

Zwei Wege zur Verbesserung der IT-Sicherheit

- Sicherheitsanalyse und nachfolgende Behebung von Schwachstellen liegen in einer Hand
- Sicherheitsanalyse und nachfolgende Behebung werden unabhängig voneinander durchgeführt

Alles aus einer Hand - Nachteile

- Konflikt zwischen Umsatzinteressen des Auftragnehmers einerseits sowie den sicherheitsrelevanten und finanziellen Interessen des Auftraggebers andererseits
- Objektive Empfehlungen durch den Auftragnehmer sind nicht möglich
- Mögliche „Betriebsblindheit“ bei langfristiger Zusammenarbeit

Vorteile einer unabhängigen Sicherheitsanalyse

- Auftragnehmer hat keine finanziellen Interessen an ggf. überzogenen Sicherheitsmaßnahmen
- Auftragnehmer hat keine wirtschaftlichen Beziehungen mit bestimmten Herstellern
- Auch „traditionell gewachsene“ Schwachstellen werden erkannt

4 Verfahren zur Analyse der IT-Sicherheit

- IT-Grundschutz nach BSI
- Risikoanalyse
- Differenz-Sicherheitsanalyse
- Penetrationstest

Analyseverfahren im Überblick

Penetrations-
test

Differenz-
sicherheits-
analyse

Risiko-
analyse

IT-Grundschutz nach BSI

-  grundlegend
-  optional

Aufwand und Nutzen der Analyseverfahren

- IT-Grundschatz nach BSI ist als grundlegendes Verfahren einfach und kostengünstig
- IT-Grundschatz ist die Basis für die optionalen Verfahren
- Optionale Verfahren sind nur mit hohem Aufwand umsetzbar
- Optionale Verfahren sind in sicherheitskritischen Umgebungen nützlich

Das BSI

- Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) wurde 1991 gegründet
- Das BSI ist herstellerunabhängig
- Das BSI entwickelt Sicherheitskriterien im staatlichen Auftrag zur Abwehr von Bedrohungen im IT-Umfeld
- Das BSI ist Herausgeber des IT-Grundschutzhandbuchs

Das IT-Grundschutzhandbuch des BSI

- Ist als Quasistandard auch international anerkannt
- Wird ständig weiterentwickelt
- Enthält Gefährdungs- und Maßnahmekataloge für unterschiedlichste IT-Umgebungen
- ist frei verfügbar

Ablauf eines IT- Grundschutzprojektes

1. Initiierung des Sicherheitsprozesses
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung
5. Basis-Sicherheitscheck
6. Umsetzung von Sicherheitsmaßnahmen
7. Zertifizierung (optional)

1. Initiierung des Sicherheitsprozesses

- Erstellung einer Sicherheitsleitlinie
- Benennung eines internen Sicherheitsverantwortlichen
- Beauftragung eines externen Sicherheitsverantwortlichen (optional)

1.1. - Sicherheitsleitlinie

- Umfasst wichtige Ziele des Unternehmens hinsichtlich der Sicherheit
- Ist Maßstab für folgendes Handeln aller Beteiligten
- Enthält keine Details

Sicherheitsleitlinie – Beispiele für Inhalte

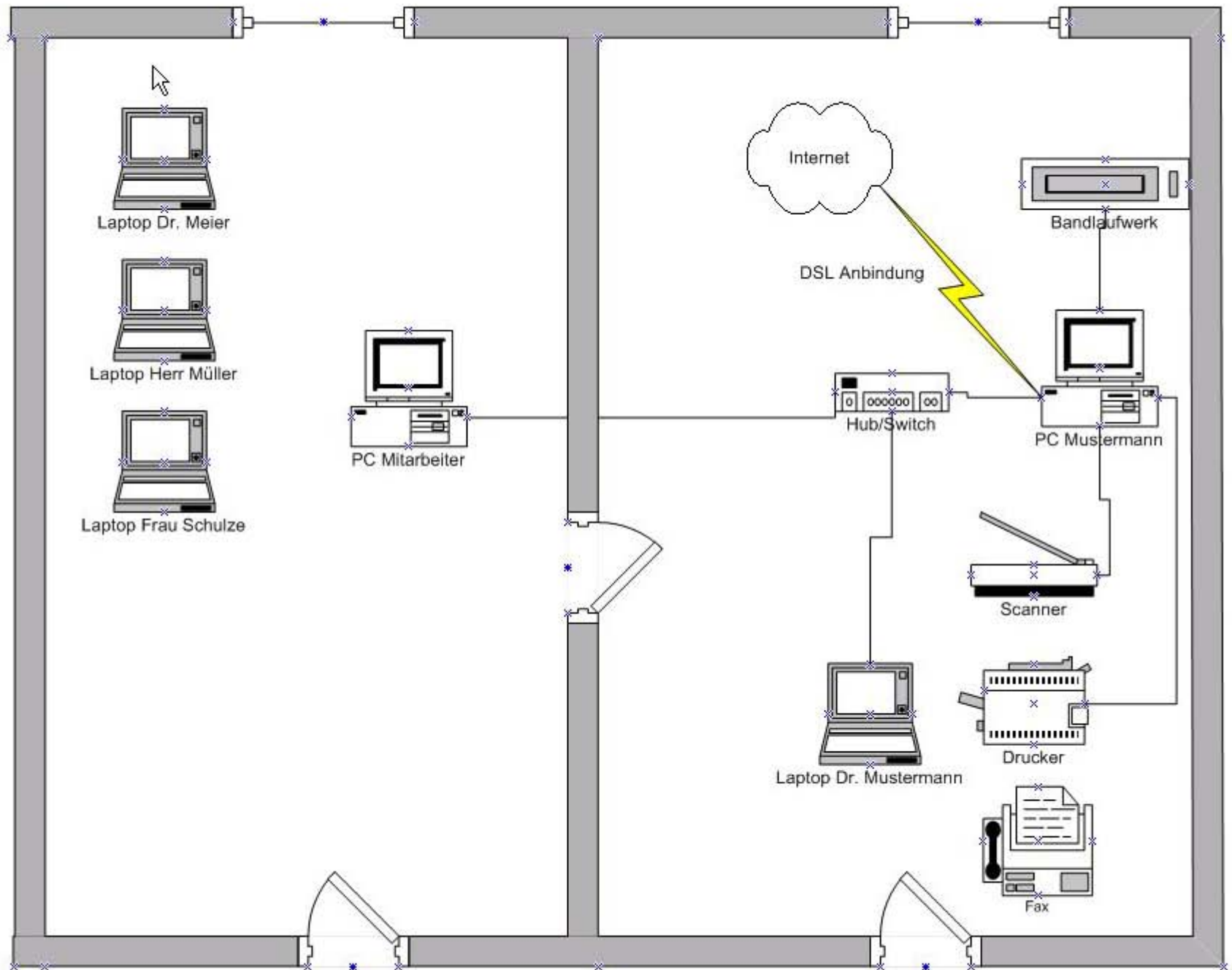
- Persönliche Daten von Mitarbeitern oder Kunden dürfen nicht nach außen dringen
- Nach Ausfall von Hardware/Software muss die Arbeitsfähigkeit vollständig innerhalb von 48 Stunden wiederhergestellt sein
- Unsere IT darf niemals Quelle von Angriffen auf Dritte sein
- ...

