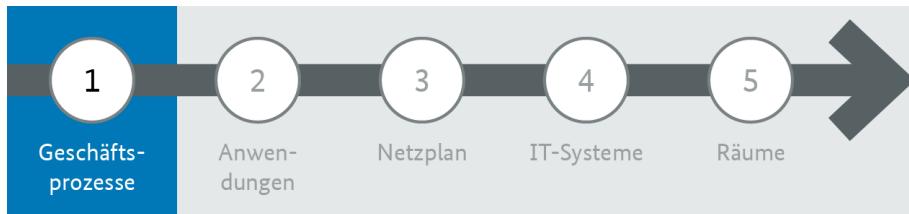


zu. Weitere typische Beispiele für Gruppierungen sind gleich ausgestattete und genutzte Büroräume oder die Kommunikationsverbindungen zwischen einem Switch und den Clients einer Gruppe. In den nachfolgenden Abschnitten werden weitere Beispiele für zweckmäßige Gruppenbildungen genannt.

**!** Überlegen Sie sich sorgfältig, welche Objekte Sie zu Gruppen zusammenfassen. Wenn Sie Komponenten zusammenfassen, die unterschiedlichen Schutzbedarf haben, dann können Sicherheitslücken entstehen.

## Lerneinheit 3.3: Geschäftsprozesse und Informationen erheben



Ein Sicherheitskonzept soll die **wesentlichen Informationen** einer Institution schützen. Welche dazu zählen, wird in der Regel bei einer Betrachtung der **Geschäftsprozesse** deutlich: Welche Informationen sind erforderlich, damit diese reibungslos funktionieren? Welche haben einen besonderen Geheimhaltungsbedarf und dürfen daher nur Befugten zugänglich sein? Welche Informationen unterliegen den Vorgaben des Datenschutzes, welche anderen rechtlichen Verpflichtungen (beispielsweise um die Nachweisbarkeit von geschäftlichen Vorgängen zu sichern)?

Oft kann auf eine bereits vorhandene Aufstellung der wesentlichen Geschäftsprozesse oder Fachaufgaben zurückgegriffen werden (eine „Prozesslandkarte“) oder die Prozesse können anhand von Aufgabenbeschreibungen oder eines Organigramms der Institution identifiziert werden.

### Ergebnisdarstellung

Tabellen bieten eine übersichtliche Möglichkeit, die Ergebnisse der Erhebung der Prozesse und Informationen darzustellen. Für jeden Geschäftsprozess sollten Sie die folgenden Angaben vermerken:

- eine eindeutige Kennung (Nummer oder Kürzel),
- einen Namen für den Prozess,
- eine kurze Beschreibung des Ziels, der Abläufe und der verarbeiteten Informationen,
- die für den Prozess Verantwortlichen,
- wichtige Anwendungen, die für den Prozess benötigt werden.

### Beispiel

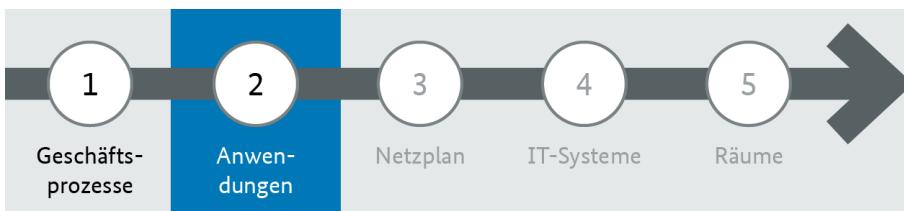
**RecS** Die folgende Tabelle zeigt einen Teil der für die RECPLAST GmbH erfassten Geschäftsprozesse. Diese werden durch das Präfix „GP“ als Geschäftsprozess gekennzeichnet und fortlaufend durchnummieriert.

Die für einen Prozess benötigten Anwendungen werden in einer separaten Tabelle zugeordnet.

