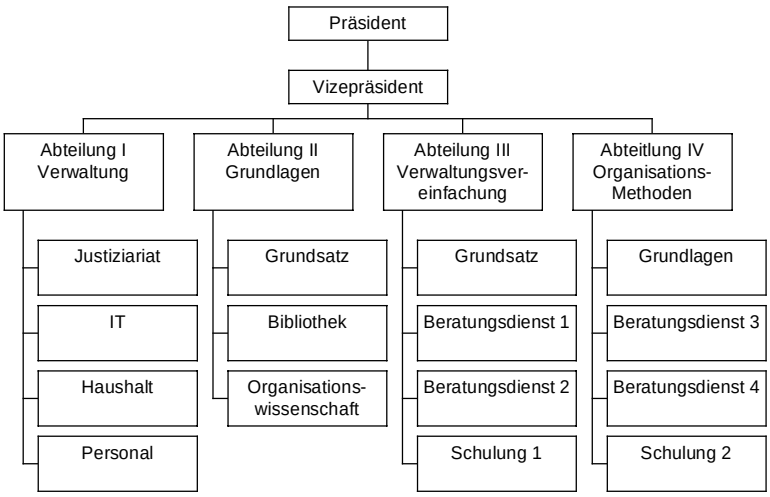
Beispiel: Bundesamt für Organisation und Verwaltung (BOV)

Im Folgenden wird anhand einer fiktiven Behörde, dem Bundesamt für Organisation und Verwaltung (BOV), beispielhaft beschrieben, wie das IT-Grundschutzhandbuch in den einzelnen Schritten angewandt wird.

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. Das BOV ist auf zwei Standorte verteilt, in Bonn ist die Haupstelle des BOV angesiedelt, in Berlin wird eine Außenstelle unterhalten. Von den insgesamt 130 Mitarbeitern mit IT-gestützten Arbeitsplätzen sind 90 in Bonn und 40 in Berlin tätig. Sämtliche Bildschirmarbeitsplätze besitzen einen Internet-Zugang.

Um die Dienstaufgaben leisten zu können, sind alle Arbeitsplätze vernetzt worden. Die Außenstelle Berlin ist über eine angemietete 2 Megabit-Standleitung angebunden. Alle zu Grunde liegenden Normen und Vorschriften sowie Formulare und Textbausteine sind ständig für jeden Mitarbeiter abrufbar. Sie werden zusammen mit allen relevanten Arbeitsergebnisse in einer zentralen Datenbank vorgehalten. 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:

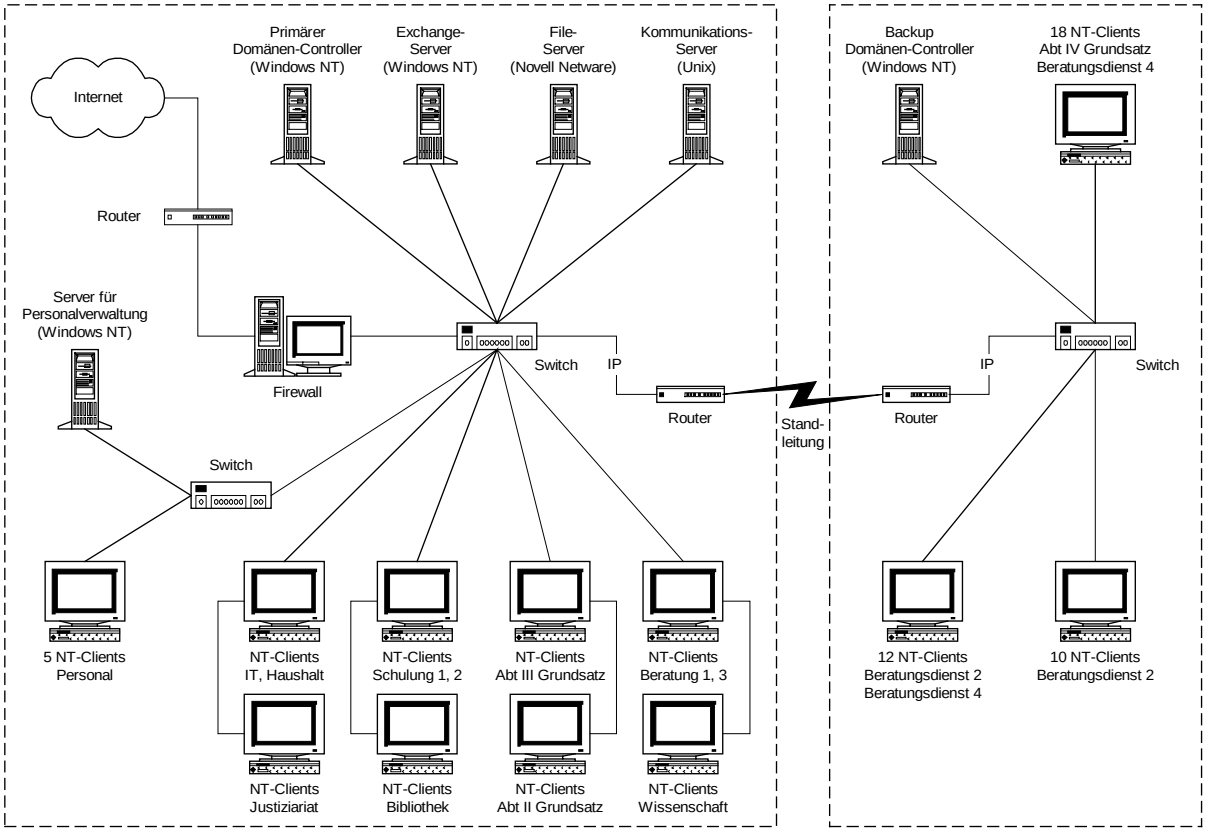


Fachaufgaben/Geschäftsprozesse BOV

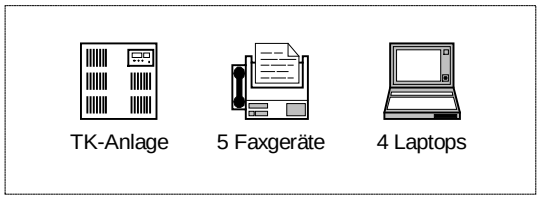
Das BOV berät Behörden in Fragen der Verwaltungsvereinfachung und der Organisationsmethoden. Dazu werden auf Anforderung auch Erhebungen bei den Bedarfsträgern durchgeführt. Schwerpunkt der Tätigkeit ist die Mitwirkung bei der Erarbeitung von Konzepten zur Verwaltungsvereinfachung und Organisation. Die hierbei gewonnenen allgemeingültigen Erkenntnisse werden über eine regelmäßig herausgebene Schriftenreihe in anonymisierter und überarbeiteter Form auch anderen Bedarfsträgern als "Hilfe zur Selbsthilfe" zur Verfügung gestellt. Das BOV führt zudem Schulungsveranstaltungen zu diesen Themenbereichen durch.