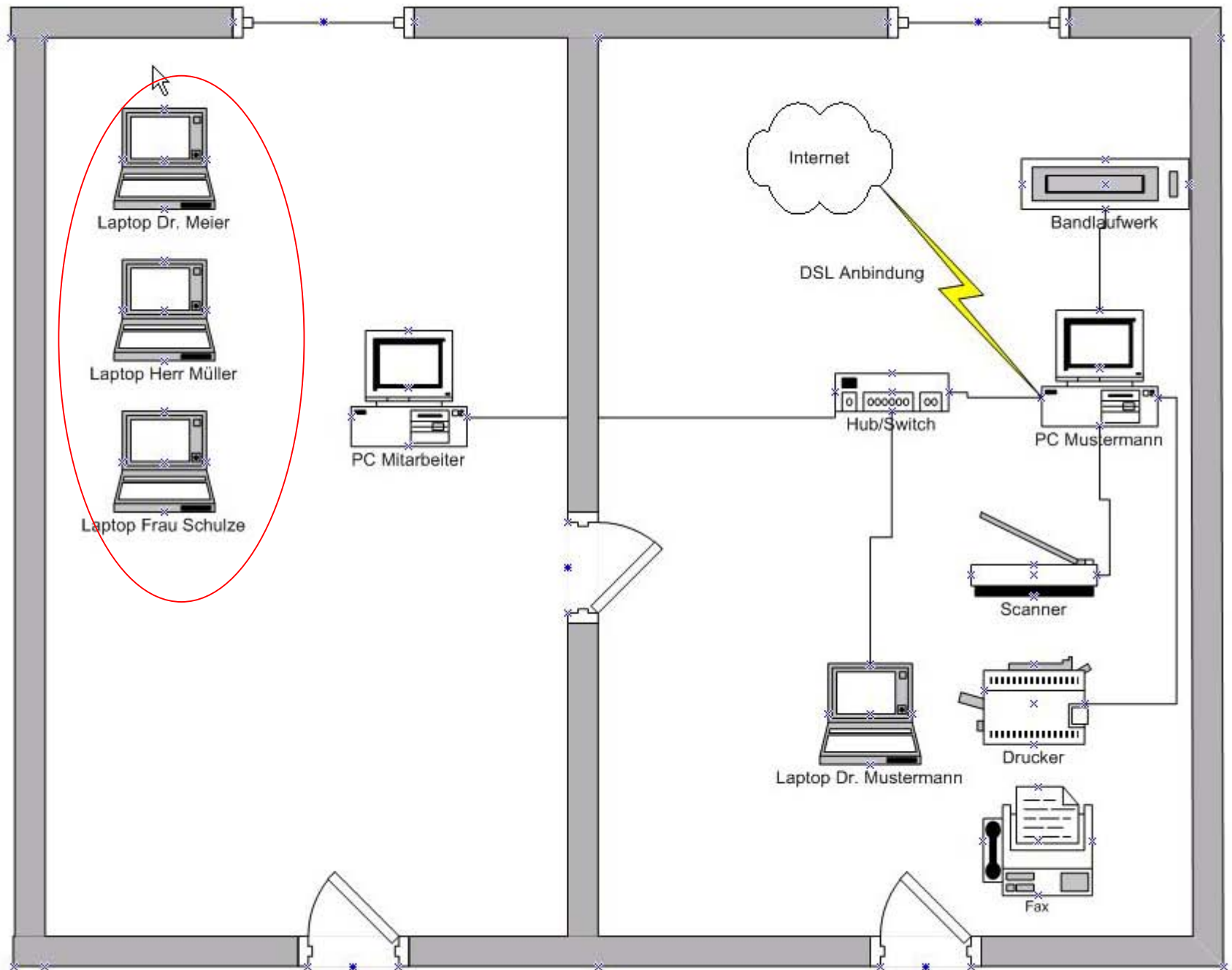
1.2. Sicherheitsverantwortliche(r)

- Ist/sind für die Umsetzung aller folgenden Schritte verantwortlich
- Delegation untergeordneter Aufgaben an Mitarbeiter ist möglich

2. Strukturanalyse

- Erstellung/Prüfung des Netzplanes
- Zusammenfassung gleichartiger Komponenten zu logischen Objekten





3. Schutzbedarfsfeststellung

- Objekte werden hinsichtlich der drei Grundwerte der IT-Sicherheit
 - Vertraulichkeit
 - Verfügbarkeit
 - Integritätkategorisiert
- Der Schutzbedarf ist entweder normal, hoch oder sehr hoch