Kennung	Name (Art) und Beschreibung des Prozesses sowie der verwendeten Informationen	Verantwortlicher	Mitarbeiter
GP001	<b>Produktion (Kerngeschäft):</b> Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis hin zur Einlagerung des produzierten Materials. Hierzu gehören innerhalb der Produktion die internen Transportwege, die Produktion und Fertigung der verschiedenen Komponenten und das Verpacken der Teile. Es werden alle Informationen über Aufträge, Lagerbestände und Stücklisten verarbeitet.	Leiter Produktion	Alle Mitarbeiter
GP002	<b>Angebotswesen (unterstützender Prozess):</b> In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im Regelfall werden Kundenanfragen formlos per E-Mail oder Fax geschickt. Die Angebote werden elektronisch erfasst und ein schriftliches Angebot per Post an den Kunden versendet. Im Angebotswesen werden Kundendaten, Lagerbestände, Anfragen und Angebote bearbeitet.	Leiter Angebotswesen	Vertrieb
GP003	<b>Auftragsabwicklung (Kerngeschäft):</b> Kunden schicken die Bestellungen im Regelfall per Fax oder E-Mail. Alle Belege müssen ausgedruckt und elektronisch erfasst werden. Eine Auftragsbestätigung erhält der Kunde nur, wenn er dies ausdrücklich wünscht oder der Produktionsprozess von der üblichen Produktionszeit abweicht. Die Auftragsabwicklung verwendet Kundendaten, Lagerbestände, Aufträge und Bestellungen.	Leiter Auftragsabwicklung	Vertrieb
GP004	<b>Einkauf (unterstützender Prozess):</b> In der Einkaufsabteilung werden alle erforderlichen Artikel bestellt, die nicht für den Produktionsprozess erforderlich sind. In dieser Abteilung werden externe Projekte verhandelt, IT-Verträge gestaltet und Verbrauchsmaterial im organisatorischen Umfeld (Papier, Toner etc.) beschafft. Die verwendeten Informationen sind Lagerbestände, Bedarfsmeldungen und Informationen über Lieferanten.	Leiter Einkauf	Einkauf
GP005	<b>Disposition (Kerngeschäft):</b> 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 Jahresplänen und verschiedenen Bestellwerten.	Leiter Disposition	Disposition, Produktion

Tabelle 1: Liste der Geschäftsprozesse der RECPLAST GmbH (Auszug)

## Lerneinheit 3.4: Anwendungen erheben



Als Anwendungen erfassen Sie **IT-Lösungen**, die Geschäftsprozesse und die Erledigung von Fachaufgaben unterstützen und die aufgrund ihres Bedarfs an Geheimhaltung, Korrektheit und Unverfälschtheit oder Verfügbarkeit zumindest ein **Mindestmaß an Schutz** erfordern. Zur Identifikation der in dieser Hinsicht wesentlichen und folglich in der Strukturanalyse zu dokumentierenden Anwendungen bieten sich Gespräche oder gemeinsame Workshops mit Benutzern, Anwendungs- und Geschäftsprozessverantwortlichen sowie sachkundigen Mitarbeitern der IT-Abteilung an.

Für jede als wesentlich identifizierte Anwendung sollten Sie **folgende Angaben** in einer Tabelle erfassen:

- eine eindeutige Kennung (Nummer oder Kürzel),
- einen Namen für die Anwendung,
- eine kurze Beschreibung des Ziels, der Funktion und der verarbeiteten Informationen,
- die für die Anwendung Verantwortlichen,
- die Benutzer dieser Anwendung.

Zusätzlich müssen Sie die Abhängigkeiten zwischen Anwendungen und Geschäftsprozessen oder Fachaufgaben dokumentieren, also festhalten, in welchen Prozessen und Fachaufgaben eine gegebene Anwendung benutzt wird.

