# IT-Sicherheitsleitfaden für mittelständische Wirtschaftsunternehmen

Herausgeber:
Netzwerk emsländischer IT-Leiter
**„DE-IT-Emsland"**
Arbeitskreis IT-Sicherheit

September 2006

# IT-Sicherheitsleitfaden für mittelständische Wirtschaftsunternehmen

Für das Netzwerk emsländischer IT-Leiter „DE-IT-Emsland“:
Der Arbeitskreis IT-Sicherheit:

**Jörg Brundiers, ANF-Framatome - ANP**
**Uwe Ehmke, Berentzen-Gruppe AG**
**Martin Knief, BP-Erdöl-Raffinerie-Emsland**
**Reiner Korth, Kernkraftwerke Lippe-Ems GmbH**
**Klaus Laake, Erwin Müller GmbH**
**Torsten Marx, Klasmann Deilmann GmbH**
**Volker Paus, Metabowerke GmbH – Business Unit Elektra Beckum**
**Prof.Dr.Reinhard Rauscher, FH-Osnabrück, Standort Lingen**
**Jürgen Vogler, Emsland GmbH**
**Marco Zimmermann, Erwin Müller GmbH**

# Vorwort

In wohl kaum einem anderen unternehmerischen Bereich wachsen die Anforderungen und damit die Herausforderungen so schnell wie im betrieblichen informationstechnologischen Umfeld.

Der mittelständische IT-Leiter steht dabei zentral in der Verantwortung, die Funktionssicherheit und Verfügbarkeit aller betrieblich eingesetzten Hard- und Softwarekomponenten zu gewährleisten. Ein Ausfall der Datenverarbeitungsanlagen und der damit verbundenen Produktion ist in der Regel mit hohen Kosten verbunden, von der Gefahr einer möglichen nachfolgenden Insolvenz des Betriebes ganz zu schweigen. Dabei ist die IT fast täglich neuen Gefahren von innen und außen, egal ob bewusst oder unbewusst verursacht, ausgesetzt. Eine den einzelbetrieblichen Umständen angepasste IT- Sicherheitsstrategie ist deshalb unausweichlich.

Im Arbeitskreis „IT-Sicherheit“ des emsländischen Netzwerkes von IT- Leitern „DE-IT-Emsland“ treffen sich regelmäßig Führungskräfte größerer emsländischer Unternehmen zur gemeinsamen Risikoanalyse. In Diskussionen und Informationsveranstaltungen zeigte sich schnell, dass die vielfältigen Sicherheitserfordernisse durch den Erfahrungsaustausch transparenter und in der Praxis erprobte Lösungsansätze gerne an die Netzwerkpartner weiter vermittelt wurden.
Man beschloss, die vorhandenen Erkenntnisse aufzubereiten und zusammenzufassen und allen interessierten Betrieben als Leitfaden zur Verfügung zu stellen. Die vorliegende Arbeit fasst die Beiträge der einzelnen Netzwerkmitglieder zusammen. Die Ergebnisse sind dazu geeignet, den Rahmen für weiterführende Überlegungen in den einzelnen Betrieben zu bilden.
Dieser Rahmen beschränkt sich nach Meinung der Autoren auf das Wesentliche und erhebt keinen Anspruch auf Vollständigkeit. Er richtet das Augenmerk auf die dringlichsten IT-Sicherheitserfordernisse im betrieblichen Alltag unserer Zeit. Aus der Praxis für die Praxis.

Meppen, im September 2006
Die Verfasser

# Inhaltsverzeichnis

# IT-Sicherheitsziele

Die IT-Sicherheitsziele müssen festgelegt werden, damit angemessene Maßnahmen definiert werden können. Der erste Schritt bei der Beschäftigung mit IT-Sicherheit ist die Bestandsaufnahme der Rahmenbedingungen (Gesetze, Verträge, Kundenanforderungen, Konkurrenzsituation). [1]In einem weiteren Schritt werden IT-Anwendungen klassifiziert und in ihrer Bedeutung für die Erfüllung unternehmerische Ziele eingestuft. Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und IT-Systemen spielen dabei eine wichtige Rolle.

### Zu berücksichtigende Gesetze

1. KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, z.B. Forderung nach Risikomanagement)
2. GmbH-Gesetz
3. HGB (§ 317, Abs. 4)
4. Gesetz zur Nutzung von Telediensten
5. Telekommunikationsgesetz
6. Urheberrechte
7. Richtlinien auf EU-Ebene
8. Datenschutzgesetz
9. Strafgesetzbuch
10. BASEL II

### Zu berücksichtigende Verträge
Hier müssen firmenspezifische Einträge erfolgen

### Zu berücksichtigende Kundenanforderungen
Hier müssen firmenspezifische Einträge erfolgen

### Zu berücksichtigende Konkurrenzsituation
Hier müssen firmenspezifische Einträge erfolgen

### Zu berücksichtigende ISO-Zertifizierung
Hier müssen firmenspezifische Einträge erfolgen

[1] Vgl. Leitfaden IT-Sicherheit 2004, S. 23

# Rollendefinition der IT und IT-Sicherheit

Die IT- und Kommunikationstechnik bildet die Basis für (fast) alle Geschäftsprozesse. Sie ermöglichen und optimieren elektronische Geschäftsprozesse, sie unterstützen den Anwender in seiner täglichen Aufgabenerfüllung. Fallen IT-Systeme aus, besteht die Gefahr von wirtschaftlichen Schäden.

## Definitionen

**Sicherheit**
Zustand des Geschütztseins vor Gefahren oder Schaden (Definition nach Duden)

**IT-Sicherheit**
Schutz von Informationen und IT-Systemen bzgl. Vertraulichkeit, Verfügbarkeit und Integrität

**IT-Sicherheitsmaßnahmen**
Es handelt sich um Maßnahmen zur Erreichung einer angemessenen IT-Sicherheit unter Berücksichtigung von technischen, organisatorischen, personellen und infrastrukturellen Aspekten

**IT-Sicherheitskonzept**
Ein IT-Sicherheitskonzept beinhaltet die IT-Strukturanalyse (Ist-Aufnahme), die Schutzbedarfsfeststellung, die Grundschutzanalyse und die Realisierungsplanung

**IT-Sicherheitsmanagement**
Die Kernaufgabe bildet die Erstellung des IT-Sicherheitskonzepts

**IT-Sicherheitsprozess**
Der IT-Sicherheitsprozess umfasst alle Maßnahmen zur Erreichung eines angemessenen Sicherheitsniveaus, von der Definition von Sicherheitszielen bis zur Aufrechterhaltung im laufenden Betrieb

- Die IT-Sicherheit muss unter folgenden Aspekten betrachtet werden
  - rechtliche Aspekte wie Verantwortung/Haftung bei Versäumnissen bzgl. IT-Sicherheit und Schutz vertraulicher und personenbezogener Daten/Informationen
  - wirtschaftliche Aspekte wie Schäden in Folge von IT-Risiken
  - spezifische Bedrohungen wie Viren, Würmer, Trojaner, Störfaktor Mensch, Katastrophen etc.