Beispiele bez. des Schutzbedarfs

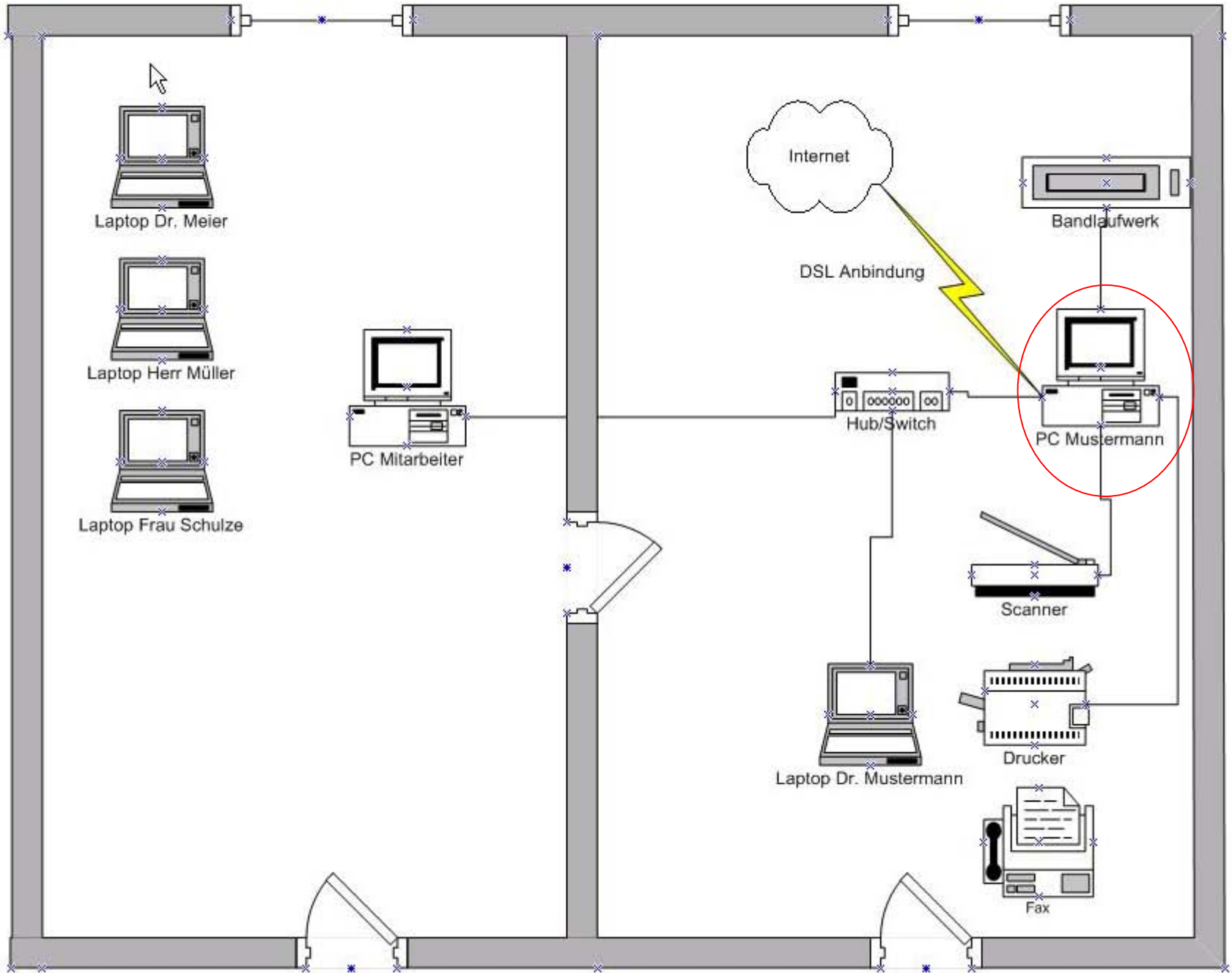
- Ein nicht mit dem internen Netzwerk verbundener Internet – PC hat z.B. einen geringen Schutzbedarf
- Ein Server, auf dem zentral alle Projekte gespeichert sind hat i.d.R. einen hohen Schutzbedarf

Feststellung des Schutzbedarfs

- Normal, wenn die Auswirkung von Sicherheitsvorfällen gering sind
- Hoch, wenn die Auswirkung von Sicherheitsvorfällen das Unternehmen erheblich schädigen können
- Sehr hoch, wenn die Auswirkung von Sicherheitsvorfällen die Existenz des Unternehmen gefährden können

Schutzbedarf - Konsequenzen

- Normaler Schutzbedarf eines Objekts - Anwendung des Grundschutzhandbuchs ist i.d.R. ausreichend
- Erhöhter Schutzbedarf eines Objekts – zusätzliche Maßnahmen sind meist erforderlich



Erhöhter Schutzbedarf - Beispiele

- Das Objekt enthält persönliche Daten (Kunden, Mitarbeiter, etc)
- Über das Objekt wird die Internetanbindung hergestellt
- Das Objekt enthält wichtige Projektdaten
- ...

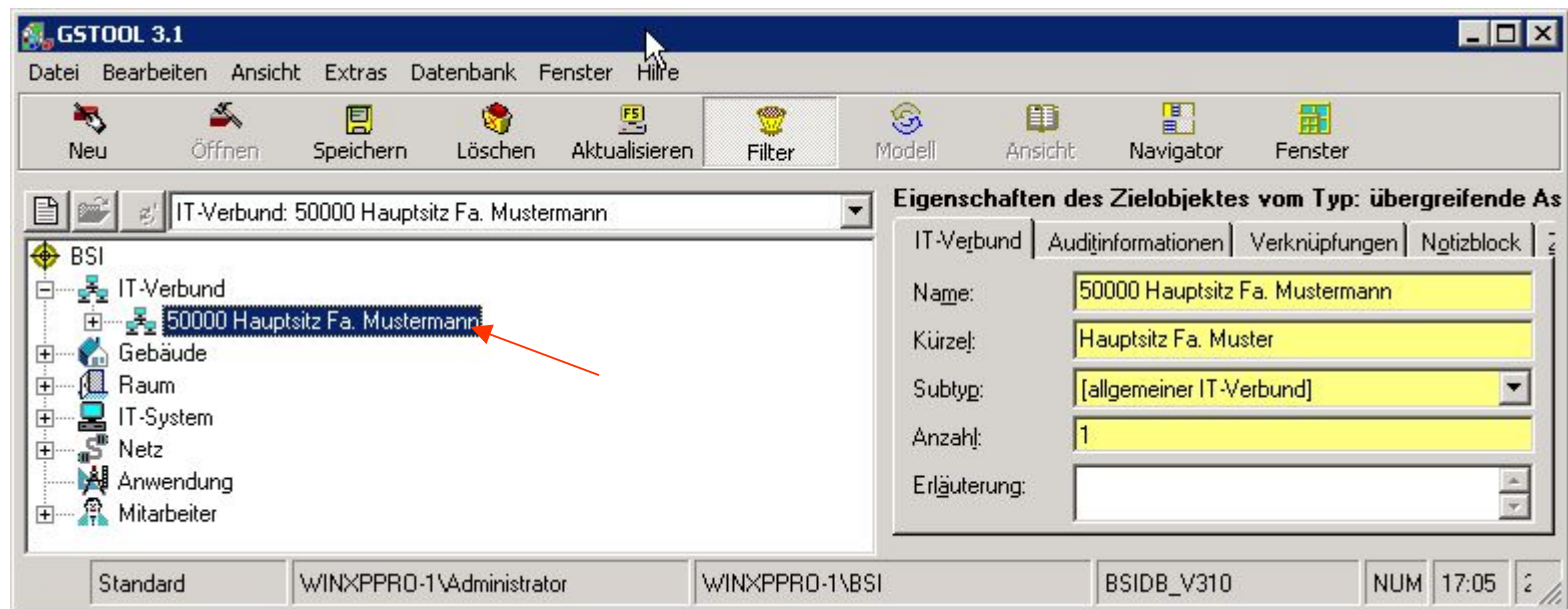
4. Modellierung

- Objekte und Maßnahmenbündel (Bausteine) werden gem. der Vorgaben des GSHB miteinander verknüpft
- Liste der zu überprüfenden Maßnahmen wird objektbezogen erstellt
- Liste der Maßnahmen wird ggf. hinsichtlich der Priorität gefiltert