Ergebnis: Netzplanerhebung

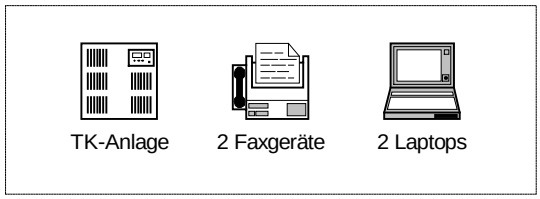
Für die vorhandene IT des BOV wurde ein Netzplan erarbeitet, der als Input für die IT-Strukturanalyse benutzt wird.



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



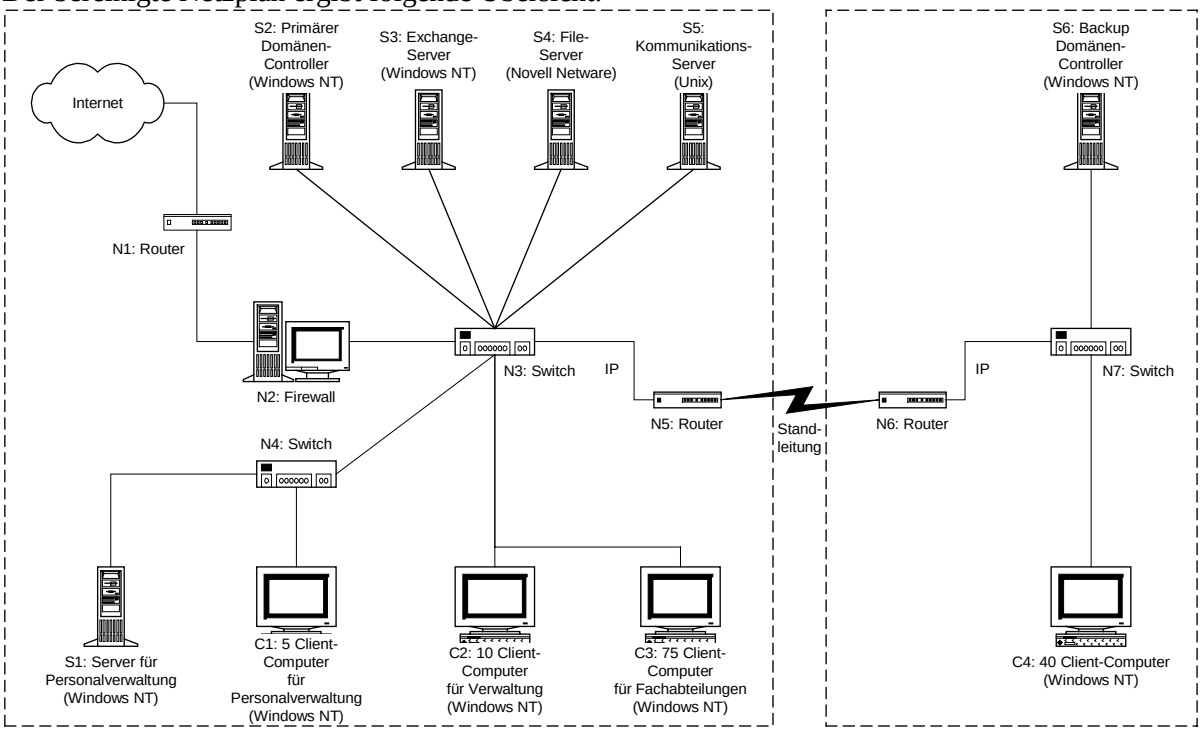
Liegenschaft Bonn



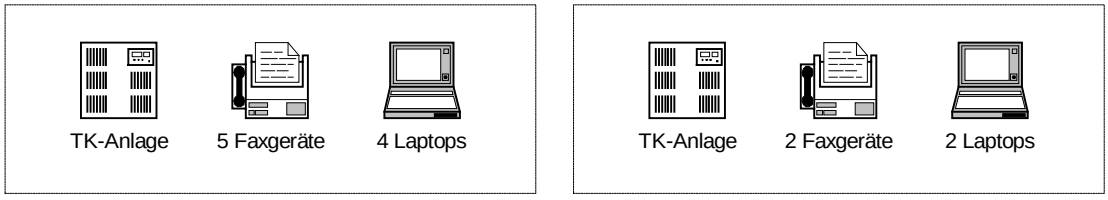
Liegenschaft Berlin

Ergebnis: Netzplan-Bereinigung

Der bereinigte Netzplan ergibt folgende Übersicht:



