Bundesamt
für Sicherheit in der
Informationstechnik

Beispiel:

Bundesamt für Organisation und Verwaltung (BOV)

Stand: August 2008

Bundesamt für Sicherheit in der Informationstechnik
Referat IT-Sicherheitsmanagement und IT-Grundschutz

Postfach 20 03 63
53133 Bonn

Tel.: +49 228 99 9582- 5369
E-Mail: grundschutz@bsi.bund.de
Internet: http://www.bsi.bund.de/gshb

Inhaltsverzeichnis

1. Beispiel: Bundesamt für Organisation und Verwaltung (BOV)

Im Folgenden wird anhand einer fiktiven Behörde, dem Bundesamt für Organisation und Verwaltung (BOV), beispielhaft die Anwendung der IT-Grundschutz-Vorgehensweise beschrieben.

Das BOV ist eine imaginäre Bundesoberbehörde, die Organisationskonzepte, organisatorische Regelungen und Verwaltungsvorschriften für den Bundesbereich entwirft, diesbezügliche Beratungen durchführt und Schulungen anbietet. Das BOV ist eine Behörde mit 150 Mitarbeitern, von denen 130 an Bildschirmarbeitsplätzen arbeiten. Räumlich ist das Bundesamt in die Hauptstelle Bonn und eine Außenstelle in Berlin aufgeteilt. In Berlin werden unter anderem die Teilaufgaben Grundsatz, Normung und Koordinierung wahrgenommen. Von den insgesamt 130 Mitarbeitern mit IT-gestützten Arbeitsplätzen sind 90 in Bonn und 40 in Berlin tätig.

Um die Fachaufgaben leisten zu können, sind alle Arbeitsplätze vernetzt worden und besitzen einen Internet-Zugang. Die Außenstelle Berlin ist über eine angemietete Standleitung angebunden. Alle den Fachaufgaben zu Grunde liegenden Normen und Vorschriften sowie Formulare und Textbausteine sind ständig für jeden Mitarbeiter abrufbar. Alle relevanten Arbeitsergebnisse werden in eine zentrale Datenbank eingestellt. Entwürfe werden ausschließlich elektronisch erstellt, weitergeleitet und unterschrieben. Zur Realisierung und Betreuung aller benötigten Funktionalitäten ist in Bonn ein IT-Referat installiert worden.

Nachfolgend ist das Organigramm des BOV dargestellt:

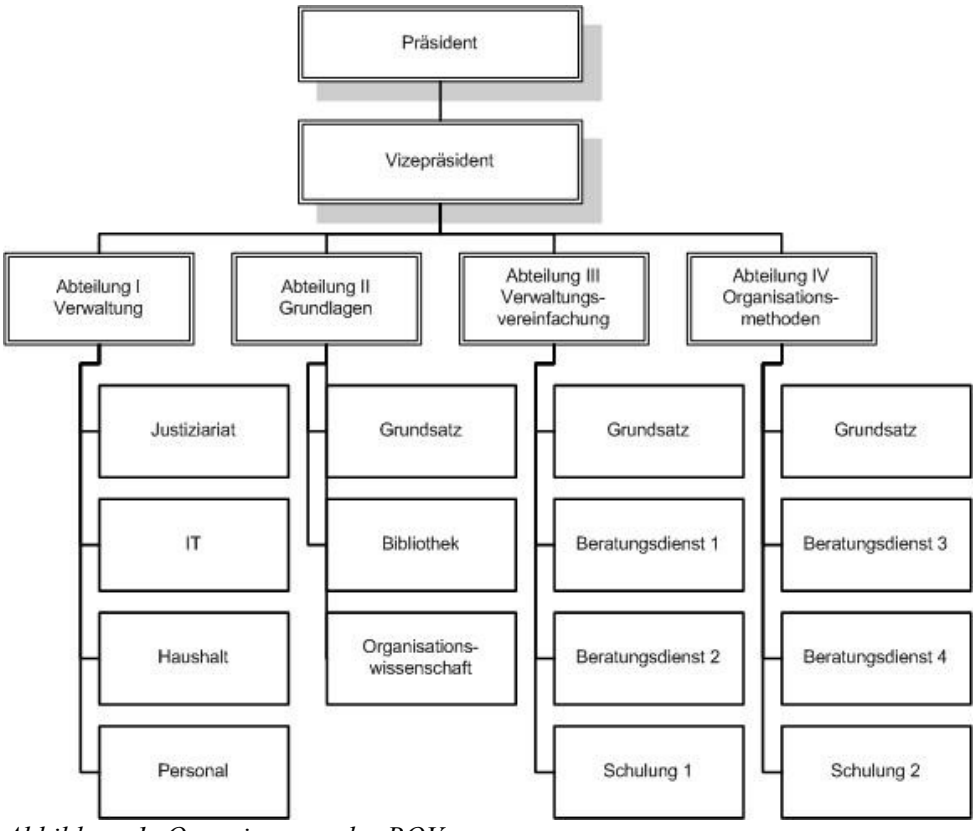

Abbildung 1: Organigramm des BOV

2. Strukturanalyse

2.1 Ergebnis: Erfassung der Anwendungen

Schwerpunkt der Tätigkeit des BOV ist die Beratung und Mitwirkung bei der Erarbeitung von Konzepten zur Verwaltungsvereinfachung und von Organisationsmethoden. Auf Anforderungen werden Erhebungen bei den Bedarfsträgern durchgeführt. Die hierbei gewonnenen allgemeingültigen Erkenntnisse werden über eine regelmäßig herausgegebene Schriftenreihe in anonymisierter und überarbeiteter Form auch anderen Interessenten als "Hilfe zur Selbsthilfe" zur Verfügung gestellt. Das BOV führt zudem Schulungsveranstaltungen zu diesen Themenbereichen durch.

Die Geschäftsprozesse des BOV werden elektronisch gepflegt und sind nach einem zweistufigen Schema benannt. Hinter dem Kürzel GP wird die Nummer des Hauptprozesses angegeben, die Nummer des Unterprozesses folgt nach einem Bindestrich, zum Beispiel GP0-2.

Nachfolgend wird ein Auszug aus der Erfassung der Anwendungen und der zugehörigen Informationen für das BOV dargestellt:

Nr.	Anwendung	Art der Information *	Verantwortlich	Anwender	Geschäftsprozesse
1	Personaldatenverarbeitung	P	Z1	Z1	GP0-1, GP0-2
2	Beihilfeabwicklung	P	Z2	alle	GP0-2
3	Reisekostenabrechnung	P/V/F	Z2	alle	GP0-1, GP0-3
4	Benutzer-Authentisierung	P/S	IT1	alle	GP0, GP5, GP6
5	Systemmanagement	S	IT3	IT3	alle
6	Bürokommunikation	P/V/F/S	IT3	alle	alle
7	zentrale Dokumentenverwaltung	P/V/F/S	Z1	alle	GP0, GP5
8	USB-Sticks zum Datenträgeraustausch	P/V/F	IT3	IT3	GP0-1, GP0-3

Tabelle 1: Erfassung der Anwendungen und zugehöriger Informationen

* Legende:

P = personenbezogene Daten

V = verwaltungsspezifische Informationen des BOV, beispielsweise Organisationsstrukturen und Dienstanweisungen

F = fachliche Informationen des BOV, beispielsweise Korrespondenz mit den Kunden

S = systemspezifische/technische Informationen, beispielsweise Konfigurationsdateien von IT-Systemen

Die Art der Information wird hier für jede Anwendung kurz miterfasst, um schneller einschätzen zu können, welcher Schutzbedarf sich für die jeweiligen Anwendungen ergibt, die diese Informationen verarbeiten.

2.2 Ergebnis: Netzplanerhebung

Einen geeigneten Ausgangspunkt für die weitere technische Analyse stellt ein Netzplan (beispielsweise in Form eines Netztopologieplans) dar. Ein Netzplan ist eine graphische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung. Netzpläne oder ähnliche graphische Übersichten sind auch aus betrieblichen Gründen in den meisten Institutionen vorhanden.