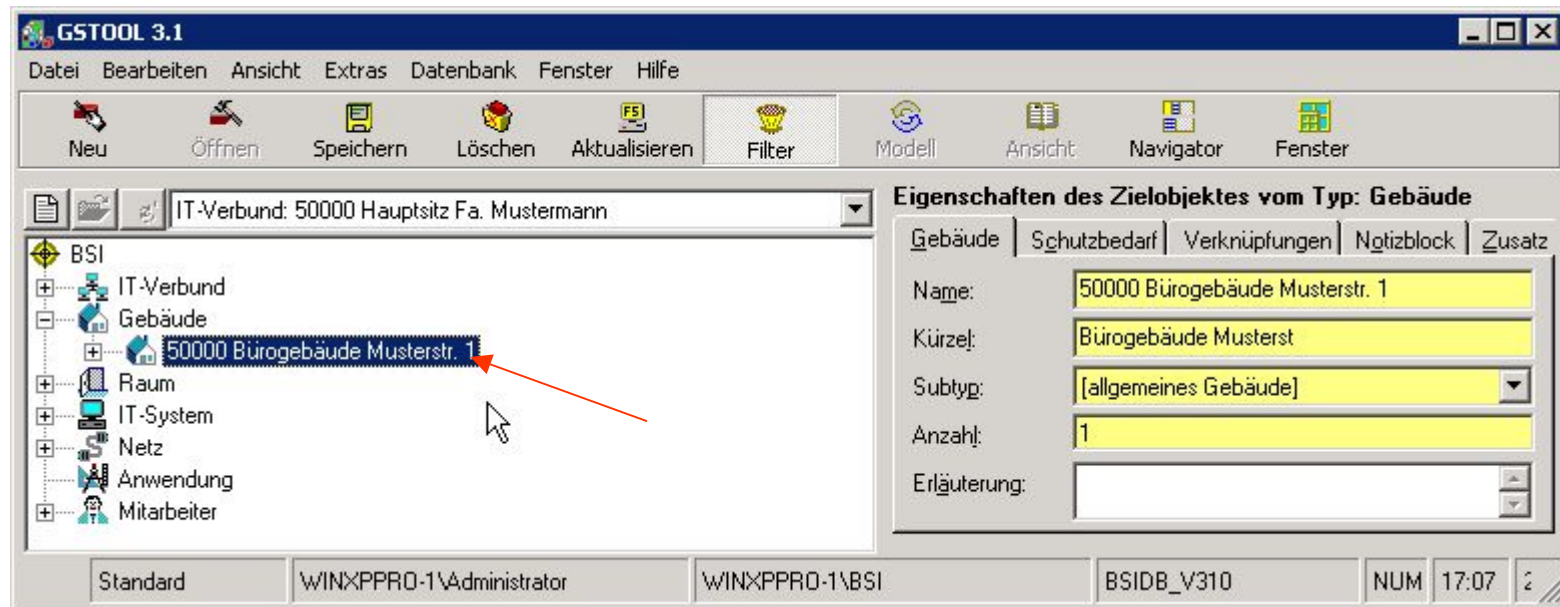
Ablauf der Modellierung

- Objekte werden erfasst und katalogisiert
- Objekte werden einander zugeordnet (Räume zu Gebäuden, IT-Systeme zu Räumen, Anwendungen zu IT-Systemen etc.)
- Bausteine des GSHB und deren Maßnahmen werden Objekten zugeordnet