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



Liegenschaft Bonn Liegenschaft Berlin

Ergebnis: Erfassung der IT-Systeme

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

Nr.	Beschreibung	Plattform	Anzahl	Aufstel-lungsort	Status	Benutzer
S1	Server für Personalverwaltung	Windows NT-Server	1	Bonn, R 1.01	in Betrieb	Personalreferat
S2	Primärer Domänen-Controller	Windows NT-Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
S3	Exchange-Server für E-Mail	Windows NT-Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
S4	File-Server für Arbeitsergebnisse und Grundlagendokumente	Novell 4.x-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 NT-Server	1	Berlin, R E.03	in Betrieb	alle IT-Anwender
S7	Faxserver	Windows NT	1	Bonn, R 3.10	in Planung	alle IT-Anwender
C1	Gruppe von Clients der Personaldatenverarbeitung	Windows NT-Workstation	5	Bonn, R 1.02 - R 1.06	in Betrieb	Personalreferat
C2	Gruppe von Clients in der Verwaltungsabteilung	Windows NT-Workstation	10	Bonn, R 1.07 - R 1.16	in Betrieb	Verwaltungsabteilung
C3	Gruppe von Clients in den Fachabteilungen II und III	Windows NT-Workstation	75	Bonn, R 2.01 - R 2.75	in Betrieb	Fachabteilung I und II
C4	Gruppe von Clients in der Fachabteilung IV	Windows NT-Workstation	40	Berlin, R 2.01 - R 2.40	in Betrieb	Fachabteilung III
C5	Gruppe der Laptops für den Standort Bonn	Laptop unter Windows 95	4	Bonn, R 1.06	in Betrieb	alle IT-Anwender in der Haupstelle Bonn
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows 95	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	Application 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
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

Ergebnis: Erfassung der IT-Anwendungen

Die Erfassung der IT-Anwendungen des BOV und deren Zuordnung zu den IT-Systemen ergibt folgende Übersicht:

Server									
Beschreibung der IT-Anwendungen			**IT-Systeme**						
Anw.-Nr.	IT-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	Benutzerauthentifikation	X		X				X	
A5	Systemmanagement			X					
A6	Exchange (E-Mail, Terminkalender)	X			X				
A7	zentrale Dokumentenverwaltung					X			
A8	Printservice für Bonner Standort					X			
A9	BOV-Intranet						X		
A10	Datenbank der Grundlagendokumente						X		
A11	Printservice für Berliner Standort							X	
A12	Faxservice								X
A13	Office-Anwendungen (Textverarbeitung, Tabellenkalkulation)								
A14	Internetzugang								
A15	Präsentationsdurchführung								
A16	Filterfunktionalität								
A17	Application-Gateway								
A18	TK-Vermittlung								
A19	Faxen								

Legende: Sj X Ai bedeutet "Anwendung Ai ist mit dem IT-System Sj verknüpft"

Clients									
Beschreibung der IT-Anwendungen			**Betroffene IT-Systeme**						
Anw.-Nr.	IT-Anwendung/Informationen	Pers.-bez. Daten	C1	C2	C3	C4	C5	C6	
A1	Personaldatenverarbeitung	X	X						
A2	Beihilfeabwicklung	X	X						
A3	Reisekostenabrechnung	X	X						
A4	Benutzerauthentifikation	X							
A5	Systemmanagement								
A6	Exchange (E-Mail, Terminkalender)	X	X	X	X	X			
A7	zentrale Dokumentenverwaltung				X	X			
A8	Printservice für Bonner Standort			X	X				
A9	BOV-Intranet		X	X	X	X			
A10	Datenbank der Grundlagendokumente				X	X			
A11	Printservice für Berliner Standort					X			
A12	Faxservice		X	X	X	X			
A13	Office-Anwendungen (Textverarbeitung, Tabellenkalkulation)		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								

Legende: Sj X Ai bedeutet "Anwendung Ai ist mit dem IT-System Sj verknüpft"

Netzkopplungselemente									
Beschreibung der IT-Anwendungen			**Betroffene IT-Systeme**						
Anw.-Nr.	IT-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	Benutzerauthentifikation	X			X	X	X	X	X
A5	Systemmanagement				X	X	X	X	X
A6	Exchange (E-Mail, Terminkalender)	X	X	X	X	X	X	X	X
A7	zentrale Dokumentenverwaltung				X		X	X	X
A8	Printservice für Bonner Standort				X				
A9	BOV-Intranet				X	X	X	X	X
A10	Datenbank der Grundlagendokumente				X		X	X	X
A11	Printservice für Berliner Standort								X
A12	Faxservice				X	X	X	X	X
A13	Office-Anwendungen (Textverarbeitung, Tabellenkalkulation)								
A14	Internetzugang		X	X	X	X	X	X	X
A15	Präsentationsdurchführung								
A16	Filterfunktionalität		X						
A17	Application-Gateway			X					
A18	TK-Vermittlung								
A19	Faxen								

Legende: Sj X Ai bedeutet "Anwendung Ai ist mit dem IT-System Sj verknüpft"

Telekommunikationskomponenten									
Beschreibung der IT-Anwendungen			**Betroffene IT-Systeme**						
Anw.-Nr.	IT-Anwendung/Informationen	Pers.-bez. Daten	T1	T2	T3	T4			
A1	Personaldatenverarbeitung	X							
A2	Beihilfeabwicklung	X							
A3	Reisekostenabrechnung	X							
A4	Benutzerauthentifikation	X							
A5	Systemmanagement								
A6	Exchange (E-Mail, Terminkalender)	X							
A7	zentrale Dokumentenverwaltung								
A8	Printservice für Bonner Standort								
A9	BOV-Intranet								
A10	Datenbank der Grundlagendokumente								
A11	Printservice für Berliner Standort								
A12	Faxservice								
A13	Office-Anwendungen (Textverarbeitung, Tabellenkalkulation)								
A14	Internetzugang								
A15	Präsentationsdurchführung								
A16	Filterfunktionalität								
A17	Application-Gateway								
A18	TK-Vermittlung	X	X	X					
A19	Faxen				X	X			

Legende: Sj X Ai bedeutet "Anwendung Ai ist mit dem IT-System Sj verknüpft"

Ergebnis: Schutzbedarfsfeststellung der IT-Anwendungen:

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

Die Schutzbedarfskategorien wurden wie folgt für das BOV individualisiert:

Schutzbedarfskategorie "niedrig bis mittel"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen - Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. - Ein möglicher Mißbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
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 des IT- Systems ist größer als 24 Stunden.
5. Negative Außenwirkung	- Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	- Der finanzieller Schaden ist kleiner als 50.000,- DM.

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	- Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. - Ein möglicher Mißbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
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.
5. Negative Außenwirkung	- Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist erwarten.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden liegt zwischen 50.000,- DM und 5.000.000,-DM.

