Security VU WS2009

Protokoll Gruppe 5

Lab2

Harald Demel, Matr. Nr. 0728129
tuempl@gmail.com
Richard Holzeis, Matr. Nr. 0726284
richard_holzeis@gmx.at
Manuel Mausz, Matr. Nr. 0728348
manuel-tu@mausz.at

Wien, am 16. Jänner 2010

Inhaltsverzeichnis

Phase 1: IT-Strukturanalyse....3
Erfassung der Anwendungen und der zugehörigen Informationen....3
Netzplanerhebung....4
Erhebung der IT-Systeme....5
Zuordnung der Anwendungen zu den betroffenen IT-Systemen....6
Erfassung der Räume....7
Phase 2: Schutzbedarfsfeststellung....8
Schutzbedarfsfeststellung für Anwendungen....8
Schutzbedarfsfeststellung für IT-Systeme....10
Schutzbedarfsfeststellung für Räume....12
Schutzbedarfsfeststellung für Kommunikationsverbindungen....13
Phase 3: Modellierung nach IT-Grundschutz....16
Modellierung des IT-Verbunds nach IT-Grundschutz....16
Phase 4: Basis-Sicherheitscheck....18
Schicht 1 - Übergegeordnete Aspekte der IT-Sicherheit....18
1.0 IT-Sicherheitsmanagement....18
1.1 Organisation....19
1.2 Personal....20
1.3 Notfallvorsorge-Konzept....21
1.4 Datensicherungskonzept....22
1.6 Computer-Virenschutzkonzept....23
1.9 Hard- und Software-Management....24
1.10 Standardsoftware....27
1.13 IT-Sicherheitssensibilisierung und Schulung....28
Schicht 3 - Sicherheit der IT-Systeme....29
3.102 Server unter Unix....29
3.209 Client unter Windows XP....31
Schicht 5 - Sicherheit in Anwendungen....33
5.3 E- Mail....33
5.7 Datenbanken....35
5.11 Apache-Webserver....37
Phase 5: Sicherheitsbewertung des IT-Verbunds....38

Phase 1: IT-Strukturanalyse

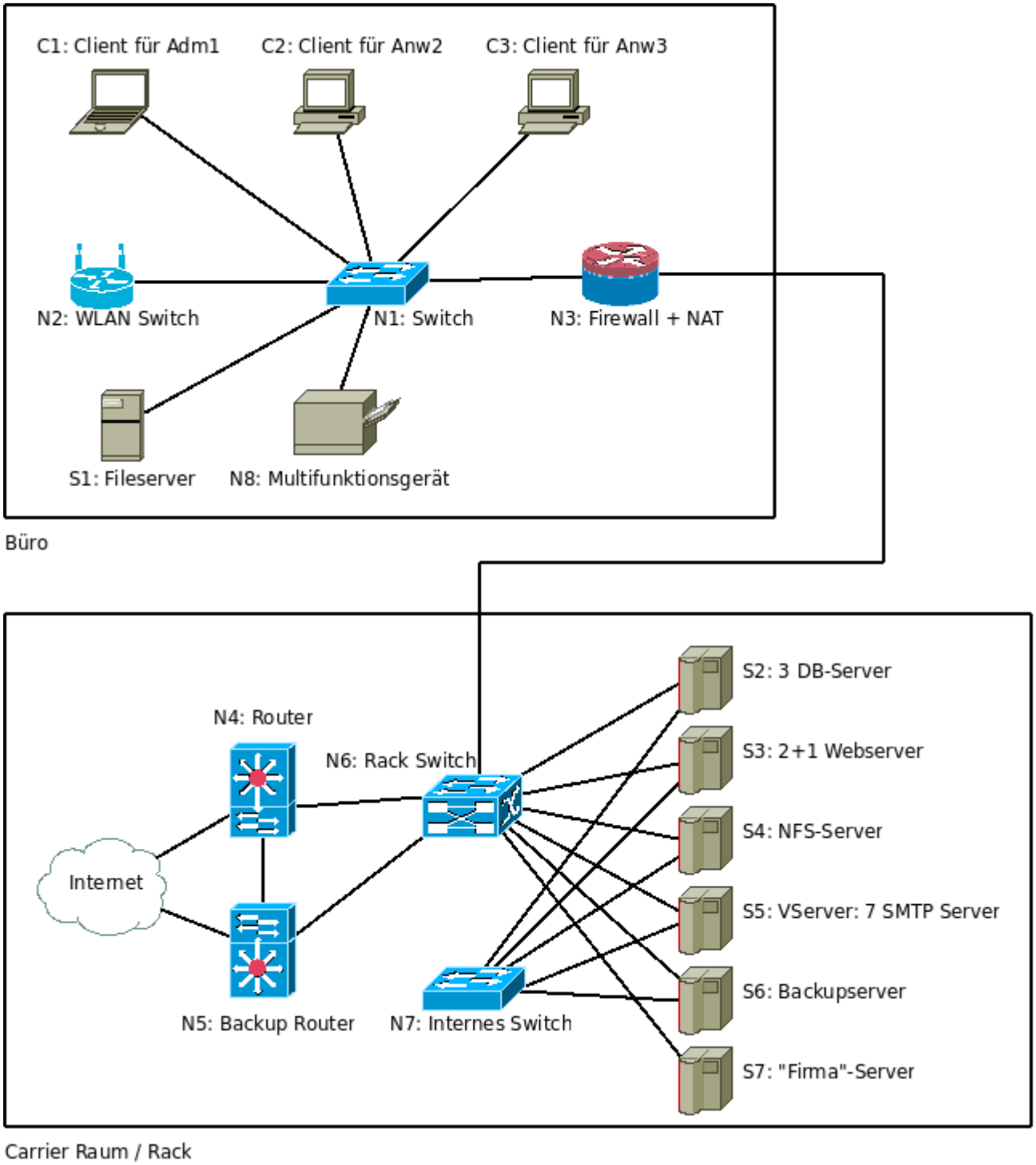
Erfassung der Anwendungen und der zugehörigen Informationen

Nr.	Anwendung	Art der Information	Verantwortlich	Benutzer
A1	Personaldatenverarbeitung	P	Anw3	Anw3
A2	Benutzerdatenverarbeitung	P/V/S	Adm1, Anw3	alle
A3	Systemmanagement	S	Adm1	alle
A4	Bürokommunikation	P/V/F/S	Adm1	alle
A5	DNS-Service	S	Adm1	alle
A6	Fileserver (intern)	P/V/F/S	Adm1	alle
A7	Fileserver	P/F/S	Adm1	alle
A8	HTTP-Service	S	Adm1	alle
A9	Datenbank-Service	P/F/S	Adm1	alle
A10	E-Mail-Service	P/V/F/S	Adm1	alle

