Bundesamt
für Sicherheit in der
Informationstechnik

Beschreibung des Beispielunternehmens RECPLAST GmbH

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

Verzeichnis der Abbildungen

Tabellenverzeichnis

1. Einleitung zu diesem Dokument

In diesem Dokument werden die einzelnen Schritte bei der Variante „Standard-Absicherung“ der IT-Grundschutz-Methodik nach BSI Standard 200-2 veranschaulicht. Das Dokument richtet sich an alle, die an der Umsetzung des IT-Grundschutzes interessiert sind oder diesen bereits umgesetzt haben. Die Anwender des IT-Grundschutzes sollen durch dieses Dokument eine ausführliche Hilfestellung und wertvolle praktische Umsetzungstipps erhalten. Der Aufbau des Dokuments orientiert sich an der Vorgehensweise der IT-Grundschutz-Methodik. Zuerst wird das fiktive Beispielunternehmen RECPLAST GmbH beschrieben und anschließend die einzelnen Schritte des IT-Grundschutzes an der RECPLAST GmbH durchgespielt.

Der Darstellung liegt die Edition 2019 des IT-Grundschutz-Kompendiums zugrunde.

Aus Gründen der Lesbarkeit wurde in den Dokumenten die männliche Form gewählt, dennoch beziehen sich die Angaben auf Angehörige aller Geschlechter.

2. Beschreibung der RECPLAST GmbH

Die RECPLAST GmbH 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.

Das Auftragsvolumen, die 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.

3. Geltungsbereich

Der Informationsverbund der RECPLAST ist wie folgt definiert:

- Kurzbezeichnung: RECPLAST GmbH
- Langbezeichnung: Die RECPLAST GmbH mit allen Geschäftsprozessen, Anwendungen und IT-Systemen zur Erbringung der Produktion.

Der Informationsverbund erstreckt sich auf die gesamte RECPLAST GmbH.

3.1. Organisatorische Gliederung

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

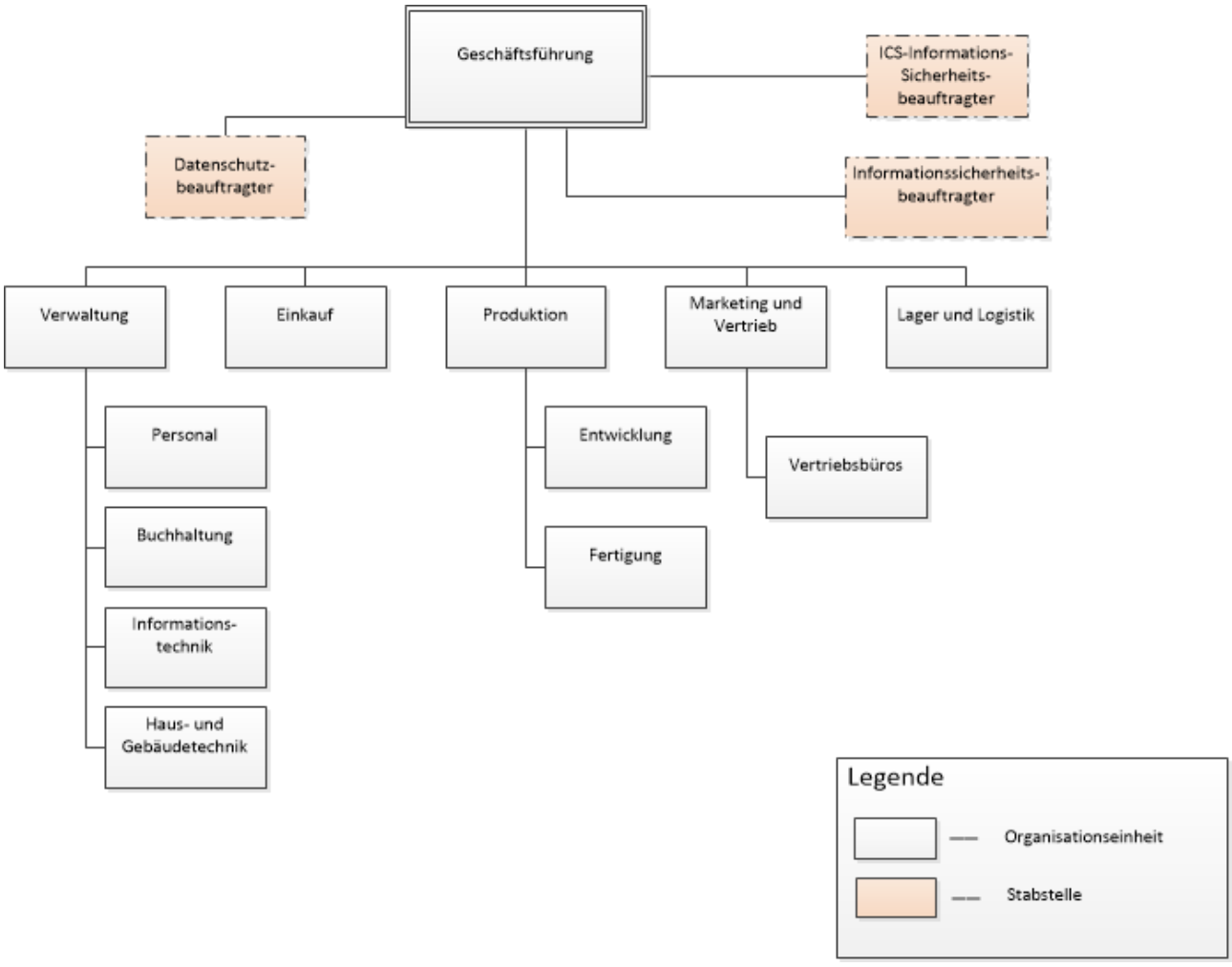

Abbildung 1: Organigramm der RECPLAST GmbH

3.2. Standorte und Mitarbeiter

Die Geschäftsführung hat zusammen mit den Verwaltungsabteilungen und den Abteilungen für Einkauf, Marketing und Vertrieb ein neues Gebäude in **Bad Godesberg** bezogen, während Entwicklung, Produktion, Material- und Auslieferungslager am ursprünglichen Firmensitz im Bonner Stadtteil **Beuel** verblieben sind.

Zusätzlich gibt es **Vertriebsbüros** in Berlin, München und Paderborn.

Darüber hinaus nutzen Mitarbeiter ihre Laptops und verbinden sich **remote** mit dem Firmennetzwerk.

Das Unternehmen beschäftigt insgesamt rund 500 Mitarbeiter, von denen 175 in der Verwaltung in Bad Godesberg, 310 in der Produktion und im Lager in Beuel und jeweils drei Mitarbeiter in den Vertriebsbüros in Berlin, München und Paderborn tätig sind.

3.3. Vereinfachter Netzplan der RECPLAST

In der untenstehenden Darstellung wird der Aufbau des Netzes der RECPLAST vereinfacht veranschaulicht.

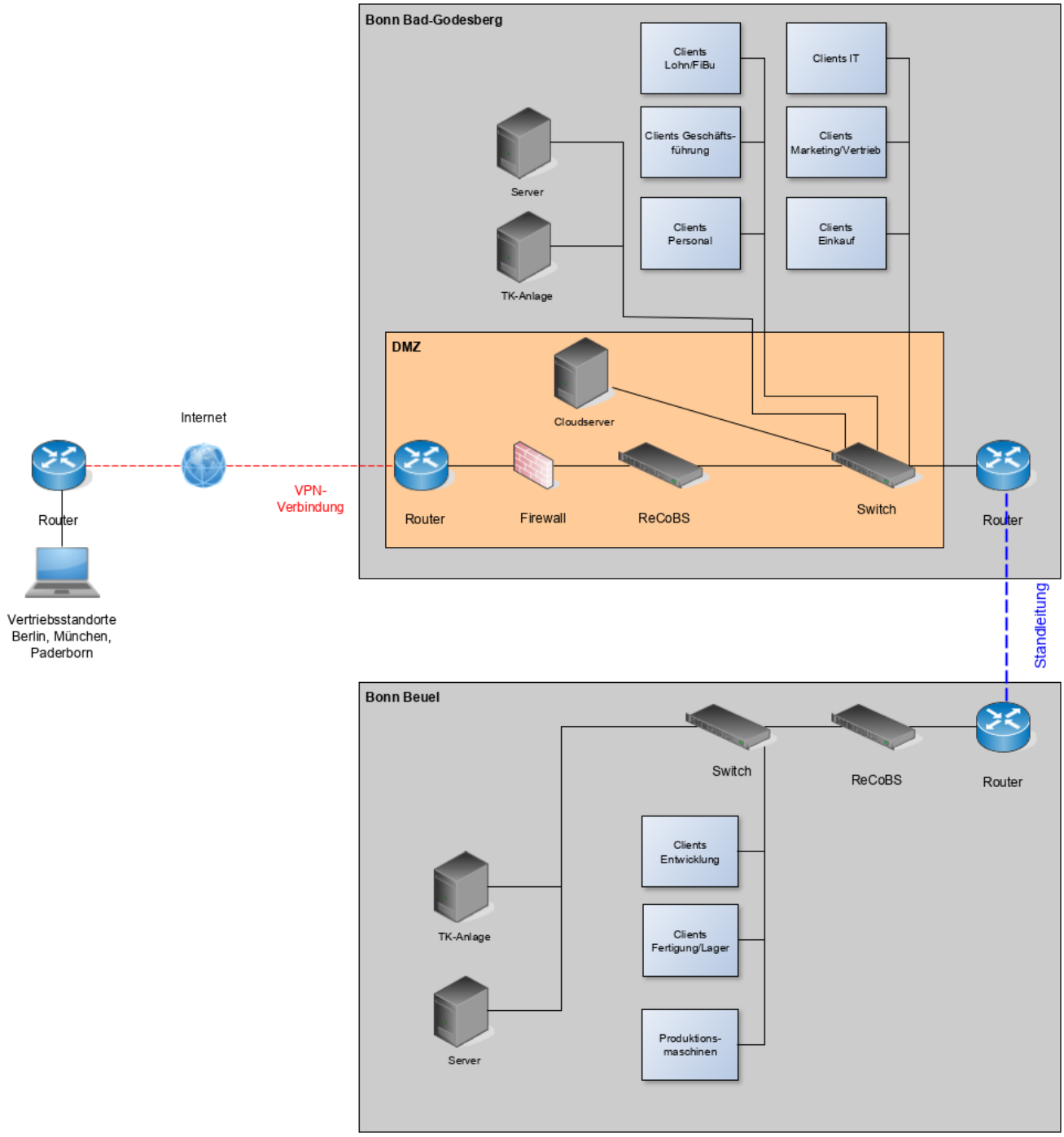

Abbildung 2: Vereinfachter Netzplan der RECPLAST

3.4. Informationstechnik

Am Standort **Bad Godesberg** ist im Zuge des Umzugs ein zentral administriertes Windows-Netz mit insgesamt 126 angeschlossenen Arbeitsplätzen eingerichtet worden. Die Arbeitsplatzclients sind einheitlich mit dem Betriebssystem Windows 10, den üblichen Büro-Anwendungen (Standardsoftware für Textverarbeitung, Tabellenkalkulation und für die Erstellung von Präsentationen) und Client-Software zur E-Mail-Nutzung ausgestattet. Zusätzlich ist je nach Aufgabengebiet auf verschiedenen Clients Spezialsoftware installiert.

Den Mitarbeitern des Standorts Bad Godesberg stehen zusätzlich 42 Laptops zur Verfügung.

Im Netz des Standorts Bad Godesberg (siehe Abbildung 3) werden die folgenden Server für folgende Zwecke eingesetzt:

- Zwei Server dienen als Virtualisierungshosts,
- Ein virtueller Server dient als Domänen-Controller (Virtualisierungshost 1),
- ein virtueller Server dient der Dateiablage (Virtualisierungshost 1),
- ein virtueller Server dient als Druckserver (Virtualisierungshost 1),
- ein virtueller Server dient als Wiki-Server (Virtualisierungshost 2),
- ein virtueller Server dient als internes Ticketsystem (Virtualisierungshost 2),
- ein Server dient als Backupserver,
- ein virtueller Server dient als Windows-Update-Server (Virtualisierungshost 2),
- ein virtueller Sever dient als Linux-Update-Server (Virtualisierungshost 2),
- ein Server dient als Cloudserver,
- ein Server dient als Datenbankserver für die Personal- und Finanzdaten,
- ein weiterer Datenbankserver dient der Kunden- und Auftragsbearbeitung,
- ein weiterer Datenbankserver dient dem Systemmanagement,
- ein Server dient als Kommunikations-Server (Mail-Server, Termin- und Adressverwaltung).

Die beiden Virtualisierungshosts sind unabhängig voneinander konfiguriert und betreiben unterschiedliche virtuelle Maschinen. Alle IT-Systeme auf den Virtualisierungsservern werden als einzelne virtuelle Maschinen betrieben.

Der **Standort Beuel** verfügt über weitere IT-Systeme. Die Produktion erfolgt durch zwei leistungsfähige, speicherprogrammierbare Maschinen, die über den Server zur Produktionssteuerung kontrolliert und konfiguriert werden. Darüber hinaus werden die Produktionsprozesse durch ein SCADA-System (Supervisory Control and Data Acquisition-System) überwacht. Die Programme und Konfigurationen werden in der Entwicklungsabteilung erstellt. Die Arbeitsplatzclients in Beuel haben die gleiche Grundausstattung wie die Clients in der Verwaltung in Bad Godesberg. Zusätzlich ist auf mehreren PCs CAD/CAM-Software (CAD/CAM: Computer Aided Design/Computer Aided Manufacturing) installiert.