 Achten Sie bei der Erfassung der Anwendungen auf eine **angemessene Granularität**. Beispielsweise ist es in der Regel nicht sinnvoll, ein Office-Produkt in seine einzelnen Bestandteile (z. B. Textverarbeitung, Präsentation, Tabellenkalkulation) zu zerlegen und diese dann gesondert zu beschreiben. Wenn Sie zu feinteilig erfassen, erzeugen Sie einen unnötigen Aufwand für die nachfolgenden Phasen der Sicherheitskonzeption durch ein Übermaß an zu behandelnden Objekten. Bei einer zu groben Betrachtung der Anwendungen verhindern Sie erforderliche Differenzierungen, insbesondere auch bei der Festlegung erforderlicher Schutzmaßnahmen.

#### Beispiel: Anwendungen der RECPLAST GmbH

 Eine vollständige Übersicht aller Anwendungen, die in den Geschäftsprozessen der RECPLAST GmbH bedeutsam sind, würde den Rahmen dieses Kurses sprengen. Die nachfolgenden Tabellen enthalten daher nur einen Ausschnitt, um zu verdeutlichen, wie Sie Anwendungen und ihren Zusammenhang mit den Geschäftsprozessen dokumentieren.

Bezeichnung	Name und Beschreibung der Anwendung	Anzahl	Benutzer	Verantwortlich/Administrator
A001	<b>Textverarbeitung, Präsentation, Tabellenkalkulation:</b> Alle geschäftlichen Informationen werden in einem Office-Produkt verarbeitet: Geschäftsbriebe, Analysen oder Präsentationen.	290	Alle Mitarbeiter	IT-Betrieb
A002	<b>Lotus Notes:</b> Diese Anwendung wird von allen Mitarbeitern für die Bearbeitung von -E-Mails, Terminen und Kontakten genutzt.	290	Alle Mitarbeiter	IT-Betrieb
...				
A009	<b>Auftrags- und Kundenverwaltung</b> Mit dieser datenbankgestützten Anwendung werden Kundenstammdaten und Auftragsdaten verarbeitet sowie die Informationen für Produktion und Lieferung vorbereitet.	55	Marketing & Vertrieb	Marketing & Vertrieb
A010	<b>Active Directory:</b> Diese Anwendung soll dem IT-Betrieb die Arbeit erleichtern und doppelte Benutzereingaben reduzieren. Zu allen Nutzern der IT-Systeme werden Informationen zu Gruppenzugehörigkeit, Rechten und Authentisierungsmerkmalen verarbeitet und gespeichert. Diese Anwendung ist über beide Domain Controller verfügbar.	2	Administratoren	IT-Betrieb
...				
A013	<b>Druckservice BG:</b> Über diesen Dienst können alle Mitarbeiter in Bad Godesberg die dortigen Drucker benutzen. Er ist auf dem Druckserver in Bad Godesberg verfügbar, kann aber bei Bedarf auch auf dem Druckserver in Beuel gestartet werden.	1	Alle Mitarbeiter in Bad Godesberg	IT-Betrieb

Bezeichnung	Name und Beschreibung der Anwendung	Anzahl	Benutzer	Verantwortlich/Administrator
A014	<b>Druckservice Beuel:</b> Über diesen Dienst können alle Mitarbeiter in Beuel die dortigen Drucker benutzen. Er ist auf dem Druckserver in Beuel verfügbar, kann aber bei Bedarf auch auf dem Druckserver in Bad Godesberg gestartet werden.	1	Alle Mitarbeiter in Beuel	IT-Betrieb
A015	<b>Firewall:</b> Die Anwendung steuert die Kommunikation zwischen dem Firmennetz und dem Internet und ermöglicht die verschlüsselte Kommunikation der Vertriebsbüros über VPN-Tunnel.	1	Alle Mitarbeiter	IT-Betrieb
A016	<b>TK-Vermittlung:</b> Über die beiden miteinander gekoppelten TK-Anlagen in Bad Godesberg und Beuel werden ein- und ausgehende Telefongespräche und Fax-Dokumente vermittelt und ein Telefonverzeichnis gepflegt.	2	Alle Mitarbeiter	IT-Betrieb