- Dabei werden folgende Werte geschützt
  - Betriebliches Know-How
  - Betriebsgeheimnisse
  - personenbezogene Daten
  - IT-Systeme

- bzw. folgende Schadensfälle vermieden
  - Ausfall von IT-Systemen (durch Zerstörung, Diebstahl, menschliche Fehler, etc. )
  - fehlendes Backup
  - Viren
  - Hackerangriff
  - Personalausfall (z.B. Administrator)
  - Innentäter

- Die "Schutzbedarfsfeststellung" ist notwendiger Bestandteil jeder Sicherheitsanalyse. Sie soll sicherstellen, dass die definierten Schutzziele und die hieraus abgeleiteten Sicherheitsmaßnahmen angemessen sind und den individuellen Gegebenheiten entsprechen. Da sich Rahmenbedingungen im Laufe der Zeit ändern können, sollte regelmäßig überprüft werden, ob die Einstufung des Schutzbedarfs noch der aktuellen Situation entspricht. Bei der Schutzbedarfsfeststellung ist die Orientierung an den drei Grundwerten der IT-Sicherheit **Vertraulichkeit, Integrität** und **Verfügbarkeit** hilfreich [1]

[1] vgl. Leitfaden IT-Sicherheit 2004, S. 23

# Der IT-Sicherheitsbeauftragte[1]

Diese Person kann in einer Stabsstelle der Unternehmensleitung zugeordnet werden. Sie baut eigene Fachkompetenz zur IT-Sicherheit auf und ist für alle IT-Sicherheitsfragen in der Organisation zuständig. Die Benennung eines IT-Sicherheitsbeauftragten ist gesetzlich bisher nicht vorgeschrieben.

**Aufgaben**

- im gesamten IT-Sicherheitsprozess mitzuwirken
- dem IT-Sicherheitsmanagement-Team und der Leitungsebene zu berichten
- die IT-Sicherheitsleitlinie zu erstellen
- die Erstellung des IT-Sicherheitskonzepts zu koordinieren
- die Erstellung des Notfallvorsorgekonzepts und anderer Teilkonzepte zu koordinieren
- die Erstellung des Realisierungsplans für IT-Sicherheitsmaßnahmen und die Initiierung und Überprüfung der Umsetzung
- den Informationsfluss zwischen IT-Sicherheitsbeauftragten, die zuständig für bestimmte IT-Bereiche, IT-Projekte sowie IT-Systeme sind, sicherzustellen und
- auftretende sicherheitsrelevante Zwischenfälle festzustellen und zu untersuchen

# IT-Strukturanalyse

Die IT-Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines IT-Sicherheitskonzepts nach IT-Grundschutz benötigt werden. Sie gliedert sich in die Teilaufgaben

[1] Vgl. Web-Kurs zur Einführung in das IT-Grundschutzhandbuch, Kapitel 2: IT-Sicherheitsmanagement

- Netzplanerhebung
- Komplexitätsreduktion durch Gruppenbildung und
- Erhebung der IT-Systeme:
  - Übersicht Server
  - Übersicht Clients
  - Übersicht Netzkomponenten
  - Übersicht Telekommunikationskomponenten

## Netzplanerhebung

Die Netzplanerhebung wird am Beispielunternehmen „RECPLAST GmbH“ aufgezeigt[1]

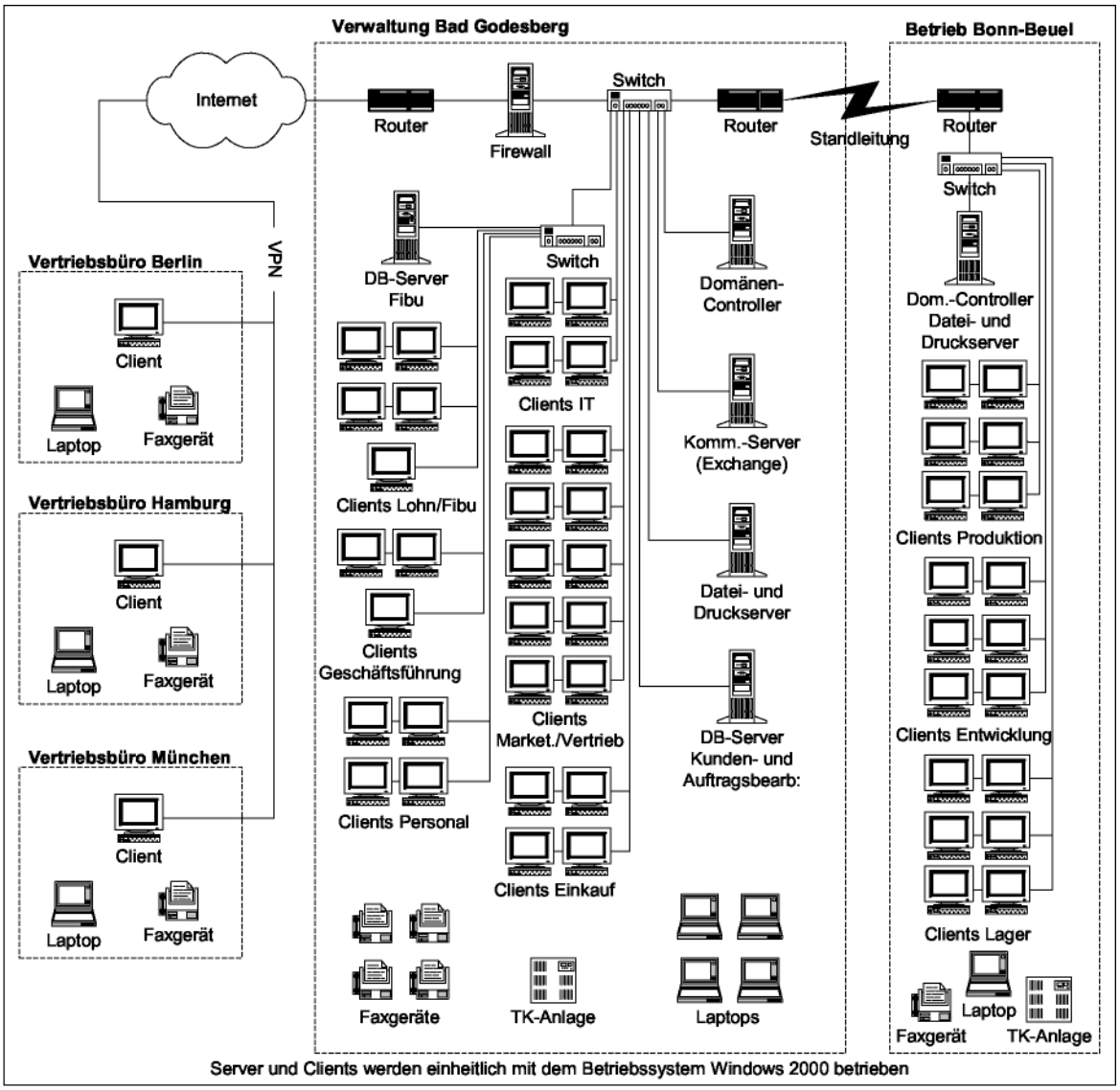
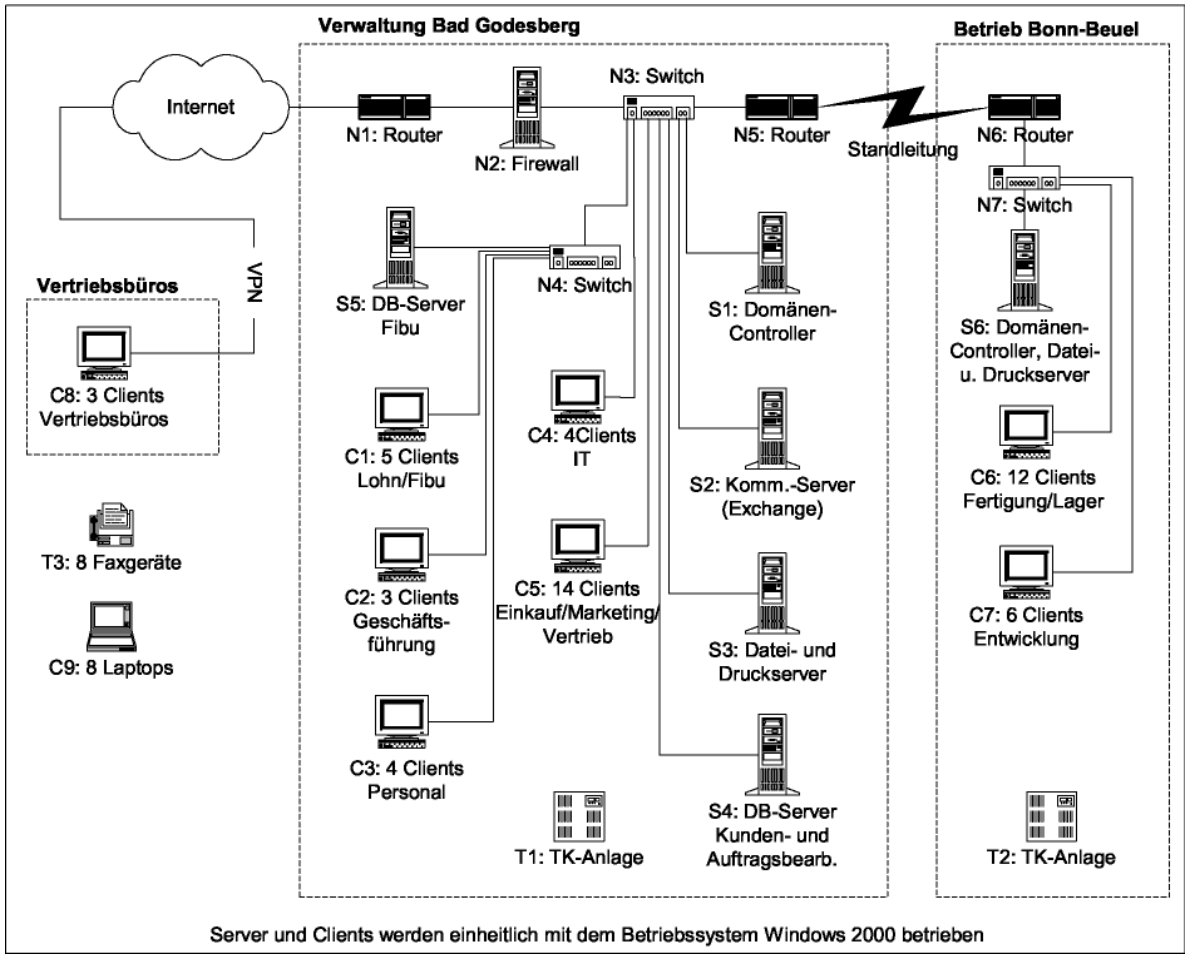