Am Standort Beul gibt es weitere Server:

- Virtualisierungsserver
    - Virtueller Server 1.1 Domänen-Controller
    - Virtueller Server 1.2 Dateiserver
    - Virtueller Server 1.3 Druckserver
- Server für die Produktionssteuerung

- Server für die Betriebsdatenerfassung.

Den Mitarbeitern des Standorts Beuel stehen 80 Arbeitsplatzclients und 19 Laptops zur Verfügung.

Die beiden Standorte Bad Godesberg und Beuel sind über eine angemietete Standleitung miteinander verbunden.

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 mittels Authentisierung und VPN. Den Mitarbeitern der Vertriebsbüros stehen je 3 Laptops zur Verfügung

Von **unterwegs** aus erfolgt der Remote-Zugriff auf das Unternehmensnetz über VPN.

Das **Unternehmensnetz** ist über DSL an das Internet angebunden. Der Internet-Zugang ist über eine Firewall und einen Switch mit Paketfilter abgesichert. Alle Clients haben E-Mail-Zugang sowie die Möglichkeit zur freien Internetrecherche. Die Webseite des Unternehmens wird auf einem Webserver des Providers vorgehalten.

Weitere, zu berücksichtigende Informationstechnik:

- Telekommunikationsanlagen in Bad Godesberg und Beuel,
- Alarmanlagen zur Sicherung der Gebäude in Bad Godesberg und Beuel,
- acht Faxgeräte (davon vier in Bad Godesberg, jeweils eins in den Vertriebsbüros und eins in Beuel).

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.

4. Sicherheitsmanagement

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

Umfassende Informationen zu den behandelten Themen und weiteren Aspekten, die beim Aufbau eines Managementsystems für Informationssicherheit 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

4.1. Initiierung des Sicherheitsprozesses

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.

Zur initialen Erstellung des Sicherheitskonzeptes wird ein zeitlich befristetes Projekt „Sicherheitskonzept“ eingerichtet, das folgende Ergebnisse erzielen soll:

1. Erstellung von Vorschlägen und Entscheidungsvorlagen für eine Leitlinie zur Informationssicherheit.
2. Erstellung eines Vorschlags für ein Sicherheitskonzept und einen zugehörigen Realisierungsplan.
3. Erstellung eines Vorschlags 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. Dem IS-Management-Team gehören der Datenschutzbeauftragte, die 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.

4.2. 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.

Die Kommunikation der Leitlinie erfolgt über das interne Wiki-System. 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.

4.3. 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 Informationstechnik muss so betrieben werden, dass Geschäftsinformationen 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.

4. Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für das Unternehmen relevanten Gesetze, Vorschriften und vertragliche Verpflichtungen eingehalten werden.
5. Finanzielle Schäden und ein negatives Image für das Unternehmen müssen verhindert werden.

Verantwortlichkeiten

Die **Geschäftsführung** trägt 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, Eigentümer von Zielobjekten) 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.

5. 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 Informationsverbundes gehörigen Geschäftsprozesse, Anwendungen und Informationen,
2. Netzplanerhebung,
3. Erfassung der IT-Systeme sowie
4. Erfassung der Räume und Gebäude.

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.

5.1. Erfassung der Geschäftsprozesse, Anwendungen und Informationen

Das Organigramm (siehe Abbildung 1) veranschaulicht die organisatorische Gliederung der RECPLAST GmbH.

Jeder Abteilung lassen sich verschiedene Geschäftsprozesse zuordnen, beispielsweise

- Einkauf: Der Prozess Einkauf,
- Informationstechnik: Prozesse wie der Betrieb von Servern und Clients, Benutzer-Service, Verwaltung des Mobile Device Management, oder Netzadministration,
- Marketing & Vertrieb: Pflege der Webseite,
- Personalabteilung: Prozesse wie Einstellung, Entlassung und Gehaltszahlung sowie
- Fertigung der Produktionsabteilung: Die Prozesse zur Umwandlung der Altkunststoffe in wiederverwertbare Regranulate sowie zur Herstellung der neuen Produkte aus diesen 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 Zuordnung der Prozesse zu den Standorten der RECPLAST GmbH erfolgt tabellarisch.

Geschäftsprozess	Standort Bad-Godesberg	Standort Beuel	Standort Vertriebsbüros
GP001 Produktion		X	
GP002 Angebotswesen	X		
GP003 Auftragsabwicklung	X		

Geschäftsprozess	Standort Bad-Godesberg	Standort Beuel	Standort Vertriebsbüros
GP004 Einkauf	X		
GP005 Disposition		X	
GP006 Personalverwaltung	X		
GP006a Gehaltszahlung	X		
GP006b Neueinstellung	X		
GP006c Entlassung Mitarbeiter	X		
GP007 IT-Betrieb	X	X	X
GP007a Betrieb Server	X	X	
GP007b Betrieb Clients	X	X	X
GP007c Betrieb Netze	X	X	
GP007d Betrieb Produktions-IT	X	X	
GP008 Betrieb der Webseite	X		X
GP009 Betrieb des Intranets	X		
GP010 Verwaltung des Mobile Device Managements	X		
GP011 Nutzung einer Cloud-Umgebung	X	X	X

Tabelle 1: Zuordnung Geschäftsprozesse zu den Standorten

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

Kürzel	Name	Beschreibung	Prozess-Art
GP001	Produktion	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.	Kerngeschäft
	Mitarbeiter:	Produktion	

Kürzel	Name	Beschreibung	Prozess-Art
GP002	Angebotswesen	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 oder Mail an den Kunden versendet. Im Angebotswesen werden Kundendaten, Lagerbestände, Anfragen und Angebote bearbeitet.	Unterstützender Prozess
	Mitarbeiter:	Vertrieb	
GP003	Auftragsabwicklung	Kunden schicken die Bestellungen im Regelfall per Fax oder E-Mail. Zusätzlich bietet die Webseite der RECPLAST einen Webshop an, über den Bestellungen aufgegeben werden können. Bestellungen erzeugen eine automatisch generierte 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.	Kerngeschäft
	Mitarbeiter:	Vertrieb	
GP004	Einkauf	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.	Unterstützender Prozess
	Mitarbeiter:	Einkauf	
GP005	Disposition	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.	Kerngeschäft

Kürzel	Name	Beschreibung	Prozess-Art
	Mitarbeiter:	Disposition, Produktion	
GP006	Personalverwaltung	In dieser Abteilung werden alle Aufgaben bearbeitet, die zur administrativen Abwicklung des Personalwesens erforderlich sind. Die dazu genutzten Daten sind personenbezogen.	Unterstützender Prozess
	Mitarbeiter:	Geschäftsführung, Personal	
GP006a	Gehaltszahlung	Teilprozess von GP006. In der Personalabteilung wird insbesondere die monatliche Gehaltszahlung vorbereitet und durchgeführt. Die dazu genutzten Daten sind personenbezogen.	Unterstützender Prozess
	Mitarbeiter:	Personal	
GP006b	Neueinstellung	Teilprozess von GP006. Die Abteilung ist auch an der Neueinstellung von Mitarbeitern beteiligt. Es fallen Informationen an, die dem Datenschutz unterliegen.	Unterstützender Prozess
	Mitarbeiter:	Geschäftsführung, Personal	
GP007	IT-Betrieb	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.	Unterstützender Prozess
	Mitarbeiter:	Informationstechnik	
GP007a	Betrieb Server	Teilprozess von GP007. Dieser Prozess umfasst Beschaffung, Installation, Konfiguration und Pflege der erforderlichen Hard- und Software. Dazu wird mit Konfigurationsdaten der Systeme gearbeitet.	Unterstützender Prozess
	Mitarbeiter:	Informationstechnik	
GP007b	Betrieb Clients	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.	Unterstützender Prozess
	Mitarbeiter:	IT-Betrieb	

Kürzel	Name	Beschreibung	Prozess-Art
GP007c	Betrieb Netze	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.	Unterstützender Prozess
	Mitarbeiter:	IT-Betrieb	
GP007d	Betrieb Produktions-IT	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.	Unterstützender Prozess
	Mitarbeiter:	IT-Betrieb	
GP008	Betrieb der Webseite	Die Webseite wird durch einen externen Dienstleister gehostet. Die Webseite enthält Neuigkeiten, Ansprechpartner, Kontaktformular und einen Shop.	Unterstützender Prozess
	Mitarbeiter:	Vertrieb	
GP009	Betrieb des Intranets	Das Intranet ist eine Wiki-Web-Anwendung. Hierüber werden Dokumente und neue interne Informationen verteilt.	Unterstützender Prozess
	Mitarbeiter:	Alle Mitarbeiter	
GP010	Verwaltung des Mobile Device Managements	Die RECPLAST GmbH nutzt zur Verwaltung der Smartphones und Tablets ein Mobile Device Management.	Unterstützender Prozess
	Mitarbeiter:	Informationstechnik	
GP011	Nutzung einer Cloud-Umgebung	Die Cloud dient zum Datenaustausch zwischen mobilem Endgerät und den Clients bzw. Notebooks.	Unterstützender Prozess
	Mitarbeiter:	Alle Mitarbeiter	

Tabelle 2: Ausschnitt mit den wichtigsten Geschäftsprozessen

Bei der Erhebung der Anwendungen werden die wichtigsten Anwendungen einer Institution erfasst, die zur Erfüllung der Geschäftsprozesse notwendig sind, also diejenigen,

- deren Daten, Informationen und Programme den höchsten Bedarf an den Schutz der 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.

Die nachfolgende Tabelle enthält die erhobenen Anwendungen der RECPLAST GmbH:

Kürzel	Name	Beschreibung	Plattform/Baustein	Anzahl	Status
A001	Textverarbeitung, Präsentation, Tabellenkalkulation	Alle geschäftlichen Informationen werden in einem Office-Produkt verarbeitet, Geschäftsbriefe, Analysen oder Präsentationen.	Office-Produkt	279	Betrieb
	Benutzer:	Alle Mitarbeiter			
A002	E-Mail-Client	Diese Anwendung wird von allen Mitarbeitern für die Bearbeitung von Mailnachrichten, Terminen und Kontakten genutzt.	Allgemeine Groupware	279	Betrieb
	Benutzer:	Alle Mitarbeiter			
A003	Web-Browser	Auf jedem Client ist ein Web-Browser für die Intranetnutzung und eine Linkweiche (als Teil des ReCoBS-Clients) zum Aufruf externer Inhalte über das Remote-Controlled-Browser-System (ReCoBS) installiert.	Web-Browser	279	Betrieb
	Benutzer:	Alle Mitarbeiter			
A004	Prozessleitsystem	Die Anwendung dient der Steuerung der SPS-Systeme	ICS-System	1	Betrieb
	Benutzer:	Produktion			
A005	Entwicklungssystem	Zur Entwicklung von SPS-Programmierungen	Standardsoftware	75	Betrieb
	Benutzer:	Entwicklung			
A006	Personaldatenverarbeitung	Über die Anwendung steuert die Personalverwaltung alle Prozesse bezüglich der Mitarbeiter. Es werden Checklisten für Ein- und Austritt von Mitarbeitern, Informationen über Lohn usw. gepflegt.	Datenbank-anwendung	21	Betrieb
	Benutzer:	Personal, Geschäftsführung			
A007	Reisekostenabrechnung	Über die Anwendung werden die Reisekostenabrechnungen der Mitarbeiter dokumentiert und verrechnet.	Programmierte Excel-Anwendung	42	Betrieb
	Benutzer:	Personal, Buchhaltung			

Kürzel	Name	Beschreibung	Plattform/Baustein	Anzahl	Status
A008	Finanzbuchhaltung	Über diese Anwendung werden von der Finanzbuchhaltungen Lastschriften eingezogen, Rechnungen verwaltet und Überweisungen getätigt.	Datenbank-anwendung	53	Betrieb
	Benutzer:	Buchhaltung, Personal, Geschäftsführung			
A009	Auftrags- und Kundenverwaltung	Die Anwendung wird genutzt, um die Kontaktdaten und Auftragsdaten der entsprechenden Kunden zentral zu verwalten.	Datenbank-anwendung	135	Betrieb
	Benutzer:	Vertrieb, Geschäftsführung, Einkauf, Buchhaltung			
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.	Active Directory	2	Betrieb
	Benutzer:	Alle Mitarbeiter			
A011	Systemmanagement	Die Anwendung dient der Inventarisierung der Hardware sowie dem Fernzugriff auf die Clientsysteme.	Datenbank-anwendung	35	Betrieb
	Benutzer:	IT-Betrieb			
A012	Zentrale Dokumentenverwaltung	Die zentrale Dokumentenverwaltung dient zur Ablage, Versionierung etc. von Dokumenten.	Fileserver	2	Betrieb
	Benutzer:	Alle Mitarbeiter			
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.	Druckservice	1	Betrieb
	Benutzer:	IT-Betrieb, Geschäftsführung, Einkauf, Personal, Buchhaltung, Haustechnik, Vertrieb			

