:

Gefährdung (bedrohte Grundwerte)	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.8 Ausfall oder Störung der Stromversorgung (A)	häufig	begrenzt	mittel
G 0.9 Ausfall oder Störung von Kommunikationsnetzen (A)	häufig	begrenzt	mittel
G 0.14 Ausspähen von Informationen (Spionage) (C)	mittel	begrenzt	gering
G 0.15 Abhören (C)	selten	beträchtlich	mittel
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten (C, A)	selten	begrenzt	gering
G 0.18 Fehlplanung oder fehlende Anpassung (C, I, A)	mittel	begrenzt	gering
G 0.19 Offenlegung schützenswerter Informationen (C)	mittel	Begrenzt	gering
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle (C, I, A)	selten	begrenzt	gering
G 0.21 Manipulation von Hard- oder Software (C, I, A)	selten	begrenzt	gering
G 0.22 Manipulation von Informationen (I)	mittel	begrenzt	gering
G 0.23 Unbefugtes Eindringen in IT-Systeme (C. I. A)	mittel	beträchtlich	mittel
G 0.25 Ausfall von Geräten oder Systemen (A)	mittel	beträchtlich	mittel
G 0.26 Fehlfunktion von Geräten oder Systemen (A)	mittel	begrenzt	gering
G 0.27 Ressourcenmangel (A)	mittel	begrenzt	gering
G 0.28 Software-Schwachstellen oder -Fehler (C, I, A)	häufig	begrenzt	mittel
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen (C, I, A)	selten	beträchtlich	mittel
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen (C, I, A)	mittel	beträchtlich	mittel
G 0.32 Missbrauch von Berechtigungen (C, I, A)	selten	beträchtlich	mittel
G 0.39 Schadprogramme (C, I, A)	mittel	beträchtlich	mittel
G 0.40 Verhinderung von Diensten (Denial of Service) (A)	mittel	begrenzt	gering

Gefährdung (bedrohte Grundwerte)	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.43 Einspielen von Nachrichten (I)	selten	vernachlässigbar	gering
G 0.44 Unbefugtes Eindringen in Räumlichkeiten (C, I, A)	selten	beträchtlich	mittel
G 0.45 Datenverlust (C, A)	mittel	beträchtlich	mittel
G 0.46 Integritätsverlust schützenswerter Informationen (I)	selten	beträchtlich	mittel

Tabelle 30: Risikobewertung

7.6 Risikobehandlung

Im Anschluss an die Risikobewertung ist zu entscheiden, wie die identifizierten Risiken zu behandeln sind. Dabei kommen gemäß BSI-Standard 200-3 grundsätzlich vier Möglichkeiten der Risikobehandlung infrage, und zwar

- die **Risikovermeidun**g beispielsweise durch Verzicht auf risikobehaftete Prozesse oder technische Komponenten,
- die **Risikoreduktion** beispielsweise durch zusätzliche Maßnahmen zur Verringerung von Schadensauswirkungen, Eintrittshäufigkeiten oder beidem,
- der **Risikotransfer** beispielsweise durch Abschluss einer Versicherung zur Vorbeugung gegen finanzielle Schäden,
- die **Risikoakzeptanz** beispielsweise, weil die mit dem Risiko verbundenen Chancen genutzt werden sollen und zusätzliche Maßnahmen zur Reduktion oder Verlagerung des Risikos für nicht erforderlich angesehen werden.

Nach einer Prüfung wurde bei der RECPLAST GmbH festgestellt, dass die als „gering“ bewerteten Risiken durch die vorhandenen Sicherheitsmaßnahmen ausreichend abgedeckt sind, so dass diese Risiken akzeptiert wurden. Für die als „mittel“ eingestuften Risiken wurden die in der folgenden Tabelle dargestellten Entscheidungen getroffen:

Gefährdung	Risikobehandlungsoption
G 0.8 Ausfall oder Störung der Stromversorgung	**Risikoakzeptanz:** Eine Störung an einem der beiden Standorte wird durch die Redundanz der beiden Virtualisierungsserver abgedeckt. Das Risiko eines gleichzeitigen Stromausfalls in Beuel und Bad Godesberg wird als gering eingeschätzt und übernommen.
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	**Risikoreduktion:** Eine Störung der Verbindung zwischen den lokalen Netzen der beiden Standorte hätte beträchtliche Auswirkungen auf die Zuverlässigkeit der Virtualisierungsserver. Deshalb soll diese Verbindung durch eine zweite, unabhängige Standleitung redundant ausgelegt werden.
G 015 Abhören (hier bei Live-Migration)	**Risikoakzeptanz:** Auf das Live-Migration-Netz dürfen nur befugte Administratoren zugreifen. Diesen wird vertraut. Das bestehende Restrisiko wird von der RECPLAST GmbH als vertretbar eingeschätzt und übernommen.
G 0.23 Unbefugtes Eindringen in IT-Systeme	**Risikoakzeptanz:** Aufgrund der bereits umgesetzten Maßnahmen zum Schutz des Zugangs zum und des Zugriffs auf den Server wurde das verbleibende Restrisiko für vertretbar gehalten.

Gefährdung	Risikobehandlungsoption
G 0.25 Ausfall von Geräten oder Systemen (hier Ausfall des Virtualisierungsservers)	**Risikoreduktion** durch ergänzende Sicherheitsmaßnahme: Der Server ist bereits redundant ausgelegt; damit ist sichergestellt, dass die virtuelle Infrastruktur bei einem Ausfall weiterhin problemlos betrieben wird. Um die Ausfallzeit weiter zu verkürzen, wird das System so konfiguriert, dass bei einem Ausfall automatisch auf den Rechner am anderen Standort umgeschaltet wird.
G 0.28 Software-Schwachstellen oder -Fehler	**Risikoakzeptanz:** Die Administratoren verfolgen die aktuellen Meldungen über Schwachstellen der Software des Systems und spielen verfügbare Sicherheitspatches zeitnah ein. Weitere Maßnahmen wurden nicht für nötig erachtet.
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	**Risikoakzeptanz:** Die Zugriffsrechte auf Virtualisierungs- und Betriebssystemschicht sind strikt reglementiert. Den Administratoren werden zudem als vertrauenswürdig eingestuft, so dass weitergehende Maßnahmen zur Kontrolle der Administrationszugriffe in Relation zum hierfür erforderlichen Aufwand als nicht erforderlich eingestuft wurden.
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	**Risikoreduktion:** Zwar werden die Administratoren grundsätzlich als zuverlässig angesehen, jedoch steht in den nächsten Monaten ein Betriebssystemupgrade an. Zur Vorbereitung und zur Vermeidung künftiger Fehler sollen die Administratoren eine Schulung in die Besonderheiten dieser Software erhalten.
G 0.32 Missbrauch von Berechtigungen	**Risikoakzeptanz:** Die vorhandenen Berechtigungen werden als hinreichend restriktiv angesehen. Den Administratoren wird vertraut, so dass weitergehende Kontrollen ihrer Tätigkeit nicht geplant werden.
G 0.39 Schadprogramme	**Risikoreduktion:** Die technischen Maßnahmen zur Risikominimierung für den Server werden als hinreichend erachtet. Da sich aber diese Gefährdungen insbesondere auch aufgrund von Leichtfertigkeit oder anderen Fehlern der Benutzer ergeben, ist eine grundsätzliche Sensibilisierungsmaßnahme zu den Gefahren durch Schadsoftware, Phishing, Social Engineering etc. geplant. Diese Maßnahme zielt auf alle IT-Systeme des Unternehmens ab (damit auch den Server).
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	**Risikoreduktion:** Zwar sind die Maßnahmen und Regelungen zum Zutrittsschutz grundsätzlich ausreichend, jedoch zeigten Begehungen Mängel in der Umsetzung. Es werden daher zusätzliche Kontrollen und Sensibilisierungen zur Einhaltung der Regelungen geplant
G 0.45 Datenverlust	**Risikoakzeptanz:** Die Backup-Verfahren für den Server werden als ausreichend gewertet.
G 0.46 Integritätsverlust schützenswerter Informationen	**Risikoreduktion:** Es wird geplant, mithilfe von Prüfprogrammen regelmäßig zu testen, ob es zu Integritätsverletzungen an wichtigen Systemdateien oder anderen kritischen Daten gekommen ist.