Erfassung IT-Verbund



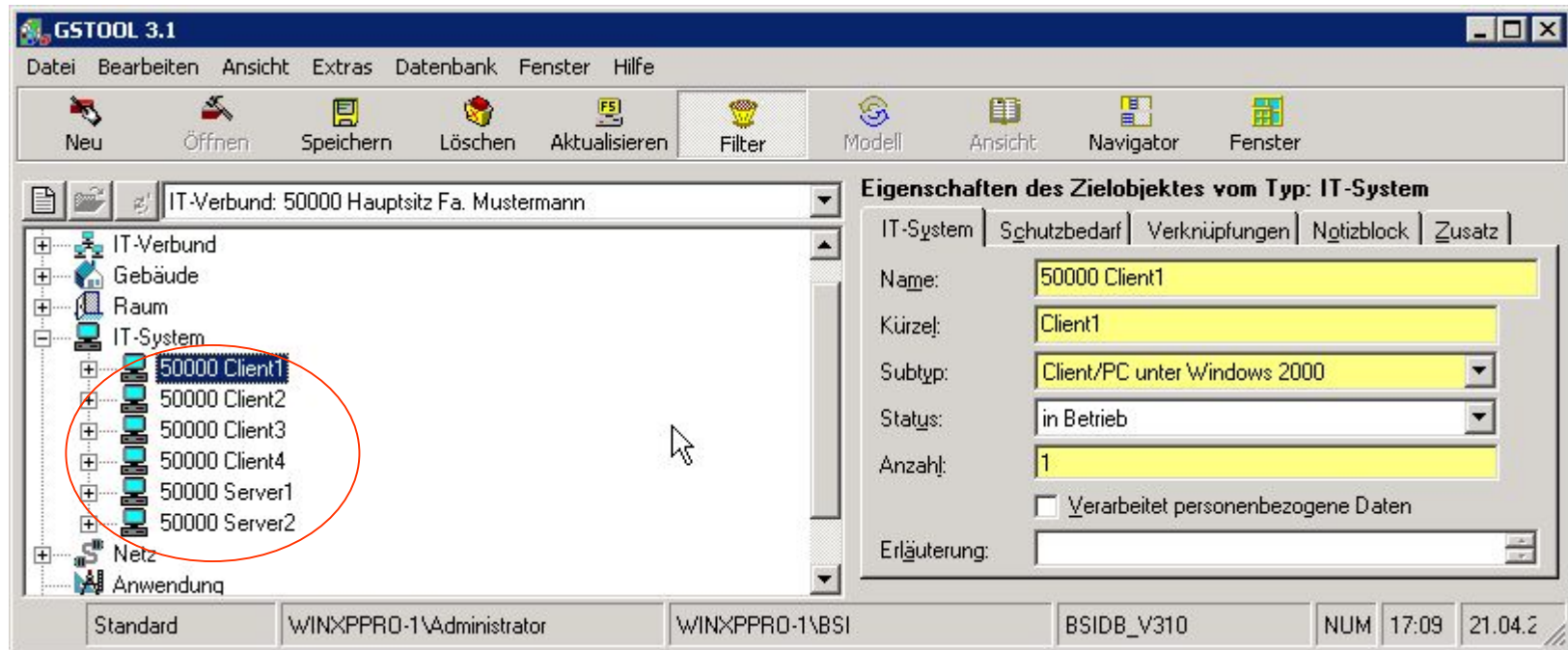
Erfassung Gebäude



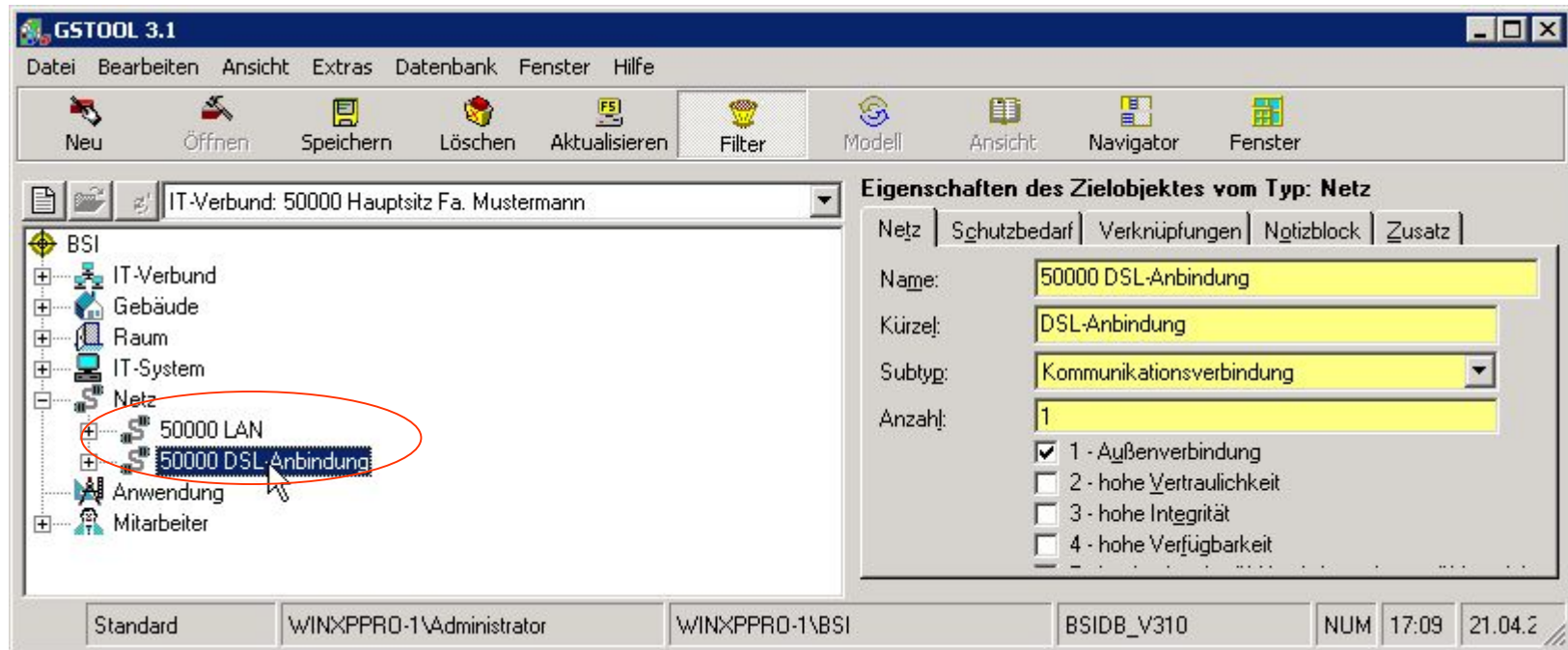
Erfassung Räume



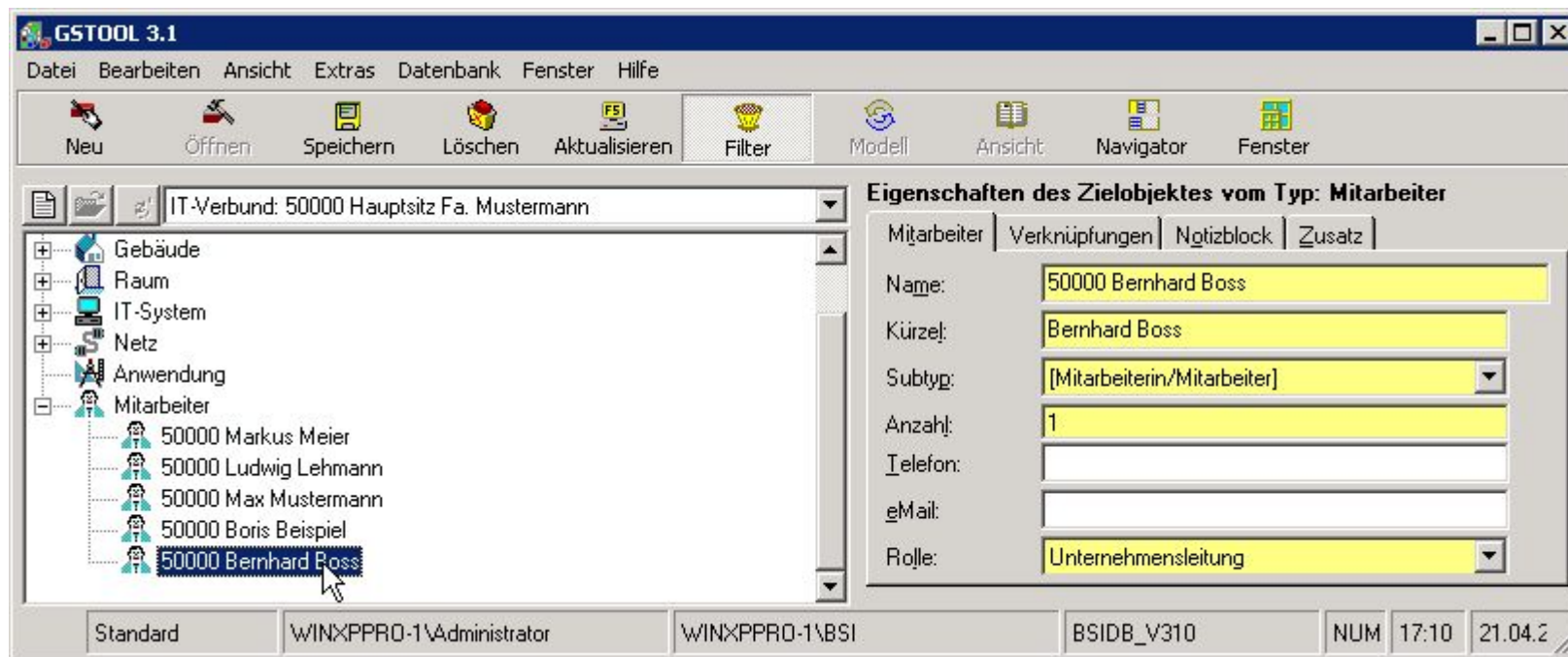
Erfassung Systeme



Erfassung Netze



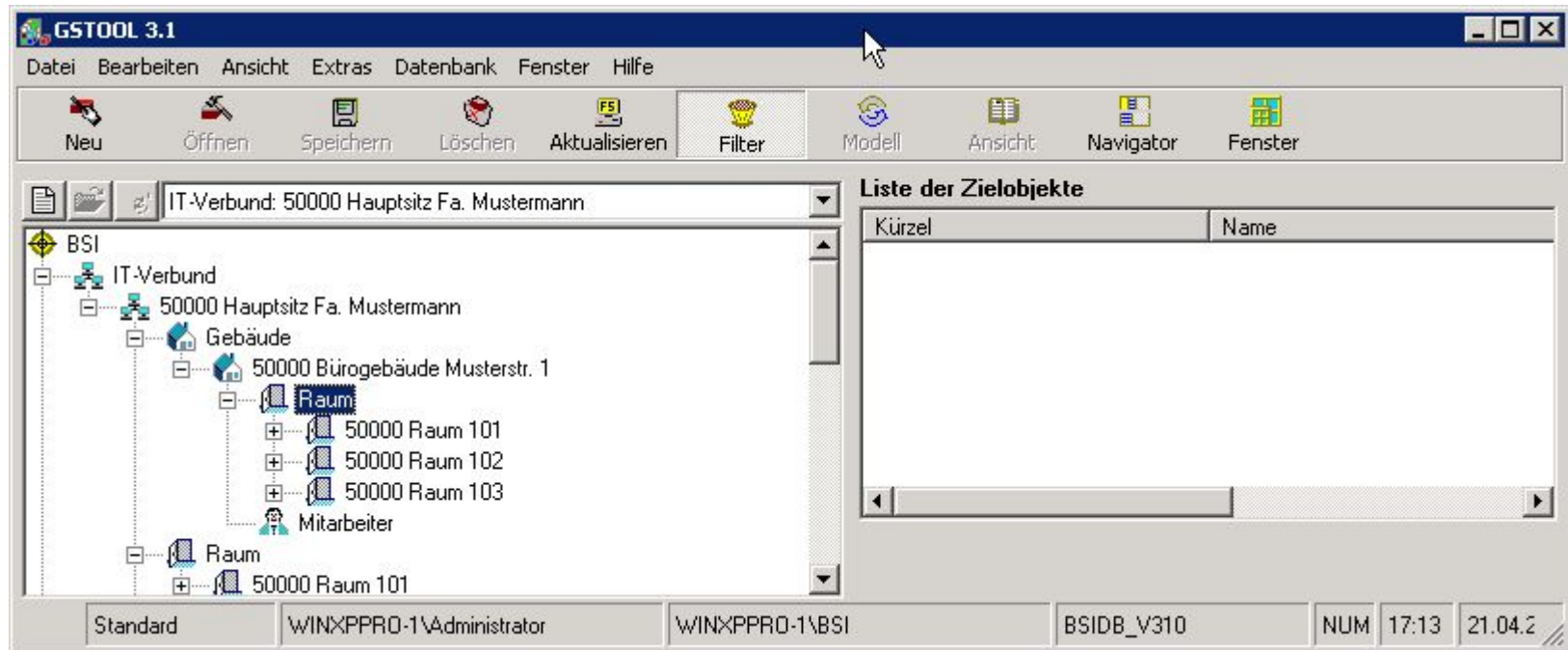
Erfassung Mitarbeiter



Zuordnung

- Die Objekte werden logisch miteinander verknüpft
- Abhängigkeiten werden herausgearbeitet

Zuordnung von Räumen zu Gebäuden



Zuordnung von Benutzern, Anwendungen, Netzen zu Systemen

The screenshot displays the GSTOOL 3.1 application window. The title bar reads 'GSTOOL 3.1'. The menu bar includes 'Datei', 'Bearbeiten', 'Ansicht', 'Extras', 'Datenbank', 'Fenster', and 'Hilfe'. The toolbar contains icons for 'Neu', 'Öffnen', 'Speichern', 'Löschen', 'Aktualisieren', 'Filter', 'Modell', 'Ansicht', 'Navigator', and 'Fenster'. The main workspace shows a tree view under the path 'IT-Verbund: 50000 Hauptsitz Fa. Mustermann'. The tree structure is as follows:

- 50000 Raum 101
 - IT-System
 - 50000 Client1 (selected)
 - Netz
 - 50000 LAN
 - Anwendung
 - Autocad 2000
 - Corel Draw
 - Office 2000
 - Mitarbeiter
 - 50000 Max Mustermann
 - 50000 Client2

The right-hand pane, titled 'Eigenschaften des Zielobjektes vom Typ: IT-System', shows the following details for '50000 Client1':

- IT-System | Schutzbedarf | Verknüpfungen | Notizblock | Zusatz
- Name: 50000 Client1
- Kürzel: Client1
- Subtyp: Client/PC unter Windows 2000
- Status: in Betrieb
- Anzahl: 1