Legende:

- P = personenbezogene Daten
- V = verwaltungsspezifische Informationen, beispielsweise Organisationsstrukturen und Dienstanweisungen
- F = fachliche Informationen, beispielsweise Korrespondenz mit den Kunden
- S = systemspezifische/technische Informationen, beispielsweise Konfigurationsdateien von IT-Systemen

Netzplanerhebung



Erhebung der IT-Systeme

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender
C1	Client für Adm1	Laptop, Linux	1	Haupt, R1	in Betrieb	Adm1
C2	Client für Anw2	Windows Vista	1	Haupt, R1	in Betrieb	Anw2
C3	Client für Anw3	Windows XP	1	Haupt, R1	in Betrieb	Anw3
N1	Büro Switch	Switch	1	Haupt, R1	in Betrieb	Adm1
N2	WLAN Switch	Switch	1	Haupt, R1	in Betrieb	Adm1
N3	Firewall + NAT + DHCP	Embedded Linux	1	Haupt, R1	in Betrieb	Adm1
S1	Fileserver	Linux	1	Haupt, R1	in Betrieb	Adm1
N8	Drucker, Fax, Scanner	Multifunktionsgerät	1	Haupt, R1	in Betrieb	alle Mitarbeiter
T1	TK-Anlage	ISDN-TK-Anlage	1	Haupt, R1	in Betrieb	alle Mitarbeiter
N4	Router	Router	1	Haupt, R2	in Betrieb	Adm1
N5	Backuprouter (Hot Standby)	Router	1	Haupt, R2	in Betrieb	Adm1
N6	Rack Switch	Switch	1	Haupt, R2	in Betrieb	Adm1
N7	Internes Switch	Switch	1	Haupt, R2	in Betrieb	Adm1
S2	Datenbankserver	Linux	3	Haupt, R2	in Betrieb	Adm1
S3	Webserver (inkl. Cold Standby)	Linux	3	Haupt, R2	in Betrieb	Adm1
S4	NFS-Server	Linux	1	Haupt, R2	in Betrieb	Adm1
S5	VServer: 7 SMTP Server	Linux mit XEN	1	Haupt, R2	in Betrieb	Adm1
S6	Backupserver	Linux	1	Haupt, R2	in Betrieb	Adm1
S7	Server für Firma (Web, E-Mail, etc..)	Linux	1	Haupt, R2	in Betrieb	Adm1

Zuordnung der Anwendungen zu den betroffenen IT-Systemen

Beschreibung der Anwendungen		**IT-Systeme**									
Nr.	**Anwendung / Informationen**	C1	C2	C3	S1	S2	S3	S4	S5	S6	S7
A1	Personaldatenverarbeitung			X	X						
A2	Benutzerdatenverarbeitung	X	X	X		X	X	X			
A3	Systemmanagement	X	X			X	X				
A4	Bürokommunikation				X						X
A5	DNS-Service										X
A6	Fileserver (intern)				X						
A7	Fileserver							X			
A8	HTTP-Service					X	X	X			X
A9	Datenbank-Service					X					X
A10	E-Mail-Service								X		X

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

Erfassung der Räume

Raum			IT / Informationen
Bez.	**Art**	**Lokation**	**IT-Systeme / Datenträger**
R1	Büroraum	Haupt	C1, C2, C3, N1, N2, N3, S1, N8, TK-Anlage
R2	Serverraum	Haupt	N4, N5, N6, N7, S2, S3, S4, S5, S6 (Tagessicherung der Server S3 + S4 + S5), S7, leere Datenträger

Die Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines Sicherheitskonzepts nach IT-Grundschutz benötigt werden. Dabei geht es um die Erfassung der Bestandteile (Informationen, Anwendungen, IT-Systeme, Räume, Kommunikationsnetze), die zur Erfüllung der im Geltungsbereich festgelegten Geschäftsprozesse oder Fachaufgaben benötigt werden. Dazu wurden geschäftskritische Informationen und Anwendungen ermittelt und die betroffenen IT-Systeme, Räume und Netze erfasst.

Phase 2: Schutzbedarfsfeststellung

Schutzbedarfsfeststellung für Anwendungen

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutzbedarf**	**Begründung**
A1	Personaldatenverarbeitung	X	Vertraulichkeit	hoch	Personaldaten sind besonders schutzbedürftige personenbezogene Daten, deren Bekanntwerden 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 aufgrund der Überschaubarkeit der Datenmenge überbrückt werden.
A2	Benutzerdatenverarbeitung	X	Vertraulichkeit	hoch	Benutzerdaten sind besonders schutzbedürftige personenbezogene Daten, deren Bekanntwerden die Betroffenen erheblich beeinträchtigen können. Weiters ist ein erheblicher Imageverlust zu befürchten.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfügbarkeit	hoch	Bei einem längeren Ausfall ist ein erheblicher Imageverlust zu befürchten.
A3	Systemmanagement		Vertraulichkeit	hoch	Beinhaltet wichtige Passwörter. Wirkt sich direkt auf Sicherheit des Gesamtsystems aus.
			Integrität	hoch	Wirkt sich direkt auf Verfügbarkeit des Gesamtsystems aus.
			Verfügbarkeit	hoch	Fehlerbehebung im System muss schnell möglich sein.
A4	Bürokommunikation	X	Vertraulichkeit	hoch	Kann Personaldaten und Benutzerdaten beinhalten.
			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 aufgrund der Überschaubarkeit der Datenmenge überbrückt werden.
A5	DNS-Service		Vertraulichkeit	normal	Keine Personendaten.
			Integrität	normal	Nur für Bürosystem relevant.
			Verfügbarkeit	normal	Nur für Bürosystem relevant.
A6	Fileserver (intern)		Vertraulichkeit	hoch	Kann Personaldaten und Benutzerdaten beinhalten.
			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 aufgrund der Überschaubarkeit der Datenmenge überbrückt werden.
A7	Fileserver		Vertraulichkeit	normal	Nur für Bilder genutzt. Diese unterliegen keiner Zugangsbeschränkung.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfügbarkeit	hoch	Bei einem längeren Ausfall ist ein erheblicher Imageverlust zu befürchten.
A8	HTTP-Service		Vertraulichkeit	normal	Keine Personendaten.
			Integrität	hoch	Veränderungen könnten zum Ausspionieren von Benutzerdaten verwendet werden.
			Verfügbarkeit	hoch	Bei einem längeren Ausfall ist ein erheblicher Imageverlust zu befürchten.
A9	Datenbank-Service	X	Vertraulichkeit	hoch	Benutzerdaten sind besonders schutzbedürftige personenbezogene Daten, deren Bekanntwerden die Betroffenen erheblich beeinträchtigen können. Weiters ist ein erheblicher Imageverlust zu befürchten.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfügbarkeit	hoch	Bei einem längeren Ausfall ist ein erheblicher Imageverlust zu befürchten.
A10	E-Mail-Service	X	Vertraulichkeit	hoch	Benutzerdaten und Inhalte sind besonders schutzbedürftige personenbezogene Daten, deren Bekanntwerden die Betroffenen erheblich