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	- Eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. - Ein möglicher Mißbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
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 Außenwirkung	- Ein landes- bzw. bundesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	Der finanzielle Schaden ist größer als 5.000.000,- DM.

IT-Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grund-wert**	**Schutz-bedarf**	**Begründung**
A1	Personaldatenverarbeitung	X	Vertrau-lichkeit	hoch	Personaldaten sind besonders schutzbedürftige personenbezogene Daten, deren Bekanntwerden die Betroffenen erheblich beeinträchtigen können.
			Integrität	mittel	Der Schutzbedarf ist nur mittel, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfüg-barkeit	mittel	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A2	Beihilfeabwicklung	X	Vertrau-lichkeit	hoch	Beihilfedaten sind besonders schutzbedürftige personenbezogene Daten, die z. T. auch Hinweise auf Erkrankungen und ärztliche Befunde enthalten. Ein Bekanntwerden kann die Betroffenen erheblich beeinträchtigen.
			Integrität	mittel	Der Schutzbedarf ist nur mittel, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfüg-barkeit	mittel	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A3	Reisekostenabrechnung	X	Vertrau-lichkeit	hoch	Die Daten der Reisekostenabrechnung sind ebenfalls personenbezogen und damit schützenswert.
			Integrität	mittel	Der Schutzbedarf ist nur mittel, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfüg-barkeit	mittel	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A4	Benutzerauthentifikation		Vertrau-lichkeit	mittel	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 Schutzbedarf.
			Verfüg-barkeit	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".

IT-Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grund-wert**	**Schutz-bedarf**	**Begründung**
A5	Systemmanagement		Vertrau-lichkeit	mittel	Es werden keine vertraulichen Daten erzeugt oder gespeichert. Der Schutzbedarf ist mittel.
			Integrität	hoch	Über die Anwendung Systemmanagement werden sämtliche Rechner der Organisation konfiguriert und administriert. Fehler in den Konfigurationsdateien können alle Rechner betreffen. Insbesondere erscheint es möglich, dass auch Sicherheitseinstellungen beeinträchtigt werden können. Daher ist der Schutzbedarf "hoch".
			Verfüg-barkeit	mittel	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 "mittel".
A6	Exchange (E-Mail, Terminka-lender		Vertrau-lichkeit	mittel	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 mittleren Schutzbedarf.
			Integrität	mittel	Fehlerhafte Mails werden in der Regel erkannt und können keinen ernsthaften Schaden anrichten. Daher ist der Schutzbedarf "mittel". Dies gilt auch unter Berücksichtigung der Nutzungshäufigkeit dieses Mediums.
			Verfüg-barkeit	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 Dokumentenverwal-tung		Vertrau-lichkeit	mittel	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 "mittel".
			Integrität	mittel	Fehlerhafte Daten, die in dieser Anwendung gespeichert sind, werden erkannt und können nachträglich bereinigt werden. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	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".

IT-Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grund-wert**	**Schutz-bedarf**	**Begründung**
A8	Printservice für Bonner Standort		Vertrau-lichkeit	mittel	Es werden mit dieser Anwendung keine vertraulichen Daten verarbeitet. Die Personalabteilung benutzt diese Anwendung nicht, da dort die Rechner mit lokalen Arbeitsplatzdruckern ausgestattet sind. Der Schutzbedarf ist "mittel".
			Integrität	mittel	Sofern Daten fehlerhaft ausgedruckt werden, kann dies in der Regel leicht festgestellt und korrigiert werden. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	mittel	Ausfälle bis zu 72 sind hinnehmbar, da auch noch lokale Arbeitsplatzdrucker vorhanden sind. Der Schutzbedarf ist "mittel".
A9	BOV Intranet		Vertrau-lichkeit	mittel	Die Daten, die über diese Anwendung im Intranet bekanntgemacht werden, sind nicht vertraulich. Der Schutzbedarf ist daher "mittel".
			Integrität	mittel	Fehlerhafte Daten im Intranet des BOV können in der Regel leicht erkannt und korrigiert werden. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	mittel	Ausfälle der Anwendung bis zu 72 Stunden sind hinnehmbar. Der Schutzbedarf ist "mittel".
A10	Datenbank für der Grundlagen-dokumente		Vertrau-lichkeit	mittel	Die Datenbank mit den Grundlagendokumenten enthält nur Daten, die bereits veröffentlicht wurden. Der Schutzbedarf ist daher "mittel".
			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".
			Verfüg-barkeit	hoch	Diese Anwendung wird von jedem Mitarbeiter der Fachabteilung zur Erfüllung der Fachaufgabe zwingend benötigt. Ausfälle sind allenfalls bis zu 24 Stunden tolerierbar. Hieraus folgt hoher Schutzbedarf.
A11	Printservice für Berliner Standort		Vertrau-lichkeit	mittel	Mit dieser Anwendung werden keine vertraulichen Daten erzeugt oder verarbeitet. Der Schutzbedarf ist "mittel".
			Integrität	mittel	Sofern Daten fehlerhaft ausgedruckt werden, kann dies in der Regel leicht festgestellt und korrigiert werden. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	mittel	Ausfälle bis zu 72 sind hinnehmbar, da auch noch lokale Arbeitsplatzdrucker vorhanden sind. Der Schutzbedarf ist "mittel".

IT-Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grund-wert**	**Schutz-bedarf**	**Begründung**
A12	Faxservice		Vertrau-lichkeit	mittel	Über den Faxserver sollen Dokumente mit anderen Behörden ausgetauscht werden. Diese Dokumente sollen keine vertrauliche Daten erhalten. Der Schutzbedarf ist "mittel".
			Integrität	mittel	Fehler in den übermittelten Dokumenten können rasch erkannt und korrigiert werden. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	mittel	Die Kommunikation mittels Fax hat in den letzten Jahren im BOV mit Einführung von E-Mail erheblich an Bedeutung verloren. 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 vorzuhalten. Ein Ausfall des Systems von bis zu 4 Tagen ist hinnehmbar. Der Schutzbedarf ist "mittel".
A13	Office-Anwendung (Textver-arbeitung, Tabellenkalkulation)		Vertrau-lichkeit	mittel	Mit dieser Anwendung werden keine vertraulichen Daten verarbeitet. Der Schutzbedarf ist "mittel".
			Integrität	mittel	Fehlerhafte Daten können in der Regel leicht erkannt und korrigiert werden. Zu erwartende Schäden aufgrund verfälschter Daten liegen deutlich unter 25.000,-- DM. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	mittel	Der Ausfall dieser Anwendung auf einem einzelen Clients 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 "mittel".
A14	Internetzugang		Vertrau-lichkeit	mittel	Es werden mit dieser Anwendung keine vertraulichen Daten verarbeitet. Der Schutzbedarf ist daher "mittel".
			Integrität	mittel	Fehlerhafte Daten können in der Regel leicht erkannt und korrigiert werden. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	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".