Kürzel	Name	Beschreibung	Plattform/Baustein	Anzahl	Status
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.	Druckservice	1	Betrieb
	Benutzer:	IT-Betrieb, Produktion, Disposition, Entwicklung			
A015	Firewall	Die Anwendung steuert die Kommunikation zwischen dem Firmennetz und dem Internet und ermöglicht die verschlüsselte Kommunikation der Vertriebsbüros über VPN-Tunnel.	Firewall	1	Betrieb
	Benutzer:	Alle Mitarbeiter			
A016	Steuerung der Produktionsanlagen	Die Anwendung dient zur Steuerung der Produktionsanlagen.	ICS-System	1	Betrieb
	Benutzer:	Produktion			
A017	Content Management System	Software zur Gestaltung und Pflege der Webseite.	Webanwendung	1	Betrieb
	Benutzer:	Vertrieb			
A018	Backupsoftware	Software, welche ein regelmäßiges Backup durchführt.	Backupsoftware	1	Betrieb
	Benutzer:	IT-Betrieb			
A019	Webserver	Webserver für jeweils Intranet und Webseite	Webserver	2	Betrieb
	Benutzer:	Alle Mitarbeiter			
A020	Datenbanksystem	Datenbanksystem für die entsprechenden Anwendungen. Da die Datenbanken auf jeweils eigenen Servern liegen, ist die Anwendung mehrfach vorhanden.	Datenbank-anwendung	3	Betrieb
	Benutzer:	IT-Betrieb			
A021	Internes Ticketsystem	Ticketsystem zur Verwaltung und Management der Geschäftsprozesse	Webanwendung	1	Betrieb
	Benutzer:	Alle Mitarbeiter			

Kürzel	Name	Beschreibung	Plattform/Baustein	Anzahl	Status
A022	Internes Wiki	Das interne Wiki dient zum Informationsaustausch innerhalb der RECPLAST GmbH. Das interne Wiki ist gleichzeitigt das Intranet.	Webanwendung	1	Betrieb
	Benutzer:	Alle Mitarbeiter			
A023	Virtualisierungs-software	Software, um die virtuellen Systeme bereitzustellen.	Virtualisierung	2	Betrieb
	Benutzer:	IT-Betrieb			
A024	Voice over IP	Die Anwendung steuert die Telekommunikation über die beiden TK-Anlagen.	VoIP	2	Betrieb
	Benutzer:	Alle Mitarbeiter			
A025	Chat-Anwendung	Die Chat-Anwendung soll den Kontakt zwischen den Mitarbeitern vereinfachen. Die Anwendung ist ein im Mail-Client integriertes Modul.	Chat	290	Betrieb
	Benutzer:	Alle Mitarbeiter			
A026	Mobile Device Management	Anwendung zur Verwaltung der Smartphones. Die Anwendung wird über die Fa. GetMobileDevice GmbH über eine Cloud bereitgestellt.	Webanwendung	1	Betrieb
	Benutzer:	IT-Betrieb			
A027	ReCoBS	Auf jedem Client ist ein Remote-Controlled-Browser-Client (ReCoBS-Client/Viewer) für die freie Internetrecherche und den Aufruf externer Inhalte über das ReCoBS (sowie eine Linkweiche für die Intranetnutzung über den internen Browser) installiert.	ReCoBS	1	Betrieb
	Benutzer:	Alle Mitarbeiter			
A028	Updateverwaltung Windows	Die Anwendung dient zur Updateverteilung an Windows-Clients.	Integriertes Windows-Tool	1	Betrieb
	Benutzer:	IT-Betrieb			
A029	Updateverwaltung Linux	Die Anwendung dient zur Bereitstellung der Updates für Linux-Geräte.	Integriertes Linux-Tool	1	Betrieb
	Benutzer:	IT-Betrieb			
A030	Cloud-APP	Über die APP ist der Zugriff auf die Austausch Cloud der RECPLAST GmbH möglich.	Mobile Anwendung	70	Betrieb

Kürzel	Name	Beschreibung	Plattform/Baustein	Anzahl	Status
	Benutzer:	Alle Mitarbeiter			
A031	Cloud-Umgebung	Die Cloud-Umgebung dient zum Austausch der Daten zwischen Mobile Devices und den Arbeitsplatzrechnern, sowie zum Zugriff auf Daten mittels eines Mobile Devices.	Webanwendung	1	Betrieb
	Benutzer:	Alle Mitarbeiter			
A032	CAD/CAM	Die Anwendung dient der Simulation und Erstellung von Konstruktionsmodellen für die CNC-Bearbeitung.	CAD/CAM	24	Betrieb
	Benutzer:	Produktion			

Tabelle 3: Anwendungen der RECPLAST GmbH

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

Exemplarisch werden fünf Prozesse in der Tabelle dargestellt.

Kürzel	Name		
GP001	Produktion		
	Zuordnung	Kürzel	Name
	benötigt	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	benötigt	A004	Prozessleitsystem
	benötigt	A005	Entwicklungssystem
	benötigt	A009	Auftrags- und Kundenverwaltung
	benötigt	A010	Active Directory
	benötigt	A012	Zentrale Dokumentenverwaltung
	benötigt	A014	Druckservice Beuel
	benötigt	A016	Steuerung der Produktionsanlagen
	Benötigt	A027	ReCoBS-Client/Viewer
	benötigt	A032	CAD/CAM
GP002	Angebotswesen		
	Zuordnung	Kürzel	Name
	benötigt	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	benötigt	A002	E-Mail-Client
	benötigt	A003	Web-Browser
	benötigt	A009	Auftrags- und Kundenverwaltung
	benötigt	A010	Active Directory
	benötigt	A012	Zentrale Dokumentenverwaltung
	benötigt	A013	Druckservice Bad Godesberg
	benötigt	A020	Datenbanksystem

Kürzel	Name		
	benötigt	A027	ReCoBS-Client/Viewer
	benötigt	A024	Voice over IP
GP003	Auftragsabwicklung		
	Zuordnung	Kürzel	Name
	benötigt	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	benötigt	A002	E-Mail-Client
	benötigt	A008	Finanzbuchhaltung
	benötigt	A009	Auftrags- und Kundenverwaltung
	benötigt	A010	Active Directory
	benötigt	A012	Zentrale Dokumentenverwaltung
	benötigt	A013	Druckservice Bad Godesberg
	benötigt	A020	Datenbanksystem
	benötigt	A024	Voice over IP
GP004	Einkauf		
	Zuordnung	Kürzel	Name
	benötigt	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	benötigt	A002	E-Mail-Client
	benötigt	A003	Web-Browser
	benötigt	A008	Finanzbuchhaltung
	benötigt	A010	Active Directory
	benötigt	A012	Zentrale Dokumentenverwaltung
	benötigt	A013	Druckservice Bad Godesberg
	benötigt	A024	Voice over IP
	benötigt	A027	ReCoBS-Client/Viewer
GP005	Disposition		
	Zuordnung	Kürzel	Name
	benötigt	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	benötigt	A002	E-Mail-Client
	benötigt	A003	Web-Browser
	benötigt	A008	Finanzbuchhaltung
	benötigt	A009	Auftrags- und Kundenverwaltung
	benötigt	A010	Active Directory
	benötigt	A012	Zentrale Dokumentenverwaltung
	benötigt	A013	Druckservice Bad Godesberg
	benötigt	A014	Druckservice Beuel
	benötigt	A020	Datenbanksystem
	benötigt	A024	Voice over IP

Kürzel	Name		
	benötigt	A027	ReCoBS-Client/Viewer

Tabelle 4: Beispiel für die Zuordnung von Geschäftsprozessen zu Anwendungen

5.2. Erhebung des Netzplans

Bei der RECPLAST GmbH dient ein Netzplan als Ausgangspunkt für die Erhebung der technischen Systeme im Rahmen der Strukturanalyse. Die Abbildung 3 zeigt eine, detaillierte Darstellung dieses Netzplans.

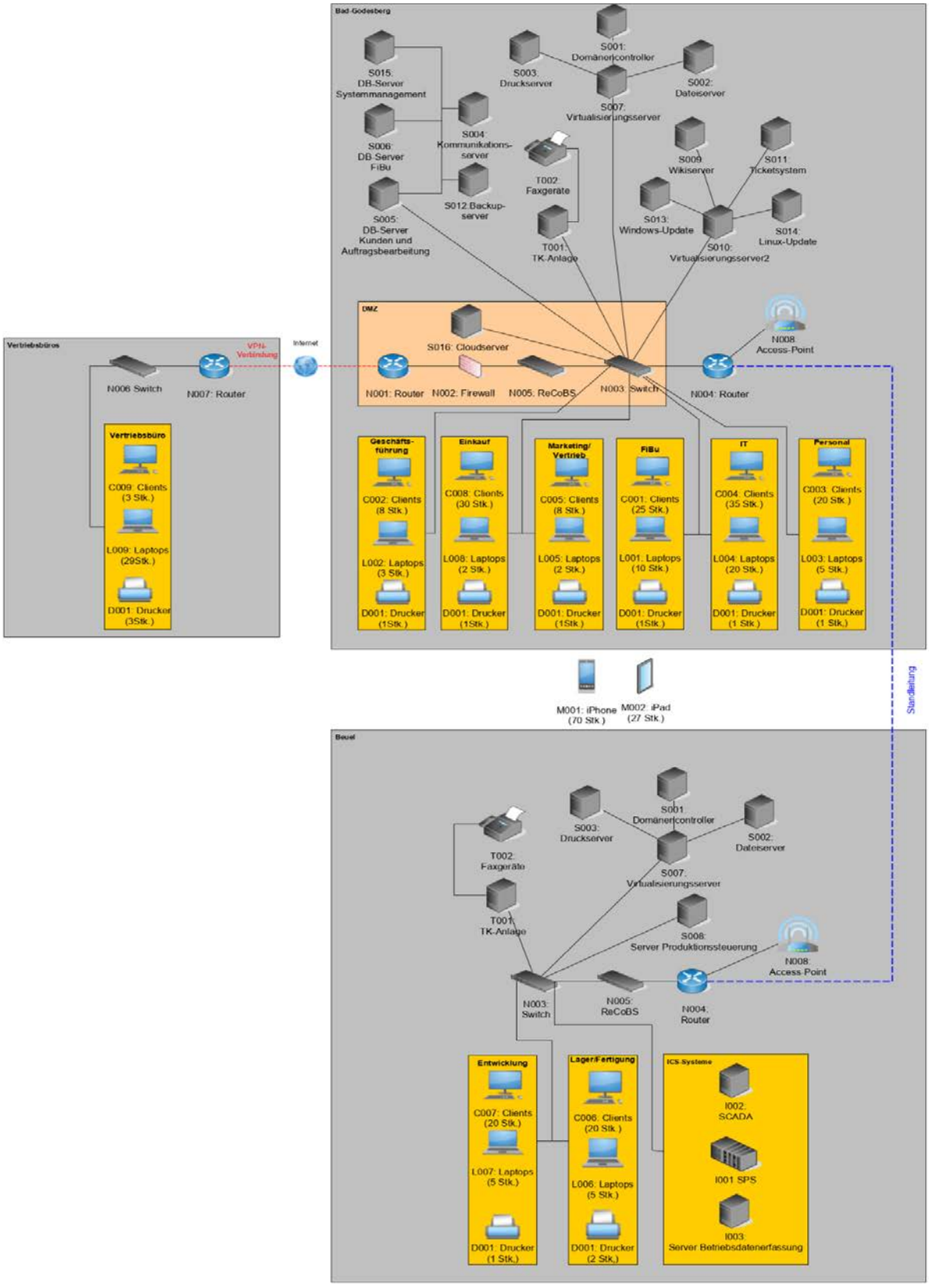

Abbildung 4: Detaillierter Netzplan der RECPLAST GmbH

In beiden Netzplänen sind die IT-Komponenten, soweit dies sinnvoll ist, zu Gruppen zusammengefasst. 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 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 Clients 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 Clients 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 Clients der IT-Administratoren laufen Anwendungen, die für die Verwaltung des Netzes erforderlich sind. Von daher verlangen auch diese Clients eine besondere Aufmerksamkeit und werden nicht mit anderen zusammengefasst.

5.3. Erhebung der IT-Systeme

Bei der Erhebung der IT-Systeme geht es darum, die vorhandenen und geplanten IT-Systeme und die jeweiligen Informationen zusammenzustellen. Dazu zählen:

- alle im Netz vorhandenen IT-Systemen (Clients und Server), Gruppen von IT-Systemen und aktiven Netzkomponenten, Netzdrucker, aber auch
- Telekommunikationskomponenten (wie TK-Anlagen, Faxgeräte und Mobiltelefone) und
- IoT-Geräte wie zum Beispiel ein Sprachassistent.

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

Erläuterung zur Lesart der Tabellen: 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.