					beeinträchtigen können. Weiters ist ein erheblicher Imageverlust zu befürchten.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können.
			Verfügbarkeit	hoch	Bei einem längeren Ausfall ist ein erheblicher Imageverlust zu befürchten.

Schutzbedarfsfeststellung für IT-Systeme

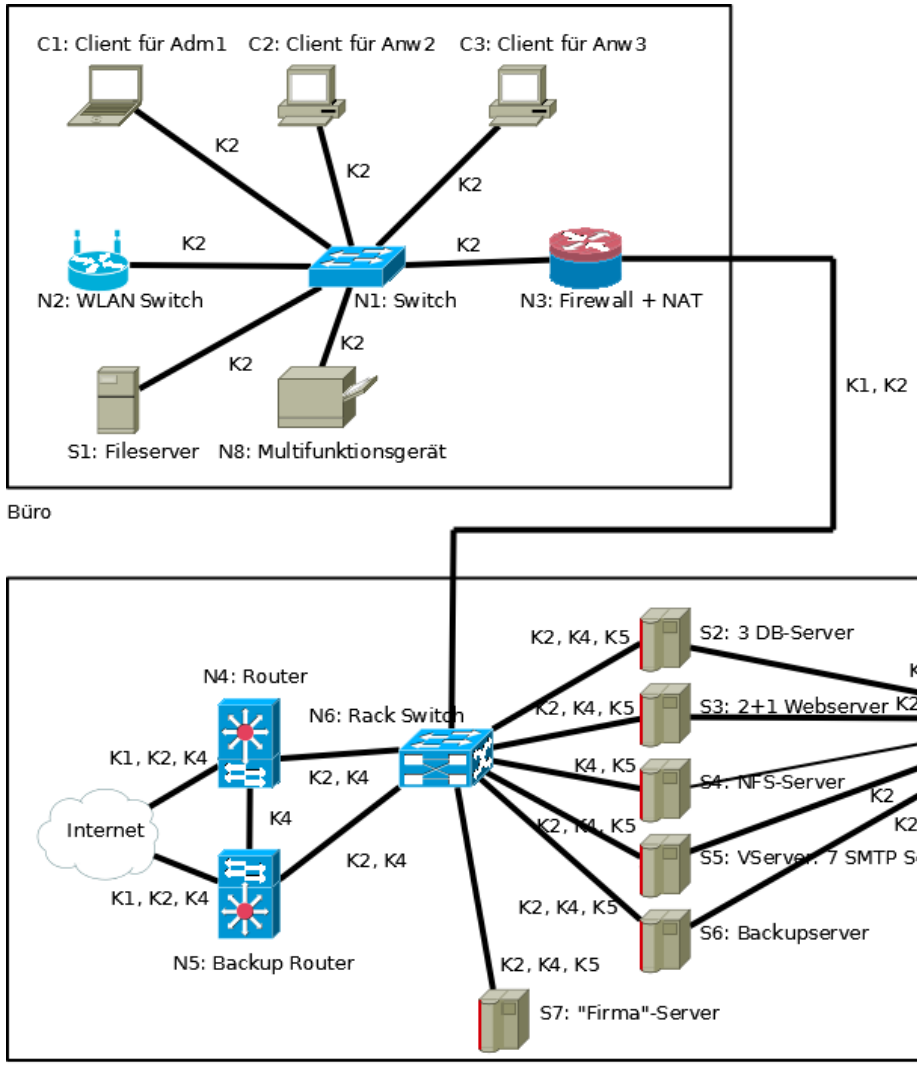
IT-System		Schutzbedarfsfeststellung		
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
C1	Client für Adm1	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Ist leicht ersetzbar.
		Verfügbarkeit	normal	Ist leicht ersetzbar.
C2	Client für Anw2	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Ist leicht ersetzbar.
		Verfügbarkeit	normal	Ist leicht ersetzbar.
C3	Client für Anw3	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Ist leicht ersetzbar.
		Verfügbarkeit	normal	Ist leicht ersetzbar.
S1	Fileserver	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	normal	Maximumprinzip
S2	Datenbankserver	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip

		Verfügbarkeit	hoch	Maximumprinzip
S3	Webserver (inkl. Cold Standby)	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip
S4	NFS-Server	Vertraulichkeit	normal	Nur für Bilder genutzt. Diese unterliegen keiner Zugangsbeschränkung.
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip
S5	VServer: 7 SMTP Server	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip
S6	Backupserver	Vertraulichkeit	hoch	Enthält Benutzerdaten.
		Integrität	hoch	Drohender Datentotalverlust.
		Verfügbarkeit	hoch	Bei einem längeren Ausfall ist ein erheblicher Imageverlust zu befürchten.
S7	Server für Firma (Web, E-Mail, etc..)	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbarkeit	hoch	Maximumprinzip

Schutzbedarfsfeststellung für Räume

Raum			IT / Informationen	Schutzbedarf		
Bez.	**Art**	**Lokation**	**IT-Systeme / Datenträger**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
R1	Büroraum	Haupt	C1, C2, C3, N1, N2, N3, S1, N8, TK-Anlage	hoch	normal	normal
R2	Serverraum	Haupt	N4, N5, N6, N7, S2, S3, S4, S5, S6 (Tagessicherung der Server S2 + S3 + S4), S7, leere Datenträger	hoch	hoch	hoch

Schutzbedarfsfeststellung für Kommunikationsverbindungen



		Kritisch aufgrund				
Verbindung		**K1 Außenverbindung**	**K2 hohe Vertraulichkeit**	**K3 hohe Integrität**	**K4 hohe Verfügbarkeit**	**K5 keine Übertragung**
N4	Internet	X	X		X	
N5	Internet	X	X		X	
N4	N6		X		X	
N5	N6		X		X	
N4	N5				X	
N6	S2		X		X	X
N6	S3		X		X	X
N6	S4				X	X
N6	S5		X		X	X
N6	S6		X		X	X
N6	S7		X		X	X
N7	S2		X			
N7	S3		X			
N7	S4					
N7	S5		X			
N7	S6		X			
N6	N3	X	X			
N3	N1		X			
N1	C1		X			
N1	C2		X			