IT-Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grund-wert**	**Schutz-bedarf**	**Begründung**
A15	Präsentationsdurchführung		Vertrau-lichkeit	mittel	Vorträge und Ergebnispräsentationen enthalten keine vertrauliche Daten. Der Schutzbedarf ist "mittel".
			Integrität	mittel	Fehlerhafte Daten können leicht erkannt und korrigiert werden. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	mittel	Ausfälle bis zu 5 Werktagen sind hinnehmbar. In dringenden Fällen kann auf einen anderen Laptop zurückgegriffen werden. Der Schutzbedarf ist "mittel".
A16	Filterfunktionalität		Vertrau-lichkeit	mittel	Über diese Anwendungen werden keine vertrauliche Daten geleitet, da es lediglich der Anbindung des Netzes an das Internet dient. Der Schutzbedarf ist "mittel".
			Integrität	hoch	An die Integrität der Routingtabelle und der Filterregeln sind hohen Anforderungen zu stellen, da ansonsten direkte Angriffe auf die Firewall möglich sind, was zu Netzeinbrüchen und ggf. der Kompromittierung vertraulicher Daten führen kann. Der Schutzbedarf ist "hoch".
			Verfüg-barkeit	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 ledig für maximal 24 Stunden tragbar. Der Schutzbedarf ist "hoch".
A17	Applications-Gateway		Vertrau-lichkeit	mittel	Die Firewall sichert das interne Netz gegen das Internet ab. Über dieses System werden keine vertrauliche Daten weitergeleitet. Der Schutzbedarf ist "mittel".
			Integrität	hoch	An die Integrität der Konfigurationsdaten und des Betriebssystems sind hohe Anforderungen zu stellen, da ansonsten ggf. Netzeinbrüche möglich werden, die dazu führen können, dass vertrauliche Daten kompromittiert werden. Der Schutzbedarf ist "hoch".
			Verfüg-barkeit	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 ledig für maximal 24 Stunden tragbar. Der Schutzbedarf ist "hoch".

IT-Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grund-wert**	**Schutz-bedarf**	**Begründung**
A18	TK-Vermittlung		Vertrau-lichkeit	mittel	Ein Bekanntwerden der Daten beeinträchtigt die Betroffenen nur unerheblich. Der Schutzbedarf ist "mittel".
			Integrität	mittel	Fehler in der Konfiguration können leicht erkannt und korrigiert werden. Die zu erwartenden Schäden aufgrund fehlerhafter Gebührenerfassung liegen unter 1.000,-- DM. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	hoch	Die TK-Anlage ist ein wesentliches Kommunikationsmittel. Ein Aufall würde die Arbeitsfähigkeit des BOV erheblich beeinträchtigen und außerdem zu einem wesentlichen Ansehensverlust führen. Der Schutzbedarf ist "hoch".
A19	Faxen		Vertrau-lichkeit	mittel	Über die Faxgeräte werden Dokumente mit anderen Behörden ausgetauscht. Diese Dokumente dürfen nach der bestehenden Dienstanweisung keine vertrauliche Daten erhalten. Der Schutzbedarf ist "mittel".
			Integrität	mittel	Veränderungen an den übermittelten Daten können leicht erkannt und schnell korrigiert werden. Der Schutzbedarf ist "mittel".
			Verfüg-barkeit	mittel	Der Ausfall eines einzelnen Gerätet führt nur zu minimalen Einschränkungen in der Erledigung der Fachaufgabe. Dies resultiert auch aus der Verlagerung auf die E-Mail. Ausfälle bis zu 5 Tagen sind problemlos hinzunehmen. Der Schutzbedarf ist "mittel".