**Abbildung 2: Netzplan der RECPLAST GmbH**

[1] Vgl. BSI Schulung IT-Grundschutz, Beispielunternehmen „RECPLAST GmbH“

## Komplexitätsreduktion durch Gruppenbildung[1]




## Erhebung der IT-Systeme

### Übersicht Server[2]

| Nr. | Beschreibung | Plattform | Standort | Anzahl | Status | Benutzer/Admin. |
|---|---|---|---|---|---|---|
| S1 | Domänen-Controller | Windows 2000 Server | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | alle IT-Benutzer/ IT-Administration |
| S2 | Interner Kommuni-kationsserver | Windows 2000 Server | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | alle IT-Benutzer/ IT-Administration |
| S3 | Datei- und Druckserver | Windows 2000 Server | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | alle IT-Benutzer/ IT-Administration |
| S4 | DB-Server Kunden- und Auftragsbearbeitung | Windows 2000 Server | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | Marketing und Vertrieb, Fertigung, Lager/ IT-Administration |
| S5 | DB-Server Finanzbuchhaltung | Windows 2000 Server | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | Mitarbeiter Lohn/Fibu |
| S6 | Server Beuel | Windows 2000 Server | Beuel, R. 2.01 (Serverraum) | 1 | In Betrieb | Alle Mitarbeiter in Beuel |

[1] Vgl. BSI Schulung IT-Grundschutz, Beispielunternehmen „RECPLAST GmbH“
[2] Vgl. a.a.O.

## Übersicht Clients[1]

| Nr. | Beschreibung | Plattform | Standort | Anzahl | Status | Benutzer/Admin. |
|---|---|---|---|---|---|---|
| C1 | Clients in der Finanzbuchhaltung | Windows 2000 Client | BG, R. 2.10 – 2.12 | 4 | In Betrieb | Mitarbeiter in der Finanzbuchhaltung |
| C2 | Clients der Geschäftsführung | Windows 2000 Client | BG, R. 1.10 – 1.13 | 3 | In Betrieb | Geschäftsführung |
| C3 | Clients der Personalabteilung | Windows 2000 Client | BG, R. 1.07 – 1.09 | | In Betrieb | Mitarbeiter der Personalabteilung |
| C4 | Clients der Informationstechnik | Windows 2000 Client | BG, R. 1.03 – 1.06 | 4 | In Betrieb | Mitarbeiter IT / IT-Administration |
| C5 | Clients Kunden- und Auftragsbearbeitung | Windows 2000 Client | BG, R. 2.03 – 2.09 | 14 | In Betrieb | Einkauf, Marketing und Vertrieb |
| C6 | Clients Fertigung und Lager | Windows 2000 Client | Beuel, R. 2.10 – 2.13 | 12 | In Betrieb | Mitarbeiter Fertigung und Lager |
| C7 | Clients in Entwicklungsabteilung | Windows 2000 Client | Beuel, R. 2.14 – 2.20 | 6 | In Betrieb | Entwicklung/ IT-Administration |
| C8 | Clients in Vertriebsbüros | Windows 2000 Client | Vertriebsbüros (Berlin, Hamburg, München) | 3 | In Betrieb | Mitarbeiter in Vertriebsbüros/ IT-Administration |
| C9 | Laptops | Windows 2000 Client | 4 in BG, je 1 in Beuel und in den Vertriebsbüros | 8 | In Betrieb | Mitarbeiter Vertrieb/ IT-Administration |