N1	C3		X			
N1	N2		X			
N1	S1		X			
N1	N8		X			

Die Einteilung der Anwendungen, IT-Systeme und Räume hilft einen Überblick über die erforderliche Sicherheit in verschiedenen Bereichen zu gewinnen. Anhand dieser Schutzbedarfsfeststellung können dann geeignete Maßnahmen definiert und umgesetzt werden. Die Erfassung hat gezeigt, dass in fast allen Bereichen und auf fast allen Systemen vertrauliche Daten verarbeitet und gespeichert werden. Daher ist besonders darauf zu achten diese Daten vor unerlaubtem Zugriff zu schützen.

Phase 3: Modellierung nach IT-Grundschutz

Modellierung des IT-Verbunds nach IT-Grundschutz

Nr.	Titel des Bausteins	Zielobjekt / Zielgruppe	Hinweise
B 1.0	Sicherheitsmanagement	Haupt	
B 1.1	Organisation	Haupt	Es gibt nur einen Standort in einem Rechenzentrum, wo sich auch die Büros befinden.
B 1.2	Personal	Gesamte Belegschaft	Die Personalverwaltung erfolgt zentral in Wien.
B 1.3	Notfallvorsorgekonzept	Sämtliche Server	Fällt ein Server aus ist das ganze Service beendet.
B 1.4	Datensicherungskonzept	Datenbanken	Für den Fall dass ein Server defekt wird.
B 1.6	Computer-Virenschutzkonzept	Sämtliche Server	
B 1.7	Kryptokonzept	Sensible Daten in den Datenbanken	
B 1.9	Hard- und Software -Management		
B 1.10	Standardsoftware	Gekaufte Software	
B 1.13	IT-Sicherheitssensibilisierung und -schulung	Personal	Es werden vertrauliche Informationen verwaltet.
B 2.9	Rechenzentrum	Büro - Serverräume	Büroräume sind im 1.Stock des Rechenzentrum
B 3.102	Server unter UNIX	Sämtliche Server	Server laufen unter Linux Debian
B 3.203	Laptop	1 Laptop	Der Laptop läuft unter Ubuntu
B 3.208	Internet-PC	3 Computer	Die Computer hängen in einem lokalen Netzwerk aus welchen sie sich geteilt ins Internet verbinden.
B 3.209	Client unter XP	2 ArbeitsPC	1x XP und 1x Vista
B 3.301	Sicherheitsgateway (Firewall)	1 NAT	

B 3.302	Router und Switches	1 NAT	
B 3.404	Mobiltelefon	Personal	Jeder Mitarbeiter darf sein Handy verwenden.
B 3.406	Drucker, Kopierer und Multifunktionsgeräte	1 Multifunktionsgerät	
B 4.1	Heterogene Netze	Sämtliche Server	Es handelt sich um ein kleines Teilnetz
B 4.2	Netz- und Systemmanagement	Sämtliche Server	
B 4.6	WLAN	Sämtliche PC's	
B 5.3	E-Mail	Sämtliche PC's	
B 5.7	Datenbanken	Sämtliche Server	
B 5.11	Apache Webserver	2 x Webserver	

Das ist ein IT-Grundschutz-Modell des Informationsverbunds, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des Informationsverbunds beinhaltet.

Phase 4: Basis-Sicherheitscheck

Schicht 1 - Übergegeordnete Aspekte der IT-Sicherheit

1.0 IT-Sicherheitsmanagement

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/Begründung für Nicht- Umsetzung
M 2.192 (A)	Erstellung einer IT-Sicherheitsleitlinie				X	
M 2.335 (A)	Festlegung der IT-Sicherheitsziele und -strategie				X	
M 2.336 (A)	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene				X	
M 2.193 (A)	Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit				X	
M 2.195 (A)	Erstellung eines IT-Sicherheitskonzepts				X	
M 2.197 (A)	Integration der Mitarbeiter in den Sicherheitsprozess			X		
M 2.337 (A)	Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse				X	
M 2.338 (Z)	Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien				X	
M 2.339 (Z)	Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit				X	
M 2.199 (A)	Aufrechterhaltung der IT-Sicherheit				X	
M 2.200 (C)	Managementreporte und -bewertungen der IT-Sicherheit				X	
M 2.201 (C)	Dokumentation des IT-Sicherheitsprozesses				X	
M 2.340 (A)	Beachtung rechtlicher Rahmenbedingungen				X	

1.1 Organisation

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.1 (A)	Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz				X	
M 2.2 (C)	Betriebsmittelverwaltung				X	
M 2.4 (B)	Regelungen für Wartungs- und Reparaturarbeiten				X	
M 2.5 (A)	Aufgabenverteilung und Funktionstrennung				X	
M 2.40 (A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates				X	Es gibt keinen Personal-/Betriebsrat
M 2.225 (B)	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten				X	
M 2.6 (A)	Vergabe von Zutrittsberechtigungen			X		Es wird nicht vollständig protokolliert
M 2.7 (A)	Vergabe von Zugangsberechtigungen		X			
M 2.8 (A)	Vergabe von Zugriffsrechten		X			
M 2.14 (A)	Schlüsselverwaltung		X			Es gibt zusätzlich noch einen Fingerabdruck test
M 2.16 (B)	Beaufsichtigung oder Begleitung von Fremdpersonen		X			
M 2.18 (Z)	Kontrollgänge		X			Es gibt ein Wachpersonal
M 2.37 (Z)	Der aufgeräumte Arbeitsplatz				X	
M 2.39 (B)	Reaktion auf Verletzungen der Sicherheitspolitik				X	
M 2.177 (Z)	Sicherheit bei Umzügen				X	
M 2.13 (A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln			X		Es gibt keine Richtlinie