Ergebnis: Schutzbedarfsfeststellung der IT-Systeme

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

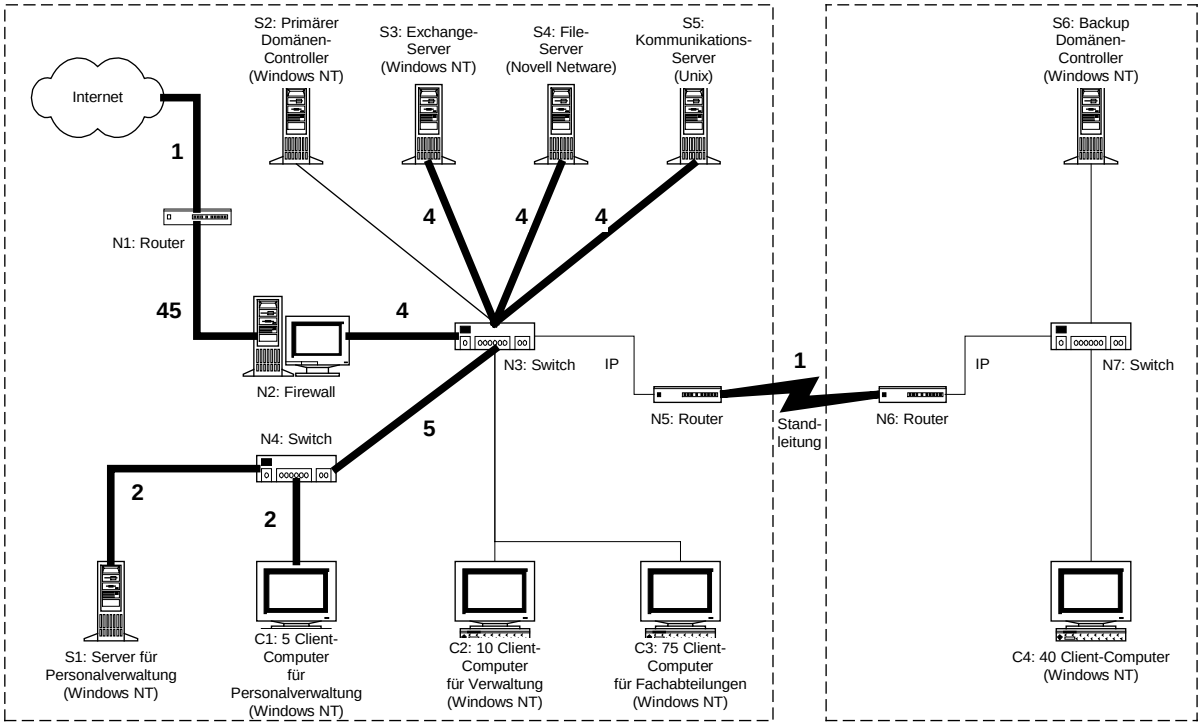
IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutz-bedarf**	**Begründung**
S1	Server für Personalverwaltung	Vertraulichkeit	hoch	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Maximumprinzip.
S2	Primärer Domänen-Controller	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	hoch	Maximumprinzip.
		Verfügbarkeit	mittel	Gemäß der Schutzbedarfsfeststellung für Anwendung A 4 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 "mittel".
S3	Exchange-Server für E-Mail	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	hoch	Maximumprinzip.
S4	File-Server für Arbeitsergebnisse und Grundlagendokumente	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	hoch	Der Schutzbedarf ergibt sich aus Anwendung A 8.
S5	Kommunikationsserver für Intranet	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	hoch	Maximumprinzip.
		Verfügbarkeit	hoch	Maximumprinzip.
S6	Backup-Domänen-Controller	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	hoch	Maximumprinzip.
		Verfügbarkeit	mittel	Für die Anwendung A 4 wurden für den Grundwert "Verfügbarkeit der Schutzbedarf "hoch" festgestellt. Da die Benutzerauthentikation aber sowohl auf dem Server S2 als auch auf dem Server S 6 möglich ist, ist ein Ausfall bis zu 72 Stunden hinnehmbar. Der Schutzbedarf ist daher "mittel". Dies gilt auch hinsichtlich möglicher Kumulationseffekte mit der Anwendung A 11.
S7	Faxserver	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Maximumprinzip.
C1	Gruppe von Clients in der Personaldatenverarbeitung	Vertraulichkeit	hoch	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Maximumprinzip.

IT-System		Schutzbedarfsfeststellung		
C2	Gruppe von Clients in der Verwaltungsabteilung	Vertraulichkeit	mittel	Auf den Clients werden keine vertraulichen Daten verarbeitet. Der Schutzbedarf ist "mittel".
		Integrität	mittel	Fehlerhafte Daten können in der Regel leicht erkannt und korrigiert werden. Zu erwartende Schäden aufgrund verfälschter Daten liegen deutlich unter 25.000,-- DM. Der Schutzbedarf ist "mittel".
		Verfügbarkeit	mittel	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	mittel	s. C2.
		Integrität	mittel	s. C2.
		Verfügbarkeit	mittel	s. C2.
C4	Gruppe von Clients in der Fachabteilung IV	Vertraulichkeit	mittel	s. C2.
		Integrität	mittel	s. C2.
		Verfügbarkeit	mittel	s. C2.
C5	Laptop für den Standort Bonn	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Maximumprinzip.
C6	Laptop für den Standort Berlin	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Maximumprinzip.
N1	Router zum Internetzugang	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	hoch	Maximumprinzip.
		Verfügbarkeit	hoch	Maximumprinzip.
N2	Firewall	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	hoch	Maximumprinzip.
		Verfügbarkeit	hoch	Maximumprinzip.
N3	Switch	Vertraulichkeit	mittel	Es handelt sich um den zentralen Verteiler des BOV. Vertrauliche Daten fließen nicht über diese Netzkomponente. Der Schutzbedarf ist "mittel".
		Integrität	mittel	Fehlfunktionen können leicht erkannt und beseitigt werden. Der Schutzbedarf ist "mittel".
		Verfügbarkeit	hoch	Der Switch ist die zentrale Komponente im Netz der Niederlassung 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".
N4	Switch für den Personalbereich	Vertraulichkeit	hoch	Über diesen Switch sind die Clients der Personalverwaltung mit dem Server S1 verbunden. Daher fließen über diese Netzkomponente vertrauliche Daten. Der Schutzbedarf ist daher ebenso wie beim Server S1 und den Clients C1 "hoch".
		Integrität	mittel	Fehlfunktionen können leicht erkannt und beseitigt werden. Der Schutzbedarf ist "mittel".
		Verfügbarkeit	mittel	Ausfälle bis zu 5 Arbeitstagen können durch die Mitarbeiter durch mauelle Verfahren überbrückt werden. Der Schutzbedarf ist "mittel".

IT-System		Schutzbedarfsfeststellung		
N5	Router zur Berlin-Anbindung	Vertraulichkeit	mittel	Über dieses System fließen keinerlei vertrauliche Daten. Der Schutzbedarf ist daher "mittel".
		Integrität	mittel	Fehler in den übertragenen Daten können im Rahmen der üblichen Qualitätssicherung leicht erkannt und korrigiert werden. Der Schutzbedarf ist "mittel".
		Verfügbarkeit	mittel	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 "mittel".
N6	Router zur Bonnanbindung	Vertraulichkeit	mittel	Über dieses System fließen keinerlei vertrauliche Daten. Der Schutzbedarf ist daher "mittel".
		Integrität	mittel	Fehler in den übertragenen Daten werden im Rahmen der üblichen Qualitätssicherung leicht erkannt und korrigiert. Der Schutzbedarf ist "mittel".
		Verfügbarkeit	mittel	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 "mittel".
N7	Switch	Vertraulichkeit	mittel	Über dieses System fließen keinerlei vertrauliche Daten. Der Schutzbedarf ist daher "mittel".
		Integrität	mittel	Fehler in den übertragenen Daten werden im Rahmen der üblichen Qualitätssicherung leicht erkannt und korrigiert. Der Schutzbedarf ist "mittel".
		Verfügbarkeit	mittel	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 "mittel".
T1	TK-Anlage Bonn	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	hoch	Maximumprinzip.
T2	TK-Anlage Berlin	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Für die Anwendung A 18 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 Auskall 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 "mittel".
T3	Gruppe Faxgeräte Bonn	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Maximumprinzip.
T4	Gruppe Faxgeräte Berlin	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Maximumprinzip.