IT-Systeme

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
C001	Clients der Finanzbuchhaltung	Bei den Clients handelt es sich um handelsübliche Clients.	30	Betrieb	Windows 10
	Benutzer:	Buchhaltung			
C002	Clients der Geschäftsführung	Bei den Clients handelt es sich um handelsübliche Clients.	8	Betrieb	Windows 10
	Benutzer:	Geschäftsführung			
C003	Clients der Personalabteilung	Bei den Clients handelt es sich um handelsübliche Clients.	8	Betrieb	Windows 10
	Benutzer:	Personal			
C004	Clients der Informationstechnik	Bei den Clients handelt es sich um handelsübliche Clients.	25	Betrieb	Windows 10
	Benutzer:	IT-Betrieb			
C005	Clients des Marketings & Vertrieb	Bei den Clients handelt es sich um handelsübliche Clients.	35	Betrieb	Windows 10
	Benutzer:	Vertrieb			
C006	Clients der Fertigung und Lager	Bei den Clients handelt es sich um handelsübliche Clients.	20	Betrieb	Windows 10
	Benutzer:	Disposition, Produktion			
C007	Clients der Entwicklungsabteilung	Bei den Clients handelt es sich um handelsübliche Clients.	60	Betrieb	Windows 10
	Benutzer:	Entwicklung			
C008	Clients der Einkaufsabteilung	Bei den Clients handelt es sich um handelsübliche Clients.	20	Betrieb	Windows 10
	Benutzer:	Einkauf			
C009	Clients in den Vertriebsbüros	Bei den Clients handelt es sich um handelsübliche Clients.	3	Betrieb	Windows 10
	Benutzer:	Vertrieb			
L001	Laptops der Finanzbuchhaltung	Bei den Laptops handelt es sich um handelsübliche Laptops.	2	Betrieb	Windows 10
	Benutzer:	Buchhaltung			
L002	Laptops der Geschäftsführung	Bei den Laptops handelt es sich um handelsübliche Laptops.	3	Betrieb	Windows 10
	Benutzer:	Geschäftsführung			

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
L003	Laptops der Personalabteilung	Bei den Laptops handelt es sich um handelsübliche Laptops.	2	Betrieb	Windows 10
	Benutzer:	Personal			
L004	Laptops der Informationstechnik	Bei den Laptops handelt es sich um handelsübliche Laptops.	10	Betrieb	Windows 10
	Benutzer:	IT-Betrieb			
L005	Laptops Marketing & Vertrieb	Bei den Laptops handelt es sich um handelsübliche Laptops.	20	Betrieb	Windows 10
	Benutzer:	Vertrieb			
L006	Laptops von Fertigung und Lager	Bei den Laptops handelt es sich um handelsübliche Laptops.	4	Betrieb	Windows 10
	Benutzer:	Disposition, Produktion			
L007	Laptops der Entwicklungsabteilung	Bei den Laptops handelt es sich um handelsübliche Laptops.	15	Betrieb	Windows 10
	Benutzer:	Entwicklung			
L008	Laptops der Einkaufsabteilung	Bei den Laptops handelt es sich um handelsübliche Laptops.	5	Betrieb	Windows 10
	Benutzer:	Einkauf			
L009	Laptops in den Vertriebsbüros	Bei den Laptops handelt es sich um handelsübliche Laptops.	9	Betrieb	Windows 10
	Benutzer:	Vertrieb			
S001	Domänen-Controller	Der Domänen-Controller regelt die Authentifizierung von Computern und Benutzern	2	Betrieb	Windows Server 2012
	Benutzer:	Alle Mitarbeiter			
S002	Dateiserver	Der Dateiserver dient zur Dokumentenablage	2	Betrieb	Windows Server 2012
	Benutzer:	Alle Mitarbeiter			
S003	Druckserver	Der Druckserver stellt die Prozesse und Ressourcen für die Druckservices zur Verfügung.	2	Betrieb	Windows Server 2012
	Benutzer:	Alle Mitarbeiter			

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
S004	Kommunikationsserver	Server für die interne und externe Mail-Kommunikation	2	Betrieb	Windows Server 2012
	Benutzer:	Alle Mitarbeiter			
S005	DB-Server der Kunden- und Auftragsbearbeitung	Der Datenbankserver enthält die Datenbank mit den Informationen zu den Kunden sowie Aufträgen	1	Betrieb	Windows Server 2012
	Benutzer:	Vertrieb, Geschäftsführung, Einkauf, Buchhaltung			
S006	DB-Server der Finanzbuchhaltung	Der Datenbankserver enthält die Datenbank mit den Informationen der Finanzbuchhaltung.	1	Betrieb	Windows Server 2012
	Benutzer:	Geschäftsführung, Buchhaltung			
S007	Virtualisierungsserver	Bei dem Server handelt es sich um einen Virtualisierungshost.	2	Betrieb	Linux
	Benutzer:	IT-Betrieb			
S008	Server für Produktionssteuerung	Der Server dient zur Steuerung der Produktionsmaschinen	1	Betrieb	Linux
	Benutzer:	Produktion			
S009	Wiki-Server	Der Server für den Betrieb des Intranets/Wiki	1	Betrieb	Linux
	Benutzer:	Alle Mitarbeiter			
S010	Virtualisierungsserver2	Virtualisierungshost	1	Betrieb	Linux
	Benutzer:	IT-Betrieb			
S011	Ticketsystem	Server, welcher das interne Ticketsystem betreibt	1	Betrieb	Linux
	Benutzer:	Alle Mitarbeiter			
S012	Backupserver	Der Backupserver führt die Prozesse für das regelmäßige Backup aus.	1	Betrieb	Windows Server 2012
	Benutzer:	IT-Betrieb			
S013	Windows-Update-Server	Der Windows-Update-Server wird für das Einspielen von Updates auf die Windows Clients und Server benötigt.	1	Betrieb	Windows Server 2012
	Benutzer:	IT-Betrieb			
S014	Linux-Update-Server	Updateserver für die Linux-Betriebssysteme	1	Betrieb	Windows Server 2012

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
	Benutzer:	IT-Betrieb			
S015	DB-Server fürs Systemmanagement	Der Datenbankserver enthält die Datenbank mit den Informationen IT-Systeme	1	Betrieb	Windows Server 2012
	Benutzer:	IT-Betrieb			

Tabelle 5: Übersicht über die IT-Systeme

ICS-Systeme

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
I001	Speicherprogrammierbare Produktionsmaschinen	Die speicherprogrammierbaren Produktionsmaschinen dienen zur Erstellung der Produkte	2	Betrieb	SPS
	Benutzer:	Produktion			
I002	SCADA	Das SCADA dient zur Überwachung und Steuerung technischer Prozesse	1	Betrieb	SCADA
	Benutzer:	Produktion			
I003	Server für die Betriebsdatenerfassung	Der Server erfasst die Betriebsdaten der Produktion.	1	Betrieb	Linux
	Benutzer:	Produktion			

Tabelle 6: Übersicht über die Industrial Control System (ICS)

IoT-Systeme

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
O001	Video-Überwachung	Die Videoüberwachung dient zur Überwachung der Eingänge, sowie kritischer Bereiche in den Gebäuden	1	Betrieb	Video-Überwachung
	Benutzer:	IT-Betrieb, Geschäftsführung			
O002	Kühlschrank	In der IT-Abteilung ist ein Kühlschrank, der mittels einer internen Kamera und einer App eine Inventarliste führt.	1	Betrieb	IoT-System
	Benutzer:	IT-Betrieb			
O003	Alarmanlage	Alarmanlagen für Gebäude in Bad Godesberg und Beuel	2	Betrieb	Alarmanlage
	Benutzer:	Alle Mitarbeiter			
O004	Kaffeevollautomat	Der Kaffeevollautomat ist über eine Weboberfläche konfigurierbar.	1	Betrieb	IoT-System
	Benutzer:	Alle Mitarbeiter			
O005	Sprachassistent	Der Sprachassistent wird in Bad-Godesberg für die Lichtsteuerung in den Besprechungsräumen genutzt.	3	Betrieb	IoT-System

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
	Benutzer:	Alle Mitarbeiter			

Tabelle 7: Übersicht über die Internet of Things-Systeme (IoT)

Zur Erhebung gehört auch eine Zuordnung von Anwendungen auf IT-Systeme. Der untenstehende Tabellenausschnitt zeigt die Zuordnung von Anwendungen zu Servern.

Kürzel	Name		
S001	Domänen-Controller		
	Zuordnung	Kürzel	Name
	nötig für	A002	E-Mail-Client
	nötig für	A009	Auftrags- und Kundenverwaltung
	nötig für	A010	Active Directory
	nötig für	A012	Zentrale Dokumentenverwaltung
	nötig für	A021	Internes Ticketsystem
	nötig für	A022	Internes Wiki

Tabelle 8: Beispiel für die Zuordnung von Anwendungen zu Servern

Die nachstehende Tabelle zeigt beispielhaft die Zuordnung von Clients und Laptops auf Anwendungen.

Kürzel	Name		
C001	Clients der Finanzbuchhaltung		
	Zuordnung	Kürzel	Name
	nötig für	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	nötig für	A002	E-Mail-Client
	nötig für	A003	Web-Browser
	nötig für	A007	Reisekostenabrechnung
	nötig für	A008	Finanzbuchhaltung
	nötig für	A009	Auftrags- und Kundenverwaltung
	nötig für	A027	ReCoBS-Client/Viewer
C002	Clients der Geschäftsführung		
	Zuordnung	Kürzel	Name
	nötig für	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	nötig für	A002	E-Mail-Client
	nötig für	A003	Web-Browser
	nötig für	A006	Personaldatenverarbeitung
	nötig für	A008	Finanzbuchhaltung

Kürzel	Name		
	nötig für	A009	Auftrags- und Kundenverwaltung
	nötig für	A027	ReCoBS-Client/Viewer
C004	Clients der Informationstechnik		
	Zuordnung	Kürzel	Name
	nötig für	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	nötig für	A002	E-Mail-Client
	nötig für	A003	Web-Browser
	nötig für	A011	Systemmanagement
	nötig für	A027	ReCoBS-Client/Viewer
C006	Clients der Fertigung und Lager		
	Zuordnung	Kürzel	Name
	nötig für	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	nötig für	A002	E-Mail-Client
	nötig für	A003	Web-Browser
	nötig für	A032	CAD/CAM
	nötig für	A027	ReCoBS-Client/Viewer
L001	Laptops der Finanzbuchhaltung		
	Zuordnung	Kürzel	Name
	nötig für	A001	Textverarbeitung, Präsentation, Tabellenkalkulation
	nötig für	A002	E-Mail-Client
	nötig für	A003	Web-Browser
	nötig für	A006	Personaldatenverarbeitung
	nötig für	A007	Reisekostenabrechnung
	nötig für	A008	Finanzbuchhaltung
	nötig für	A009	Auftrags- und Kundenverwaltung
	nötig für	A027	ReCoBS-Client/Viewer
L002	Laptops der Geschäftsführung		
	Zuordnung	Kürzel	Name
	nötig für	A001	Textverarbeitung, Präsentation, Tabellenkalkulation

Kürzel	Name		
	nötig für	A002	E-Mail-Client
	nötig für	A003	Web-Browser
	nötig für	A006	Personaldatenverarbeitung
	nötig für	A008	Finanzbuchhaltung
	nötig für	A009	Auftrags- und Kundenverwaltung
	nötig für	A027	ReCoBS-Client/Viewer

Tabelle 9: Beispiel für die Zuordnung Clients zu Anwendungen

Neben Server und Clients werden auch die Netz- und Telekommunikationskomponenten erfasst und die verschiedenen Kommunikationsverbunden aufgeführt:

Netz- und Telekommunikationskomponenten

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
N001	Router zum Internet	Der Router ist der Knotenpunkt zum Internet.	1	Betrieb	DSL-Router
	Benutzer:	Alle Mitarbeiter			
N002	Firewall	Die Firewall dient zum Schutz zwischen dem Internet und dem internen Netz der RECPLAST GmbH sowie zur Verbindung von außerhalb mittels VPN. Die Firewall bildet eine DMZ.	1	Betrieb	Firewall
	Benutzer:	Alle Mitarbeiter			
N003	Zentrale Switche in Bad Godesberg und Beuel	Die Switche dienen zur Paketverteilung im internen Netzwerk.	2	Betrieb	Switch
	Benutzer:	Alle Mitarbeiter			
N004	Router zur Verbindung der Standorte BG und BE	Der Router verbindet die beiden Standorte über eine Standleitung	2	Betrieb	Router
	Benutzer:	Alle Mitarbeiter			
N005	ReCoBS	Die ReCoBS-Netzkomponente dient zum Bereitstellen des Web-Browsers für die freie Internetrecherche.	2	Betrieb	ReCoBS
	Benutzer:	Alle Mitarbeiter			
N006	Switche in den Vertriebs-büros	Die gemanagten Switche dienen zur Paketverteilung und als Layer-3-Switch auch als Paketfilter-Firewall im internen Netzwerk.	3	Betrieb	Switch
	Benutzer:	Vertrieb			
N007	Router zum Internet der Vertriebsbüros	Der Router ist der Knotenpunkt zum Internet in den Vertriebsbüros	3	Betrieb	Router
	Benutzer:	Vertrieb			

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
N008	WLAN-Access-Points	Die Access-Points dienen zum Verteilen des WLAN's	4	Betrieb	
	Benutzer:	Alle Mitarbeiter			
T001	Telefonanlagen Bad Godesberg und Beuel	Die Telefonanlagen sind miteinander gekoppelt und verteilen die Gespräche über das VoIP-Protokoll.	2	Betrieb	TK-Anlagen
	Benutzer:	Alle Mitarbeiter			
T002	Faxgeräte	4 in Bad Godesberg, jeweils 1 in Beuel und den Vertriebsbüros	8	Betrieb	Fax-Geräte
	Benutzer:	Einkauf, Vertrieb, Produktion			

Tabelle 10: exemplarische Übersicht über die Netz- und Telekommunikationskomponenten

Kommunikationsverbindungen

Kürzel	Name	Erläuterung	Status
K001	Internetanschluss BG	Außenanschluss der RECPLAST GmbH an das Internet. Gleichzeitig Teil der Verbindung zu den Vertriebsbüros und den mobilen Clients.	Betrieb
	Benutzer:	Alle Mitarbeiter	
K002	Standleitung Bad Godesberg – Beuel	Standleitung für die Verbindung der beiden Bonner Standorte. Sie führt über öffentliches Gelände.	Betrieb
	Benutzer:	Alle Mitarbeiter	
K003	Verbindungen zwischen Netzkomponenten innerhalb der RECPLAST GmbH	Die Netzkomponenten werden untereinander mittels Glasfaser oder Kupferkabel verbunden.	Betrieb
	Benutzer:	Alle Mitarbeiter	
K004	Verbindungen zwischen Switches und Servern	Die Switche und Server werden mittels Kupferkabel verbunden.	Betrieb
	Benutzer:	Alle Mitarbeiter	
K005	Verbindungen zwischen Switches und Clients	Die Clients und Switche werden über Kupferkabel verbunden.	Betrieb
	Benutzer:	Alle Mitarbeiter	
K006	Verbindungen zwischen Switches und Produktionsmaschinen	Die Produktionsmaschinen werden mittels Kupferkabel verbunden.	Betrieb
	Benutzer:	IT-Betrieb, Produktion	
K007	Internetanschlüsse der Vertriebsbüros	Die Vertriebsbüros werden über einen Router an das Internet angebunden.	Betrieb
	Benutzer:	Vertrieb	
K008	Mobile Internetanschlüsse der Laptops	Die Laptops können sich per WLAN in das Netzwerk einwählen.	Betrieb
	Benutzer:	Alle Mitarbeiter	

Tabelle 11: Übersicht über Kommunikationsverbindungen

5.4. Erhebung der räumlichen Gegebenheiten

Bei der Strukturanalyse wurden unter anderem die in der folgenden Tabelle aufgeführten Gebäude und Räume erfasst.