## Übersicht Netzkomponenten[2]

| Nr. | Beschreibung | Plattform | Standort | Anzahl | Status | Benutzer/Admin. |
|---|---|---|---|---|---|---|
| N1 | Router zum Internet | DSL-Router | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | Alle IT-Benutzer/ IT-Administration |
| N2 | Firewall | Windows 2000 | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | Alle IT-Benutzer/ IT-Administration |
| N3 | Zentraler Switch in Bad Godesberg | | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | alle IT-Benutzer/ IT-Administration |
| N4 | Switch für Personalabteilung | | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | Personalabteilung, GF, Lohn, Fibu/ IT-Administration |
| N5 | Router zur Anbindung des Standorts Beuel | Router | BG, R. 1.02 (Serverraum) | 1 | In Betrieb | alle IT-Benutzer/ IT-Administration |
| N6 | Router zur Anbindung nach Bad Godesberg | Router | Beuel, R. 2.02 (Technikraum) | 1 | In Betrieb | alle IT-Benutzer/ IT-Administration |
| N7 | Switch in Beuel | | Beuel, R. 2.02 (Technikraum) | 1 | In Betrieb | alle IT-Benutzer/ IT-Administration |

[1] Vgl. BSI Schulung IT-Grundschutz, Beispielunternehmen „RECPLAST GmbH“
[2] Vgl. a.a.O.

**Übersicht Telekommunikationskomponenten[1]**

| Nr. | Beschreibung | Plattform | Standort | Anzahl | Status | Benutzer/Admin. |
|---|---|---|---|---|---|---|
| T1 | Telefonanlage BG | ISDN-TK-Anlage | BG, R. 1.01 | 1 | In Betrieb | alle Mitarbeiter in BG/ IT-Administration |
| T2 | Telefonanlage Beuel | ISDN-TK-Anlage | Beuel, R. 2.02 | 1 | In Betrieb | alle Mitarbeiter in Beuel/ IT-Administration |
| T3 | Faxgeräte | | 4 in BG, je 1 in Beuel und in den Vertriebsbüros | 8 | In Betrieb | Alle Mitarbeiter |

## Erfassung der IT-Anwendungen und der zugehörigen Informationen[2]

Hier sollten alle IT-Anwendungen erfasst werden, deren Daten, Informationen und Programme den höchsten Bedarf an Vertraulichkeit (Geheimhaltung), Integrität (Korrektheit, Unverfälschtheit) und Verfügbarkeit (kürzeste tolerierbare Ausfallzeit) besitzen

| 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 | Benutzer-Authentisierung | X | | X | | | | X | |
| A5 | Systemmanagement | | | X | | | | | |
| A6 | E Xchange (E-Mail, Terminkalender) | X | | | X | | | | |
| A7 | zentrale Dokumentenverwaltung | | | | | X | | | |

Legende: $A_i$ X $S_j$ = Die Ausführung der IT-Anwendung $A_i$ hängt vom IT-System $S_j$ ab.

[1] Vgl. BSI Schulung IT-Grundschutz, Beispielunternehmen „RECPLAST GmbH“
[2] Vgl. IT-Grundschutzhandbuch, CD-Version März 2005, Bonn, BSI

# Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung gliedert sich in 4 Schritte:

- Schutzbedarf der IT-Anwendungen
- Schutzbedarf der IT-Systeme
- Schutzbedarf der Übertragungsstrecken
- Schutzbedarf der IT-Räume

Nach dem BSI-Grundschutzhandbuch wird der Schutzbedarf in 3 Kategorien unterteilt:

- niedrig bis mittel
- hoch
- sehr hoch

Die Schutzbedarfsfeststellung untersucht in jedem Schritt den Schutzbedarf hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität. Die mögliche Höhe eines materiellen oder ideellen Schadens bestimmt letztendlich den Schutzbedarf. Mögliche Schadensszenarien sind:

- Verstoß gegen Gesetze, Vorschriften und Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Auswirkungen
- Finanzielle Auswirkungen

| IT-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 | mittel | Der Schutzbedarf ist nur mittel, da Fehler rasch erkannt und die Daten nachträglich korrigiert werden können. |
| | | | Verfügbarkeit | mittel | Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden. |
| A2 | Beihilfeabwicklung | X | Vertraulichkeit | 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. |
| | | | Verfügbarkeit | mittel | Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden. |

**Tabelle 1: Beispiel Schutzbedarf von IT-Anwendungen**

Die Ergebnisse der Schutzbedarfsfeststellung können in einer Tabelle abgebildet werden. Die vorstehende Tabelle zeigt ein Beispiel aus dem BSI-Grundschutzhandbuch[1].

Für die weitere Vorgehensweise der IT-Sicherheitskonzeption müssen nun alle Ergebnisse der Schutzbedarfsfeststellung interpretiert werden. Für Objekte mit hohem oder sehr hohem Schutzbedarf sollten ergänzende Sicherheitsanalysen erfolgen.

## Realisierung von IT-Sicherheitsmaßnahmen

- **Handlungsplan**

Aufgrund der Vielzahl von Aufgaben im Bereich IT-Sicherheit sollte ein Handlungsplan erstellt werden, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen IT-Sicherheitsmaßnahmen regelt. Die Priorisierung sollte Kosten-Nutzen-Aspekte berücksichtigen

- **Verantwortlichkeit**

Für alle IT-Sicherheitsmaßnahmen müssen Zuständigkeiten, Verantwortlichkeiten und Vertretungsregeln festgelegt werden. Die wichtigsten Passwörter müssen für Notfälle sicher hinterlegt werden

- **Information und Schulung**

Die bestehenden Richtlinien und Zuständigkeiten müssen allen Zielpersonen bekannt sein. Die betroffenen Mitarbeiter müssen über einzelne Maßnahmen und den damit verbundenen Konsequenzen unterrichtet werden. Hilfreich sind hier Checklisten mit Hinweisen für den Eintritt und den Austritt von Mitarbeitern. (Berechtigungen, Schlüssel, Unterweisung etc.) Ein besonderes Augenmerk sollte hierbei auf Auszubildende und Praktikanten gelegt werden

- **Dokumentation**

Das IT-Sicherheitskonzept sollte dokumentiert und regelmäßig aktualisiert werden

[1] IT-Grundschutzhandbuch: 2. EL Stand Oktober 2000, S. 52

# Sicherheit von IT-Systemen

## Als wichtig erachtete Aktivitäten[1]

### Patch-Management

- Nach der Erstinstallation sind sofort alle verfügbaren Patches für Betriebssysteme und Applikationen einspielen. Hier werden oft die Unix-Systeme vernachlässigt, aber auch hier gibt es Updates und Patches. Um IT-Systeme abzusichern, ist eine regelmäßige Informationsbeschaffung über neu aufgedeckte Schwachstellen und Hilfsmittel zu deren Beseitigung notwendig.