Ergebnis: Schutzbedarfsfeststellung der Kommunikationsverbindungen

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



In der graphischen Darstellung sind die kritischen Verbindungen durch "fette" Linien markiert. Die Zahlen neben den Linien kennzeichnen den Grund (bzw. die Gründe), warum die jeweilige Verbindung kritisch ist, und sind in den Spaltenköpfen der nachfolgenden Tabelle erläutert.

Kritische Verbindungen								
Beschreibung der Verbindung		Kritisch aufgrund				Nicht übertragen werden dürfen Informationen mit		
Nr.	Verbindung	1 Außen-verbindung	2 hohe Ver-traulichkeit	3 hohe Integrität	4 hohe Ver-fügbarkeit	5 hoher Ver-traulichkeit	6 hoher Integrität	7 hoher Ver-fügbarkeit
1	N1 ⇔ Internet	X						
2	N5 ⇔ N6	X						
3	S1 ⇔ N4		X					
4	S3 ⇔N3				X			
5	S4 ⇔ N3				X			
6	S5 ⇔ N3				X			

Kritische Verbindungen								
Beschreibung der Verbindung		Kritisch aufgrund				Nicht übertragen werden dürfen Informationen mit		
7	C1 ⇔ N4		X					
8	N1 ⇔ N2				X	X		
9	N2 ⇔ N3				X			
10	N4 ⇔ N3					X		

Begründungen für die Einstufung als kritische Verbindung:

Nr.	Begründung
1 u. 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 u. 5	Diese Kommunikationsverbindung ist kritisch, da die Systeme S3 und S4 einen hohen Schutzbearf für den Grundwert Verfügbarkeit haben. Die Verbindung erbt den Schutzbedarf, da keine redundate 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 N 2
10	Diese Kommunikationsbeziehung ist kritisch, da hierüber keine vertrauliche Daten aus dem hinter dem Switch N 4 liegenden Netzsegment übertragen werden dürfen. Insoweit handelt es sich hier um die Kopplung eines weniger schutzbedürftigen Netz mit einem höher schutzbedürtigen.

Ergebnis: Schutzbedarfsfeststellung für IT-genutzte Räume

Raum			IT	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	mittel
R B.02	Technikraum	Gebäude Bonn	TK-Anlage	mittel	mittel	hoch
R 1.01	Serverraum	Gebäude Bonn	S1, N4	hoch	mittel	mittel
R 1.02 - R 1.06	Büroräume	Gebäude Bonn	C1	hoch	mittel	mittel
R 1.07-1.16	Büroräume	Gebäude Bonn	C2	mittel	mittel	mittel
R 2.01 - R 2.75	Büroräume	Gebäude Bonn	C3, einige mit Faxgeräten	mittel	mittel	mittel
R 3.09	Serverraum	Gebäude Bonn	N1, N2, N3, N5	mittel	hoch	hoch
R 3.10	Serverraum	Gebäude Bonn	S2, S3, S4, S5	mittel	hoch	hoch
R. 3.11	Schutzschrank im Raum R 3.11	Gebäude Bonn	Backup-Datenträger (Tagessicherung der Server S1 bis S5)	hoch	hoch	mittel
R E.03	Serverraum	Gebäude Berlin	S6, N6, N7	mittel	hoch	mittel
R 2.01 - R 2.40	Büroräume	Gebäude Berlin	C4, einige mit Faxgeräten	mittel	mittel	mittel

Modellierung übergeordneter Aspekte

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stich-probe	Ansprech-partner	Hinweise
3.0	IT-Sicherheits-management	gesamtes BOV			
3.1	Organisation	Standort Bonn			Der Baustein Organisation muss für die Standorte Bonn und Berlin separat bearbeitet werden, da in Berlin eigene organisatorische Regelungen gelten.
3.1	Organisation	Standort Berlin			
3.2	Personal	gesamtes BOV			Die Personalverwaltung des BOV erfolgt zentral in Bonn.
3.3	Notfallvorsorge-konzept	Standort Bonn			Das Notfallvorsorgekonzept ist für die hochverfügbaren IT-Systeme in Bonn zu bearbeiten.
3.4	Datensicherungs konzept	gesamtes BOV			
3.6	Computer-Virenschutz-konzept	gesamtes BOV			
3.7	Kryptokonzept	Standort Bonn			Da im BOV Daten mit hohem Vertraulichkeitsbedarf bearbeitet werden, ist dieser Baustein zu bearbeiten. Im Zuge dessen sollte die Entscheidung gefällt werden, ob kryptographische Mechanismen zum Einsatz kommen sollen oder ob gleichwertige Ersatzmaßnahmen gewählt werden.
3.8	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 Sicherheits-vorfällen gelten sowohl für die Standorte Bonn und Berlin.
9.1	Standardsoftware	gesamtes BOV			Der Einsatz von Standard-software wird zentral am Standort Bonn verwaltet.