Kürzel	Name	Erläuterung	Anzahl	Plattform
GB001	Verwaltungsgebäude Bad Godesberg	Das Hauptgebäude der RECPLAST GmbH.	1	Allgemeines Gebäude
	Benutzer:	IT-Betrieb, Geschäftsführung, Einkauf, Personal, Buchhaltung, Vertrieb		
GB002	Produktionsgebäude Beuel	Das neue Gebäude der RECPLAST GmbH, an dem alle Produktionsrelevanten Tätigkeiten durchgeführt werden. Zusätzlich befindet sich hier die Produktion.	1	Allgemeines Gebäude
	Benutzer:	Entwicklung, Produktion, Disposition		
R001	Technikraum	BG, R. 1.01	1	Technikraum
	Benutzer:	IT-Betrieb		
R002	Serverraum	BG, R. 1.02	1	Serverraum
	Benutzer:	IT-Betrieb		
R003	Büros IT-Abteilung	BG, R. 1.03 - 1.06	4	Büroraum
	Benutzer:	IT-Betrieb		
R009	Serverraum	Beuel R. 2.01	1	Serverraum
	Benutzer:	IT-Betrieb		
R010	Technikraum	Beuel, R. 2.02	1	Technikraum
	Benutzer:	IT-Betrieb		
R011	Büros Fertigung/Lager	Beuel, R. 2.10 - 2.13	4	Büroraum
	Benutzer:	Disposition, Produktion		
R012	Büros Entwicklungsabteilung	Beuel, R. 2.14 - 2.20	7	Büroraum
	Benutzer:	Entwicklung		
R013	Produktionshalle	Die Halle mit der für die Produktion relevanten Technik.	1	Werkhalle
	Benutzer:	Produktion		
R014	Vertriebsbüros	Vertriebsbüros in Berlin, Paderborn und München	3	Häuslicher Arbeitsplatz
	Benutzer:	Vertrieb		
R018	Technikraum Vertriebsbüros	Der Technikraum enthält die relevante Technik für die Vertriebsbüros.	1	Technikraum
	Benutzer:	IT-Betrieb		

Kürzel	Name	Erläuterung	Anzahl	Plattform
R019	Datenträgerarchiv	In dem Raum befindet sich ein feuerfester Safe, der die Backups enthält.	1	Datenträgerarchiv
	Benutzer:	IT-Betrieb, Geschäftsführung		

Tabelle 12: Beispiel für Gebäude und Räume

Die nachstehende Tabelle zeigt beispielhaft die Zuordnung von Räumen und IT-Systemen bzw. IT-Komponenten.

R002	Serverraum Bad Godesberg		
	Zuordnung	Kürzel	Name
	beinhaltet	N001	Router zum Internet
	beinhaltet	N002	Firewall
	beinhaltet	N003	Zentrale Switche in Bad Godesberg und Beuel
	beinhaltet	N004	Router zur Verbindung der Standorte BG und BE
	beinhaltet	N005	ReCoBS zur freien Internetrecherche
	beinhaltet	S001	Domänen-Controller
	beinhaltet	S002	Dateiserver
	beinhaltet	S003	Druckserver
	beinhaltet	S004	Kommunikationsserver
	beinhaltet	S005	DB-Server der Kunden- und Auftragsbearbeitung
	beinhaltet	S006	DB-Server der Finanzbuchhaltung

Tabelle 13: Zuordnung Räume zu IT-Systemen

5.5. Liste der Dienstleister

Für die Zuordnung zu den Dienstleistern gilt folgende Definition: Dienstleister haben Zutritt, Zugang oder Zugriff zu Zielobjekten.

Es werden die folgenden Dienstleister eingesetzt:

Firma	Anschrift	Branche	Beschreibung	Ansprech-partner
Die Putzfee AG	Hinter der Pforte 7, 50674 Köln	Gebäude-reinigung	Reinigung der Gebäude	Herr B. Schmidt
GetMobileDevice GmbH	Über der Kante 12, 53225 Bonn	IT-Branche	Mobile Device Management	Frau E. Ellermann
Hosting Website GmbH&Co.KG	Stefans Straße 107, 75181 Pforzheim	IT-Branche	Hosting der Webseite	Frau C. Meier

Firma	Anschrift	Branche	Beschreibung	Ansprech-partner
Telfcom	Musterstraße 1, 12345 Musterstadt	Telekommunikation	Dienstleister für die TK-Anlage	Herr A. Güll
Indust GmbH & Co.KG	Industriestraße 13, 12345 Musterstadt	ICS-Anlagen	Dienstleister für die industriellen Anlagen	Frau A. Fuchs
VPN Ware GmbH	Alte Straße 6, 12345 Musterstadt	IT-Branche	Dienstleister für die Wartung des VPN	Frau K. Lehmann

Tabelle 14: Liste der Dienstleister

6. 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 Schutzmaßnahmen der Standard-Absicherung?

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 Geschäftsprozesse mit Hilfe dieser Kategorien
3. die Ableitung des Schutzbedarfs der in der Strukturanalyse erfassten Anwendungen aus dem Schutzbedarf der Geschäftsprozesse,
4. die Ableitung des Schutzbedarfs der IT-Systeme aus dem Schutzbedarf der Anwendungen,
5. daraus abgeleitet die Feststellung des Schutzbedarfs der Kommunikationsverbindungen und der räumlichen Gegebenheiten sowie
6. die Dokumentation und Auswertung der vorgenommenen Einschätzungen.

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

6.1. Anpassung der Schutzbedarfskategorien

Bei der RECPLAST GmbH wurden die Schutzbedarfskategorien vom einberufenen Sicherheits-management-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 beträchtliche bis existenzbedrohende Auswirkungen auf die RECPLAST GmbH:

- Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen existenzbedrohende juristische Konsequenzen oder Konventionalstrafen.
- 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.

6.2. Schutzbedarfsfeststellung für Geschäftsprozesse

Zunächst ist der Schutzbedarf der bei der Strukturanalyse erfassten Geschäftsprozesse festzustellen. Dies bedeutet, dass für jeden Geschäftsprozess mit Hilfe der zuvor festgelegten Kategorien bestimmt werden muss, wie groß der Bedarf an Vertraulichkeit, Integrität und Verfügbarkeit ist. Die folgende Tabelle zeigt einen Ausschnitt der Ergebnisse dieser Aktivität bei der RECPLAST GmbH.

Geschäftsprozess	**Schutzbedarfsfeststellung**			
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
GP001	Produktion	Vertraulichkeit	Hoch	Durch die Entwicklung von Software, welche für die Produktion benötigt wird, ist die Vertraulichkeit hoch.
		Integrität	Hoch	Gefälschte oder falsche Daten können die Produktion verändern und so zu finanziellen Schäden zwischen 50.000 und 500.000 Euro.
		Verfügbarkeit	Sehr Hoch	Ein Ausfall kann bis zu 2 Stunden akzeptiert werden. Ein Ausfall hätte finanzielle Auswirkungen oberhalb von

Geschäftsprozess	Schutzbedarfsfeststellung			
				500.000 Euro und einen hohen Imageschaden, da Produkte eventuell nicht rechtzeitig hergestellt werden können.
GP002	Angebotswesen	Vertraulichkeit	Hoch	Es werden personenbezogene Daten verarbeitet, die einen besonderen Schutz benötigen.
		Integrität	Hoch	Fehlerhafte Daten werden schnell erkannt und behoben, können jedoch hohe finanzielle Auswirkungen zur Folge haben.
		Verfügbarkeit	Normal	Ein Ausfall von mehr als 24 Stunden kann akzeptiert werden. Die Aufgaben können notfalls auch manuell überbrückt werden.
GP003	Auftragsabwicklung	Vertraulichkeit	Hoch	Es werden personenbezogene Daten verarbeitet. Diese Daten müssen besonders geschützt werden.
		Integrität	Hoch	Fehlerhafte oder manipulierte Daten können zu finanziellen Schäden zwischen 50.000 und 500.000 Euro führen.
		Verfügbarkeit	Hoch	Ein Ausfall kann bis zu 24 Stunden akzeptiert werden, da die Tätigkeiten übergangsweise manuell ausgeführt werden können.
GP004	Einkauf	Vertraulichkeit	Hoch	Es werden Verträge und Projekte verhandelt, die nur den befugten Mitarbeitern und Kunden zugänglich sein sollen.
		Integrität	Normal	Fehlerhafte Daten werden in der Regel schnell erkannt und können leicht behoben werden.
		Verfügbarkeit	Normal	Ein Ausfall kann länger als 24 Stunden akzeptiert werden.
GP005	Disposition	Vertraulichkeit	Normal	Es werden keine vertraulichen Daten verarbeitet.

Geschäftsprozess	Schutzbedarfsfeststellung			
		Integrität	Hoch	Fehlerhafte Daten können zu finanziellen Schäden von 50.000 bis zu 500.000 Euro führen, da die Produktion ohne die richtige Menge an Materialien nicht produzieren kann.
		Verfügbarkeit	Hoch	Ein Ausfall der Disposition kann zum Stillstand der Produktion führen, der einen hohen finanziellen Schaden mit sich bringt.
GP010	Verwaltung des Mobile Device Managements	Vertraulichkeit	Hoch	Es werden personenbezogene Daten sowie vertrauliche Endgerätedaten verarbeitet.
		Integrität	Hoch	Fehlerhafte oder manipulierte Daten bzw. Einstellungen können zu Sicherheitsproblemen führen.
		Verfügbarkeit	Hoch	Beim Verlust eines Gerätes muss das Gerät unverzüglich gesperrt werden, damit keinen firmeninternen Daten an die Öffentlichkeit gelangen. Aus diesem Grund kann ein Ausfall bis zu maximal 24 Stunden akzeptiert werden.

Tabelle 15: Schutzbedarf Geschäftsprozesse

6.3. Schutzbedarfsfeststellung für Anwendungen

Der Schutzbedarf einer Anwendung hängt im Wesentlichen von dem Schutzbedarf der Geschäftsprozesse ab, für deren Erledigung die Anwendung benötigt wird. Dieser Schutzbedarf vererbt sich auf den Schutzbedarf der Anwendungen. Bei der Vererbung lassen sich folgende Fälle unterscheiden:

- In vielen Fällen lässt sich der höchste Schutzbedarf aller Geschäftsprozesse, für den die Anwendungen zur Erledigung relevant sind, übernehmen (Maximumprinzip).
- Der Schutzbedarf der Anwendung kann höher sein als der Schutzbedarf der einzelnen Geschäftsprozesse (Kumulationseffekt). Dies ist beispielsweise der Fall, wenn eine Anwendung für mehrere Geschäftsprozesse mit normalem Schutzbedarf benötigt wird. Der Ausfall eines dieser Geschäftsprozesse könnte von der RECPLAST GmbH toleriert werden. Wenn aber mehrere Geschäftsprozesse gleichzeitig ausfallen würden, dann kann ein hoher Schaden entstehen.
- Der Schutzbedarf einer Anwendung kann niedriger sein als der Schutzbedarf der zugeordneten Geschäftsprozesse, wenn ein Geschäftsprozess mit hohem Schutzbedarf auf mehrere Anwendungen verteilt ist, und die Anwendung nur weniger wichtige Aufgaben erledigt. (Verteilungseffekt). Der Schutzbedarf für die Anwendungen sollte für jeden der drei Grundwerte

(Vertraulichkeit, Integrität und Verfügbarkeit) festgelegt und anschließend (z.B. tabellarisch) dokumentiert werden.

Die folgende Tabelle enthält einen Ausschnitt der Schutzbedarfsfeststellung für die Anwendungen der RECPLAST GmbH.

Anwendung	**Schutzbedarfsfeststellung**			
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
A005	Entwicklungssystem	Vertraulichkeit	Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP001 Produktion
		Integrität	Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP001 Produktion
		Verfügbarkeit	Hoch	Verteilungseffekt: Beim Ausfall des Entwicklungssystems auf einem Client kann auf einem Ersatzclient weitergearbeitet werden.
A010	Active Directory	Vertraulichkeit	Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP001 Produktion
		Integrität	Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP001 Produktion
		Verfügbarkeit	Sehr Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP001 Produktion
A011	Systemmanagement	Vertraulichkeit	Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses

Anwendung	Schutzbedarfsfeststellung			
				GP07d1 Betrieb Produktions-IT
		Integrität	Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP07d1 Betrieb Produktions-IT
		Verfügbarkeit	Sehr Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP07d1 Betrieb Produktions-IT
A027	ReCoBS-Client/Viewer	Vertraulichkeit	Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP001 Produktion
		Integrität	Hoch	Maximumprinzip: Maximumprinzip gemäß des verknüpften Geschäftsprozesses GP001 Produktion
		Verfügbarkeit	Normal	Verteilungseffekt: Bei einem Ausfall kann auf einem Ersatzclient über ReCoBS recherchiert werden.