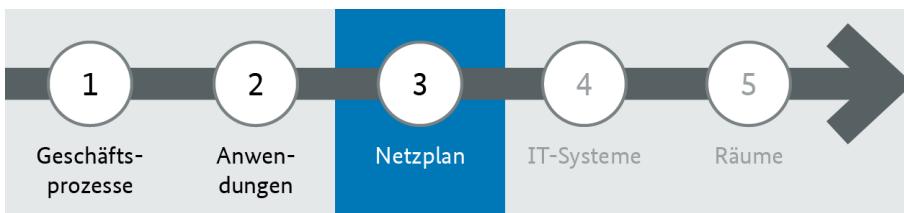
Tabelle 2: Liste der Anwendungen (Auszug)

Die folgende Tabelle zeigt auszugsweise, in welchen Geschäftsprozessen diese Anwendungen verwendet werden:

Geschäftsprozess	Anwendung								
	A001	A002	...	A009	A010	...	A013	A014	...
GP001 Produktion	X			X	X			X	
GP002 Angebotswesen	X	X		X	X		X		
GP003 Auftragsabwicklung	X	X		X	X		X		
GP004 Einkauf	X	X			X		X		
GP005 Disposition	X	X		X	X		X		

Tabelle 3: Zuordnung von Anwendungen zu Geschäftsprozessen

## Lerneinheit 3.5: Netzplan erheben



Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihre Verbindungen. Im Einzelnen sollte der Plan mindestens die folgenden Objekte enthalten:

- die in das Netz eingebundenen **IT-Systeme**;  
dazu zählen Computer (Clients und Server), Netzdrucker sowie aktive Netzkomponenten (Switches Router, WLAN Access Points) usw.
- die **Verbindungen zwischen diesen IT-Systemen**;  
LAN-Verbindungen (z. B. Ethernet), Backbone-Technik (z. B. ATM) usw.
- die **Außenverbindungen der IT-Systeme**;  
bei diesen sollte zusätzlich die Art der Verbindung gekennzeichnet sein (z. B. Internet-Anbindung, DSL) usw.

In der Regel hat Ihre IT-Administration einen solchen Netzplan bereits erstellt. Ein Netz und die darin eingesetzten Komponenten unterliegen jedoch häufigen Veränderungen, sodass die Aktualität der vorhandenen Pläne nicht unbedingt gewährleistet ist.



Überprüfen Sie daher, ob der Netzplan, den Sie für die Strukturanalyse verwenden, in allen Angaben noch korrekt ist. Befragen Sie z. B. den IT-Verantwortlichen, den Administrator oder Netz- und Systemmanager zur Aktualität der Ihnen vorliegenden Pläne.

Viele Unternehmen oder Behörden verwenden Software, mit denen ein Netzplan automatisch aufgrund der im Netz vorgefundenen Gegebenheiten erzeugt werden kann. Eine solche Darstellung enthält in der Regel jedoch weitaus mehr Informationen als für die Strukturanalyse tatsächlich benötigt werden. Insbesondere fehlt eine angemessene Zusammenfassung der IT-Systeme zu Gruppen. Es empfiehlt sich daher derartige Netzpläne zu „bereinigen“, also den Umfang der Informationen auf das tatsächlich Benötigte zu beschränken und die einzelnen Komponenten zweckmäßig zu gruppieren.

### Beispiel



Die untenstehende Abbildung zeigt einen solchen bereinigten Netzplan für die RECPLAST GmbH. Hier wurden unter anderem die folgenden Gruppen gebildet:

- Die Desktops 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 IT-Ausstattung, übereinstimmende Aufgaben und Regelungen sowie eine identische Zugangsmöglichkeit zum Firmennetz aus. Sie lassen sich in gewisser Weise mit häuslichen Telearbeitsplätzen vergleichen. Sie wurden deswegen zu einer Gruppe zusammengefasst.
- Die nicht vernetzten Komponenten **Faxgeräte** und **TK-Anlagen** wurden jeweils standortübergreifend zu einer Gruppe zusammengefasst, da für den Umgang mit diesen Geräten übereinstimmende organisatorische Regelungen gelten.
- Die **Laptops** wurden getrennt von den Arbeitsplatzrechnern einer Abteilung gruppiert, da für sie wegen der mobilen Nutzung zusätzliche Sicherheitsanforderungen beachtet werden müssen.