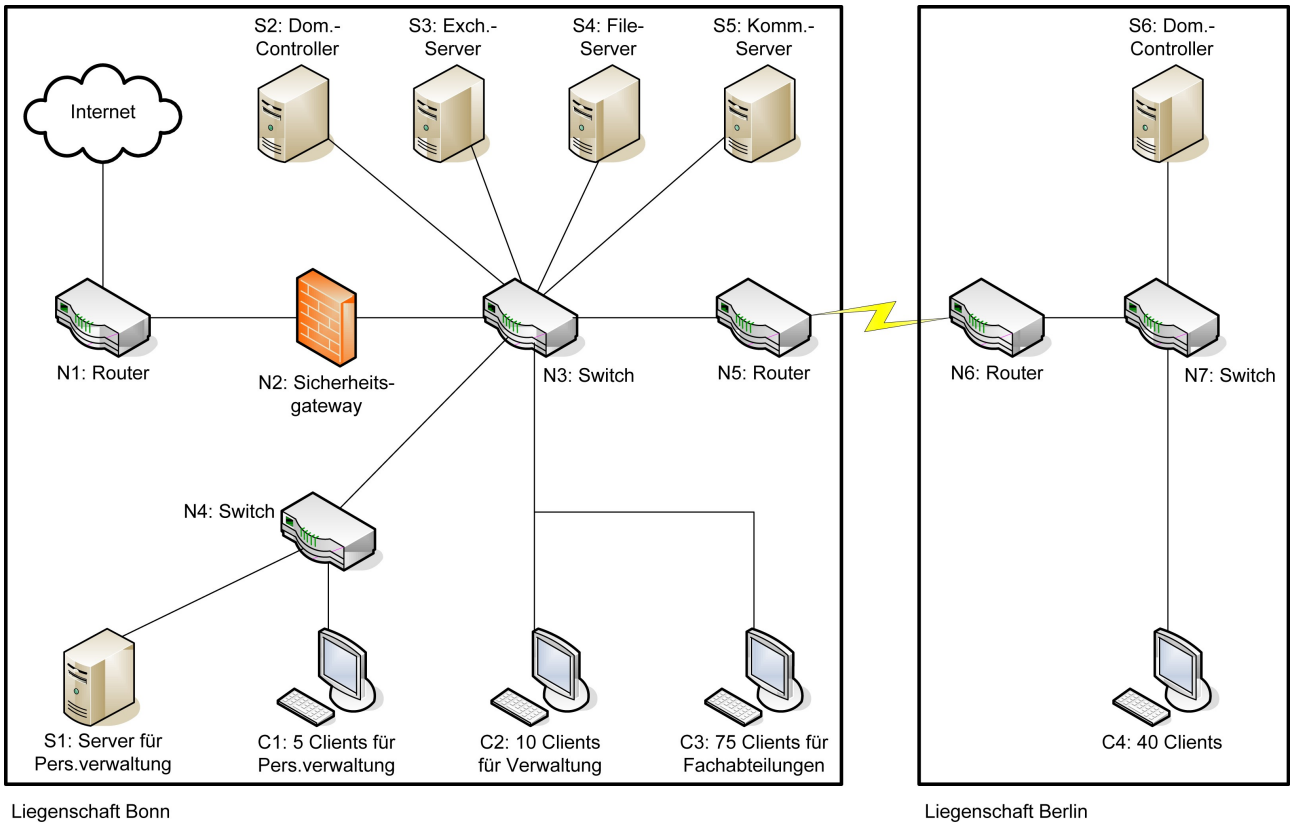

Abbildung 2: Bereinigter Netzplan

In dem dargestellten Netzplan sind die IT-Systeme durch eine Nummer (Server, Clients und aktive Netzkomponenten in der Form S*n*, C*n* bzw. N*n*) und die Funktion gekennzeichnet.

Sowohl in Bonn als auch in Berlin wurden die Clients in geeignete Gruppen zusammengefasst. Zwar sind alle 130 Clients nahezu gleich konfiguriert, sie unterscheiden sich jedoch im Hinblick auf die zu verarbeitenden Informationen, die Anwendungen, die Einbindung in das Netz und die infrastrukturellen Rahmenbedingungen. Die Gruppe C1 repräsentiert die 5 Clients in der Personalabteilung. Diese haben Zugriff auf den Server S1 der Personalabteilung in Bonn. C2 und C3 fassen die 10 Clients der Verwaltungsabteilung bzw. die 75 Clients der Fachabteilungen in Bonn zusammen. Sie unterscheiden sich lediglich im Hinblick auf die genutzten Anwendungsprogramme.

Schließlich werden durch die Gruppe C4 die Clients der Fachabteilungen in der Liegenschaft Berlin dargestellt. Von den Gruppen C1 bis C3 unterscheiden sie sich durch die umgebende Infrastruktur und die abweichende Einbindung in das Gesamtnetz.

Weiterhin kommen sowohl in der Liegenschaft Bonn als auch in Berlin IT-Systeme zum Einsatz, die nicht in das LAN eingebunden sind:

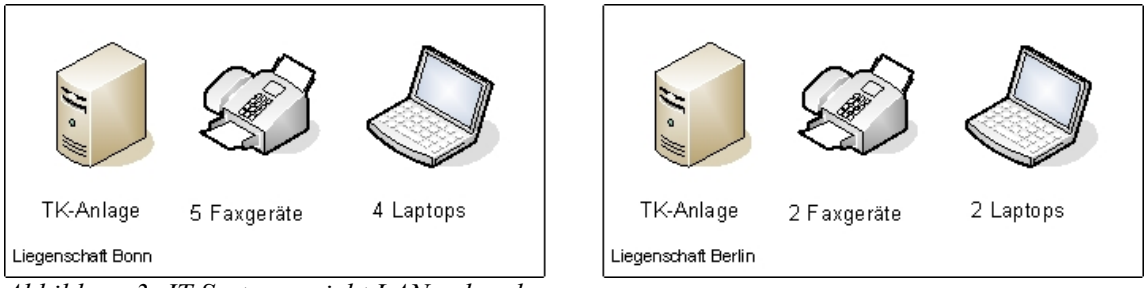

Abbildung 3: IT-Systeme, nicht LAN gebunden

2.3 Ergebnis: Erfassung der IT-Systeme

Die Erfassung der IT-Systeme des BOV ergibt folgende Übersicht:

Nr.	Beschreibung	Plattform	An-zahl	Aufstel-lungsort	Status	Anwender
S1	Server für Personalverwaltung	Server 2003	1	Bonn, R 1.01	in Betrieb	Personalreferat
S2	Primärer Domänen-Controller	Windows Server 2003	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
S3	Exchange-Server für E-Mail	Windows Server 2003	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
S4	File-Server für Arbeitsergebnisse und Grundlagendokumente	Unix-Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender außer Personalreferat
S5	Kommunikationsserver für Intranet	Unix-Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
S6	Backup-Domänen-Controller	Windows Server 2003	1	Berlin, R E.03	in Betrieb	alle IT-Anwender
S7	Faxserver	Unix-Server	1	Bonn, R 3.10	in Planung	alle IT-Anwender

Nr.	Beschreibung	Plattform	An-zahl	Aufstel-lungsort	Status	Anwender
C1	Gruppe von Clients der Personaldaten-verarbeitung	Windows Vista	5	Bonn, R 1.02 R 1.06	in Betrieb	Personalreferat
C2	Gruppe von Clients in der Verwaltungs-abteilung	Windows Vista	10	Bonn, R 1.07 R 1.16	in Betrieb	Verwaltungs-abteilung
C3	Gruppe von Clients in den Fachabteilungen II und III	Windows XP	75	Bonn, R 2.01 R 2.75	in Betrieb	Fachabteilung I und II
C4	Gruppe von Clients in der Fachabteilung IV	Windows XP	40	Berlin, R 2.01 - R 2.40	in Betrieb	Fachabteilung III
C5	Gruppe der Laptops für den Standort Bonn	Laptop unter Windows Vista	4	Bonn, R 1.06	in Betrieb	alle IT-Anwender in der Hauptstelle Bonn
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows Vista	2	Berlin, R 2.01	in Betrieb	alle IT-Anwender in der Außenstelle Berlin
N1	Router zum Internet-Zugang	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N2	Firewall	Applica-tion Gateway auf Unix	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N3	Switch	Switch	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N4	Switch für Personalbereich	Switch	1	Bonn, R. 1.01	in Betrieb	Personalreferat
N5	Router zur Berlin-Anbindung	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N6	Router zur Bonn-Anbindung	Router	1	Berlin, E.03	in Betrieb	alle IT-Anwender

Nr.	Beschreibung	Plattform	An-zahl	Aufstel-lungsort	Status	Anwender
N7	Switch	Switch	1	Berlin, E.03	in Betrieb	alle IT-Anwender
T1	TK-Anlage für Bonn	ISDN-TK-Anlage	1	Bonn, B.02	in Betrieb	alle Mitarbeiter in der Hauptstelle Bonn
T2	TK-Anlage für Berlin	ISDN-TK-Anlage	1	Berlin, E.03	in Betrieb	alle Mitarbeiter in der Außenstelle Berlin
T3	Gruppe Faxgeräte für Bonn	Faxgerät	5	Bonn, R 1.02, R 2.01, R 2.30, R 2.55, R 2.71	in Betrieb	alle Mitarbeiter in der Hauptstelle Bonn
T4	Gruppe Faxgeräte für Berlin	Faxgerät	2	Berlin, R 2.01 und R 2.21	in Betrieb	alle Mitarbeiter in der Außenstelle Berlin

Tabelle 2: Erfassung der IT-Systeme

Die erfassten Anwendungen des BOV und deren Zuordnung zu den IT-Systemen ergibt folgende Übersichten:

Server									
Beschreibung der Anwendungen			**IT-Systeme**						
Anw.-Nr.	**Anwendung/Informationen**	**Pers.-bez. Daten**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**
A1	Personaldatenverarbeitung	X	X						
A2	Beihilfeabwicklung	X	X						
A3	Reisekostenabrechnung	X	X						
A4	Benutzerauthentisierung	X		X				X	
A5	Systemmanagement			X					
A6	Exchange (E-Mail, Termin-kalender)	X			X				
A7	zentrale Dokumentenverwaltung					X			

Server									
Beschreibung der Anwendungen			**IT-Systeme**						
Anw.-Nr.	**Anwendung/Informationen**	**Pers.-bez. Daten**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**
A8	USB-Sticks zum Datenträger-austausch								
A9	BOV-Intranet						X		
A10	Datenbank der Grundlagendokumente						X		
A11	Printservice					X		X	
A12	Faxservice								X
A13	Office-Anwendungen (Textver-arbeitung, Tabellenkalkulation)								
A14	Internetzugang								
A15	Präsentationsdurchführung								
A16	Filterfunktionalität								
A17	Application-Gateway								
A18	TK-Vermittlung								
A19	Faxen								

Tabelle 3: Erfassung der Anwendungen mit Zuordnung zu den IT-Systemen (Server)

Legende: Sj X Ai bedeutet "Die Ausführung der Anwendung Ai hängt vom IT-System Sj ab."