- Verarbeitet personenbezogene Daten
- Erläuterung: (empty text box)

The status bar at the bottom shows the following information: Standard | WINXPPRO-1\Administrator | WINXPPRO-1\BSI | BSIDB_V310 | NUM 17:18 | 21.04.2

Ergebnis der Modellierung

The screenshot displays the GSTOOL 3.1 software interface. The main window shows a layered model (Schichtenmodell) for BSI, with the following structure:

- Schichtenmodell: BSI
 - 50000 Hauptsitz Fa. Mustermann
 - übergreifende Aspekte
 - Infrastruktur
 - IT-Systeme
 - Netze
 - IT-Anwendungen

On the right side, there is a panel titled "Liste der IT-Bausteine" (List of IT Building Blocks) with a table:

Nr.	Bezeichnung
B 3.00	IT-Sicherheitsmanagement
B 3.01	Organisation
B 3.02	Personal
B 3.03	Notfallvorsorge-Konzept
B 3.04	Datensicherungskonzept
B 3.06	Computer-Virenschutzkonzept
B 3.07	Kryptokonzept
B 3.08	Behandlung von Sicherheitsvo...
B 3.09	Hard- und Software-Managem...
R 3.10	Outsourcing

The status bar at the bottom shows the following information: Standard, WINXPPRO-1\Administrator, WINXPPRO-1\BSI, BSIDB_V310, NUM 17:22, 21.04.2

Maßnahmen gem. GS HB (alle)

The screenshot displays the GSTOOL 3.1 application window. The title bar reads "GSTOOL 3.1". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Extras", "Datenbank", "Fenster", and "Hilfe". The toolbar contains icons for "Neu", "Öffnen", "Speichern", "Löschen", "Aktualisieren", "Filter", "Modell", "Ansicht", "Navigator", and "Fenster".