1.2 Personal

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 3.51 (Z)	Geeignetes Konzept für Personaleinsatz und -qualifizierung		X			
M 3.50 (Z)	Auswahl von Personal			X		keine Überprüfung der vorgelegten Unterlagen
M 3.1 (A)	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter				X	
M 3.2 (A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen		X			steht im Vertrag
M 3.10 (A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters				X	
M 3.33 (Z)	Sicherheitsüberprüfung von Mitarbeitern				X	
M 3.3 (A)	Vertretungsregelungen				X	
M 3.4 (A)	Schulung vor Programmnutzung				X	
M 3.5 (A)	Schulung zu IT-Sicherheitsmaßnahmen				X	
M 3.7 (Z)	Anlaufstelle bei persönlichen Problemen			X		Kleines Team, wo man sich gut kennt und über Probleme sprechen kann.
M 3.8 (Z)	Vermeidung von Störungen des Betriebsklimas			X		Es gibt eine jährliche Weihnachtsfeier + /Geburtstagsfeiern
M 3.11 (A)	Schulung des Wartungs- und Administrationspersonals				X	
M 3.6 (A)	Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern				X	

1.3 Notfallvorsorge-Konzept

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 6.1 (A)	Erstellung einer Übersicht über Verfügbarkeitsanforderungen		X			Wird über ein monitoring tool aufgezeichnet.
M 6.2 (A)	Notfall-Definition, Notfall-Verantwortlicher				X	
M 6.3 (C)	Erstellung eines Notfall-Handbuches				X	
M 6.75 (Z)	Redundante Kommunikationsverbindungen			X		Es gibt ein Festnetz und Mobil – Telefone.
M 6.14 (B)	Ersatzbeschaffungsplan				X	
M 6.15 (Z)	Lieferantenvereinbarungen (optional)				X	
M 6.4 (B)	Dokumentation der Kapazitätsanforderungen der IT-Anwendungen		X			
M 6.5 (B)	Definition des eingeschränkten IT-Betriebs				X	
M 6.6 (B)	Untersuchung interner und externer Ausweichmöglichkeiten				X	
M 6.7 (A)	Regelung der Verantwortung im Notfall				X	
M 6.8 (A)	Alarmierungsplan				X	
M 6.9 (C)	Notfall-Pläne für ausgewählte Schadensereignisse				X	
M 6.10 (C)	Notfall-Plan für DFÜ-Ausfall				X	
M 6.11 (B)	Erstellung eines Wiederanlaufplans				X	
M 6.13 (A)	Erstellung eines Datensicherungsplans				X	
M 6.16 (Z)	Abschließen von Versicherungen (optional)				X	
M 6.12 (C)	Durchführung von Notfallübungen			X		Feueralarmübungen

1.4 Datensicherungskonzept

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 6.33 (B)	Entwicklung eines Datensicherungskonzepts				X	
M 6.34 (B)	Erhebung der Einflussfaktoren der Datensicherung				X	
M 6.35 (B)	Festlegung der Verfahrensweise für die Datensicherung				X	
M 6.36 (A)	Festlegung des Minimaldatensicherungskonzeptes				X	
M 2.137 (A)	Beschaffung eines geeigneten Datensicherungssystems				X	
M 2.41 (A)	Verpflichtung der Mitarbeiter zur Datensicherung				X	
M 6.21 (C)	Sicherungskopie der eingesetzten Software				X	
M 6.37 (A)	Dokumentation der Datensicherung				X	
M 6.20 (A)	Geeignete Aufbewahrung der Backup-Datenträger		X			Vom Service gibt es ein Backup auf einer andere HDD aber im selben Raum. Es gibt kein Backup der Daten.
M 6.22 (A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen				X	
M 6.32 (A)	Regelmäßige Datensicherung		X			Jede Woche.
M 6.41 (A)	Übungen zur Datenrekonstruktion				X	

1.6 Computer-Virenschutzkonzept

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.154 (A)	Erstellung eines Computer-Virenschutzkonzepts				X	
M 2.155 (A)	Identifikation potentiell von Computer-Viren betroffener IT-Systeme			X		eMails am Server werden gescannt.
M 2.156 (A)	Auswahl einer geeigneten Computer-Virenschutz-Strategie				X	
M 2.160 (A)	Regelungen zum Computer-Virenschutz				X	
M 2.157 (A)	Auswahl eines geeigneten Computer-Viren-Suchprogramms				X	
M 4.84 (A)	Nutzung der BIOS-Sicherheitsmechanismen				X	
M 2.158 (A)	Meldung von Computer-Virusinfektionen			X		In einem kleinen Team können sich die MA schnell austauschen.
M 2.159 (A)	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme				X	
M 2.224 (A)	Vorbeugung gegen Trojanische Pferde			X		Es gibt einen Spamfilter.
M 4.3 (A)	Regelmäßiger Einsatz eines Anti-Viren-Programms			X		eMails werden am Server regelmäßig nach Viren gescannt.
M 4.33 (A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung				X	
M 4.253 (A)	Schutz vor Spyware				X	
M 6.23 (A)	Verhaltensregeln bei Auftreten eines Computer-Virus				X	

1.9 Hard- und Software-Management

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.3 (B)	Datenträgerverwaltung				X	
M 2.9 (A)	Nutzungsverbot nicht freigegebener Hard- und Software				X	
M 2.11 (A)	Regelung des Passwortgebrauchs				X	
M 2.12 (C)	Betreuung und Beratung von IT-Benutzern				X	
M 2.30 (A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen				X	
M 2.214 (A)	Konzeption des IT-Betriebs				X	
M 2.216 (C)	Genehmigungsverfahren für IT-Komponenten				X	
M 2.217 (B)	Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen				X	
M 2.218 (C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten				X	
M 2.220 (A)	Richtlinien für die Zugriffs- bzw. Zugangskontrolle				X	
M 2.221 (B)	Änderungsmanagement				X	
M 2.223 (B)	Sicherheitsvorgaben für die Nutzung von Standardsoftware				X	
M 2.226 (A)	Regelungen für den Einsatz von Fremdpersonal				X	
M 4.133 (Z)	Geeignete Auswahl von Authentikationsmechanismen		X			Fingerabdrücke und Sicherheitskarten
M 4.134 (C)	Wahl geeigneter Datenformate				X	
M 5.68 (Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation			X		email (pop3, imap, smtp) kann ssl, interface vom admin (kein https)
M 5.77 (Z)	Bildung von Teilnetzen				X	