Modellierung der Infrastruktur

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stich-probe	Ansprech-partner	Hinweise
4.1	Gebäude	Liegenschaft Bonn			
4.1	Gebäude	Liegenschaft Berlin			
4.2	Verkabelung	Liegenschaft Bonn			Die Verkabelung ist in beiden Gebäuden jeweils einheitlich ausgeführt.
4.2	Verkabelung	Liegenschaft Berlin			
4.3.1	Büroraum	Büroräume der Personalverwal-tung	1 R 1.09 (Bonn)		Es soll ein Büroraum der Personalverwaltung untersucht werden. Dabei ist zu beachten, dass in den Büroräumen der Personalverwaltung vertrau-liche Daten verarbeitet werden.
4.3.1	Büroraum	Büroräume der Zentralabteilung und der Abteilun-gen II und III	2 R 1.15 R 2.08 (Bonn)		Als Stichprobe soll jeweils ein Büroraum der Zentralabteilung und der Fachabteilungen unter-sucht werden.
4.3.1	Büroraum	Büroräume in Berlin	1 R 2.05 (Berlin)		Es ist ausreichend, in Berlin einen Büroraum zu unter-suchen, da es sich dort um Standardräume handelt.
4.3.2	Serverraum	R 1.01 (Bonn)			Der Baustein wird auf jeden Serverraum einmal angewandt.
4.3.2	Serverraum	R 3.09 (Bonn)			
4.3.2	Serverraum	R 3.10 (Bonn)			
4.3.2	Serverraum	R E.03 (Berlin)			
4.3.3	Datenträger-archiv	R U.02 (Bonn)			In diesem Raum werden die Backup-Datenträger aufbe-wahrt.
4.3.4	Raum für Technische Infrastruktur	R B.02 (Bonn)			In diesem Raum ist die TK-Anlage installiert.
4.4	Schutzschränke	R 3.11 (Bonn)			In diesem Schutzschrank wird die Tagessicherung der Server aufbewahrt.

Modellierung der IT-Systeme

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stich-probe	Ansprech-partner	Hinweise
5.3	Tragbarer PC	C5	1 in R 1.06 (Bonn)		Aus den Laptops in Bonn bzw. Berlin wird jeweils eine Stich-probe ausgewählt.
5.3	Tragbarer PC	C6	1 in R 2.01 (Berlin)		
5.5	PC unter Windows NT	C1	1 in R 1.09 (Bonn)		Ein Client aus der Personalverwaltung wird unter-sucht. Bei der Untersuchung ist zu beachten, dass die Rechner im Personalreferat einen hohen Schutzbearf für den Grundwert "Vertrauchlichkeit" aufweisen.
5.5	PC unter Windows NT	C2	1 in R 1.15 (Bonn)		Ein Client aus der Zentral-verwaltung wird als Stichprobe untersucht.
5.5	PC unter Windows NT	C3	1 in R 2.09 (Bonn)		Ein Client aus der Abteilung III wird als Stichprobe untersucht.
5.5	PC unter Windows NT	C4	1 in R 2.05 (Berlin)		Ein Client aus der Abteilung IV wird als Stichprobe untersucht.
5.6	PC unter Windows 95	C5	1 in R 1.06 (Bonn)		Hier wird jeweils die gleiche Stichprobe wie bei Baustein 5.3 untersucht. Baustein 5.6 behan-delt die Betriebssystem-spezifi-schen Aspekte.
5.6	PC unter Windows 95	C6	1 in R 2.01 (Berlin)		
6.1	Servergestütztes Netz	S1			In diesem Baustein werden die nicht Betriebssystem-spezifi-schen Sicherheitsaspekte bei Servern behandelt. Die Server S1 bis S6 und die Firewall N2 sind unterschiedlich konfigu-riert. Der Baustein 6.1 wird daher auf jedes dieser Systeme getrennt angewandt.
6.1	Servergestütztes Netz	S2			
6.1	Servergestütztes Netz	S3			
6.1	Servergestütztes Netz	S4			

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stich-probe	Ansprech-partner	Hinweise
6.1	Servergestütztes Netz	S5			
6.1	Servergestütztes Netz	N2			
6.1	Servergestütztes Netz	S6			
6.2	Unix-Server	S5			Der Server S5 und die Firewall N2 werden unter Unix betrieben. Sie sind jedoch völlig unterschiedlich konfiguriert. Der Baustein 6.2 wird daher getrennt auf diese beiden Systeme angewandt.
6.2	Unix-Server	N2			
6.4	Windows NT Netz	S1			Die Server S1, S2, S3 und S6 werden unter Windows NT 4.0 betrieben. Sie sind jedoch unterschiedlich konfiguriert. Der Baustein 6.4 wird daher getrennt auf diese Systema angewandt. Der Faxserver soll zwar auch unter Windows NT betrieben werden, ist aber noch in Planung. Eine Untersuchung ist daher gegenwärtig nicht angezeigt.
6.4	Windows NT Netz	S2			
6.4	Windows NT Netz	S3			
6.4	Windows NT Netz	S6			
6.6	Novell Netware 4.x	S4			
8.1	TK-Anlage	T1 (Bonn)			
8.1	TK-Anlage	T2 (Berlin)			
8.2	Faxgerät	T3 (Bonn)	1		Aus den Faxgeräten in Bonn bzw. Berlin wird jeweils eine Stichprobe untersucht.
8.2	Faxgerät	T4 (Berlin)	1		

Modellierung der Netze

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stich-probe	Ansprech-partner	Hinweise
6.7	Heterogene Netze	Netz in Bonn			Da die Netzsegmente aufgrund der geringen Anzahl an Systemen übersichtlich sind, reicht es aus, diesen Baustein jeweils einmal für das gesamte Netz in Bonn bzw. Berlin zu bearbeiten.
6.7	Heterogene Netze	Netz in Berlin			
6.8	Netz- und Systemmanage-ment	gesamtes BOV			Als Plattform für das Systemmanagement wird S2 benutzt. Damit werden sämtliche Clients im BOV verwaltet.
7.3	Firewall	N2			

Modellierung der Anwendungen

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Stich-probe	Ansprech-partner	Hinweise
7.4	E-Mail	gesamtes BOV			
7.5	WWW-Server	S5			S5 dient als Server für das Intranet.
8.5	Fax-Server	S 7			Der Fax-Server ist gegenwärtig nicht Untersuchungsgenstand, da er noch in Planung ist. Baustein 8.5 wird aber bei der Planung des Servers berücksichtigt.
9.2	Datenbanken	S5			Auf dem Server S5 kommt eine Datenbank zum Einsatz.