Tabelle 16: Schutzbedarf Anwendungen

6.4. 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.

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 folgende Tabelle enthält einen Ausschnitt der Schutzbedarfsfeststellung für die Server, Clients, Laptops, Netz- und Telekommunikationskomponenten der RECPLAST GmbH.

IT-System	**Schutzbedarfsfeststellung**			
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
C001	Clients der Finanzbuchhaltung	Vertraulichkeit	Hoch	Maximumprinzip: Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A008 (Finanzbuchhaltung)
		Integrität	Hoch	Maximumprinzip: Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A008 (Finanzbuchhaltung)
		Verfügbarkeit	Normal	Verteilungseffekt: Bei Ausfall eines Clients kann die Aufgabe an einem anderen Client wahrgenommen werden oder kurzfristig ein Laptop zur Verfügung gestellt werden.
L003	Laptops der Personalabteilung	Vertraulichkeit	Hoch	Maximumprinzip: Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A006 (Personaldatenverarbeitung)
		Integrität	Hoch	Maximumprinzip: Maximumprinzip gemäß der verknüpften Anwendungen zum Beispiel A006 (Personaldatenverarbeitung)
		Verfügbarkeit	Normal	Verteilungseffekt: Bei Ausfall eines Laptops kann die Aufgabe an einem anderen Laptop wahrgenommen werden.
N001	Router zum Internet	Vertraulichkeit	Hoch	Maximumprinzip:

IT-System	Schutzbedarfsfeststellung			
				Es werden vertrauliche Daten über den Router übertragen.
		Integrität	Hoch	Maximumprinzip: Fehlerhafte Daten können zu Problemen bei der Übertragung der Daten kommen und zu einem Imageschaden führen.
		Verfügbarkeit	Sehr Hoch	Kumulationseffekt: Der Router zum Internet ist die Hauptanbindung der RECPLAST GmbH an das Internet. Alle Netzwerkabhängigen Geräte sind von dieser Anbindung abhängig. Ein Ausfall von mehr als 2 Stunden ist nicht tolerierbar.
S001	Domänen-Controller	Vertraulichkeit	Hoch	Maximumprinzip: Maximumprinzip gemäß Anwendung A010 (Active Directory).
		Integrität	Hoch	Maximumprinzip: Maximumprinzip gemäß Anwendung A010 (Active Directory)
		Verfügbarkeit	Normal	Verteilungseffekt: 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 von mehr als 24 Stunden ist hinnehmbar (Verteilungseffekt).
T001	Telefonanlagen Bad Godesberg und Beuel	Vertraulichkeit	Hoch	Maximumprinzip: Es werden unter Umständen vertrauliche Daten übermittelt.
		Integrität	Hoch	Maximumprinzip: Gefälschte Daten können zu Informationsabfluss führen bzw. Abhören der Kommunikation.

IT-System	Schutzbedarfsfeststellung			
		Verfügbarkeit	Normal	Verteilungseffekt: Die Kommunikation per Telefon ist noch ein großer Bestandteil der RECPLAST GmbH. Bei Ausfall kann die Kommunikation über die zweite Anlage laufen. Ein Ausfall von mehr als 24 Stunden ist tolerierbar.

Tabelle 17: Schutzbedarf IT-Systeme

6.5. 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 eingesehen und bearbeitet werden. Daher muss verhindert werden, dass diese Daten bei ihrer Übertragung von unbefugten Mitarbeitern eingesehen werden können.

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

Kommunikations-verbindung	Schutzbedarfsfeststellung			
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
K001	Internetanschluss BG	Vertraulichkeit	Sehr Hoch	Maximumprinzip: Es werden vertrauliche Daten übertragen und verarbeitet.
		Integrität	Hoch	Maximumprinzip: Gefälschte Daten können einen Imageschaden zur Folge haben, da der Großteil der Kommunikation über das Internet erfolgt.

Kommunikations-verbindung	Schutzbedarfsfeststellung			
		Verfügbarkeit	Sehr Hoch	Kumulationseffekt: Der Internetanschluss ist die Hauptverbindung der RECPLAST GmbH. Alle Systeme sind von diesem Netzanschluss abhängig., wodurch sich der Schutzbedarf kumuliert. Ein Ausfall kann bis zu 2 Stunden toleriert werden. Dies hat sehr hohe finanzielle Schäden zur Folge.
K002	Standleitung Bad Godesberg – Beuel	Vertraulichkeit	Sehr Hoch	Maximumprinzip: Es werden vertrauliche Firmendaten übertragen.
		Integrität	Hoch	Maximumprinzip: Eine Manipulation der Daten kann zu finanziellen Schäden führen, da eventuell falsche Daten zur Produktion übertragen werden.
		Verfügbarkeit	Sehr Hoch	Maximumprinzip: Die Standleitung verbindet die beiden Standorte der RECPLAST GmbH. Ein Ausfall hätte einen Stillstand der Produktion zur Folge und kann daher maximal 2 Stunden toleriert werden.
K006	Verbindungen zwischen Switches und Produktionsmaschinen	Vertraulichkeit	Hoch	Maximumprinzip: Es werden vertrauliche Daten verarbeitet, welche Ziel der Wirtschaftsspionage sein könnten.
		Integrität	Hoch	Maximumprinzip: Falsche Daten können zu Fehlproduktionen führen. Dies hätte einen hohen finanziellen Schaden zur Folge.
		Verfügbarkeit	Sehr Hoch	Kumulationseffekt: Die Verbindung für die Produktionsmaschinen sind für den Kernprozess notwendig. Ohne diese kann die RECPLAST GmbH

Kommunikations-verbindung	Schutzbedarfsfeststellung			
				keinen Gewinn erzielen. Ein Ausfall ist bis zu 2 Stunden tolerierbar.

Tabelle 18: Schutzbedarf Kommunikationsverbindungen

6.6. 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 einen Ausschnitt des Ergebnisses 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.

Räumlichkeit	Schutzbedarfsfeststellung			
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
GB001	Verwaltungsgebäude Bad Godesberg	Vertraulichkeit	Sehr Hoch	Maximumprinzip: In dem Gebäude werden firmeninterne Dokumente verarbeitet und gelagert. Diese sind besonders schützenswert.
		Integrität	Sehr Hoch	Maximumprinzip: Gemäß Maximumprinzip der Kommunikationsverbindungen in dem Gebäude.
		Verfügbarkeit	Sehr Hoch	Maximumprinzip: Aufgrund der Vielzahl der Systeme, Netzkomponenten etc. in dem Gebäude ist die Verfügbarkeit als sehr hoch einzuschätzen. Ein Ausfall bis zu 2 Stunden ist tolerierbar.
R003	Büros IT-Abteilung	Vertraulichkeit	Hoch	Maximumprinzip: Gemäß Maximumprinzip der Clients der IT-Abteilung.
		Integrität	Hoch	Maximumprinzip:

Räumlichkeit	Schutzbedarfsfeststellung			
				Gemäß Maximumprinzip der Clients der IT-Abteilung.
		Verfügbarkeit	Normal	Maximumprinzip: Gemäß Maximumprinzip der Clients der IT-Abteilung. Im Notfall kann auf ein anderes Büro bzw. ein Besprechungsraum ausgewichen werden.
R009	Serverraum	Vertraulichkeit	Sehr Hoch	Maximumprinzip: Gemäß Maximumprinzip der sich im Serverraum befindlichen IT-Systeme.
		Integrität	Hoch	Maximumprinzip: Gemäß Maximumprinzip der sich im Serverraum befindlichen IT-Systeme.
		Verfügbarkeit	Sehr Hoch	Kumulationseffekt: Gemäß Maximumprinzip der sich im Serverraum befindlichen IT-Systeme.

Tabelle 19: Schutzbedarf Räume

7. 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.
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
ISMS.1 Sicherheitsmanagement	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
Schicht ORP: Organisation und Personal			
ORP.1 Organisation	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
ORP.2 Personal	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
ORP.3 Sensibilisierung und Schulung	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
ORP.4 Identitäts- und Berechtigungsmanagement	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
ORP.5 Compliance Management (Anforderungsmanagement)	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
Schicht CON: Konzeption und Vorgehensweisen			
CON.1 Kryptokonzept	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	

Baustein	Zielobjekte	Begründung	Ansprechpartner
CON.2 Datenschutz	Informationsverbund	Ein Datenschutz-Management-System ist etabliert.	
CON.3 Datensicherung	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
CON.4 Auswahl und Einsatz von Standardsoftware	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen	Informationsverbund	Es werden eigene Anwendungen bzw. Skripte entwickelt.	
CON.6 Löschen und Vernichten	Informationsverbund	Gemäß Kapitel 2.2 "Zuordnung anhand des Schichtenmodells" des IT-Grundschutz Kompendiums	
CON.7 Informationssicherheit auf Auslandsreisen	Informationsverbund	Die Mitarbeiter der RECPLAST GmbH sind international tätig.	
Schicht OPS: Betrieb			
OPS.1.1.2 Ordnungsgemäße IT-Administration	Informationsverbund	Die IT wird von der RECPLAST GmbH administriert.	
OPS.1.1.3 Patch- und Änderungsmanagement	Informationsverbund	Ein Patch- und Änderungsmangement ist etabliert.	
OPS.1.1.4 Schutz vor Schadprogrammen	Informationsverbund	Jeder Client verfügt über einen Schutz vor Schadprogramme.	
OPS.1.1.5 Protokollierung	Informationsverbund	Es wird im Informationsverbund protokolliert.	
OPS.1.1.6 Software-Tests und -Freigaben	Informationsverbund	Software-Tests und -Freigaben werden durch die RECPLAST GmbH durchgeführt.	
OPS.1.2.2 Archivierung	Informationsverbund	Die RECPLAST GmbH hat Archivierungspflichten einzuhalten.	
OPS.1.2.3 Informations- und Datenträgeraustausch	Nicht relevant	Es werden keine Datenträger ausgetauscht.	

Baustein	Zielobjekte	Begründung	Ansprechpartner
OPS.1.2.4 Telearbeit	Nicht relevant	Telearbeit ist nicht möglich.	
OPS.2.1 Outsourcing für Kunden	A019; A026	Es werden Outsourcing-Dienstleitungen bezogen.	
OPS.2.2 Cloud-Nutzung	A026; A030; A031	Die RECPLAST GmbH nutzt Cloud-Lösungen.	
OPS.2.4 Fernwartung	Informationsverbund	Die Fernwartung ist möglich.	
OPS.3.1 Outsourcing für Dienstleister	Nicht Relevant	Es werden keine Outsourcing-Dienstleistungen angeboten.	
Schicht APP: Anwendungen			
APP.1.1 Office-Produkte	A001	Auf jedem Arbeitsplatzrechner ist Office-Software installiert.	
APP.1.2 Web-Browser	A003	Auf jedem Arbeitsplatzrechner ist ein Webbrowser installiert.	
APP.1.4 Mobile Anwendungen (Apps)	A030	Die RECPLAST GmbH nutz eine Mobile Anwendung.	
APP.2.1 Allgemeiner Verzeichnisdienst	A010	Es wird ein Active Directory eingesetzt.	
APP.2.2 Active Directory	A010	Es wird ein Active Directory eingesetzt.	
APP.2.3 OpenLDAP	Nicht relevant	OpenLDAP wird nicht eingesetzt.	
APP.3.1 Webanwendungen	A017; A021; A022; A026; A031	Es werden diverse Webanwendungen von der RECPLAST GmbH genutzt.	
APP.3.2 Webserver	A019	Es wird ein Webserver betrieben.	

Tabelle 20: Modellierung

8. IT-Grundschutz-Check

In einem ersten IT-Grundschutz-Check wird vor der Durchführung der 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
- Zielobjekt A001 Textverarbeitung, Präsentation, Tabellenkalkulation
    - APP.1.1 Office-Produkte
- Zielobjekt: C001 Clients der Finanzbuchhaltung
    - SYS.2.2.3 Clients unter Windows 10

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.