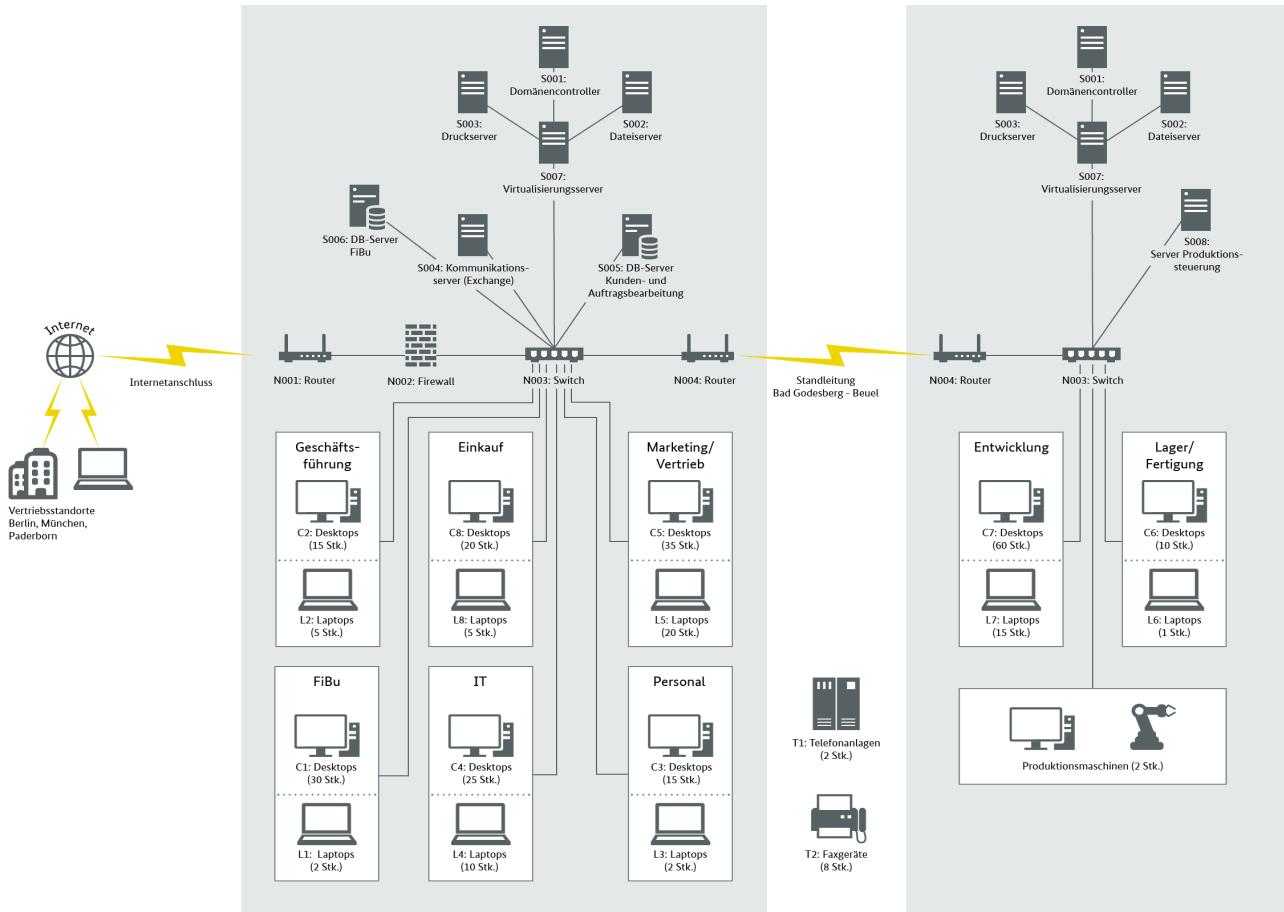
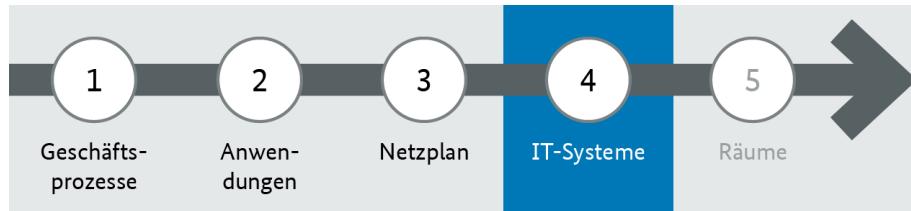