Clients								
Beschreibung der Anwendungen			**Betroffene IT-Systeme**					
Anw.-Nr.	**Anwendung/Informationen**	**Pers.-bez. Daten**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**
A1	Personaldatenverarbeitung	X	X					
A2	Beihilfeabwicklung	X	X					
A3	Reisekostenabrechnung	X	X					
A4	Benutzerauthentisierung	X						
A5	Systemmanagement							
A6	Exchange (E-Mail, Termin-kalender)	X	X	X	X	X		
A7	zentrale Dokumentenverwaltung				X	X		
A8	USB-Sticks zum Datenträger-austausch		X	X	X	X	X	X
A9	BOV-Intranet		X	X	X	X		
A10	Datenbank der Grundlagen-dokumente				X	X		
A11	Printservice			X	X	X		
A12	Faxservice		X	X	X	X		
A13	Office-Anwendungen (Text-verarbeitung, Tabellen-kalkulation)		X	X	X	X	X	X
A14	Internetzugang		X	X	X	X		
A15	Präsentationsdurchführung						X	X
A16	Filterfunktionalität							
A17	Application-Gateway							
A18	TK-Vermittlung							
A19	Faxen							

Tabelle 4: Erfassung der Anwendungen mit Zuordnung zu den IT-Systemen (Clients)

Legende: Cj X Ai bedeutet "Die Ausführung der Anwendung Ai hängt vom IT-System Cj ab."

Netzkopplungselemente									
Beschreibung der Anwendungen			**Betroffene IT-Systeme**						
Anw. -Nr.	**Anwendung/Informationen**	**Pers.-bez. Daten**	**N1**	**N2**	**N3**	**N4**	**N5**	**N6**	**N7**
A1	Personaldatenverarbeitung	X				X			
A2	Beihilfeabwicklung	X				X			
A3	Reisekostenabrechnung	X				X			
A4	Benutzerauthentisierung	X			X	X	X	X	X
A5	Systemmanagement				X	X	X	X	X
A6	Exchange (E-Mail, Termin-kalender)	X	X	X	X	X	X	X	X
A7	zentrale Dokumentenverwaltung				X		X	X	X
A8	USB-Sticks zum Datenträger-austausch								
A9	BOV-Intranet				X	X	X	X	X
A10	Datenbank der Grundlagen-dokumente				X		X	X	X
A11	Printservice				X				X
A12	Faxservice				X	X	X	X	X
A13	Office-Anwendungen (Textver-arbeitung, Tabellenkalkulation)								
A14	Internetzugang		X	X	X	X	X	X	X
A15	Präsentationsdurchführung								
A16	Filterfunktionalität		X						
A17	Application-Gateway			X					
A18	TK-Vermittlung								

Netzkopplungselemente									
Beschreibung der Anwendungen			**Betroffene IT-Systeme**						
Anw.-Nr.	**Anwendung/Informationen**	**Pers.-bez. Daten**	**N1**	**N2**	**N3**	**N4**	**N5**	**N6**	**N7**
A19	Faxen								

Tabelle 5: Erfassung der Anwendungen mit Zuordnung zu den IT-Systemen (Netzkopplungselemente)

Legende: Nj X Ai bedeutet "Die Ausführung der Anwendung Ai hängt vom IT-System Nj ab."

Telekommunikationskomponenten						
Beschreibung der Anwendungen			**Betroffene IT-Systeme**			
Anw.-Nr.	**Anwendung/Informationen**	**Pers.-bez. Daten**	**T1**	**T2**	**T3**	**T4**
A1	Personaldatenverarbeitung	X				
A2	Beihilfeabwicklung	X				
A3	Reisekostenabrechnung	X				
A4	Benutzerauthentisierung	X				
A5	Systemmanagement					
A6	Exchange (E-Mail, Termin-kalender)	X				
A7	zentrale Dokumentenverwaltung					
A8	USB-Sticks zum Datenträger-austausch					
A9	BOV-Intranet					
A10	Datenbank der Grundlagen-dokumente					
A11	Printservice					
A12	Faxservice					

Telekommunikationskomponenten						
Beschreibung der Anwendungen			**Betroffene IT-Systeme**			
Anw.-Nr.	**Anwendung/Informationen**	**Pers.-bez. Daten**	**T1**	**T2**	**T3**	**T4**
A13	Office-Anwendungen (Text-verarbeitung, Tabellenkalkulation)					
A14	Internetzugang					
A15	Präsentationsdurchführung					
A16	Filterfunktionalität					
A17	Application-Gateway					
A18	TK-Vermittlung	X	X	X		
A19	Faxen				X	X

Tabelle 6: Erfassung der Anwendungen mit Zuordnung zu den IT-Systemen (Telekommunikations-komponenten)

Legende: Tj X Ai bedeutet "Die Ausführung der Anwendung Ai hängt vom IT-System Tj ab."

2.4 Ergebnis: Erfassung der Räume

Für die weitere Vorgehensweise der Modellierung nach IT-Grundschutz ist es hilfreich, eine Übersicht über die Liegenschaften, vor allem die Räume, zu erstellen, in denen IT-Systeme aufgestellt oder die für den IT-Betrieb genutzt werden. Dazu gehören Räume, die ausschließlich dem IT-Betrieb dienen (wie Serverräume, Datenträgerarchive), solche, in denen unter anderem IT-Systeme betrieben werden (wie Büroräume), aber auch die Wegstrecken, über die Kommunikations-verbindungen laufen. Wenn IT-Systeme statt in einem speziellen Technikraum in einem Schutz-schrank untergebracht sind, ist der Schutzschrank wie ein Raum zu erfassen.

Hinweis: Bei der Erhebung der IT-Systeme sind schon die Aufstellungsorte miterfasst worden.

Die nachfolgende Tabelle zeigt eine Übersicht über die Räume:

Raum			IT / Informationen
Bezeichnung	**Art**	**Lokation**	**IT-Systeme / Datenträger**
R 1.01	Serverraum	Gebäude Bonn	S1, N4

Raum			IT / Informationen
Bezeichnung	**Art**	**Lokation**	**IT-Systeme / Datenträger**
R 3.09	Serverraum	Gebäude Bonn	N1, N2, N3, N5
R 3.10	Serverraum	Gebäude Bonn	S2, S3, S4, S5, S7
B 02	Technikraum	Gebäude Bonn	T1
R 3.11	Schutzschrank im Raum R 3.11	Gebäude Bonn	Backup-Datenträger (Tages-sicherung der Server S1 bis S5)
R U.02	Datenträger-archiv	Gebäude Bonn	Backup-Datenträger (Wochen-sicherung der Server S1-S5)
R 1.02	Büroraum	Gebäude Bonn	C1, T3
R 1.06	Büroraum	Gebäude Bonn	C1, C5
R 1.07	Büroraum	Gebäude Bonn	C2,
R 1.16	Büroraum	Gebäude Bonn	C2
R 2.01	Büroraum	Gebäude Bonn	C3, T3, T4
R 2.75	Büroraum	Gebäude Bonn	C3
R 2.30	Büroraum	Gebäude Bonn	T3
R 2.55	Büroraum	Gebäude Bonn	T3
R 2.71	Büroraum	Gebäude Bonn	T3
R E.03	Serverraum	Gebäude Berlin	S6, N6, N7, T2

Raum			IT / Informationen
Bezeichnung	**Art**	**Lokation**	**IT-Systeme / Datenträger**
R 2.01 – R 2.40	Büroräume	Gebäude Berlin	C4, C6
R 2.21	Büroraum	Gebäude Berlin	T4

Tabelle 7: Raumübersicht

3. Schutzbedarfsfeststellung

3.1 Definition der Schutzbedarfskategorien

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich der IT-Grundschutz im Weiteren auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien unterteilt wird:

	Schutzbedarfskategorien
"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 8: Schutzbedarfskategorien

Die Schäden, die bei dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für einen Geschäftsprozess bzw. eine Anwendung einschließlich ihrer Daten entstehen können, lassen sich in Schadensszenarien einordnen. Um die Schutzbedarfskategorien "normal", "hoch" und "sehr hoch" voneinander abgrenzen zu können, bietet es sich an, die Grenzen für die einzelnen Schadens-szenarien zu bestimmen. Für das BOV wurden die Schutzbedarfskategorien wie folgt individualisiert:

Schutzbedarfskategorie "normal"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. - Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.

Schutzbedarfskategorie "normal"	
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. - Die maximal tolerierbare Ausfallzeit der Server und des LANs ist größer als 24 Stunden.
5. Negative Innen- oder Außenwirkung	- Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	- Der finanzieller Schaden ist kleiner als 25.000,- Euro.

Tabelle 9: Schadensszenarien der Schutzbedarfskategorie „normal“

Schutzbedarfskategorie "hoch"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. - Vertragsverletzungen mit hohen Konventionalstrafen.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. - Ein IT-Systemausfall ist nur zwischen einer und 24 Stunden tolerabel.

Schutzbedarfskategorie "hoch"	
5. Negative Innen- oder Außenwirkung	- Eine breite Ansehens- oder Vertrauens-beeinträchtigung ist erwarten.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden liegt zwischen 25.000,- Euro und 2.500.000,- Euro.

Tabelle 10: Schadensszenarien der Schutzbedarfskategorie „hoch“

Schutzbedarfskategorie "sehr hoch"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Fundamentaler Verstoß gegen Vorschriften und Gesetze. - Vertragsverletzungen, deren Haftungsschäden ruinös sind.
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Es handelt sich um personenbezogene Daten, durch deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. - Gefahr für Leib und Leben.
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. - Ein IT-Systemausfall ist nur bis zu einer Stunde tolerabel.
5. Negative Innen- oder Außenwirkung	- Eine landes- bzw. bundesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenz-gefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden ist größer als 2.500.000,- Euro.

Tabelle 11: Schadensszenarien der Schutzbedarfskategorie „sehr hoch“

3.2 Ergebnis: Schutzbedarfsfeststellung der Anwendungen

Der Schutzbedarf der Anwendungen fließt in die Schutzbedarfsfeststellung der betroffenen technischen und infrastrukturellen Objekte, wie zum Beispiel Server und Räume, ein. Um die Ergebnisse der Schutzbedarfsfeststellung und die daraus resultierenden Entscheidungen jederzeit nachvollziehen zu können, müssen diese gut dokumentiert werden. Dabei ist darauf zu achten, dass

nicht nur die Festlegung des Schutzbedarfs dokumentiert wird, sondern auch die entsprechenden Begründungen.