Tabelle 31: Entscheidungen zur Risikobehandlung

8 Umsetzungsplanung

Als Ergebnis aus IT-Grundschutz-Check und der Entscheidungen zur Risikoplan ergibt sich eine Liste an Maßnahmen, die umgesetzt werden sollen, um die relevanten und dem Schutzbedarf des Informationsverbundes entsprechenden Sicherheitsanforderungen zu erfüllen. Bei der Umsetzungs- oder Realisierungsplanung geht es nun darum,

- das Zusammenwirken der einzelnen Maßnahmen zu prüfen, bei Bedarf einzelne Maßnahmen zu konkretisieren oder unnötige Redundanzen durch Ausschluss von Maßnahmen zu verhindern, um so zu einer angemessenen, konsolidierten Maßnahmenliste zu gelangen,
- die einmaligen und regelmäßigen Aufwände der verbliebenen Maßnahmen zu schätzen,
- für deren Umsetzung Termine und Verantwortliche festzulegen sowie
- Entscheidungen zu begleitenden Maßnahmen zu treffen, die eine erfolgreiche Umsetzung zu erleichtern können.

Das folgende Beispiel zeigt Maßnahmen für ausgewählte Zielobjekte und die zugehörigen Entscheidungen zu Terminen, Budget und Verantwortlichkeiten.

Zielobjekt	Anforderung	Umzusetzende Maßnahme	Terminplanung	Budget	Verantwortlich für Umsetzung
S003 Druckserver	SYS.1.1.A3 *Restriktive Rechtevergabe*	Die verbliebenen Gruppenberechtigungen müssen aufgelöst werden.	Drittes Quartal des Jahres	Keine Kosten	Herr Schmitt (IT-Betrieb)
	SYS.1.1.A4 *Rollentrennung*	Separate Benutzerkennungen für jeden Administrator einrichten.	31. Juli des Jahres	Keine Kosten	Herr Schmitt (IT-Betrieb)
	SYS.1.1.A8 *Regelmäßige Datensicherung*	Die Datensicherungen werden derzeit auf Bändern im Serverraum aufbewahrt. Ein externes Backup-System ist geplant. Ein Angebot für die Initialisierung liegt bereits vor (15.000 €). Die Betriebskosten müssen noch verhandelt werden.	Erstes Quartal im Folgejahr	Anschaffung: 15.000 € Betrieb: Noch offen	Frau Meyer (Einkauf)
R2, R8 Serverräume	INF.2.A14 E*insatz einer Netzersatzanlage*	Mit dem Lieferanten der Netzersatzanlage wird ein Vertrag über regelmäßige Wartung und Tests abgeschlossen	Sofort, möglichst vor dem nächsten Stromausfall	ca. 1000 € pro Jahr ohne Material	Herr Hellweg (Haustechnik), Frau Fischer (Einkauf)
RECPLAST (Informationsverbund)	ISMS.1.A14 *Sensibilisierung zur Informationssicherheit*	Das Sensibilisierungskonzept zur Informationssicherheit soll am 30. Juni fertiggestellt und von der Geschäftsführung verabschiedet sein. Erste Maßnahmen daraus werden noch im 2. Halbjahr umgesetzt.	30. Juni des Jahres	Keine Kosten	ISB, Geschäftsführung
	ORP.3.A6 *Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit*	Eine erste Schulungsreihe mit drei Terminen wird bei einem Schulungsanbieter eingekauft und im 2. Halbjahr angeboten.	2. Halbjahr	Externer Referent: 1.500 €; Arbeitszeit der MA	ISB

Tabelle 32: Umsetzungsplanung zu ausgewählten Anforderungen