Abbildung 9: Bereinigter Netzplan

## Lerneinheit 3.6: IT-Systeme erheben



Bei der Erhebung der IT-Systeme stellen Sie die vorhandenen und geplanten IT-Systeme und anderen IT-Komponenten des Informationsverbundes und die sie jeweils charakterisierenden Angaben zusammen. Dabei dokumentieren Sie auch, für welche Anwendungen ein IT-System jeweils relevant ist. Aufgrund der damit verbundenen besseren Übersichtlichkeit empfehlen sich auch dafür tabellarische Darstellungen.

### Was zählt zu den IT-Systemen?

Zu den IT-Systemen zählen

- alle im Netz vorhandenen Computer (Clients und Server), Gruppen von Computern, aktive Netzkomponenten, Netzdrucker, aber auch
- industrielle Steuerungen (Industrial Control Systems, ICS), dazu zählen

- Geräte, die im Bereich Produktion und Fertigung zur Steuerung oder Überwachung eingesetzt werden, z. B. speicherprogrammierbare Steuerungen (SPS), Maschinen, die über WLAN gesteuert werden, autonome Fahrzeuge, aber auch
- Arbeitsplatz-PCs zur Steuerung einer Maschine und die Endgeräte wie Scanner oder Drucker, die an diese PCs angeschlossen sind,
- Telekommunikationsgeräte, Mobiltelefone oder andere mobile Geräte sowie
- Objekte aus dem Bereich des Internet of Things (IoT), also Geräte, die vernetzt sind und Daten erfassen, speichern, verarbeiten und übertragen können, z. B. Webcams, Smart-Home-Komponenten oder Sprachassistenten (auch für solche Geräte finden Sie IT-Grundschutz-Bausteine).

### Welche Angaben sind für IT-Systeme erforderlich?

Eine tabellarische Übersicht sollte für jedes IT-System die folgenden Angaben enthalten:

- eindeutige Bezeichnung,
- bei Gruppen: Anzahl der zusammengefassten IT-Systeme,
- Beschreibung (insbesondere sollten Sie hier den Einsatzzweck und den Typ anführen z. B. „Server für Personalverwaltung“, „Router zum Internet“),
- Plattform (Welcher Hardwaretyp, welches Betriebssystem?),
- Standort (Gebäude und Raumnummer),
- Status (z. B. in Betrieb, im Test, in Planung) und
- Benutzer und Administrator.

Zur Dokumentation der Beziehungen zwischen IT-Systemen und Anwendungen empfiehlt sich eine Matrix, wie sie in Lerneinheit 3.4: *Anwendungen erheben* auch zur Darstellung der Abhängigkeiten zwischen Geschäftsprozessen und Anwendungen verwendet wird.

 Achten Sie bei den vernetzten IT-Systemen darauf, dass die Angaben in der Liste der IT-Systeme mit den Angaben im Netzplan übereinstimmen.