Zusammenstellung der wesentlichen Anwendungen, deren Schutzbedarf und die entsprechende Begründung:

Anwendung			**Schutzbedarfsfeststellung**		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
A1	Personaldaten-verarbeitung	X	Vertraulichkeit	hoch	Personaldaten sind besonders schutz-bedürftige personen-bezogene Daten, deren Bekannt werden die Betroffenen erheblich beeinträchtigen können.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfügbarkeit	normal	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A2	Beihilfeabwicklung	X	Vertraulichkeit	hoch	Beihilfedaten sind besonders schutz-bedürftige personenbezogene Daten, die zum Teil auch Hinweise auf Erkran-kungen und ärztliche Befunde enthalten. Ein Bekanntwerden kann die Betroffenen erheblich beeinträchtigen.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit	normal	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A3	Reisekosten-abrechnung	X	Vertraulichkeit	hoch	Die Daten der Reise-kostenabrechnung sind ebenfalls personen-bezogen und damit schützenswert.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfügbarkeit	normal	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A4	Benutzerauthen-tisierung		Vertraulichkeit	normal	Die gespeicherten Passwörter sind verschlüsselt gespeichert und damit praktisch nicht zugänglich.
			Integrität	hoch	Die Anmeldungen aller Mitarbeiter der Bonner Niederlassung für die Arbeit im Netz erfolgen über diese Anwendung. Auch die Mitarbeiter der Personalverwaltung authentisieren sich über diese Anwendung (Benutzerdatenbank des Servers S 2) gegenüber dem System S1. Hieraus folgt der hohe Schutz-bedarf.

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit	hoch	Bei Ausfall dieser Anwendung ist aufgrund der hierüber erfolgenden Authentisierung im Netz für alle Mitarbeiter praktisch der Einsatz von IT-gestützten Verfahren nicht möglich. Ein Ausfall der gesamten Anwendung ist allenfalls bis zu 24 Stunden hinnehmbar. Daher ist der Schutzbedarf "hoch".
A5	Systemmanagement		Vertraulichkeit	normal	Es werden keine vertraulichen Daten erzeugt oder gespeichert. Der Schutzbedarf ist normal.
			Integrität	hoch	Über die Anwendung Systemmanagement werden sämtliche Rechner der Organisation konfiguriert und administriert. Fehler in den Konfigurations-dateien können alle Rechner betreffen. Insbesondere besteht die Möglichkeit, dass auch Sicherheitseinstellungen beeinträchtigt werden können. Daher ist der Schutzbedarf "hoch".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit	normal	Sofern diese Anwendung ausfällt, ist es trotzdem möglich, die Administration und Konfiguration der Rechner manuell zu erledigen. Ein Ausfall bis zu 72 Stunden ist tragbar. Der Schutzbedarf ist "normal".
A6	Exchange (E-Mail, Terminkalender		Vertraulichkeit	normal	Es besteht ein striktes Verbot, vertrauliche Daten (z. B. Personaldaten) per E-Mail zu versenden. Die Daten, die auf diesem Server in Form von E-Mails gespeichert werden, besitzen daher lediglich normalen Schutzbedarf.
			Integrität	normal	Fehlerhafte E-Mails werden in der Regel erkannt und können keinen ernsthaften Schaden anrichten. Daher ist der Schutzbedarf "normal". Dies gilt auch unter Berücksichtigung der Nutzungshäufigkeit dieses Mediums.

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit	hoch	Sowohl die interne Kommunikation als auch die Kommunikation mit externen Behörden erfolgt in einem großen Umfang über E-Mail. Ein Ausfall dieses Systems führt zu einem erheblichen Ansehensverlust und ist daher allenfalls für 24 Stunden akzeptabel. Daher ist der Schutzbedarf "hoch".
A7	zentrale Dokumentenverwaltung		Vertraulichkeit	normal	Die Arbeitsergebnisse, die mit Hilfe dieser Anwendung gespeichert und verfügbar gemacht werden, sind nicht vertraulich. Sie werden z.T. veröffentlicht. Auch unter Berücksichtigung von Kumulationseffekten ergibt sich nur der Schutzbedarf "normal".
			Integrität	normal	Fehlerhafte Daten, die in dieser Anwendung gespeichert sind, werden erkannt und können nachträglich bereinigt werden. Der Schutzbedarf ist "normal".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit	hoch	Praktisch alle Mitarbeiter der Fachabteilungen sind für die Erfüllung der Aufgabe auf die mit dieser Anwendung verwalteten Daten angewiesen. Ein Ausfall ist allenfalls bis zu 24 Stunden hinnehmbar. Der Schutzbedarf ist daher "hoch".
A8	USB-Sticks zum Datenträgeraustausch		Vertraulichkeit	normal	Es werden mit dieser Anwendung keine vertraulichen Daten verarbeitet. Gemäß Regelungen zum Datenträgeraustausch ist das Speichern von personenbezogenen Daten auf USB-Sticks nicht zulässig. Der Schutzbedarf ist "normal".
			Integrität	normal	USB-Sticks werden nur zum temporären Speichern zugelassen. Fehlerhafte Daten können in der Regel leicht erkannt und korrigiert werden Der Schutzbedarf ist "normal".
			Verfügbarkeit	normal	Ausfälle sind hinnehmbar, da lokale Kopien vorhanden sind. Der Schutzbedarf ist "normal".
A9	BOV Intranet		Vertraulichkeit	normal	Die Daten, die über diese Anwendung im Intranet bekanntgemacht werden, sind nicht vertraulich. Der Schutzbedarf ist daher "normal".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Integrität	normal	Fehlerhafte Daten im Intranet des BOV können in der Regel leicht erkannt und korrigiert werden. Der Schutzbedarf ist "normal".
			Verfügbarkeit	normal	Ausfälle der Anwendung bis zu 72 Stunden sind hinnehmbar. Der Schutzbedarf ist "normal".
A10	Datenbank für Grundlagendokumente		Vertraulichkeit	normal	Die Datenbank mit den Grundlagendokumenten enthält nur Daten, die bereits veröffentlicht wurden. Der Schutzbedarf ist daher "normal".
			Integrität	hoch	Die in der Datenbank gespeicherten Grundlagendokumente sind die Grundlage für jede weitere Arbeit der Fachabteilungen. Die Mitarbeiter vertrauen auf die Richtigkeit der eingestellten Dokumente. Veränderungen werden nicht zuverlässig automatisch erkannt und führen zu fehlerhaften Arbeitsergebnissen. Der Schutzbedarf ist daher "hoch".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit	hoch	Diese Anwendung wird von jedem Mitarbeiter der Fachabteilung zur Erfüllung der Fach-aufgabe zwingend benötigt. Ausfälle sind allenfalls bis zu 24 Stunden tolerierbar. Hieraus folgt hoher Schutzbedarf.
A11	Printservice		Vertraulichkeit	normal	Mit dieser Anwendung werden keine vertraulichen Daten erzeugt oder verarbeitet. Die Personalabteilung benutzt diese Anwendung nicht, da dort die Rechner mit lokalen Arbeits-platzdruckern ausgestattet sind. Der Schutzbedarf ist "normal".
			Integrität	normal	Sofern Daten fehlerhaft ausgedruckt werden, kann dies in der Regel leicht festgestellt und korrigiert werden. Der Schutzbedarf ist "normal".
			Verfügbarkeit	normal	Ausfälle bis zu 72 Stunden sind hinnehmbar, da auch noch lokale Arbeitsplatzdrucker vorhanden sind. Der Schutzbedarf ist "normal".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
A12	Faxservice		Vertraulichkeit	normal	Über den Faxserver sollen Dokumente mit anderen Behörden ausgetauscht werden. Diese Dokumente sollen keine vertraulichen Daten erhalten. Der Schutzbedarf ist "normal".
			Integrität	normal	Fehler in den übermittelten Dokumenten können rasch erkannt und korrigiert werden. Der Schutzbedarf ist "normal".
			Verfügbarkeit	normal	Die Kommunikation mittels Fax hat in den letzten Jahren im BOV mit Einführung von E-Mail erheblich an Bedeutung verloren. Der Faxserver wird lediglich angeschafft, um die Verteilung eingehender Fax-Sendungen zu vereinfachen. Außerdem ist beabsichtig, nach endgültiger Freigabe des Faxservers sowohl in Bonn als auch in Berlin die bisher vorhandenen Faxgeräte als Ausfallreserve vor-zuhalten. Ein Ausfall des Systems von bis zu 4 Tagen ist hinnehmbar. Der Schutzbedarf ist "normal".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
A13	Office-Anwendung (Textverarbeitung, Tabellenkalkulation)		Vertraulichkeit	normal	Mit dieser Anwendung werden keine vertraulichen Daten verarbeitet. Der Schutzbedarf ist "normal".
			Integrität	normal	Fehlerhafte Daten können in der Regel leicht erkannt und korrigiert werden. Zu erwartende Schäden aufgrund verfälschter Daten liegen deutlich unter 12.500,-- Euro. Der Schutzbedarf ist "normal".
			Verfügbarkeit	normal	Der Ausfall dieser Anwendung auf einem einzelnen Client ist über einen Zeitraum von bis zu 5 Tagen ist hinnehmbar. Während dieser Übergangszeit kann auf Papierbasis oder ersatzweise auf einem Laptop weitergearbeitet werden. Der Schutzbedarf ist "normal".
A14	Internetzugang		Vertraulichkeit	normal	Es werden mit dieser Anwendung keine vertraulichen Daten verarbeitet. Der Schutzbedarf ist daher "normal".
			Integrität	normal	Fehlerhafte Daten können in der Regel leicht erkannt und korrigiert werden. Der Schutzbedarf ist "normal".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit	hoch	Die Recherche im Internet ist wesentlicher Bestandteil der Tätigkeit innerhalb der Fachabteilungen. Ein Ausfall des Systems ist aufgrund der Betroffenheit vieler Mitarbeiter ledig für maximal 24 Stunden tragbar. Der Schutzbedarf ist "hoch".
A15	Präsentationsdurchführung		Vertraulichkeit	normal	Vorträge und Ergebnispräsentationen enthalten keine vertraulichen Daten. Der Schutzbedarf ist "normal".
			Integrität	normal	Fehlerhafte Daten können leicht erkannt und korrigiert werden. Der Schutzbedarf ist "normal".
			Verfügbarkeit	normal	Ausfälle bis zu 5 Werktagen sind hinnehmbar. In dringenden Fällen kann auf einen anderen Laptop zurückgegriffen werden. Der Schutzbedarf ist "normal".
A16	Filterfunktionalität		Vertraulichkeit	normal	Über diese Anwendungen werden keine vertraulichen Daten geleitet, da sie lediglich der Anbindung des Netzes an das Internet dient. Der Schutzbedarf ist "normal".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Integrität	hoch	An die Integrität der Routingtabelle und der Filterregeln sind hohe Anforderungen zu stellen, da ansonsten direkte Angriffe auf die Firewall möglich sind, was zu Netzeinbrüchen und der Kompromittierung vertraulicher Daten führen kann. Der Schutzbedarf ist "hoch".
			Verfügbarkeit	hoch	Die Recherche im Internet und die E-Mail, die durch diese Anwendung erst ermöglicht werden, sind wesentliche Bestandteile der Tätigkeit innerhalb der Fachabteilungen. Ein Ausfall des Systems ist aufgrund der Betroffen-heit vieler Mitarbeiter für maximal 24 Stunden tragbar. Der Schutzbedarf ist "hoch".
A17	Application-Gateway		Vertraulichkeit	normal	Die Firewall sichert das interne Netz gegen das Internet ab. Über dieses System werden keine vertraulichen Daten weitergeleitet. Der Schutzbedarf ist "normal".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Integrität	hoch	An die Integrität der Konfigurationsdaten und des Betriebssystems sind hohe Anforderungen zu stellen, da mögliche Netzeinbrüche zur Kompromittierung vertraulicher Daten führen können. Der Schutzbedarf ist "hoch".
			Verfügbarkeit	hoch	Die Recherche im Internet und die E-Mail, die durch diese Anwendung erst ermöglicht werden, sind wesentliche Bestandteile der Tätigkeit innerhalb der Fachabteilungen. Ein Ausfall des Systems ist aufgrund der Betroffenheit vieler Mitarbeiter für maximal 24 Stunden tragbar. Der Schutzbedarf ist "hoch".
A18	TK-Vermittlung		Vertraulichkeit	normal	Ein Bekanntwerden der Daten beeinträchtigt die Betroffenen nur unerheblich. Der Schutzbedarf ist "normal".
			Integrität	normal	Fehler in der Konfiguration können leicht erkannt und korrigiert werden. Die zu erwartenden Schäden aufgrund fehlerhafter Gebührenerfassung liegen unter 500,-- Euro. Der Schutzbedarf ist "normal".