  In "neueren" Programmversionen wurden sicherheitsrelevante Schwachstellen in der Regel vom Hersteller beseitigt. Dies erspart jedoch nicht eine individuelle Betrachtung, da neue Versionen in der Regel auch neue Funktionen und Fehler beinhalten, die andere Gefahren mit sich bringen. Jeder Systemverantwortliche sollte in regelmäßigen Abständen die Zeit für entsprechende Suchen im Internet und für den Austausch mit Fachkollegen aufbringen. Nach wie vor gibt es zahlreiche frei erhältliche Informationsdienste, deren Angebot jenes kommerzieller Anbieter oft qualitativ übersteigt. Die Fülle ständig neu veröffentlichter Updates und Sicherheits-Patches macht zudem einen Auswahlprozess erforderlich. In der Regel können nicht alle installiert werden, insbesondere nicht im Rahmen einer Sofortmaßnahme. Daher sollte bereits im Vorfeld Einvernehmen darüber bestehen, nach welchen Auswahlkriterien bestimmt wird, welche Updates mit wie viel Zeitverzug installiert werden können bzw. müssen.

### Virenschutzkonzept

Installierte Virenscanner sollten über stündliche oder halbtägliche Aktualisierungsfunktionen verfügen. Bei Anwendung eines mehrstufigen Virenschutzkonzeptes sollte darauf geachtet werden, dass die Installation darauf abgestimmt wird.

---

[1] Vgl. Bundesamt für Sicherheit in der Informationstechnik (August 2004): Sicherheit in der Informationstechnik)

- Unnötige Dienste abschalten

  Alle Funktionen, Serverdienste und offenen Kommunikationsports, die nach außen angeboten werden, erhöhen das Risiko einer möglichen Sicherheitslücke. Deshalb sollte in jedem einzelnen Fall sorgfältig geprüft werden, ob es wirklich erforderlich ist, einen potentiellen "Problemkandidaten" zu aktivieren und nach außen anzubieten. Das damit verbundene Sicherheitsrisiko kann in Abhängigkeit von der jeweiligen Technik und Implementierung sehr unterschiedlich sein. Bei bestehenden Installationen sollte regelmäßig überprüft werden, ob einzelne Dienste oder Funktionen nicht schlicht aus Versehen oder Bequemlichkeit aktiviert sind, obwohl sie von niemandem benötigt werden.

- Schutzmechanismen der Anwendungen und des Betriebssystems sollten genutzt werden

  Viele Programme, die in einem gewöhnlichen Client-Server-basierten Netz zur Bürokommunikation genutzt werden, verfügen inzwischen über eine Vielzahl hervorragender Schutzmechanismen. Fast immer resultieren Schwachstellen aus falscher Konfiguration oder aus Unkenntnis der vorhandenen Möglichkeiten zur Absicherung. Die vom Hersteller implementierten Sicherheitsfunktionen und - mechanismen sollten daher analysiert, verstanden und eingesetzt werden, bevor existierende Sicherheitsanforderungen nicht oder nur auf Umwegen umgesetzt werden.

- Anwendungen oder Dienste sollte man möglichst nicht als „root-user“ oder Administrator laufen lassen. Ausführbare Programme verfügen - analog zu Anwendern - über bestimmte Zugriffsrechte und Systemprivilegien. In vielen Fällen erbt ein Programm einfach die Berechtigungen des Benutzers, der das Programm gestartet hat. Manchmal genügen diese Berechtigungen nicht, oder es handelt sich um Serverprozesse, die oft mit hohen Privilegien ausgestattet sein müssen. In solchen Fällen besitzen Programme manchmal so genannte „root-Rechte“ und können ebenso wie ein "allmächtiger" Systemadministrator alle Systemressourcen nutzen. Werden solche Programme von einem Angreifer zweckentfremdet, so erbt dieser wiederum alle Rechte von dem missbrauchten Programm. Auch Programme dürfen nur mit den Berechtigungen ausgestattet sein, die sie für ein fehlerfreies Funktionieren benötigen.

- Default-Einstellungen und Default-User/Passwörter sollten geprüft und sofern möglich ggf. gelöscht/geändert werden. Viele Betriebssysteme und Softwareapplikationen sind vom Hersteller derart vorkonfiguriert, dass nach erfolgter Installation ein möglichst reibungsloser (und komfortabler) Betrieb ermöglicht wird. Häufig sind Standardpasswörter und Standard-Benutzer-Accounts eingerichtet. Um Missbrauch zu vermeiden, müssen diese deaktiviert werden. Ein frisch installiertes und noch nicht an die eigenen (Sicherheits-) Bedürfnisse angepasstes System sollte deshalb nie im produktiven Betrieb genutzt werden!

- Erstellen einer System- und Installationsdokumentation/ Erstellen eines Images. Es ist ratsam, alle Arbeitsschritte vor, während und nach einer Installation schriftlich zu dokumentieren. Dies hilft einem, im Wiederholungsfall schneller ans Ziel zu gelangen und im Problemfall die möglichen Ursachen aufzufinden. Ebenso wichtig ist es, dass die Systemdokumentation auch von Dritten (beispielsweise im Sinne eines "Ersatzadministrators" oder einer Urlaubsvertretung) nachvollzogen und verstanden werden kann. Dadurch werden Ausfallrisiken reduziert, wenn der hauptamtliche Administrator plötzlich nicht mehr zur Verfügung stehen sollte. Im Fall eines erfolgten Hackereinbruchs können zudem unbefugte Veränderungen am System schneller identifiziert werden.

## Pflege von IT-Systemen

Aufgrund der überaus kritischen Lage bzgl. Viren und Sicherheitsrisiken ist ein verstärktes Augenmerk auf das Update von infrastrukturrelevanten Komponenten zu legen. Auch für das Update von Anwendungsprogrammen bzw. den zugrunde liegenden Systemen ist ein Testprocedere zu erarbeiten:

- Sicherheitsupdates sind nach erfolgreichem Test unverzüglich auf allen relevanten Systemen einzuspielen

- Es ist unabdingbar, die Virensignaturen und Scan-Engines sowie die Firewall-Software auf einem aktuellen Stand zu halten, auch hier ist für eine zeitnahe Verteilung sowohl auf Desktops als auch auf Servern Sorge zu tragen. Weite-

ren Schutz bieten Hardwarefirewalls, die ebenso mit einer aktuellen Regelbasis und dem neusten Softwarestand versehen sein müssen

- Im Bereich „Anwendungsprogramme“ sollten Updates erst nach erfolgreichem Durchlaufen von Funktionstest in der IT-Abteilung erfolgen

- Im ERP-Umfeld sollten Änderungen, Updates und Entwicklungen auf dem Testsystem ausführlich sowohl auf Funktion als auch auf Integration getestet werden, bevor sie in Betrieb genommen werden

# Beachtung von Sicherheitserfordernissen

Unternehmen haben heute eine große Menge an vertraulichen und sicherheitsrelevanten Daten. Zum Schutz dieses Datenbestandes sollten einige Grundregeln beachtet werden:

- Generell sollte wenn möglich vermieden werden, vertrauliche Daten auf den lokalen Festplatten der PC / Laptop zu speichern. Die Ablage auf entsprechenden Netzwerklaufwerken ist zu bevorzugen!
- Vertrauliche Informationen sollten bei längerer Abwesenheit in verschlossenen Containern oder Schränken abgelegt werden. Dies gilt sowohl für Dokumente in elektronischer Form als auch für Papierdokumente. Mobile Datenträger (CD, Diskette, Memory-Stick) sollten eingeschlossen werden
- Computer mit vertraulichen Daten sollten ausgeschaltet oder vor unauthorisiertem Zugang geschützt werden (z.B. per Kennwort-geschütztem Bildschirmschoner). Laptops mit sensitiven Daten müssen bei längerer Abwesenheit vor Diebstahl geschützt werden. Dies kann per Sicherheitsschloss oder alternativ durch Einschließen im Container / Schrank erfolgen
- Flipcharts und Poster sollten eingeschlossen werden, wenn sie sensitive Daten enthalten. Whiteboards sind zu säubern. Bei kurzen Abwesenheiten (z.B. während des Mittagessens) sollte der Raum alternativ abgeschlossen werden
- Vertrauliche Informationen sollten bei Reparatur und Wartungsarbeiten, die nicht vor Ort stattfinden, durch ein geeignetes Verfahren zuverlässig gelöscht werden. Im Falle von kurzzeitigen Wartungsarbeiten vor Ort sollte ein Schutz von sensitiven Daten durch die ständige Begleitung des Wartungspersonals sichergestellt werden. Bei langfristigerer Anwesenheit von externen Mitarbeitern müssen diese durch eine Geheimhaltungserklärung zur vertraulichen Behandlung der Daten verpflichtet werden
- Die o. g. Sicherheitsmaßnahmen sind in einer Betriebsvereinbarung oder Organisationsanweisung festzuhalten. Bei Bedarf ist die Androhung personalrechtlicher Konsequenzen in die Regelung aufzunehmen. Alle Mitarbeiter sollten über diese Richtlinie informiert und auf durch Missachtung entstehende Risiken und Gefah-

ren hingewiesen werden. Regelmäßige (z. B. jährliche) Schulungen in Belangen der IT-Sicherheit sind unabdingbar

- Im Rahmen der technisch möglichen bzw. installierten Protokollierungs- und Überwachungsmöglichkeiten sind Leistungs- und Verhaltenskontrollen einzelner Mitarbeiter nicht zulässig. Bei begründetem Verdacht ist zur Abwehr von Schäden, zur Feststellung von Verstößen gegen Sicherheits- und Schutzvorschriften sowie zur Feststellung von Verstößen gegen berechtigte Schutzinteressen von Mitarbeitern und Unternehmen die Überwachung mit allen technischen Möglichkeiten innerhalb des gesetzlich zugelassenen Rahmens durch autorisierte Mitarbeiter der IT-Abteilung zulässig. Hierüber ist ggf. unverzüglich die Geschäftsführung zu unterrichten. Soweit Mitarbeiter durch Feststellungen betroffen sind, ist schnellstmöglich über die Personalabteilung die Personalvertretung oder der Betriebsrat zu unterrichten. Beabsichtigte sonstige Sicherheitsüberprüfungen ohne konkreten, begründeten Verdacht bedürfen der Zustimmung der Personalvertretung.

- Nicht mehr benötigte Datenträger sind dem Stand der Technik gemäß zu entsorgen, z.B. durch Schreddern, Magneten, etc. Von einer ausschließlichen Formatierung der Datenträger ohne Spezialsoftware, wie z.B. STEGANOS, muss abgesehen werden, da sie vollkommen unzureichend ist. Bei externer Vergabe der Entsorgung sollte ein Entsorgungsnachweis verlangt werden

- Remotezugriff: siehe „Vernetzung und Internet-Anbindung“

# Passwörter und Verschlüsselung

Kennwörter schützen den Zugang zum Netzwerk und zu sensiblen Daten. Ein effektiver Umgang mit Passwörtern und Verschlüsselungsmechanismen kann durch die Beachtung folgender Punkte erreicht werden

- Kennwörter müssen vertraulich behandelt werden, dürfen keinesfalls sichtbar und ungeschützt am Arbeitsplatz hinterlegt sein und müssen Komplexitätsanforderungen genügen. Eine Kennwortlänge sollte mindestens 8 Zeichen betragen. Das Kennwort kann aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Das Kennwort muss aus drei der vier vorher genannten Bestandteile zusammengesetzt sein!
- Biometrische Verfahren sind einem Kennwortschutz vorzuziehen
- Sofern Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz und Verschlüsselung bieten, sind diese Mechanismen zu aktivieren. Voreingestellte oder leere Passwörter sind umgehend zu ersetzen
- Bei Abwesenheit vom Arbeitsplatz ist der PC in jedem Fall vor unbefugter Benutzung zu sichern. Dies kann per passwortgeschützten Bildschirmschoner oder manuell mit der Tastenkombination <Strg> <Alt> <Entf> und der Schaltfläche "Computer sperren" erfolgen
- Der Verschlüsselung von mobilen Geräten (Notebooks, PDAs) ist besondere Aufmerksamkeit zu widmen. Geeignete Maßnahmen sind z.B. Festplattenverschlüsselung, PDA-Verschlüsselung, etc...
- Gerade Notebooks sind besonders sicherheitsempfindlich bezüglich eines möglichen Datendiebstahls
- Die o. g. Informationen müssen jedem Arbeitnehmer erläutert werden und sollten in einer PC-Richtlinie festgehalten werden

# Vernetzung und Internet-Anbindung

In der heutigen Zeit spielt die Vernetzung der DV innerhalb der Unternehmen eine immer größere Rolle, Stichworte wie „Voice over IP“, VPN und Multimedia Networks tauchen immer häufiger in der Presse auf. Folgende Stichpunkte sollen Hilfestellung bei der Planung / Erneuerung einer Netzwerkstruktur geben

## Vernetzung

### Topologie

- Als Netzwerk-Topologie ist nur die sternförmige Verteilung über CAT 5 – CAT 7 Kabel zu empfehlen

- Beim Einsatz von WLAN (Funk-) Netzen ist derzeit aus Sicherheitsgründen besonders darauf zu achten, dass der WPA -Standard genutzt wird. Des Weiteren sollte die SSID unsichtbar gemacht werden

- Die BUS-Topologien ist wie die Ring-Topologie veraltet

- Nicht benötigte Netzwerkdosen sollten nicht geschaltet sein (im Patchfeld abgezogen oder im Switch abgeschaltet), um keinen unnötigen Angriffspunkt zu bieten

### Netztechnologie

- Die Verbindung der Netzwerkkabel sollten durch managebare Netzwerk-Switche geschaltet werden

- Die neueste Generation ermöglicht Authentifizierung über das Authentifizierungsverfahren RADIUS. Damit kann der Zugang zu den einzelnen Netzwerksegmenten über den RADIUS- Dienst gesteuert werden

- Des Weiteren sollten die Switche die VLAN-Technologie beherrschen, über diese können verschiedene Subnetze im LAN abgebildet werden (Server LAN, Client LAN usw. ), um die Netzsicherheit zu erhöhen