### Beispiel

 Die folgende Tabelle zeigt einen Auszug der IT-Systeme bei der RECPLAST GmbH. Durch unterschiedliche Buchstaben als erstes Zeichen der Bezeichnung wird der Typ eines IT-Systems verdeutlicht (z. B. kennzeichnet ein „S“ Server oder ein „N“ Netzkkomponenten).

Bezeichnung	Beschreibung des Objekts	Standort	Anzahl	Status	Benutzer	Verantwortlich/Administrator
N001	<b>Router Internetanbindung:</b> Dieser Router regelt die Kommunikation zwischen dem Internet und dem internen Netz.	Serverraum BG	1	In Betrieb	Administratoren	IT-Betrieb
N002	<b>Firewall Internet-Eingang:</b> Diese Firewall dient als Schutz zwischen dem Internet und dem internen Netz	Serverraum BG	1	In Betrieb	Administratoren	IT-Betrieb
N003	<b>Switches – Verteilung:</b> Der Datenfluss zwischen Internet und lokalem Netz wird über diese Switches gesteuert.	Serverräume BG und Beuel	2	In Betrieb	Administratoren	IT-Betrieb
N004	<b>Router Bonn BG – Beuel:</b> Über eine Standleitung sind die beiden Standorte in Bonn verbunden. Diese Router sichern die Verbindung ab.	Serverräume BG und Beuel	2	In Betrieb	Administratoren	IT-Betrieb

Bezeichnung	Beschreibung des Objekts	Standort	Anzahl	Status	Benutzer	Verantwortlich/Administrator
...						
S007	<b>Virtualisierungsserver (Konfiguration 1):</b> Auf dem Server können bis zu 20 virtuelle Server konfiguriert werden. Für die Verwaltung der virtualisierten Systeme wird eine Anwendung eingesetzt.	Serverräume BG und Beuel	2	In Betrieb	Administratoren	IT-Betrieb
S003	<b>Print-Server (VM):</b> Server für die Druckdienste, die zentral gesteuert werden.	Serverräume BG und Beuel	2	In Betrieb	Administratoren	IT-Betrieb
...						
C001	<b>Arbeitsplatzrechner Einkauf</b> Standard-PC mit Standardsoftware	Büros BG		In Betrieb	Mitarbeiter Einkauf	IT-Betrieb
C002	<b>Arbeitsplatzrechner Geschäftsführung</b> Standard-PC mit Standardsoftware, vertrauliche Korrespondenz	Büros BG		In Betrieb	Mitarbeiter Geschäftsf.	IT-Betrieb
L001	<b>Laptops Einkauf</b> Laptop mit Standardsoftware, mobile Nutzung	Büros BG und mobil		In Betrieb	Mitarbeiter Einkauf	IT-Betrieb
L002	<b>Laptops Geschäftsführung</b> Laptop mit Standardsoftware, mobile Nutzung, vertrauliche Korrespondenz	Büros BG und mobil		In Betrieb	Mitarbeiter Geschäftsf.	IT-Betrieb
...						
S200	<b>Alarmanlage</b> korrekte Funktion ist sehr wichtig für den Schutz aller Werte in den Gebäuden.	Gebäude in BG und Beuel	2	In Betrieb	Pförtner, FASi	Haustechnik
...						
I001	<b>SPS der Spritzgussmaschine</b> Speicherprogrammierbare Steuerung und PC zur Steuerung der Produktionsmaschine	Produktionshalle in Beuel	2	In Betrieb	Mitarbeiter Produktion	IT-Betrieb

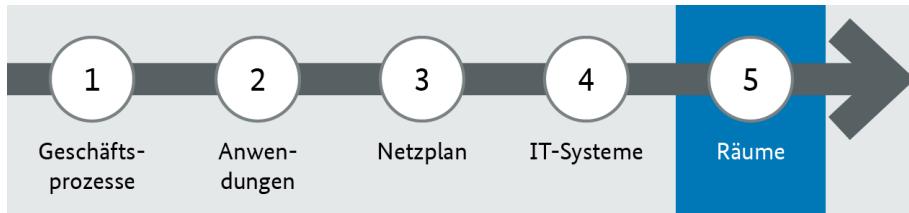
Tabelle 4: Liste der IT-Systeme (Auszug)