M 5.87 (C)	Vereinbarung über die Anbindung an Netze Dritter	X				Es wird kein Netz Dritter verwendet.
M 5.88 (C)	Vereinbarung über Datenaustausch mit Dritten	X				Es wird kein Netz Dritter verwendet.
M 2.62 (B)	Software-Abnahme- und Freigabe-Verfahren				X	
M 1.29 (Z)	Geeignete Aufstellung eines IT-Systems (optional)				X	
M 2.25 (A)	Dokumentation der Systemkonfiguration		X			Bei den Backups der Server / Desktops jedoch nicht.
M 2.26 (A)	Ernennung eines Administrators und eines Vertreters		X			
M 2.38 (B)	Aufteilung der Administrationstätigkeiten				X	Es gibt keine geregelten Zuständigkeitsbereiche
M 2.69 (B)	Einrichtung von Standardarbeitsplätzen				X	
M 2.111 (A)	Bereithalten von Handbüchern				X	
M 2.138 (B)	Strukturierte Datenhaltung			X		Es gibt eine Ordnerstruktur, diese ist jedoch nicht durchgängig.
M 2.204 (A)	Verhinderung ungesicherter Netzzugänge				X	
M 4.1 (A)	Passwortschutz für IT-Systeme				X	
M 4.65 (C)	Test neuer Hard- und Software				X	
M 4.7 (A)	Änderung voreingestellter Passwörter		X			
M 4.84 (A)	Nutzung der BIOS-Sicherheitsmechanismen				X	
M 4.135 (A)	Restriktive Vergabe von Zugriffsrechten auf Systemdateien				X	
M 1.46 (Z)	Einsatz von Diebstahl-Sicherungen				X	
M 2.9 (A)	Nutzungsverbot nicht freigegebener Hard- und Software				X	
M 2.10 (C)	Überprüfung des Hard- und Software-Bestandes				X	

M 2.22 (Z)	Hinterlegen des Passwortes	X				Der Mitarbeiter wird zu Hause angerufen und nach dem PW gefragt.
M 2.34 (A)	Dokumentation der Veränderungen an einem bestehenden System				X	
M 2.35 (B)	Informationsbeschaffung über Sicherheitslücken des Systems				X	
M 2.64 (A)	Kontrolle der Protokolldateien				X	nicht regelmäßig.
M 2.65 (C)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System				X	
M 2.110 (A)	Datenschutzaspekte bei der Protokollierung				X	
M 2.182 (A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen				X	
M 2.215 (B)	Fehlerbehandlung				X	
M 2.219 (A)	Kontinuierliche Dokumentation der Informationsverarbeitung				X	
M 3.26 (A)	Einweisung des Personals in den sicheren Umgang mit IT				X	
M 4.78 (A)	Sorgfältige Durchführung von Konfigurationsänderungen	X				Sämtliche Konfigurationen werden in den Backups gesichert.
M 4.107 (B)	Nutzung von Hersteller-Ressourcen				X	
M 4.109 (Z)	Software-Reinstallation bei Arbeitsplatzrechnern				X	
M 4.254 (Z)	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen				X	Es werden keine drahtlosen Tastaturen und Mäuse verwendet.
M 2.167 (B)	Sicheres Löschen von Datenträgern			X		Vorgehen ist nicht geregelt.
M 4.234 (B)	Aussonderung von IT-Systemen		X			
M 6.27 (C)	Sicheres Update des BIOS				X	

1.10 Standardsoftware

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.79 (A)	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware				X	
M 2.80 (A)	Erstellung eines Anforderungskatalogs für Standardsoftware				X	
M 2.82 (B)	Entwicklung eines Testplans für Standardsoftware				X	
M 4.34 (Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen				X	
M 2.66 (Z)	Beachtung des Beitrags der Zertifizierung für die Beschaffung				X	
M 2.81 (A)	Vorauswahl eines geeigneten Standardsoftwareproduktes Umsetzung				X	
M 2.83 (B)	Testen von Standardsoftware				X	
M 2.84 (A)	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware				X	
M 2.85 (A)	Freigabe von Standardsoftware				X	
M 2.86 (B)	Sicherstellen der Integrität von Standardsoftware				X	
M 2.87 (A)	Installation und Konfiguration von Standardsoftware				X	
M 2.90 (A)	Überprüfung der Lieferung				X	
M 4.42 (Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung				X	
M 2.88 (A)	Lizenzverwaltung und Versionskontrolle von Standardsoftware				X	
M 2.89 (C)	Deinstallation von Standardsoftware				X	

1.13 IT-Sicherheitssensibilisierung und Schulung

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.312 (A)	Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit				X	
M 3.44 (A)	Sensibilisierung des Managements für IT-Sicherheit	X				In dem kleinen Team gibt es kein Management
M 3.48 (A)	Auswahl von Trainern oder Schulungsanbietern				X	
M 3.45 (A)	Planung von Schulungsinhalten zur IT-Sicherheit				X	
M 3.5 (A)	Schulung zu IT-Sicherheitsmaßnahmen				X	
M 3.46 (A)	Ansprechpartner zu Sicherheitsfragen				X	
M 3.49 (B)	Schulung zur Vorgehensweise nach IT-Grundschutz				X	
M 2.198 (A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit				X	
M 3.4 (A)	Schulung vor Programmnutzung				X	
M 3.11 (A)	Schulung des Wartungs- und Administrationspersonals				X	
M 3.26 (A)	Einweisung des Personals in den sicheren Umgang mit IT				X	
M 3.47 (Z)	Durchführung von Planspielen zur IT-Sicherheit				X	

Schicht 3 - Sicherheit der IT-Systeme

3.102 Server unter Unix

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.33 (C)	Aufteilung der Administrationstätigkeiten unter Unix		X			Es gibt nur einen Administrator mit dem sudo Passwörtern
M 4.13 (A)	Sorgfältige Vergabe von IDs				X	
M 4.18 (A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus		X			
M 5.16 (B)	Übersicht über Netzdienste				X	
M 5.34 (Z)	Einsatz von Einmalpasswörtern				X	
M 5.36 (Z)	Verschlüsselung unter Unix und Windows NT				X	
M 5.38 (B)	Sichere Einbindung von DOS-PCs in ein Unix-Netz	X				Sämtliche Server laufen unter Linux
M 5.64 (Z)	Secure Shell		X			
M 5.82 (A)	Sicherer Einsatz von SAMBA		X			für die Büro PCs
M 5.83 (Z)	Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN	X				Externe Netze werden nicht verwendet.
M 4.9 (A)	Einsatz der Sicherheitsmechanismen von X-Windows	X				Windows wird nicht verwendet.
M 4.14 (A)	Obligatorischer Passwortschutz unter Unix				X	
M 4.19 (A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen				X	
M 4.20 (B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen				X	