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit	hoch	Die TK-Anlage ist ein wesentliches Kommunikationsmittel. Ein Ausfall würde die Arbeitsfähigkeit des BOV wesentlich beeinträchtigen und außerdem zu einem erheblichen Ansehensverlust führen. Der Schutzbedarf ist "hoch".
A19	Faxen		Vertraulichkeit	normal	Über die Faxgeräte werden Dokumente mit anderen Behörden ausgetauscht. Diese Dokumente dürfen nach der bestehenden Dienstanweisung keine vertraulichen Daten erhalten. Der Schutzbedarf ist "normal".
			Integrität	normal	Veränderungen an den übermittelten Daten können leicht erkannt und schnell korrigiert werden. Der Schutzbedarf ist "normal".
			Verfügbarkeit	normal	Der Ausfall eines einzelnen Geräts führt nur zu minimalen Einschränkungen in der Erledigung der Fachaufgabe. Dies resultiert auch aus der Verlagerung auf E-Mail. Ausfälle bis zu 5 Tagen sind problemlos hinzunehmen. Der Schutzbedarf ist "normal".

Tabelle 12: Schutzbedarf der Anwendungen

3.3 Ergebnis: Schutzbedarfsfeststellung der IT-Systeme

Der Schutzbedarf der Anwendungen fließt in die Schutzbedarfsfeststellung für die jeweils betroffenen IT-Systeme ein.

Die Schutzbedarfsfeststellung der IT-Systeme im BOV ergibt folgende Einschätzungen:

IT-System		**Schutzbedarfsfeststellung**		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
S1	Server für Personalverwaltung	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip
S2	Primärer Domänen-Controller	Vertraulichkeit	normal	Maximumprinzip
		Integrität	hoch	Maximumprinzip
		Verfügbarkeit	normal	Gemäß der Schutzbedarfs-feststellung für Anwendung A4 ist von einem hohen Schutzbedarf für diesen Grundwert auszugehen. Zu berücksichtigen ist aber, dass diese Anwendung auf zwei Rechnersysteme verteilt ist. Eine Authentisierung über den Back-up Domänen-Controller in Berlin ist für die Mitarbeiter des Bonner Standortes ebenfalls möglich. Ein Ausfall des Primären Domänen-Controllers kann bis zu 72 Stunden hingenommen werden. Der Schutzbedarf ist aufgrund dieser Verteilung daher "normal".
S3	Exchange-Server für E-Mail	Vertraulichkeit	normal	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
S4	File-Server für Arbeitsergebnisse und Grundlagendokumente	Vertraulichkeit	normal	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	hoch	Der Schutzbedarf ergibt sich aus Anwendung A8.
S5	Kommunikations-server für Intranet	Vertraulichkeit	normal	Maximumprinzip
		Integrität	hoch	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip
S6	Backup-Domänen-Controller	Vertraulichkeit	normal	Maximumprinzip
		Integrität	hoch	Maximumprinzip
		Verfügbarkeit	normal	Für die Anwendung A4 wurden für den Grundwert "Verfügbarkeit“ der Schutzbedarf "hoch" festgestellt. Da die Benutzerauthentisierung sowohl auf dem Server S2 als auch auf dem Server S6 durchgeführt werden kann, ist ein Ausfall bis zu 72 Stunden hinnehmbar. Der Schutzbedarf ist daher "normal". Dies gilt auch hinsichtlich möglicher Kumulationseffekte mit der Anwendung A11.
S7	Faxserver	Vertraulichkeit	normal	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip
C1	Gruppe von Clients in der Personaldaten-verarbeitung	Vertraulichkeit	hoch	Maximumprinzip

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip
C2	Gruppe von Clients in der Verwaltungs-abteilung	Vertraulichkeit	normal	Auf den Clients werden keine vertraulichen Daten verarbeitet. Der Schutzbedarf ist "normal".
		Integrität	normal	Fehlerhafte Daten können in der Regel leicht erkannt und korrigiert werden. Zu erwartende Schäden aufgrund verfälschter Daten liegen deutlich unter 12.500,-- Euro. Der Schutzbedarf ist "normal".
		Verfügbarkeit	normal	Der Ausfall eines einzelnen Clients ist über einen Zeitraum von bis zu 5 Tagen ist hinnehmbar. Während dieser Übergangszeit kann auf Papierbasis weitergearbeitet werden.
C3	Gruppe von Clients in den Fachabteilungen II und III	Vertraulichkeit	normal	siehe C2.
		Integrität	normal	siehe C2.
		Verfügbarkeit	normal	siehe C2.
C4	Gruppe von Clients in der Fachabteilung IV	Vertraulichkeit	normal	siehe C2.
		Integrität	normal	siehe C2.
		Verfügbarkeit	normal	siehe C2.
C5	Laptop für den Standort Bonn	Vertraulichkeit	normal	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
C6	Laptop für den Standort Berlin	Vertraulichkeit	normal	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip
N1	Router zum Internet-zugang	Vertraulichkeit	normal	Maximumprinzip
		Integrität	hoch	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip
N2	Firewall	Vertraulichkeit	normal	Maximumprinzip
		Integrität	hoch	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip
N3	Switch	Vertraulichkeit	normal	Es handelt sich um den zentralen Verteiler des BOV. Vertrauliche Daten fließen nicht über diese Netzkomponente. Der Schutzbedarf ist "normal".
		Integrität	normal	Fehlfunktionen können leicht erkannt und beseitigt werden. Der Schutzbedarf ist "normal".
		Verfügbarkeit	hoch	Der Switch ist die zentrale Komponente im Netz der Nieder-lassung in Bonn. Bei einem Ausfall wäre ein IT-gestütztes Arbeiten nicht mehr möglich. Ein Ausfall ist daher allenfalls 4 Stunden tolerierbar. Der Schutzbedarf ist "hoch".

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
N4	Switch für den Personalbereich	Vertraulichkeit	hoch	Über diesen Switch sind die Clients der Personalverwaltung mit dem Server S1 verbunden. Daher fließen über diese Netz-komponente vertrauliche Daten. Der Schutzbedarf ist daher ebenso wie beim Server S1 und den Clients C1 "hoch".
		Integrität	normal	Fehlfunktionen können leicht erkannt und beseitigt werden. Der Schutzbedarf ist "normal".
		Verfügbarkeit	normal	Ausfälle bis zu 5 Arbeitstagen können durch die Mitarbeiter durch manuelle Verfahren überbrückt werden. Der Schutzbedarf ist "normal".
N5	Router zur Berlin Anbindung	Vertraulichkeit	normal	Über dieses System fließen keinerlei vertrauliche Daten. Der Schutzbedarf ist daher "normal".
		Integrität	normal	Fehler in den übertragenen Daten können im Rahmen der üblichen Qualitätssicherung leicht erkannt und korrigiert werden. Der Schutzbedarf ist "normal".
		Verfügbarkeit	normal	Von einem Ausfall des Systems sind nur die Mitarbeiter der Berliner Außenstelle betroffen. Ausfallzeiten bis zu 3 Tagen sind hinnehmbar. Anfallende Daten können in der Zwischenzeit auf den lokalen Festplatten gespeichert werden. Der Schutzbedarf ist "normal".
N6	Router zur Bonn-Anbindung	Vertraulichkeit	normal	Über dieses System fließen keinerlei vertrauliche Daten. Der Schutzbedarf ist daher "normal".