Welche Netzkomponenten von den Anwendungen genutzt werden, zeigt auszugsweise die nächste Tabelle:

Bezeichnung	Beschreibung der Anwendung	Router Internet	Firewall	Switche	Router BG-Beuel
A001	Textverarbeitung, Präsentation, Tabellenkalkulation			X	X
A002	Lotus Notes	X	X	X	X
...					
A009	Auftrags- und Kundenverwaltung	X	X	X	X
A010	Active Directory			X	X
...					
A013	Druckservice BG			X	
A014	Druckservice Beuel			X	
...					

Tabelle 5: Zuordnung der Anwendungen zu Netzkomponenten (Auszug)

## Lerneinheit 3.7: Räume erheben



Wie gut Informationen und Informationstechnik geschützt sind, hängt immer auch von der Sicherheit der räumlichen Umgebung ab, in der diese benutzt oder aufbewahrt werden. Daher erfassen Sie bei der Strukturanalyse auch alle Gebäude und Räume, die im Zusammenhang mit den betrachteten Informationen und Geschäftsprozessen bedeutsam sind. Dies können Serverräume oder andere ausdrücklich IT-bezogene Räume sein, aber auch Wegstrecken von Kommunikationsverbindungen, normale Büroräume, Schulungs- und Besprechungsräume oder Archivräume.

Zur Dokumentation der Beziehungen zwischen IT-Systemen und Räumen empfiehlt sich eine Matrix, wie sie in Lerneinheit Lerneinheit 3.4: auch zur Darstellung der Abhängigkeiten zwischen Geschäftsprozessen und Anwendungen verwendet wird.

**!** Falls bei Ihnen IT-Systeme, etwa das Datenträgerarchiv, einzelne Server oder Netzkopplungsgeräte, in einem Schutzschränk untergebracht sind, sollten Sie die Schränke auch bei der Erhebung der Räume erfassen.

### Beispiel

**RecS** Nachfolgend sehen Sie einen Auszug aus der Erhebung der Räume der RECPLAST GmbH. Die Liste enthält die beiden Gebäude (Verwaltungs- und Produktionsgebäude), die in ihnen befindlichen Büro- und Serverräume sowie die drei Vertriebsbüros. Die verschiedenen Räume sind zu Gruppen zusammengefasst, durchnummeriert und mit dem Kürzel „GB“ als Gebäude oder dem Kürzel „R“ als Raum gekennzeichnet.

Bezeichnung	Beschreibung	Art	Lokation
GB1	Verwaltungsgebäude	Gebäude	Bonn-Bad Godesberg
GB2	Produktionsgebäude	Gebäude	Bonn-Beuel
...			
R002	Serverraum Bad Godesberg	Serverraum	GB1
...			
R008	Büros Einkauf/Marketing/Vertrieb	Büroräume	GB1, R. 2.03-2.09
...			
R011	Büros Entwicklungsabteilung	Büroräume	GB2, R. 2.14-2.20
...			
R099	Vertriebsbüros	Häuslicher Arbeitsplatz	Berlin, München, Paderborn

Tabelle 6: Liste der Räume (Auszug)

### Alternatives Vorgehen: mit den IT-Systemen beginnen

**!** Mit der Erhebung der Räume schließen Sie die Strukturanalyse ab. Im Prinzip ist es auch möglich, abweichend von der hier vorgestellten und empfohlenen Reihenfolge mit der Erhebung der IT-Systeme und des Netzplans zu beginnen. In diesem Fall können Sie die Erhebung wichtiger Anwendungen erleichtern, wenn Sie zunächst Anwendungen betrachten, die von zentralen Komponenten