8.1. 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	Status	Umsetzung
ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	Ja	Die Geschäftsführung hat die Erstellung der Leitlinie zur Informationssicherheit initiiert. Die Geschäftsführung hat die Gesamtverantwortung für die Informationssicherheit übernommen. Einmal im Monat erhält die Geschäftsführung einen Management-Report und kontrolliert den Umsetzungsstand der Maßnahme.
ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie	Ja	Die Geschäftsführung hat Ziele sowie eine Strategie für Informationssicherheit in der Leitlinie zur Informationssicherheit festgelegt und dokumentiert. Der Sicherheitsprozess ist an diesen Vorgaben ausgerichtet. Die Geschäftsführung hat außerdem veranlasst, dass Aktualität, Angemessenheit und wirksame Umsetzung der

Anforderung	Status	Umsetzung
		Sicherheitsziele und -strategie regelmäßig geprüft werden.
ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit	Ja	Die Geschäftsführung hat die Leitlinie zur Informationssicherheit verabschiedet und den Mitarbeitern und anderen relevanten Stellen bekanntgegeben. In dieser wird der Geltungsbereich definiert, die Sicherheitsziele und die wichtigsten Aspekte der Sicherheitsstrategie beschrieben. Die Leitlinie wird jährlich überprüft und bei Bedarf aktualisiert.
ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten	Ja	Es wurde ein fachlich qualifizierter Informationssicherheitsbeauftragter (ISB) benannt, welcher der Geschäftsführung über alle relevanten Fragestellungen zur Informationssicherheit berichtet. Durch die Richtlinien wurde sichergestellt, dass der ISB in die Unternehmensprozesse eingebunden und frühzeitig in neue Entwicklungen und Vorhaben eingebunden wird.
ISMS.1.A5 Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten	Entbehrlich	Der Informationssicherheitsbeauftragte ist ein Mitarbeiter der RECPLAST GmbH.
ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	Teilweise	Die RECPLAST GmbH hat verschiedene Rollen für die IS-Organisation definiert. Diese sind in der Leitlinie zur Informationssicherheit dokumentiert und beschrieben. Es gibt jedoch noch keine ausreichende Vertretungsregelung für alle IS-Organisations-Rollen. Die Kommunikationswege sind definiert und den Mitarbeitern mitgeteilt worden. Eine Prüfung der Organisationsstruktur findet jährlich statt.
ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen	Ja	Es wurden entsprechende Sicherheitsmaßnahmen in den einzelnen Richtlinien dokumentiert.
ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess	Ja	Die Mitarbeiter werden regelmäßig über das interne Wiki über Neuerungen etc. der IS-Organisation sowie des ISMS informiert. Zusätzlich werden die Mitarbeiter regelmäßig geschult.
ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse	Ja	Die Informationssicherheit ist in so weit in die Geschäftsprozesse integriert, dass am ISMS-Meeting regelmäßig Abteilungsleiter der Fachabteilungen teilnehmen. Diese informieren und sensibilisieren ihre Mitarbeiter im Anschluss entsprechend.
ISMS.1.A10 Erstellung eines Sicherheitskonzepts	Teilweise	Der Aufbau eines Sicherheitskonzepts ist bei der RECPLAST GmbH derzeit im Aufbau. Eine vollständige Beendigung des Sicherheitskonzepts ist erst nach dem Durchführen einer Risikoanalyse erwünscht.

Anforderung	Status	Umsetzung
ISMS.1.A11 Aufrechterhaltung der Informationssicherheit	Ja	Die erstellten Richtlinien und Konzepte der RECPLAST GmbH werden regelmäßig auf Wirksamkeit geprüft. In jedem Dokument existiert eine Dokumenteneigenschaftenübersicht, welche die Verantwortlichkeiten und Prüfungszyklen beschreibt. Zusätzlich dazu gibt es eine Dokumentenhistorie, in der vorgenommene Änderungen beschrieben werden.
ISMS.1.A12 Management-Berichte zur Informationssicherheit	Ja	Der ISB informiert die Geschäftsführung monatlich über den aktuellen Stand der Informationssicherheit anhand eines Management-Reports. Die Geschäftsführung trifft anhand des Reports eventuelle Entscheidungen. Diese werden in einem Protokoll dokumentiert. Die Reports werden entsprechend versioniert und archiviert.
ISMS.1.A13 Dokumentation des Sicherheitsprozesses	Ja	Getroffene Entscheidungen werden im Protokoll des ISMS-Meetings bzw. im Protokoll des Management-Reports sowie eventuell in der Risikoanalyse dokumentiert. In der Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen wird über den Umgang mit Dokumenten und Vertraulichkeitsstufen informiert. Die aktuellen Versionen werden im internen Wiki bereitgestellt. Archivierte Daten befinden sich auf dem Dateiablageserver.
ISMS.1.A14 Sensibilisierung zur Informationssicherheit	Ja	Die Mitarbeiter werden regelmäßig durch den ISB bzw. die Mitglieder der IS-Organisation geschult.
ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit	Ja	Der ISB hat jederzeit die Möglichkeit zur Berichtserstattung bei der Geschäftsführung. Diese sorgt dafür, dass die benötigten Ressourcen zur Verfügung stehen. Der Einsatz von Sicherheitsmaßnahmen wird immer unter dem Gesichtspunkt des wirtschaftlichen Nutzens untersucht.

Tabelle 21: Grundschutz-Check ISMS.1

8.2. APP.1.1 Office-Produkte

Im Folgenden werden die Ergebnisse des IT-Grundschutz-Checks für die Basis- und Standard-Anforderungen des Bausteins „APP.1.1 Office-Produkte“ aufgeführt. Zielobjekt ist die Anwendung „A001 Textverarbeitung, Präsentation, Tabellenkalkulation“.

Anforderung	Status	Umsetzung
APP.1.1.A1 Sicherstellen der Integrität von Office-Produkten	Ja	Es werden nur offizielle Office-Produkte installiert. Die Updates werden aus sicheren Quellen bezogen. Falls vorhanden, werden digitale Signaturen oder Prüfsummen zur Sicherstellung der Integrität genutzt.

Anforderung	Status	Umsetzung
APP.1.1.A2 Einschränken von Aktiven Inhalten	Ja	Das automatische Ausführen von aktiven Inhalten ist standardmäßig deaktiviert. Die Mitarbeiter werden regelmäßig auf die Gefahr von aktiven Inhalten hingewiesen.
APP.1.1.A3 öffnen von Dokumenten aus externen Quellen	Ja	Dokumente, welche per Mail in das interne Netz gelangen werden vom Virenscanner auf Schadsoftware geprüft. Alte Dateiformate oder nicht mehr benötigte Dateiformate werden direkt abgefangen. Die Mitarbeiter werden auf die Gefahren aufmerksam gemacht.
APP.1.1.A4 Absichern des laufenden Betriebs von Office-Produkten	Ja	Die Informationstechnik und der ISB informieren sich regelmäßig über mögliche Schwachstellen. Updates werden durch die Updateverwaltung eingespielt. In der Security Policy werden die Vorgaben für die sichere Nutzung von Anwendungen definiert.
APP.1.1.A5 Auswahl geeigneter Office-Produkte	Entbehrlich	Die Office-Produkte wurden anhand eines Anforderungskatalogs beschafft.
APP.1.1.A6 Testen neuer Versionen von Office-Produkten	Teilweise	Neue Versionen werden zuerst nur für bestimmte Mitarbeiter installiert. Diese testen die Funktionalität im Hinblick auf die Dokumentenvorlagen, Formulare etc.
APP.1.1.A7 Installation und Konfiguration von Office-Produkten	Ja	Die Konfiguration der Office-Produkte sind im Systemmanagement dokumentiert.
APP.1.1.A8 Versionskontrolle von Office-Produkten	Ja	Die Updateverwaltung führt regelmäßig einen Abgleich der aktuellen Version mit der installierten Version durch. Zusätzlich lässt sich im Systemmanagement nachvollziehen, auf welchem Client die Software installiert ist. Die Konfigurationen sind im Systemmanagement dokumentiert.
APP.1.1.A9 Beseitigung von Restinformationen vor Weitergabe von Dokumenten	Ja	Die Dokumente der RECPLAST GmbH sind klassifiziert. Je nach Klassifizierung sind Tätigkeiten an Dokumenten durchzuführen, bevor diese weitergegeben werden. Dokumente sind immer in pdf-Dateiformat zu versenden.
APP.1.1.A10 Regelung der Software-Entwicklung durch Endbenutzer	Teilweise	Eigenentwicklungen durch die Mitarbeiter sind nicht erlaubt.
APP.1.1.A11 Geregelter Einsatz von Erweiterungen für Office-Produkte	Entbehrlich	Es werden keine Erweiterungen für Office-Produkte eingesetzt.
APP.1.1.A12 Verzicht auf Cloud-Speicherung	Ja	Die Cloud-Funktionen der Office-Produkte werden institutionsweit deaktiviert. Die Dokumente werden auf dem Dateiserver der RECPLAST GmbH gespeichert. Dokumente werden über Mail zur Verfügung gestellt. Dabei sind die Vorgaben der Klassifizierung zu beachten.
APP.1.1.A13 Verwendung von Viewer-Funktionen	Ja	Bei nicht vertrauenswürdigen Dokumenten ist die Bearbeitung standardmäßig deaktiviert. Die Bearbeitung lässt sich von Benutzern aktivieren. Die Mitarbeiter werden jedoch regelmäßig auf die Gefahren hingewiesen und geschult.

Anforderung	Status	Umsetzung
APP.1.1.A14 Schutz gegen nachträgliche Veränderungen von Informationen	Ja	Die Mitarbeiter werden über die Möglichkeiten des Schutzes von Dateien vor nachträglichen Änderungen geschult. Anleitungen dazu finden sich im internen Wiki.

Tabelle 22: Grundschutz-Check APP.1.1

8.3. SYS.2.2.3 Clients unter Windows 10

Im Folgenden werden die Ergebnisse des IT-Grundschutz-Checks für die Basis- und Standard-Anforderungen des Bausteins „SYS.2.2.3 Clients unter Windows 10“ aufgeführt. Zielobjekt ist der Client „C001 Clients der Finanzbuchhaltung“.

Anforderung	Status	Umsetzung
SYS.2.2.3.A1 Planung des Einsatzes von Cloud-Diensten	Ja	Es wird kein Cloud-Dienst eingesetzt.
SYS.2.2.3.A2 Geeignete Auswahl einer Windows 10-Version und Beschaffung	Ja	Auswahl des Betriebssystems wurde umfangreich geprüft, auch unter Berücksichtigung der Vorgängerversion.
SYS.2.2.3.A3 Geeignetes Patch- und Änderungsmanagement	Ja	Patchmanagement ist etabliert.
SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen	Teilweise	Funktionsumfang für Microsofts autom. Benachrichtigungen ist eingeschränkt, befindet sich aber noch in Prüfung.
SYS.2.2.3.A5 Schutz vor Schadsoftware	Ja	Auf den Clients ist ein Virenschutzclient installiert.
SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem	Ja	Anmeldung ist nur mit RECPLAST-Konten möglich.
SYS.2.2.3.A7 Lokale Sicherheitsrichtlinien	Ja	Es gibt ein Client-Profil. Client-Profil wird getestet und freigegeben. Regelmäßiger Check des Profils.
SYS.2.2.3.A8 Zentrale Verwaltung der Sicherheitsrichtlinien von Clients	Ja	Es gibt ein Client-Profil. Client-Profil wird getestet und freigegeben. Regelmäßiger Check des Profils.
SYS.2.2.3.A9 Sichere zentrale Authentisierung der Windows-Clients	Ja	Kerberos wird eingesetzt.
SYS.2.2.3.A10 Konfiguration zum Schutz von Anwendungen in Windows 10	Ja	Datenausführungsverhinderung für alle Programme und Dienste (Opt-Out Modus) ist aktiviert.
SYS.2.2.3.A11 Schutz der Anmeldeinformationen in Windows 10	Entbehrlich	Windows 10 Enterprise wird nicht eingesetzt.
SYS.2.2.3.A12 Datei- und Freigabeberechtigungen	Ja	Berechtigungsvergabe ist geregelt. Berechtigungen werden autorisiert. Jährlich findet Inventur der Berechtigungen statt.
SYS.2.2.3.A13 Einsatz der SmartScreen-Funktionen	Ja	Microsoft SmartScreen ist deaktiviert.
SYS.2.2.3.A14 Einsatz des Sprachassistenten Cortana	Ja	Microsoft Cortana ist deaktiviert.

Anforderung	Status	Umsetzung
SYS.2.2.3.A15 Einsatz der Synchronisationsmechanismen in Windows 10	Ja	Synchronisation mit MS Cloud ist deaktiviert.
SYS.2.2.3.A16 Anbindung von Windows 10 an den Microsoft-Store	Ja	MS Store ist deaktiviert.
SYS.2.2.3.A17 Verwendung der automatischen Anmeldung	Ja	Automatische Anmeldung ist - soweit möglich - deaktiviert. Ferner Hinweis an Benutzer.
SYS.2.2.3.A18 Einsatz der Windows-Remoteunterstützung	Ja	Die Anforderungen wurden umgesetzt.
SYS.2.2.3.A19 Verwendung des Fernzugriffs über RDP	Ja	Die Anforderungen wurden umgesetzt.
SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung für privilegierte Konten	Ja	Berechtigungsvergabe ist geregelt. Berechtigungen werden autorisiert. Jährlich findet Inventur der Berechtigungen statt.

Tabelle 23: Grundschutz-Check SYS.2.2.3

9. Risikoanalyse

9.1. 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.

9.2. 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:

- der Geschäftsprozess GP001 Produktion, der einen hohen Schutzbedarf an Vertraulichkeit, Integrität und Verfügbarkeit hat,
- die Anwendung A002 E-Mail-Client, die einen hohen Bedarf an Vertraulichkeit, Integrität und Verfügbarkeit hat,
- die Clients C001 – C009, die einen hohen Bedarf an Vertraulichkeit und Integrität haben,
- die Netzkomponente N001 Router zum Internet wegen der Vertraulichkeit, Integrität und Verfügbarkeit,
- der Virtualisierungsserver S007, der in allen drei Grundwerten aufgrund der auf ihm betriebenen virtuellen Systeme einen hohen Schutzbedarf hat,

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

9.3. 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 0.29 Verstoß gegen Gesetze oder Regelungen	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 24: Gefährdungsübersicht

9.4. Gefährdungsübersicht ergänzen

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

9.5. 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 25: Definition Eintrittshäufigkeiten

Schadensauswirkungen	Beschreibung
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden. Der Schaden liegt unter 5.000 Euro.
begrenzt	Die Schadensauswirkungen sind begrenz und überschaubar. Der Schaden liegt zwischen 5.001 Euro bis 50.000 Euro.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein. Der Schaden beträgt zwischen 50.001 bis 500.000 Euro
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß annehmen. Der Schaden liegt höher als mehr als 501.000 Euro.