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
		Integrität	normal	Fehler in den übertragenen Daten werden im Rahmen der üblichen Qualitätssicherung leicht erkannt und korrigiert. Der Schutzbedarf ist "normal".
		Verfügbarkeit	normal	Von einem Ausfall des Systems sind nur die Mitarbeiter der Berliner Außenstelle betroffen. Ausfallzeiten bis zu 3 Tagen sind hinnehmbar. Anfallende Daten können in der Zwischenzeit auf den lokalen Festplatten gespeichert werden. Der Schutzbedarf ist "normal".
N7	Switch	Vertraulichkeit	normal	Über dieses System fließen keinerlei vertrauliche Daten. Der Schutzbedarf ist daher "normal".
		Integrität	normal	Fehler in den übertragenen Daten werden im Rahmen der üblichen Qualitätssicherung leicht erkannt und korrigiert. Der Schutzbedarf ist "normal".
		Verfügbarkeit	normal	Von einem Ausfall des Systems sind nur die Mitarbeiter der Berliner Außenstelle betroffen. Ausfallzeiten bis zu 3 Tagen sind hinnehmbar. Anfallende Daten können in der Zwischenzeit auf den lokalen Festplatten gespeichert werden. Der Schutzbedarf ist "normal".
T1	TK-Anlage Bonn	Vertraulichkeit	normal	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip
T2	TK-Anlage Berlin	Vertraulichkeit	normal	Maximumprinzip

IT-System		Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**Grundwert**	**Schutzbedarf**	**Begründung**
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Für die Anwendung A18 wurde für den Grundwert "Verfügbarkeit" ein hoher Schutzbedarf ermittelt. Im Vergleich zur TK-Anlage in Bonn sind hier von einem Ausfall weniger Mitarbeiter betroffen. Außerhalb des BOV dürfte ein Ausfall dieses Systems in der Niederlassung Berlin kaum auffallen, da die Masse der Telefonate über die Bonner Zentrale geführt wird. Bei einem möglichen Ausfall hält sich daher auch der Ansehensverlust in Grenzen. Der Schutzbedarf ist "normal".
T3	Gruppe Faxgeräte Bonn	Vertraulichkeit	normal	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip
T4	Gruppe Faxgeräte Berlin	Vertraulichkeit	normal	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip

Tabelle 13: Schutzbedarfsfeststellung der IT-Systeme

3.4 Ergebnis: Schutzbedarfsfeststellung für Räume

Aus den Ergebnissen der Schutzbedarfsfeststellung der Anwendungen und der IT-Systeme kann der Schutzbedarf für die jeweiligen Liegenschaften bzw. Räume abgeleitet werden.

Dieser Schutzbedarf leitet sich aus dem Schutzbedarf der im jeweiligen Raum installierten IT-Systeme, verarbeiteten Informationen oder der Datenträger, die in diesem Raum gelagert und benutzt werden.

Raum			IT / Informationen	Schutzbedarf		
Bezeichnung	**Art**	**Lokation**	**Installierte IT**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
R U.02	Datenträgerarchiv	Gebäude Bonn	Backup-Datenträger (Wochensicherung der Server S1 bis S5)	hoch	hoch	normal
R B.02	Technikraum	Gebäude Bonn	TK-Anlage	normal	normal	hoch
R 1.01	Serverraum	Gebäude Bonn	S1, N4	hoch	hoch	normal
R 1.02 – R 1.06	Büroräume	Gebäude Bonn	C1	hoch	normal	normal
R 1.07 – R 1.16	Büroräume	Gebäude Bonn	C2	normal	normal	normal
R 2.01 – R 2.75	Büroräume	Gebäude Bonn	C3, einige mit Faxgeräten	normal	normal	normal
R 3.09	Serverraum	Gebäude Bonn	N1, N2, N3, N5	normal	hoch	hoch
R 3.10	Serverraum	Gebäude Bonn	S2, S3, S4, S5	normal	hoch	hoch
R 3.11	Schutzschrank im Raum R 3.11	Gebäude Bonn	Backup-Datenträger (Tagessicherung der Server S1 bis S5)	hoch	hoch	normal
R E.03	Serverraum	Gebäude Berlin	S6, N6, N7	normal	hoch	hoch
R 2.01 – R 2.40	Büroräume	Gebäude Berlin	C4, einige mit Faxgeräten	normal	normal	normal

Tabelle 14: Schutzbedarfsfeststellung der Räume

3.5 Ergebnis: Schutzbedarfsfeststellung der Kommunikationsverbindungen

Die Schutzbedarfsfeststellung der Kommunikationsverbindungen des BOV ergibt aufgrund der Einschätzungen des Schutzbedarfs der IT-Systeme folgendes Ergebnis:

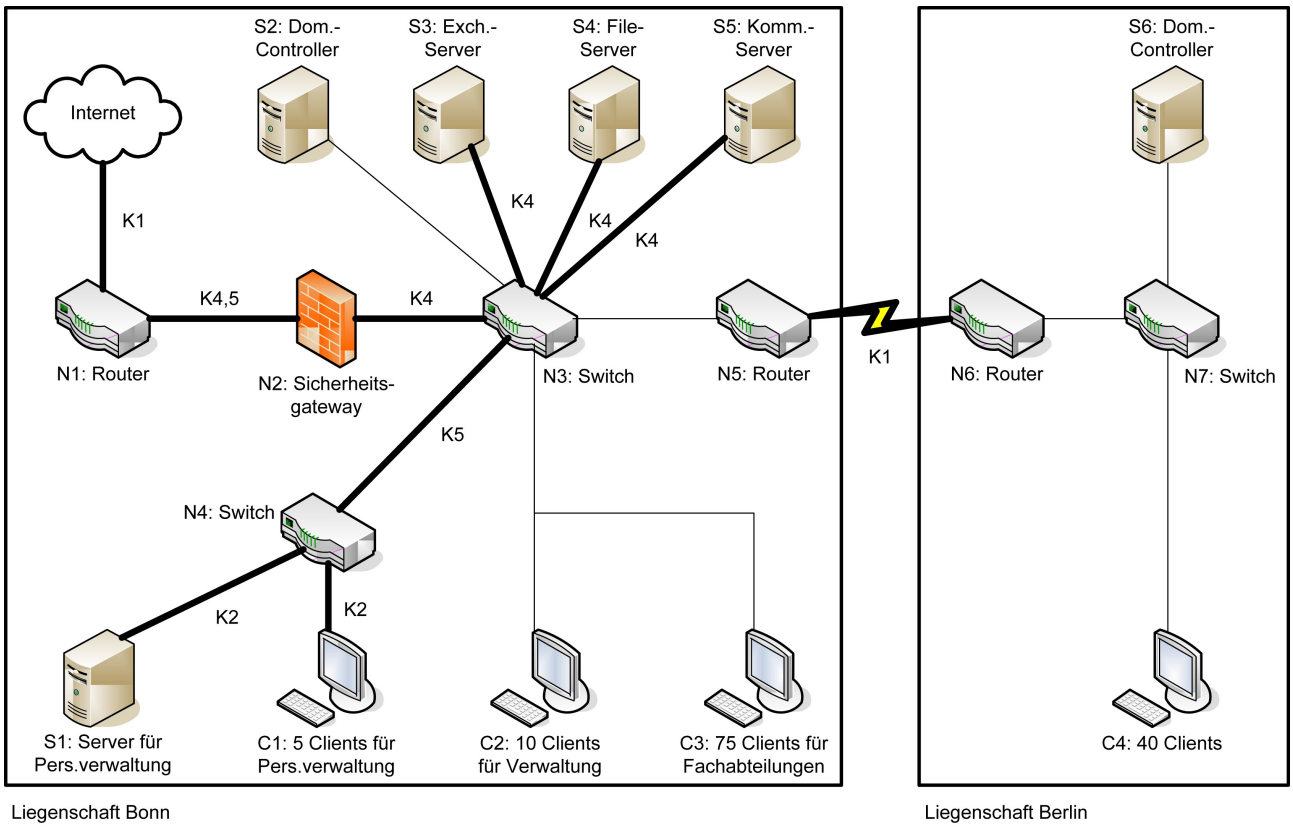

Abbildung 4: Kommunikationsverbindungen im BOV

In der graphischen Darstellung sind die kritischen Verbindungen durch "fette" Linien markiert. Die Linien sind mit dem Buchstaben "K" und einer nachfolgenden Zahl gekennzeichnet, deren Bedeutung in den Spaltenköpfen der nachfolgenden Tabelle erläutert wird.