## Überwachung der Komponenten/des Netzes

- Die Netzwerkkomponenten sollten über das Managementprotokoll SNMP gemanagt werden. Darüber können Schnittstelleninformationen und –stati abgefragt werden. Es kann auch zum Steuern eingesetzt werden, was jedoch aus Sicherheitsgründen nicht genutzt werden sollte, da lediglich der SNMP-Community-String zur Zugriffssteuerung dient. Programme zur Überwachung können bspw. sein:

  Kostenlos: **NAGIOS**
  Mittl. Preissegment: **WhatsUP** (IPSWITCH Software)
  Gehob. Preissegment: **Openview Network Nodemanager** (HP)

- Bei den meisten Netzkomponenten ist eine rudimentäre Protokollierung möglich. Es ist aus Sicherheitsgründen zu empfehlen, die Protokollierung auf einen Protokoll Server (SYSLOG-Protokoll) auszurichten. Dadurch werden alle Informationen über das Netz an einer Stelle zusammengeführt

- Alle Switche haben die Möglichkeit, den gesamten Netzwerkverkehr auf einen so genannten Monitoring-Port zu schalten. Dieser ist dafür prädestiniert, ein Einbruchserkennungsystem (Intrusion Detection System = IDS) anzuschließen und somit den Netzverkehr auf Angriffssignaturen zu untersuchen und ggf. den Administrator zu verständigen oder andere Aktionen durchzuführen (z.B. die freie Software SNORT )

## Schutz der Netzkomponenten

- Die meisten Netzkomponenten können über ein Kennwort geschützt werden. Default-Kennworte müssen durch eigene Kennwörter ersetzt werden. Alternativ kann oft auch auf das bereits oben genannte RADIUS Verfahren zurückgegriffen werden, um Kennwörter zentral verwalten zu können. Jedoch wird ein Fallback-User mit Kennwort lokal angelegt werden müssen, falls der RADIUS Server ausfällt

- Es setzt sich zum inneren Schutz der Server-Subnetze oder der Maschinensteuerung langsam, aber sicher auch die Firewalltechnologie durch.
  VLANS werden dabei über eine Firewall verbunden. Somit besteht die Möglichkeit, den Netzverkehr gezielt zu steuern

# Internet Anbindung

## Screening Router

- Die Anbindung eines Firmennetzes erfolgt über eine Einwahlverbindung oder Standleitung. Um die Einwahl durchführen zu können, muß ein Einwahlrouter genutzt werden

- Dieser Router, der vor der eigentlichen Firewall sitzt, wird Screening Router genannt, wenn er neben der Einwahl auch Filter Aufgaben als Schutz der Firewall übernimmt

- Ein zweites Gerät kann/sollte auch zusätzlich an der inneren Schnittstelle postiert werden, um die Firewall gegen Standardangriffe aus dem internen Netz zu schützen. Somit dienen sie zum Schutz und der Entlastung der Firewall

## Firewall (siehe nächste Seite)

- Die Firewall ist das wichtigste Element zum Schutz gegen Angriffe aus dem Internet. Sie sollte als Application Level Firewall ausgelegt sein, damit bietet sie neben den Möglichkeiten, auf TCP/IP-Ebene zu filtern, auch die Möglichkeit, Dienste über Proxy Verfahren zu schützen. Ein- und ausgehender Netzwerkverkehr wird somit einmal unterbrochen, es ist kein direkter Zugriff aus dem Internet möglich

- In der heutigen Zeit ist es üblich, im Internet Daten und/oder Information bereit zu stellen. Um dies gesichert durchführen zu können, benötigt die Firewall mindestens drei Netzwerkinterfaces. Das primäre Interface zeigt zum Internet/Einwahlrouter. Das sekundäre Interface wird zum inneren Screening Router

geschaltet und das tertiäre Interface bildet die so genannte Demilitarisierte Zone (DMZ). In dieser sollten Webserver, eMail Virusscan Server unter Umständen auch RAS Server platziert werden. Dadurch ist eine gesondert geschützte Zone entstanden, die über den Regelsatz der Firewall geregelt werden kann

- Die meisten aktuellen Firewall-Lösungen bieten von Haus aus Remote Management Lösungen an. Es sollte zusätzlich darauf geachtet werden, dass auch die Firewall ihre Warnungen und Meldungen separat an einen SYSLOG Server senden kann. Somit sind Angriffsversuche, wie bei den Netzwerkkomponenten, zentral protokolliert