M 4.21 (A)	Verhinderung des unautorisierten Erlangens von Administratorrechten		X			
M 4.22 (C)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System				X	
M 4.23 (A)	Sicherer Aufruf ausführbarer Dateien				X	
M 4.105 (A)	Erste Maßnahmen nach einer Unix-Standardinstallation			X		Das System wird regelmäßig aktualisiert.
M 4.106 (A)	Aktivieren der Systemprotokollierung		X			
M 5.17 (A)	Einsatz der Sicherheitsmechanismen von NFS				X	
M 5.18 (A)	Einsatz der Sicherheitsmechanismen von NIS				X	
M 5.19 (A)	Einsatz der Sicherheitsmechanismen von sendmail				X	
M 5.20 (A)	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp				X	
M 5.21 (A)	Sicherer Einsatz von telnet, ftp, tftp und rexec			X		ssh wird verwendet
M 5.35 (A)	Einsatz der Sicherheitsmechanismen von UUCP				X	
M 5.72 (A)	Deaktivieren nicht benötigter Netzdienste		X			
M 4.25 (A)	Einsatz der Protokollierung im Unix-System	X				Es wird eine eigenes Monotoring Tool verwendet
M 4.26 (B)	Regelmäßiger Sicherheitscheck des Unix-Systems				X	
M 6.31 (A)	Verhaltensregeln nach Verlust der Systemintegritätystemintegrität				X	

3.209 Client unter Windows XP

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.324 (A)	Einführung von Windows XP planen				X	
M 2.325 (A)	Planung der Windows XP Sicherheitsrichtlinie				X	
M 2.326 (A)	Planung der Windows XP Gruppenrichtlinien				X	
M 2.327 (B)	Sicherheit beim Fernzugriff unter Windows XP				X	
M 2.328 (B)	Einsatz von Windows XP auf mobilen Rechnern	X				Der einzige Laptop läuft unter LINUX
M 3.28 (A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer				X	
M 4.48 (A)	Passwortschutz unter Windows NT/2000/XP				X	
M 4.57 (A)	Deaktivieren der automatischen CD-ROM-Erkennung		X			
M 4.75 (A)	Schutz der Registrierung unter Windows NT/2000/XP				X	
M 4.147 (Z)	Sichere Nutzung von EFS unter Windows 2000/XP				X	
M 4.149 (A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP				X	
M 4.243 (Z)	Windows XP Verwaltungswerkzeuge				X	
M 4.244 (A)	Sichere Windows XP Systemkonfiguration				X	
M 4.245 (A)	Basiseinstellungen für Windows XP GPOs				X	
M 4.246 (A)	Konfiguration der Systemdienste unter Windows XP				X	
M 4.247 (A)	Restriktive Berechtigungsvergabe unter Windows XP				X	
M 5.37 (B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz				X	
M 5.89 (A)	Konfiguration des sicheren Kanals unter Windows 2000/XP				X	

M 5.90 (Z)	Einsatz von IPSec unter Windows 2000/XP				X	
M 5.123 (B)	Absicherung der Netzwerkkommunikation unter Windows XP				X	
M 2.32 (Z)	Einrichtung einer eingeschränkten Benutzerumgebung				X	
M 4.248 (A)	Sichere Installation von Windows XP				X	
M 2.329 (A)	Einführung von Windows XP SP2		X			
M 2.330 (B)	Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung				X	
M 4.49 (A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System				X	
M 4.52 (A)	Geräteschutz unter Windows NT/2000/XP				X	
M 4.146 (A)	Sicherer Betrieb von Windows 2000/XP				X	
M 4.148 (B)	Überwachung eines Windows 2000/XP Systems				X	
M 4.249 (A)	Windows XP Systeme aktuell halten		X			
M 4.56 (C)	Sicheres Löschen unter Windows-Betriebssystemen				X	
M 6.76 (C)	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes				X	
M 6.78 (A)	Datensicherung unter Windows 2000/XP				X	

Schicht 5 - Sicherheit in Anwendungen

5.3 E- Mail

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.30 (A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen				X	
M 2.42 (B)	Festlegung der möglichen Kommunikationspartner				X	
M 2.46 (Z)	Geeignetes Schlüsselmanagement				X	
M 2.118 (A)	Konzeption der sicheren E-Mail-Nutzung				X	
M 2.119 (A)	Regelung für den Einsatz von E-Mail				X	
M 2.122 (B)	Einheitliche E-Mail-Adressen		X			
M 2.274 (A)	Vertretungsregelungen bei E-Mail-Nutzung				X	
M 5.63 (Z)	Einsatz von GnuPG oder PGP				X	
M 5.67 (Z)	Verwendung eines Zeitstempel-Dienstes				X	
M 5.108 (Z)	Kryptographische Absicherung von E-Mail				X	
M 5.110 (Z)	Absicherung von E-Mail mit SPHINX (S/MIME)				X	
M 2.123 (B)	Auswahl eines Mailproviders			X		Es gibt einen Spamfilter.
M 2.120 (A)	Einrichtung einer Poststelle				X	
M 2.275 (Z)	Einrichtung funktionsbezogener E-Mailadressen			X		Es gibt eine Support E-Mail Adresse, welche von allen eingesehen wird.
M 5.22 (B)	Kompatibilitätsprüfung des Sender- und Empfängersystems				X	
M 5.32 (A)	Sicherer Einsatz von Kommunikationssoftware				X	

M 5.57 (A)	Sichere Konfiguration der Mail-Clients				X	
M 2.121 (B)	Regelmäßiges Löschen von E-Mails				X	
M 4.33 (A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung				X	
M 4.34 (Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen				X	
M 4.44 (A)	Prüfung eingehender Dateien auf Makro-Viren				X	
M 4.64 (C)	Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen				X	
M 4.199 (B)	Vermeidung gefährlicher Dateiformate				X	
M 5.53 (B)	Schutz vor Mailbomben		X			Am Server.
M 5.54 (B)	Schutz vor Mailüberlastung und Spam		X			Es gibt einen Spamfilter.
M 5.55 (B)	Kontrolle von Alias-Dateien und Verteilerlisten				X	
M 5.56 (A)	Sicherer Betrieb eines Mailservers		X			
M 5.109 (Z)	Einsatz eines E-Mail-Scanners auf dem Mailserver		X			
M 6.38 (A)	Sicherungskopie der übermittelten Daten			X		Von den Mails am Server wird ein Backup erstellt.
M 6.90 (C)	Datensicherung und Archivierung von E-Mails		X			In Form von Backups.