Nr.	Verbindung	K1 Außen-verbindung	K2 hohe Ver-traulichkeit	K3 hohe Integrität	K4 hohe Verfügbarkeit	K5 keine Übertragung
1	N1 - Internet	X				
2	N5 – N6	X				
3	S1 – N4		X			
4	S3 – N3				X	
5	S4 – N3				X	
6	S5 – N3				X	

Nr.	Verbindung	K1 Außen-verbindung	K2 hohe Ver-traulichkeit	K3 hohe Integrität	K4 hohe Verfügbarkeit	K5 keine Übertragung
7	C1 – N4		X			
8	N1 – N2				X	X
9	N2 – N3				X	
10	N4 – N3					X

Tabelle 15: Bedeutung der Kommunikationsverbindungen des BOV

Begründungen für die Einstufung als kritische Verbindung:

Nr.	Begründung
1 und 2	Alle Kommunikationsverbindungen nach außen sind grundsätzlich als kritisch anzusehen und bedürfen einer besonderen Beachtung.
3	Diese Kommunikationsverbindung ist kritisch, da die übertragenen Daten vertraulich sind.
4 und 5	Diese Kommunikationsverbindung ist kritisch, da die Systeme S3 und S4 einen hohen Schutzbedarf für den Grundwert Verfügbarkeit haben. Die Verbindung erbt den Schutzbedarf, da keine redundante Verbindung vorhanden ist.
6	Diese Kommunikationsbeziehung ist kritisch, da das System S5 hohen Schutzbedarf für den Grundwert Verfügbarkeit aufweist. Die Kommunikationsverbindung erbt den Schutzbedarf für den Grundwert Integrität nicht, da die schutzbedürftigen Daten nicht in Gänze übertragen werden. Sie erbt jedoch den Schutzbedarf für den Grundwert Verfügbarkeit, da keine redundante Verbindung vorhanden ist.
7	Diese Kommunikationsbeziehung ist kritisch, da vertrauliche Personaldaten übertragen werden.
8	Diese Kommunikationsbeziehung erbt den hohen Schutzbedarf für den Grundwert „Verfügbarkeit“ vom System N1. Diese Kommunikationsbeziehung ist zudem kritisch, da verhindert werden muss, dass aus dem Internet auf das interne Netz unkontrolliert zugegriffen werden kann.
9	Diese Kommunikationsbeziehung erbt den hohen Schutzbedarf für den Grundwert „Verfügbarkeit“ vom System N2.
10	Diese Kommunikationsbeziehung ist kritisch, da hierüber keine vertraulichen Daten aus dem hinter dem Switch N4 liegenden Netzsegment übertragen werden dürfen. Insoweit handelt es sich hier um die Kopplung eines weniger schutzbedürftigen Netzes mit einem höher schutzbedürftigen.

Tabelle 16: Gründe für die Einstufung der Verbindungen

4. Modellierung eines Informationsverbunds

Ein im Einsatz befindlicher Informationsverbund enthält typischerweise geplante und bereits realisierte Anteile. Das Ergebnis ist ein IT-Grundschutzmodell, das sowohl einen Prüfplan als auch Anteile eines Entwicklungskonzepts enthält. Alle im Prüfplan und im Entwicklungskonzept vorgesehenen Sicherheitsmaßnahmen bilden gemeinsam die Basis für die Erstellung des Sicherheitskonzepts.

Die Modellierung nach IT-Grundschutz besteht darin, für die einzelnen Bausteine zu entscheiden, ob und wie sie zur Abbildung des Informationsverbundes herangezogen werden können. In den folgenden Tabellen erfolgt, getrennt nach den Schichten, die Zuordnung von Bausteinen zu Zielobjekten:

4.1 Modellierung übergeordneter Aspekte

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 1.0	Sicherheits-management	gesamtes BOV			
B 1.1	Organisation	Standort Bonn			Der Baustein Organisation muss für die Standorte Bonn und Berlin separat bearbeitet werden, da in Berlin eigene organisatorische Regelungen gelten.
B 1.1	Organisation	Standort Berlin			
B 1.2	Personal	gesamtes BOV			Die Personal-verwaltung des BOV erfolgt zentral in Bonn.
B 1.3	Notfallvorsorge-konzept	Standort Bonn			Das Notfallvorsorge-konzept ist für die hochverfügbaren IT-Systeme in Bonn zu bearbeiten.
B 1.4	Datensicherungs-konzept	gesamtes BOV			
B 1.6	Computer-Viren-schutzkonzept	gesamtes BOV			

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 1.7	Kryptokonzept	Standort Bonn			Da im BOV Daten mit hohem Vertraulich-keitsbedarf bearbeitet werden, ist dieser Baustein zu beachten. Es sollte eine Entscheidung fallen, ob kryptographische Mechanismen zum Einsatz kommen oder gleichwertige Ersatz-maßnahmen gewählt werden.
B 1.8	Behandlung von Sicherheits-vorfällen	gesamtes BOV			Da Daten und IT-Systeme mit hohem Verfügbarkeits- und Vertraulichkeitsbedarf vorhanden sind, ist dieser Baustein zu bearbeiten. Die Regelungen zur Behandlung von Sicherheitsvorfällen gelten sowohl für die Standorte Bonn und Berlin.
B 1.10	Standardsoftware	gesamtes BOV			Der Einsatz von Standardsoftware wird zentral am Standort Bonn verwaltet.

Tabelle 17: Modellierung der Schicht übergeordnete Aspekte

4.2 Modellierung der Infrastruktur

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 2.1	Gebäude	Liegenschaft Bonn			

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 2.1	Gebäude	Liegenschaft Berlin			
B 2.2	Elektrotechnische Verkabelung	Liegenschaft Bonn			Die Verkabelung ist in beiden Gebäuden jeweils einheitlich ausgeführt.
B 2.2	Elektrotechnische Verkabelung	Liegenschaft Berlin			
B 2.3	Büroraum	Büroräume der Personal-verwaltung	1 R 1.09 (Bonn)		Es soll ein Büroraum der Personalverwaltung untersucht werden. Dabei ist zu beachten, dass in den Büroräumen der Personalverwaltung vertrauliche Daten verarbeitet werden.
B 2.3	Büroraum	Büroräume der Zentral-abteilung und der Abteilungen II und III	2 R 1.15 R 2.08 (Bonn)		Als Stichprobe soll jeweils ein Büroraum der Zentralabteilung und der Fachab-teilungen untersucht werden.
B 2.3	Büroraum	Büroräume in Berlin	1 R 2.05 (Berlin)		Es ist ausreichend, in Berlin einen Büroraum zu untersuchen, da es sich dort um Standard-räume handelt.
B 2.4	Serverraum	R 1.01 (Bonn)			Der Baustein wird auf jeden Serverraum einmal angewandt.
B 2.4	Serverraum	R 3.09 (Bonn)			
B 2.4	Serverraum	R 3.10 (Bonn)			
B 2.4	Serverraum	R E.03 (Berlin)			

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 2.5	Datenträgerarchiv	R U.02 (Bonn)			In diesem Raum werden die Backup-Datenträger aufbewahrt.
B 2.6	Raum für Technische Infrastruktur	R B.02 (Bonn)			In diesem Raum ist die TK-Anlage installiert.
B 2.7	Schutzschränke	R 3.11 (Bonn)			In diesem Schutzschrank wird die Tagessicherung der Server aufbewahrt.

Tabelle 18: Modellierung der Schicht Infrastruktur

4.3 Modellierung der IT-Systeme

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 3.203	Laptop	C5	1 in R 1.06 (Bonn)		Die Laptops in Bonn bzw. Berlin werden jeweils in einer Gruppe zusammen-gefasst.
B 3.203	Laptop	C6	1 in R 2.01 (Berlin)		
B 3.201	Allgemeiner Client	C1	1 in R 1.09 (Bonn)		Ein Client aus der Personalverwaltung wird untersucht. Bei der Untersuchung ist zu beachten, dass die Rechner im Personal-referat einen hohen Schutzbedarf für den Grundwert "Vertraulichkeit" aufweisen.
B 3.201	Allgemeiner Client	C2	1 in R 1.15 (Bonn)		Ein Client aus der Zentralverwaltung wird als Stichprobe untersucht.

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 3.209	Client unter Windows XP	C3	1 in R 2.09 (Bonn)		Ein Client aus der Abteilung III wird als Stichprobe untersucht.
B 3.209	Client unter Windows XP	C4	1 in R 2.05 (Berlin)		Ein Client aus der Abteilung IV wird als Stichprobe untersucht.
B 3.201	Allgemeiner Client	C5	1 in R 1.06 (Bonn)		Hier wird jeweils die gleiche Stichprobe wie bei Baustein B 3.203 untersucht. Da noch kein Baustein zu Windows Vista veröffentlicht wurde, wird eine ergänzende Risiko-analyse und die Anwendung des Bausteins B 3.201 Allgemeiner Client empfohlen.
B 3.201	Allgemeiner Client	C6	1 in R 2.01 (Berlin)		
B 3.101	Allgemeiner Server	S1			In diesem Baustein werden die nicht Betriebssystem-spezifischen Sicherheitsaspekte bei Servern behandelt. Die Server S1 bis S6 und die Firewall N2 sind unterschiedlich konfiguriert. Der Baustein B 3.101 wird daher auf jedes dieser Systeme getrennt angewandt.
B 3.101	Allgemeiner Server	S2			
B 3.101	Allgemeiner Server	S3			
B 3.102	Server unter Unix	S4			

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 3.101	Allgemeiner Server	S5			
B 3.101	Allgemeiner Server	N2			
B 3.101	Allgemeiner Server	S6			
B 3.102	Server unter Unix	S5			Der Server S5 und die Firewall N2 werden unter Unix betrieben. Sie sind jedoch völlig unterschiedlich konfiguriert. Der Baustein B 3.102 wird daher getrennt auf diese beiden Systeme angewandt.
B 3.102	Server unter Unix	N2			
B 3.108	Windows Server 2003	S1			Die Server S1, S2, S3 und S6 werden unter Windows Server 2003 betrieben. Sie sind jedoch unterschiedlich konfiguriert. Der Baustein B 3.108 wird daher getrennt auf diese Systeme angewandt. Der Faxserver soll zwar auch unter Windows Server 2003 betrieben werden, ist aber noch in Planung. Eine Untersuchung ist daher gegenwärtig nicht angezeigt.
B 3.108	Windows Server 2003	S2			
B 3.108	Windows Server 2003	S3			
B 3.108	Windows Server 2003	S6			
B 3.102	Server unter Unix	S4			
B 3.401	TK-Anlage	T1 (Bonn)			

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 3.401	TK-Anlage	T2 (Berlin)			
B 3.402	Faxgerät	T3 (Bonn)	1		Aus den Faxgeräten in Bonn bzw. Berlin wird jeweils eine Stichprobe untersucht.
B 3.402	Faxgerät	T4 (Berlin)	1		
B 3.301	Sicherheits-gateway (Firewall)	N2			

Tabelle 19: Modellierung der Schicht IT-Systeme

4.4 Modellierung der Netze

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 4.1	Heterogene Netze	Netz in Bonn			Da die Netzsegmente aufgrund der geringen Anzahl an Systemen über-sichtlich sind, reicht es aus, diesen Baustein jeweils einmal für das gesamte Netz in Bonn bzw. Berlin zu bearbeiten.
B 4.1	Heterogene Netze	Netz in Berlin			
B 4.2	Netz- und Sys-temmanagement	gesamtes BOV			Als Plattform für das Systemmanagement wird S2 benutzt. Damit werden sämtliche Clients im BOV verwaltet.