The main workspace is divided into two panes. The left pane shows a hierarchical tree view of IT systems:

- IT-Systeme
 - B 5.07 Windows 2000 Client
 - 50000 Client1
 - M 1.29 Geeignete Aufstellung eines IT-Sy
 - BC M 2.3 Datenträgerverwaltung
 - BC M 2.4 Regelungen für Wartungs- und Re
 - ABC M 2.9 Nutzungsverbot nicht freigegebene
 - C M 2.10 Überprüfung des Hard- und Softw
 - ABC M 2.13 Ordnungsgemäße Entsorgung von
 - C M 2.22 Hinterlegen des Passwortes
 - ABC M 2.25 Dokumentation der Systemkonfig
 - ABC M 2.26 Ernennung eines Administrators u
 - ABC M 2.30 Regelung für die Einrichtung von
 - ABC M 2.31 Dokumentation der zugelassenen
 - C M 2.32 Einrichtung einer eingeschränkter
 - ABC M 2.34 Dokumentation der Veränderunge
 - ABC M 2.35 Informationsbeschaffung über Sic
 - ABC M 2.227 Planung des Windows 2000 Ein
 - por M 2.228 Festlegen einer Windows 2000 C

The right pane, titled "Eigenschaften der Maßnahme", displays details for the selected measure "M 2.35 Informationsbeschaffung über Sicherh". The tabs are "Umsetzung", "Kosten", "Revision", "Verantwortlich", and "Notizblock".

Nr./Bezeichnung:	M 2.35	Informationsbeschaffung über Sicherh
Baustein:	B 5.07	Windows 2000 Client
Priorität:	2	Erforderlich ab: A-Eingangsstufe
Umsetzung:	unbearbeitet	
Erläuterung:		
Umsetzung bis:	21.04.2005	

The status bar at the bottom shows: Standard | WINXPPRO-1\Administrator | WINXPPRO-1\BSI | BSIDB_V310 | NUM | 17:2

Maßnahme im Detail



The screenshot shows a web browser window with the following content:

M 4.150 Konfiguration von Windows 2000 als Workstation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement
Verantwortlich für Umsetzung: Administrator

Die Verwendung von Windows 2000 auf Arbeitsplatzrechnern stellt neben den allgemeinen Sicherheitsanforderungen an die Grundkonfiguration von Windows 2000 (siehe [M.4.137 Sichere Konfiguration von Windows 2000](#)) auch spezifische, arbeitsplatzbezogene Sicherheitsanforderungen. Die auf Arbeitsplatzrechnern eingesetzte Version ist in der Regel Windows 2000 Professional, das als Clientsystem mit Windows 2000 Servern und Domänen-Controllern kommuniziert.

Für die Konfiguration als Workstation sind folgende Aspekte aus Sicherheitssicht zu berücksichtigen:

Es empfiehlt sich, keine lokalen Daten auf Arbeitsplatzrechnern zu halten. Dies hat

Abbrechen

5. Basis – Sicherheitscheck

- Überprüfung der Umsetzung von Standard-Sicherheitsmaßnahmen
- Kennzeichnung des gegenwärtigen Umsetzungsgrades jeder Maßnahme mit je einem der folgenden Werte:
 - ja
 - teilweise
 - nein
 - entbehrlich

Beispiel: Baustein i.d. Bearbeitung

The screenshot displays the GSTOOL 3.1 application window. The menu bar includes 'Datei', 'Bearbeiten', 'Ansicht', 'Extras', 'Datenbank', 'Fenster', and 'Hilfe'. The toolbar contains icons for 'Neu', 'Öffnen', 'Speichern', 'Löschen', 'Aktualisieren', 'Filter', 'Modell', 'Ansicht', 'Navigator', and 'Fenster'. The main window is divided into two panes. The left pane shows a tree view of measures under the heading 'Mustermann (Prio 1 oder 2) und Siegelstufe A'. The right pane, titled 'Eigenschaften der Maßnahme', displays the details for the selected measure 'M 2.231 Planung der Gruppenrichtlinien unter Windows 2000'. The details include: 'Nr./Bezeichnung: M 2.231 Planung der Gruppenrichtlinien unter', 'Baustein: B 5.07 Windows 2000 Client', 'Priorität: 1', 'Erforderlich ab: A-Eingangsstufe', 'Umsetzung: entbehrlich', 'Erläuterung: kein AD', and 'Umsetzung bis: 21.04.2005'. The status bar at the bottom shows 'Standard', 'WINXPPRO-1\Administrator', 'WINXPPRO-1\BSI', 'BSIDB_V310', and 'NUM 17'.

Umsetzung	Kosten	Revision	Verantwortlich	Notizblock
Nr./Bezeichnung:	M 2.231	Planung der Gruppenrichtlinien unter		
Baustein:	B 5.07	Windows 2000 Client		
Priorität:	1	Erforderlich ab:	A-Eingangsstufe	
Umsetzung:	entbehrlich			
Erläuterung:	kein AD			
Umsetzung bis:	21.04.2005			

Beispiel: ein Zwischenbericht

Bericht: Umsetzungsgrad Maßnahmen - Mozilla

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Fenster Hilfe
 Zurück Vor Neu laden Stopp file:///C:/Dokumente%20und%20Einstellungen/Adminis Suchen Drucken
 Startseite Lesezeichen mozilla.org mozillaZine mozdev.org Mozilla deutsch

IT-System: Client1, 50000 Client1 (Client/PC unter Windows 2000)

Standort: Raum 101, 50000 Raum 101

	Anzahl Maßnahmen	Durchgeführt	Nicht durchgeführt	Teilweise durchgeführt	entbehrlich	unbea
B 5.07 Windows 2000 Client	47	36 (76,60%)	0 (0,00%)	0 (0,00%)	1 (2,13%)	10 (21)
Priorität 1	23	20 (86,96%)	0 (0,00%)	0 (0,00%)	1 (4,35%)	2 (8)
Priorität 2	22	16 (72,73%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	6 (27)
Priorität 3	2	0 (0,00%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	2 (100)
Summe (Bausteine): Client1, 50000 Client1	47	36 (76,60%)	0 (0,00%)	0 (0,00%)	1 (2,13%)	10 (21)
Priorität 1	23	20 (86,96%)	0 (0,00%)	0 (0,00%)	1 (4,35%)	2 (8)
Priorität 2	22	16 (72,73%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	6 (27)
Priorität 3	2	0 (0,00%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	2 (100)

IT-System: Client2, 50000 Client2 (Client/PC unter Windows 2000)

Fertig

Baustein: vollständig umgesetzt

The screenshot displays the GSTOOL 3.1 application window. The title bar reads "GSTOOL 3.1". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Extras", "Datenbank", "Fenster", and "Hilfe". The toolbar contains icons for "Neu", "Öffnen", "Speichern", "Löschen", "Aktualisieren", "Filter", "Modell", "Ansicht", "Navigator", and "Fenster".