5.7 Datenbanken

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.80 (A)	Erstellung eines Anforderungskatalogs für Standardsoftware				X	
M 2.126 (A)	Erstellung eines Datenbanksicherheitskonzeptes		X			
M 2.131 (C)	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen				X	
M 2.132 (A)	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen				X	
M 2.134 (B)	Richtlinien für Datenbank-Anfragen				X	
M 4.72 (Z)	Datenbank-Verschlüsselung				X	
M 4.73 (C)	Festlegung von Obergrenzen für selektierbare Datensätze				X	
M 2.124 (A)	Geeignete Auswahl einer Datenbank-Software				X	
M 2.125 (A)	Installation und Konfiguration einer Datenbank		X			
M 2.127 (B)	Inferenzprävention		X			
M 2.128 (A)	Zugangskontrolle einer Datenbank		X			
M 2.129 (A)	Zugriffskontrolle einer Datenbank		X			
M 2.135 (C)	Gesicherte Datenübernahme in eine Datenbank				X	
M 4.7 (A)	Änderung voreingestellter Passwörter		X			
M 4.67 (A)	Sperren und Löschen nicht benötigter Datenbank-Accounts		X			
M 4.71 (C)	Restriktive Handhabung von Datenbank-Links				X	
M 5.58 (B)	Installation von ODBC-Treibern				X	
M 2.31 (A)	Dokumentation der zugelassenen Benutzer und Rechteprofile				X	
M 2.34 (A)	Dokumentation der Veränderungen an einem bestehenden System		X			In Form von Backups.
M 2.65 (B)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System				X	

M 2.130 (A)	Gewährleistung der Datenbankintegrität		X			
M 2.133 (A)	Kontrolle der Protokolldateien eines Datenbanksystems			X		nicht regelmäßig.
M 3.18 (A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung		X			
M 4.68 (A)	Sicherstellung einer konsistenten Datenbankverwaltung				X	
M 4.69 (B)	Regelmäßiger Sicherheitscheck der Datenbank				X	
M 4.70 (C)	Durchführung einer Datenbanküberwachung				X	
M 6.48 (A)	Verhaltensregeln nach Verlust der Datenbankintegrität				X	
M 6.49 (A)	Datensicherung einer Datenbank		X			In Form von Backups.
M 6.50 (A)	Archivierung von Datenbeständen		X			In Form von Backups.
M 6.51 (B)	Wiederherstellung einer Datenbank		X			Durch das Laden eines alten Backups.

5.11 Apache-Webserver

Maßnahme (Priorität)	Baustein	entb.	Ja	teilw.	Nein	Bemerkung/ Begründung für Nicht- Umsetzung
M 2.269 (A)	Planung des Einsatzes eines Apache-Webservers				X	
M 2.270 (Z)	Planung des SSL-Einsatzes beim Apache Webserver				X	
M 4.191 (A)	Überprüfung der Integrität und Authentizität der Apache-Pakete				X	
M 3.37 (A)	Schulung der Administratoren eines Apache-Webservers				X	
M 4.192 (A)	Konfiguration des Betriebssystems für einen Apache-Webserver		X			
M 4.193 (A)	Sichere Installation eines Apache-Webservers		X			
M 4.194 (A)	Sichere Grundkonfiguration eines Apache-Webservers				X	
M 4.195 (A)	Konfiguration der Zugriffssteuerung beim Apache-Webserver		X			
M 4.197 (B)	Servererweiterungen für dynamische Webseiten beim Apache-Webserver				X	
M 4.198 (Z)	Installation eines Apache-Webservers in einem chroot-Käfig				X	
M 5.107 (Z)	Verwendung von SSL im Apache-Webserver				X	
M 4.196 (B)	Sicherer Betrieb eines Apache-Webservers				X	Protokolle werden zwar überprüft aber nicht regelmäßig.
M 6.89 (A)	Notfallvorsorge für einen Apache-Webserver		X			Fällt ein Webserver aus gibt es einen zweiten im cold standby

Die Modellierung nach IT-Grundschutz wurde nun als Prüfplan benutzt, um anhand eines Soll-Ist-Vergleichs herauszufinden, welche Standard-Sicherheitsmaßnahmen ausreichend oder nur unzureichend umgesetzt sind.

Phase 5: Sicherheitsbewertung des IT-Verbunds

Das untersuchte Unternehmen ist ein Einzelunternehmen, bestehend nur aus insgesamt drei Mitarbeitern und hat daher entsprechend wenig interne Richtlinien aufgestellt. So fehlt es gänzlich an technischer Dokumentation der Konfiguration der bestehenden IT-Systeme. Diese und auch die tägliche Wartung wird ausschließlich vom Administrator durchgeführt, was bei einem möglichen Ausfall des Teammitglieds ein enormes Risiko darstellt. Auch sind alle Passwörter ausschließlich im Besitz des Administrators. Dementsprechend gibt es wenig bis gar keine Notfallpläne. Im Falle eines Ausfalls stehen zwar Cold-Standby Systeme parat, diese sind jedoch ebenfalls nur vom Administrator in das bestehende System einbindbar. Das Team-Mitglied Administrator hat also nicht nur eine hohe Verantwortung innerhalb des Teams und für das Unternehmen, sondern ist auch unersetzbar.

Was die Sicherheit der Systeme betrifft, wurden einige Vorkehrungen getroffen um Zugang von außerhalb auf kritische Komponenten zu unterbinden. Versuche, diese Maßnahmen zu umgehen, werden zwar von den jeweiligen Systemen protokolliert, jedoch nicht regelmäßig ausgewertet. Ein verschlüsselter Zugriff auf kritische Komponenten existiert bei der Remotekonsole der Server (SSH), jedoch nicht bei den Administratorinterfaces über HTTP. Hier wäre eine geschützte Verbindung, zum Beispiel über ein selbstsigniertes Zertifikat, anzuraten.

Die bürointerne Kommunikation, abgesehen von E-Mail, ist vom Internet über eine Firewall und ein NAT abgeschottet. Der Zugriff auf den gemeinsamen Dateiserver ist in diesem Bereich möglich. Es existiert jedoch keine Zugriffskontrolle auf dem Datenserver, was insbesondere bei möglichen Viren problematisch sein kann.

Backups der Daten werden gemacht, jedoch weder räumlich getrennt, noch in einem speziell geschütztem Bereich, auf den kein Zugriff über das Internet möglich ist, gelagert. Dies ist unter anderem auf die hohen Kosten von Standflächen im Rechenzentrum zurück zu führen.

Zugriffskontrollen werden aufgrund der kleinen Größe des Teams und dem bereits bestehenden Vertrauen untereinander nur spärlich strukturiert. Ein solches Verhalten wäre in einem größeren Unternehmen, insbesondere mit höherer Fluktuation, problematischer.