Tabelle 20: Modellierung der Schicht Netze

4.5 Modellierung der Anwendungen

Bezeichnung	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stichprobe	Ansprech-partner	Hinweise
B 5.3	E-Mail	gesamtes BOV			
B 5.4	Webserver	S5			S5 dient als Server für das Intranet.
B 5.6	Faxserver	S 7			Der Faxserver ist gegenwärtig nicht Untersuchungsgegen stand, da er noch in Planung ist. Baustein B 5.6 wird aber bei der Planung des Servers berücksichtigt.
B 5.7	Datenbanken	S5			Auf dem Server S5 kommt eine Daten-bank zum Einsatz.

Tabelle 21: Modellierung der Schicht Anwendungen

5. Ergänzende Sicherheitsanalyse

Aufgrund der Schutzbedarfsfeststellung und der besonderen Einsatzbedingungen müssen für einige Zielobjekte Sicherheitsanalysen durchgeführt werden. Die folgende Tabelle zeigt einen Ausschnitt aus den Ergebnissen:

Zielobjekt	Ergänzende Sicherheitsanalyse, Auszüge aus dem Management-Report
Domänen-Controller S2	Aufgrund seiner zentralen administrativen Funktion bestehen an den Domänen-Controller S2 hohe Anforderungen in Bezug auf Integrität. Das System verfügt bereits über einige interne Mechanismen zum Schutz vor absichtlichen oder unabsichtlichen Manipulationen. Einige technische Zusatzmaßnahmen wurden geprüft, wegen mangelnder Kompatibilität mit anderen ein-gesetzten Produkten jedoch wieder verworfen. Die IT-Leitung schlägt deshalb vor, den erhöhten Sicherheitsanforderungen des Systems S2 auf organisatorischer Ebene durch häufige und regelmäßige Audits der IT-Revision Rechnung zu tragen. Auf eine weiterführende Risikoanalyse für S2 kann in diesem Fall verzichtet werden.

Zielobjekt	Ergänzende Sicherheitsanalyse, Auszüge aus dem Management-Report
Kritische Kommunikations-verbindungen N1-N2/Internet	Die Gefährdungslage, die sich durch die Anbindung des BOV an das Internet ergibt, hat sich im Berichtszeitraum stetig erhöht. Hervorzuheben sind hier insbesondere die Problemfelder Spam und Schadsoftware. Die IT-Leitung empfiehlt deshalb, für die Internet-Anbindung eine Risikoanalyse durchzuführen.
Kritische Kommunikations-verbindungen N3-S3/S4/S5/N2	An die genannten Kommunikationsverbindungen bestehen erhöhte Anforderungen in Bezug auf Verfügbarkeit. Im Zuge der technischen Neustrukturierung, die für das nächste Quartal geplant und genehmigt ist, wird der zentrale Switch N3 abgelöst. Die neue Struktur wird redundant ausgelegt sein, um Single-Points-of-Failure konsequent zu vermeiden. Da es sich bei den genannten kritischen Kommunikationsverbindungen deshalb nur noch um Übergangslösungen handelt, empfiehlt die IT-Leitung, auf eine Risikoanalyse für diese Verbindungen vorerst zu verzichten.
Serverraum R E.03 in Berlin	Die Anforderungen an die Verfügbarkeit der in R E.03 in Berlin betriebenen Informationstechnik sind erheblich. Eine Risikoanalyse für diesen Serverraum liegt zwar vor, ist jedoch veraltet. Die IT-Leitung empfiehlt deshalb, für R E.03 in Berlin eine neue Risikoanalyse durchzuführen.

Tabelle 22: Auszug aus den Ergebnissen der Ergänzenden Sicherheitsanalyse

6. Umsetzung der Sicherheitskonzeption

In folgender Tabelle werden einige zu realisierende Maßnahmen einschließlich der Kostenschätzungen dargestellt.

Zielobjekt	Baustein	Maßnahme	Status	Kosten	Bemerkung
Gesamte Organisation	B 1.9	M 2.11 Regelung des Passwortgebrauchs	T	a) 0,- Euro b) 2 PT c) 0,- Euro/Jahr d) 0,5 PT/Jahr	
Serverraum R 3.10	B 2.4	Z 1 Installation von Wasser ableitenden Blechen mit Überwachung mittels eines Wassermelders und Aufschaltung auf den Pförtner	N	a) 4000,- Euro b) 3 PT c) 0,- Euro/Jahr d) 1 PT/Jahr	Ersetzt Maßnahme M 1.24

Zielobjekt	Baustein	Maßnahme	Status	Kosten	Bemerkung
Server S4	B 3.101	M 1.28 Lokale unterbrechungsfreie Stromversorgung	N	a) 1000,- Euro b) 1 PT c) 0,- Euro/Jahr d) 0,5 PT/Jahr	
Gruppe Clients C1	B 3.207	Z 2 Chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten	N	a) 1400,- Euro b) 2 PT c) 0,- Euro/Jahr d) 2 PT/Jahr	Diese zusätzliche Maßnahme ersetzt die Maßnahme M 4.1 in Baustein B 1.9.
...					

Tabelle 23: Maßnahmen einschließlich Kosteneinschätzung

Legende:

Maßnahme
Z 1 = Zusatzmaßnahme 1 (zusätzlich zu IT-Grundschutz-Maßnahmen)

Status (= Umsetzungsstatus)
T = Teilweise erfüllt, N = Nicht realisiert
Kosten:

a) = einmalige Investitionskosten
b) = einmaliger Personalaufwand (PT = Personentage)
c) = wiederkehrende Investitionskosten
d) = wiederkehrender Personalaufwand (PT = Personentage)

Als nächstes wird der tabellarische Realisierungsplan (Auszug) dargestellt, der sich nach der Managemententscheidung aus obiger Tabelle ergeben würde.

Realisierungsplan (Stand 01.09.20xy)						
Zielobjekt	**Baustein**	**Maßnahme**	**Umsetzung bis**	**Verantwortlich**	**Budget-Rahmen**	**Bemerkung**
Gesamte Organisation	B 1.9	M 2.11 Regelung des Passwortgebrauchs	31.12. 20xy	a) Herr Müller b) Frau Meier	a) 0,- Euro b) 2 PT c) 0,- Euro/Jahr d) 0,5 PT/Jahr	

Realisierungsplan (Stand 01.09.20xy)						
Zielobjekt	**Baustein**	**Maßnahme**	**Umsetzung bis**	**Verantwortlich**	**Budget-Rahmen**	**Bemerkung**
Serverraum R 3.10	B 2.4	Z 1 Installation von Wasser ableitenden Blechen mit Überwachung mittels eines Wassermelders und Aufschaltung auf den Pförtner	30.04. 20xy	a) Herr Schmitz b) Herr Hofmann	a) 1000,- Euro b) 2 PT c) 0,- Euro/Jahr d) 1 PT/Jahr	Installation der Bleche lediglich unter frisch- und abwasserführenden Leitungen
Server S4	B 3.101	M 1.28 Lokale unterbrechungsfreie Stromversorgung	31.10. 20xy	a) Herr Schulz b) Frau Meier	a) 500,- Euro b) 1 PT c) 0,- Euro/Jahr d) 0,5 PT/Jahr	
Gruppe Clients C1	B 3.207	Z 2 Chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten	31.12. 20xy	a) Herr Schulz b) Frau Meier	a) 1400,- Euro b) 2 PT c) 0,- Euro/Jahr d) 2 PT/Jahr	
...						

Tabelle 24: Auszug aus einem Realisierungsplan

Legende:
Verantwortlich:
a) = Verantwortlich für die Umsetzung der Maßnahme
b) = Verantwortlich für die Kontrolle der Umsetzung

Budget-Rahmen: Für die Realisierung der Maßnahme stehen zur Verfügung
a) = einmalige Investitionskosten
b) = einmaliger Personalaufwand (PT = Personentage)
c) = wiederkehrende Investitionskosten
d) = wiederkehrender Personalaufwand (PT = Personentage)

Anhand dieser Informationen kann die Umsetzung der Maßnahmen überwacht und gesteuert werden.

7. Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

Um den Informationssicherheitsprozess im Unternehmen aufrecht zu erhalten und kontinuierlich verbessern zu können, ist es nicht ausreichend, angemessene Sicherheitsmaßnahmen zu implementieren und Dokumente stetig zu aktualisieren. Vielmehr muss der gesamte Informations-sicherheitsprozesses immer wieder überprüft werden, damit Fehler und Schwachstellen erkannt und abgestellt werden können und das Zusammenspiel von Strategie, Maßnahmen und organisatorischen Abläufen optimiert werden kann.