Tabelle 26: Definition 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 Maßnahmen 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 27: Definition Risikokategorien

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

Risikomatrix

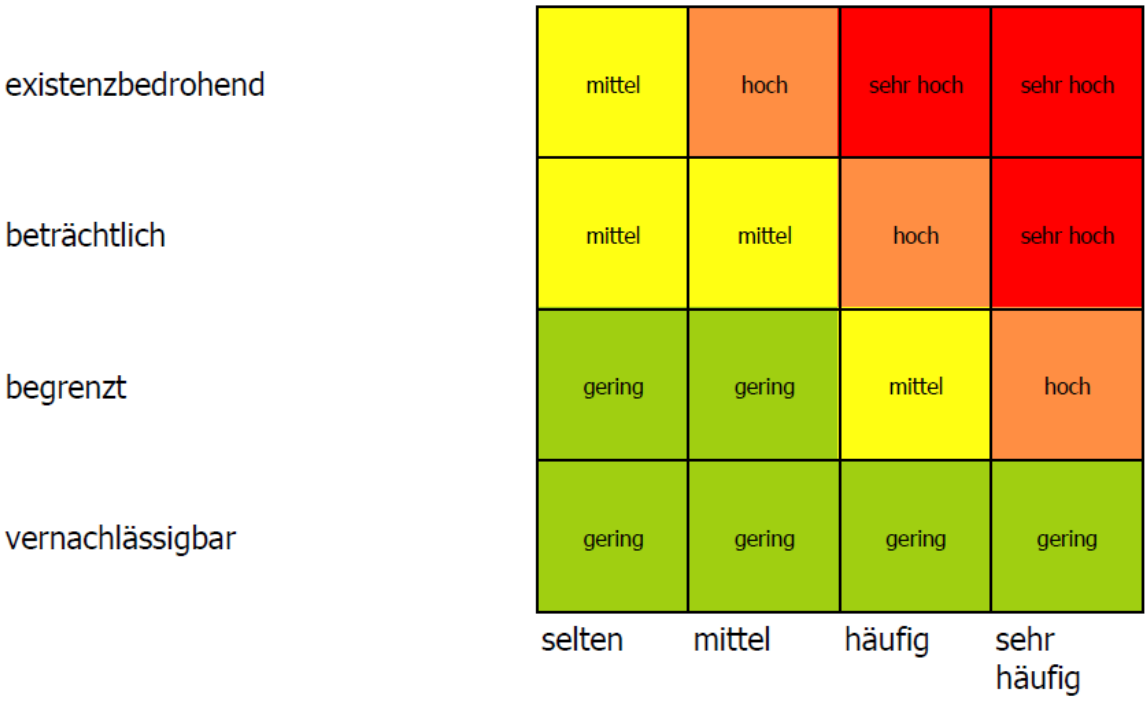

Abbildung 5: Risikomatrix

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

Gefährdung	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.8 Ausfall oder Störung der Stromversorgung	mittel	beträchtlich	mittel
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	mittel	beträchtlich	mittel
G 0.14 Ausspähen von Informationen (Spionage)	mittel	beträchtlich	mittel
G 0.15 Abhören	mittel	beträchtlich	mittel
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	selten	begrenzt	gering
G 0.18 Fehlplanung oder fehlende Anpassung	selten	begrenzt	gering
G 0.19 Offenlegung schützenswerter Informationen	mittel	beträchtlich	mittel
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	selten	begrenzt	gering
G 0.21 Manipulation von Hard- oder Software	mittel	beträchtlich	mittel
G 0.22 Manipulation von Informationen	mittel	beträchtlich	mittel

Gefährdung	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.23 Unbefugtes Eindringen in IT-Systeme	mittel	existenzbedrohend	hoch
G 0.25 Ausfall von Geräten oder Systemen	selten	begrenzt	gering
G 0.26 Fehlfunktion von Geräten oder Systemen	selten	begrenzt	gering
G 0.27 Ressourcenmangel	selten	begrenzt	gering
G 0.28 Software-Schwachstellen oder -Fehler	mittel	beträchtlich	mittel
G 0.29 Verstoß gegen Gesetze oder Regelungen	selten	begrenzt	gering
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	mittel	beträchtlich	mittel
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	selten	begrenzt	gering
G 0.32 Missbrauch von Berechtigungen	mittel	begrenzt	gering
G 0.39 Schadprogramme	häufig	begrenzt	mittel
G 0.40 Verhinderung von Diensten (Denial of Service)	selten	begrenzt	gering
G 0.43 Einspielen von Nachrichten	mittel	beträchtlich	mittel
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	selten	begrenzt	gering
G 0.45 Datenverlust	selten	begrenzt	gering
G 0.46 Integritätsverlust schützenswerter Informationen	mittel	begrenzt	mittel

Tabelle 28: Risikobewertung

9.6. Risikoanalyse auf Geschäftsprozessebene

Gefährdung	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.1 Feuer	selten	beträchtlich	mittel
G 0.2 Ungünstige klimatische Bedingungen	selten	begrenzt	gering
G 0.3 Wasser	selten	beträchtlich	gering
G 0.4 Verschmutzung, Staub, Korrosion	mittel	beträchtlich	mittel
G 0.5 Naturkatastrophen	selten	existenzbedrohend	hoch
G 0.6 Katastrophen im Umfeld	selten	existenzbedrohend	hoch

Gefährdung	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.7 Großereignisse im Umfeld	selten	begrenzt	gering
G 0.8 Ausfall oder Störung der Stromversorgung	mittel	existenzbedrohend	hoch
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	mittel	existenzbedrohend	hoch
G 0.10 Ausfall oder Störung von Versorgungsnetzen	mittel	existenzbedrohend	hoch
G 0.11 Ausfall oder Störung von Dienstleistern	selten	begrenzt	gering
G 0.12 Elektromagnetische Störstrahlung	selten	vernachlässigbar	gering
G 0.13 Abfangen kompromittierender Strahlung	selten	vernachlässigbar	gering
G 0.14 Ausspähen von Informationen (Spionage)	selten	begrenzt	gering
G 0.15 Abhören	selten	begrenzt	gering
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	selten	begrenzt	gering
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten	selten	begrenzt	gering
G 0.18 Fehlplanung oder fehlende Anpassung	mittel	beträchtlich	mittel
G 0.19 Offenlegung schützenswerter Informationen	mittel	beträchtlich	mittel
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	mittel	begrenzt	gering
G 0.21 Manipulation von Hard- oder Software	mittel	existenzbedrohend	hoch
G 0.22 Manipulation von Informationen	selten	beträchtlich	mittel
G 0.23 Unbefugtes Eindringen in IT-Systeme	selten	beträchtlich	mittel
G 0.24 Zerstörung von Geräten oder Datenträgern	mittel	existenzbedrohend	hoch
G 0.25 Ausfall von Geräten oder Systemen	mittel	existenzbedrohend	hoch
G 0.26 Fehlfunktion von Geräten oder Systemen	mittel	existenzbedrohend	hoch
G 0.27 Ressourcenmangel	mittel	beträchtlich	mittel
G 0.28 Software-Schwachstellen oder -Fehler	selten	beträchtlich	mittel

Gefährdung	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.29 Verstoß gegen Gesetze oder Regelungen	selten	begrenzt	gering
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	mittel	beträchtlich	mittel
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	mittel	beträchtlich	mittel
G 0.32 Missbrauch von Berechtigungen	mittel	beträchtlich	mittel
G 0.33 Personalausfall	mittel	beträchtlich	mittel
G 0.35 Nötigung, Erpressung oder Korruption	selten	begrenzt	gering
G 0.36 Identitätsdiebstahl	mittel	beträchtlich	mittel
G 0.37 Abstreiten von Handlungen	selten	begrenzt	gering
G 0.38 Missbrauch personenbezogener Daten	selten	begrenzt	gering
G 0.39 Schadprogramme	mittel	beträchtlich	mittel
G 0.40 Verhinderung von Diensten (Denial of Service)	selten	begrenzt	gering
G 0.41 Sabotage	mittel	existenzbedrohend	hoch
G 0.42 Social Engineering	mittel	beträchtlich	mittel
G 0.43 Einspielen von Nachrichten	selten	begrenzt	gering
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	selten	begrenzt	gering
G 0.45 Datenverlust	selten	begrenzt	gering
G 0.46 Integritätsverlust schützenswerter Informationen	mittel	beträchtlich	mittel

Tabelle 29: Risikoanalyse Geschäftsprozess

9.7. 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 **Risikovermeidung** 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.

Im nachfolgenden wird die Risikobehandlung für das Zielobjekt S007 Virtualisierungsserver dargestellt:

Gefährdung	Risikobehandlungsoption
G 0.8 Ausfall oder Störung der Stromversorgung	**Risikoreduktion**: Es soll eine redundante Stromversorgung geschaffen werden.
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	**Risikoreduktion**: Es soll ein zweiter Internetprovider beauftragt werden.
G 0.14 Ausspähen von Informationen (Spionage)	**Risikoreduktion**: Es soll eine Zwei-Faktor-Authentifizierung eingerichtet werden.
G 0.15 Abhören	**Risikoreduktion**: Es soll eine Zwei-Faktor-Authentifizierung eingerichtet werden.
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.18 Fehlplanung oder fehlende Anpassung	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.19 Offenlegung schützenswerter Informationen	**Risikoreduktion**: Es soll eine Angriffserkennung sowie eine Zwei-Faktor-Authentifizierung eingerichtet werden.
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.21 Manipulation von Hard- oder Software	**Risikoreduktion**: Es soll eine Angriffserkennung eingerichtet werden.
G 0.22 Manipulation von Informationen	**Risikoreduktion**: Es soll eine Angriffserkennung eingerichtet werden.
G 0.23 Unbefugtes Eindringen in IT-Systeme	**Risikoreduktion**: Es soll eine Angriffserkennung sowie eine Zwei-Faktor-Authentifizierung eingerichtet werden.
G 0.25 Ausfall von Geräten oder Systemen	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.26 Fehlfunktion von Geräten oder Systemen	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.27 Ressourcenmangel	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.

Gefährdung	Risikobehandlungsoption
G 0.28 Software-Schwachstellen oder -Fehler	**Risikoreduktion**: Es soll eine Angriffserkennung eingerichtet werden.
G 0.29 Verstoß gegen Gesetze oder Regelungen	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	**Risikoreduktion**: Es sollen geteilte Kennwörter zur Administration von kritischen Vorgängen eingerichtet werden.
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.32 Missbrauch von Berechtigungen	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.39 Schadprogramme	**Risikoreduktion**: Es soll Appliaction Whitelisting eingesetzt sowie eine Angriffserkennung eingerichtet werden.
G 0.40 Verhinderung von Diensten (Denial of Service)	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.43 Einspielen von Nachrichten	**Risikoreduktion**: Es soll eine Angriffserkennung eingerichtet werden.
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.45 Datenverlust	**Risikoakzeptanz**: Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
G 0.46 Integritätsverlust schützenswerter Informationen	**Risikoreduktion**: Es sollen geteilte Kennwörter zur Administration von kritischen Vorgängen eingerichtet werden.

Tabelle 30: Risikobehandlung

10. Realisierungsplan

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. Auf Anmerkungen der zugehörigen Entscheidungen zu Terminen, Budget und Verantwortlichkeiten wurde in diesem Beispiel verzichtet.

Zielobjekt	Anforderung	Umzusetzende Maßnahme
C001 – C009 Clients	SYS.2.1.A12 Kompatibilitätsprüfung von Software	Der Beschaffungsprozess wird von der Einkaufsabteilung überarbeitet und vervollständigt.
	SYS.2.1.A17 Einsatzfreigabe	Es wird ein Freigabeprozess definiert und eingesetzt.
	SYS.2.1.A21 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras	Aufgrund der Vielzahl an Videokonferenzen der Mitarbeiter des Vertriebs wird die Funktion für alle Mitarbeiter des Vertriebs aktiviert.
	SYS.2.1.A37 Schutz vor unbefugten Anmeldungen	Es wird eine Zwei-Faktor-Authentisierung angeschafft.
	SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen	Nach erfolgreicher Prüfung wird über das Deaktivieren der Einstellungen entschieden.
GB001 Verwaltungsgebäude Bad Godesberg, GB002 Produktionsgebäude Beuel	INF.4.A5 Abnahme der IT-Verkabelung	Es wird bezüglich der Nutzung des Protokolls sensibilisiert.
	INF.4.A7 Entfernen und Deaktivieren nicht mehr benötigter IT-Verkabelung	Die IT-Verkabelungen werden auf nicht mehr benötigte Kabel überprüft.
N002 Firewall	NET.3.2.A16 Aufbau einer „P-A-P“-Struktur	Es wird eine P-A-P-Netzstruktur aufgebaut.
	NET.3.2.A26 Auslagerung von funktionalen Erweiterungen auf dedizierte Hardware	Beim Erreichen des End of Life-Cycles wird eine neue dedizierte Firewall angeschafft.
	NET.3.2.A29 Einsatz von Hochverfügbarkeitslösungen	Es soll eine weitere Firewall beschafft werden.

Tabelle 31: Umsetzungsplanung