The main window is divided into two panes. The left pane shows a tree view of assets under the folder "Mustermann (Prio 1 oder 2) und Siegelstufe A". The tree structure is as follows:

- 50000 Hauptsitz Fa. Mustermann
 - übergreifende Aspekte / 50000 Hauptsitz Fa. Mustermann
 - 50000 Bürogebäude Musterstr. 1
 - 50000 Client1
 - B 5.07 Windows 2000 Client (selected)
 - ABC M 2.9 Nutzungsverbot nicht freigegebener Hard-
 - ABC M 2.13 Ordnungsgemäße Entsorgung von schüt;
 - ABC M 2.25 Dokumentation der Systemkonfiguration
 - ABC M 2.26 Ernennung eines Administrators und eine
 - ABC M 2.30 Regelung für die Einrichtung von Benutz
 - ABC M 2.31 Dokumentation der zugelassenen Benutz
 - ABC M 2.34 Dokumentation der Veränderungen an ei
 - ABC M 2.35 Informationsbeschaffung über Sicherheit;
 - ABC M 2.227 Planung des Windows 2000 Einsatzes
 - ABC M 2.228 Festlegen einer Windows 2000 Sicherh

The right pane, titled "Eigenschaften der Bausteinzuzuordnung", shows the details for the selected asset "B 5.07 Windows 2000 Client". The tabs are "Allgemein", "Befragung", "Gefährdungen", and "Notizblock". The "Allgemein" tab is active, showing:

- Nr./Bezeichnung: B 5.07 Windows 2000 Client
- Bearbeitet: ja
- Im Zielobjekt: (nicht referenziert)
- Erläuterung: (empty text area)
- Erfasst am: 21.04.2005

The status bar at the bottom shows the following information: Standard, WINXPPRO-1\Administrator, WINXPPRO-1\BSI, BSID6_V310, NUM, 20:2

6. Umsetzung von Sicherheitsmaßnahmen

- Abarbeitung der Empfehlungen des GSHB
- Erfolgt nicht durch den Auditor sondern durch einen IT-Dienstleister oder internes Personal
- Optional: Nachkontrolle

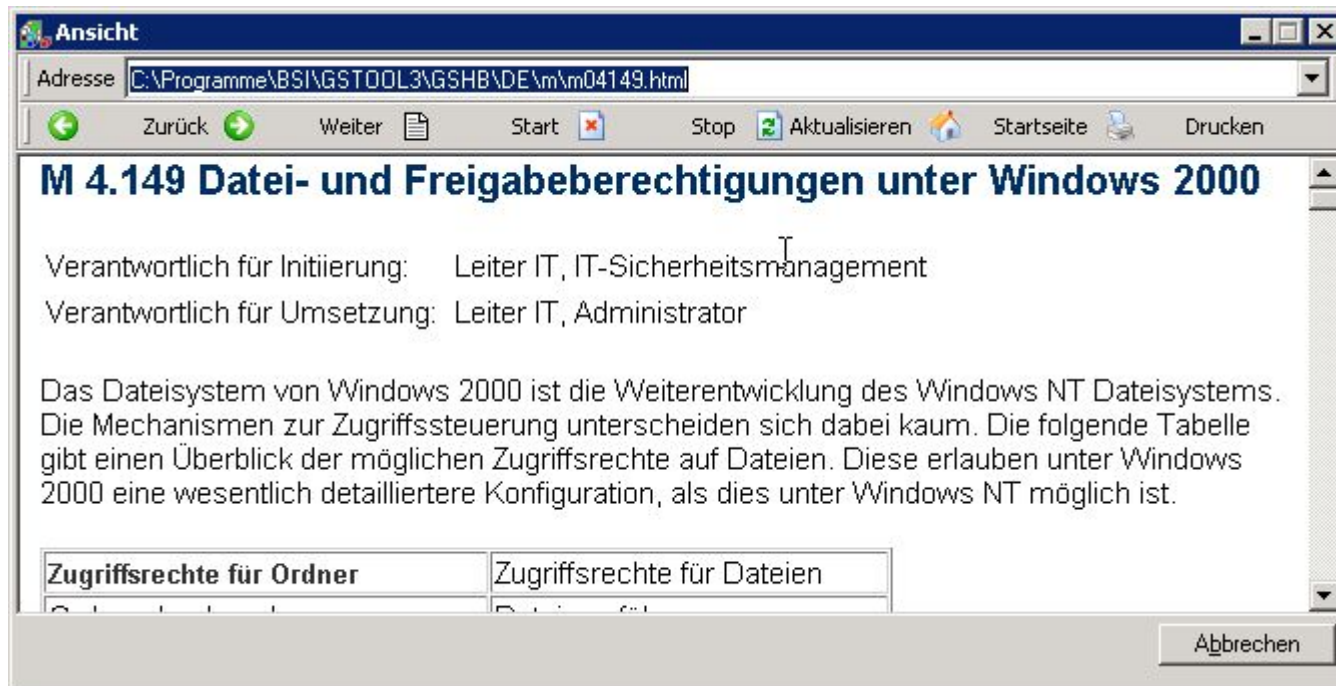
Beispiel: nicht umgesetzte Maßnahme

The screenshot shows the GSTOOL 3.1 application window. The menu bar includes 'Datei', 'Bearbeiten', 'Ansicht', 'Extras', 'Datenbank', 'Fenster', and 'Hilfe'. The toolbar contains icons for 'Neu', 'Öffnen', 'Speichern', 'Löschen', 'Aktualisieren', 'Filter', 'Modell', 'Ansicht', 'Navigator', and 'Fenster'. The main window is divided into two panes. The left pane shows a tree view of measures under the folder 'Mustermann (Prio 1 oder 2) und Siegelstufe A'. The right pane, titled 'Eigenschaften der Maßnahme', displays the details for the selected measure 'M 4.149 Datei- und Freigabeberechtigungen unter Windows 2000'. The 'Umsetzung' (Implementation) status is set to 'nein' (no).

Eigenschaften der Maßnahme				
Umsetzung	Kosten	Revision	Verantwortlich	Notizblock
Nr./Bezeichnung:	M 4.149	Datei- und Freigabeberechtigungen unter Windows 2000		
Baustein:	B 5.07	Windows 2000 Client		
Priorität:	1	Erforderlich ab:	A-Eingangsstufe	
Umsetzung:	nein			

Standard WINXPPRO-1\Administrator WINXPPRO-1\BSI BSIDB_V310 NUM 11:27 22.04.2005

Informationen zu Maßnahmedetails



The screenshot shows a web browser window with the following content:

Adresse: C:\Programme\BSI\GSTOOL3\GSHB\DE\m\m04149.html

Zurück Weiter Start Stop Aktualisieren Startseite Drucken

M 4.149 Datei- und Freigabeberechtigungen unter Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement
Verantwortlich für Umsetzung: Leiter IT, Administrator

Das Dateisystem von Windows 2000 ist die Weiterentwicklung des Windows NT Dateisystems. Die Mechanismen zur Zugriffssteuerung unterscheiden sich dabei kaum. Die folgende Tabelle gibt einen Überblick der möglichen Zugriffsrechte auf Dateien. Diese erlauben unter Windows 2000 eine wesentlich detailliertere Konfiguration, als dies unter Windows NT möglich ist.

Zugriffsrechte für Ordner	Zugriffsrechte für Dateien

Abbrechen

7. Zertifizierung (optional)

- Selbsterklärung oder Zertifizierung durch das BSI
- Kann einen Wettbewerbsvorteil bedeuten
- Bisher wenig verbreitet