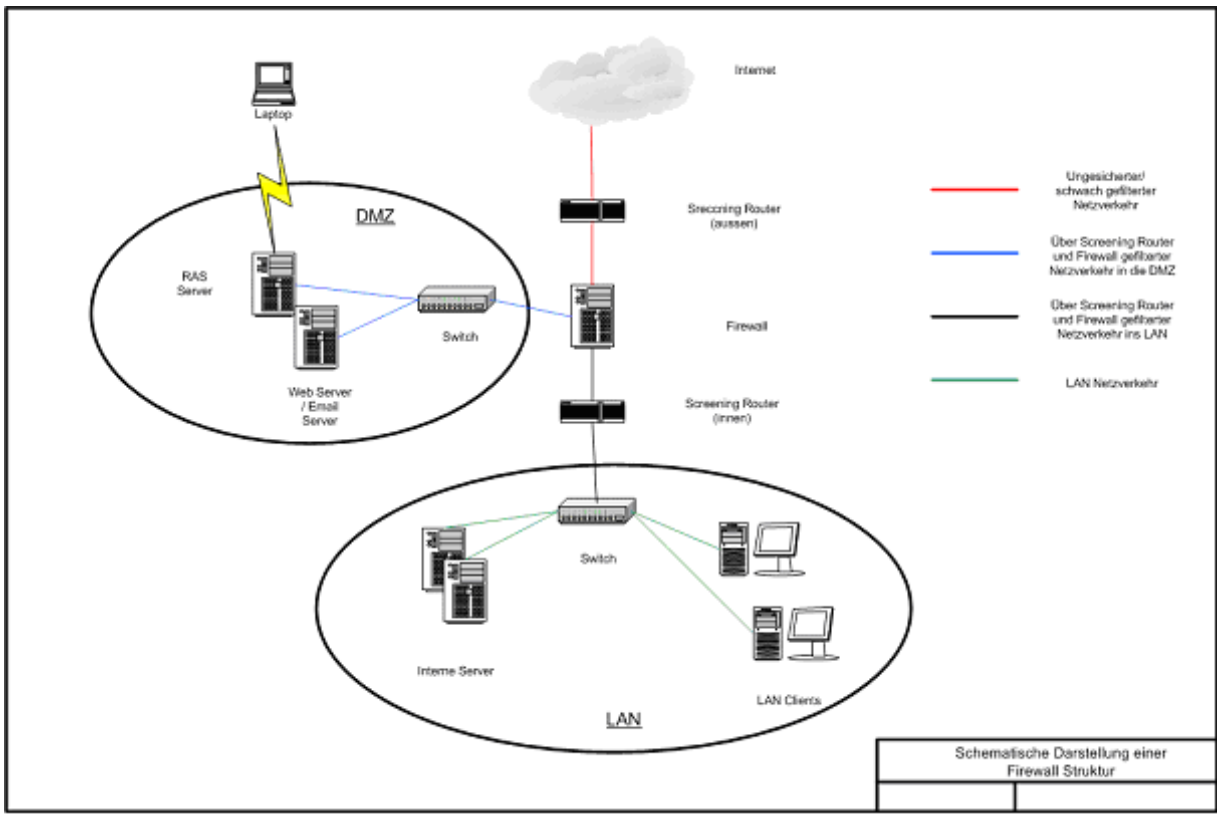



Abb. Beispiel einer Firewall-Struktur

# Datensicherung

## Backupstrategie

Die Datensicherung ist organisatorisch und technisch in zwei Bereiche aufgeteilt. Auf der einen Seite das ERP-System mit seiner Datenbank (z.B. ORACLE); auf der Anderen, der „Office“- Bereich mit allen File- und Applikationsservern (z.B. MS Server, Linux Suse Server,  MS Exchchange, Citrix, IIS, Apache).
Beide Datensicherungsbereiche sind Hard- und Softwareseitig getrennt. Grundsätzlich sind zwei Sicherungsstrategien während einer Datenbanksicherung denkbar:

a) Die Online-Sicherung. Diese Technik setzt nicht voraus, das die zu sichernde Datenbank gestoppt werden muss. Im Falle einer notwendigen Rücksicherung hat man einen sehr aktuellen Datenbestand zur Verfügung, der notwendige Neueingaben auf ein Minimum reduziert. Diese Technik wird mit Hilfe von so genanten „Agents“ realisiert, die für viele Datenbanken und Betriebssystem zur Verfügung stehen
b) Die Offline-Sicherung. Im Gegensatz zur Online-Sicherung muss bei dieser Technik  die zu sichernde Datenbank gestoppt werden. Es ist bei einer Planung darauf zu achten – gerade auch bzgl. notwendiger Job’s, die häufig während der Systemruhe laufen müssen- , dass das Zeitfenster für diese Art der Sicherung noch ausreichend vorhanden ist. Ein Vorteil dieser Sicherung ist, das die gesicherten Daten per DB-Kopie leichter auf neue Systeme aufgesetzt werden können. Dieses ist interessant für den Aufbau von Testumgebungen

## UNIX / ERP/ Oracle

- Datensicherung UNIX werden mittels Betriebssystembefehle (z.B. cpio) auf ein lokales Sicherungslaufwerk (z.B. täglich nachts alle fünf Arbeitstage übermittelt. Bei neuen SP’s und Costumizing Hinterlegung im Tresor)
- Datensicherung ORACLE via Software (z.B Networker online auf externen DLT, sowie Recovermanager als 2. Instanz 14-tägiger Wiederholzyklus)
- Tabellenexport auf 2 verschiedene Server für partielle Tabellenrücksicherung mit Oracle-EXP-Tool (im täglichen Wechsel auf einem der Server)

## Office

- Sicherung der gesamten „Office“–Umgebung auf einer zentralen Tape-Libary (z.B. mit Veritas Backup EXE). Dieser Vorgang sollte täglich als Vollsicherung für alle Server durchgeführt werden. Hierbei werden die Bänder in den folgenden Turnus erstellt:
- Die Bänder Mo-Do. können jeweils in der darauffolgenden Woche überschrieben werden
- Die Freitagsbänder 1-5 sollten alle 4-5 Wochen überschrieben werden
- Der letzte Tag des Monats sollte als Monatssicherung ein Jahr vorgehalten werden
- Die Tape-Libary sollte räumlich von den zu sichernden Servern getrennt werden. Für MS-SQL und MS-Exchange sind „Onlineagents“ von Veritas vorhanden

## Einbeziehung auch tragbare Computer und nicht vernetzter Systeme

Dies ist nicht notwendig, wenn die vorhandenen Notebooks nicht als Büroarbeitsplatz, sondern für externe Termine genutzt werden. In solchen Fällen oder auch bei nicht vernetzten Systemen empfiehlt es sich, nach der Installation ein Image vom System auf DVD zu brennen (z.B. Norton Ghost). Eigene Dateien müssen in eigener Verantwortung gesichert werden. Bei sensiblen Daten auf Notebooks und Workstations ist es auf jeden Fall notwendig, diese vor dem Zugriff von außen zu schützen. Im Teilnehmerkreis wird für diesen Zugriffsschutz z.B. eine Verschlüsselungssoftware (z.B. SafeGuard®Easy) eingesetzt. Mit dieser Technik ist es möglich, Datenpartitionen der Notebooks oder Workstation zugriffssicher für unbefugte Personen zu verschlüsseln

## Regelmäßige Kontrolle der Sicherungsbänder

- Im Bereich des ERP-Systems sollte eine Rücksicherung regelmäßig getestet werden
- Im Bereich der Fileserver unregelmäßig mit Stichproben

- Es sollten täglich alle Sicherungsprotokolle überprüft werden
- Bei Fehlern im Sicherungsjob werden die betroffenen Server bei einem Rücksicherungstest bevorzugt

## Dokumentation von Sicherungs- und Rücksicherungsverfahren

Es sollte neben einer Dokumentation auch eine Durchführungsanweisung vorliegen

# Notfallvorsorge

## Ermittlung der DV-Abhängigkeit

- Hilfreich ist die Durchführung von Anwenderinterviews um die Abhängigkeit von der DV zu ermitteln. Die Arbeitsabläufe sollten dokumentiert und die Hilfsmittel beschrieben werden

- Zur Identifikation der kritischen Geschäftsprozesse sind bestehende Dokumentationen und das QM-System heranzuziehen

- Die maximale Ausfalldauer ist mit den betroffenen Abteilungen zu ermitteln und mit der Geschäftsleitung abzustimmen

## Erstellen diverser Listen

- Listen von Telefonnummern und Ansprechpartnern der Kunden sind regelmäßig zu überarbeiten und in Papierform oder auf Datenträger an geeigneter Stelle aufzubewahren

- Für den Wiederanlauf ist eine Aufstellung der produktionskritischen Lieferanten erforderlich

- Eine Liste der verfügbaren Handynummern der Mitarbeiter (privat und dienstlich) sollte an geeigneter Stelle aufbewahrt werden

- Für die vorübergehende Aufrechterhaltung des Geschäftsbetriebs können Notfaxnummern z. B. von Mitarbeitern oder befreundeten Unternehmen festgelegt werden

## Erstellen diverser Formulare

- Für die Aufrechterhaltung des Geschäftsbetriebs während der fehlenden DV-Unterstützung sollten Vordrucke für die manuelle Auftragsannahme und Bestellung per Fax vorhanden sein oder geschaffen werden

- Zur Information der Kunden sind vorgefertigte Formulare erforderlich, die die Situation schildern und die Handynummern der Ansprechpartner enthalten

## Präventivmaßnahmen

- Die wichtigsten Daten (Bänder, Kundenlisten, Auftragsbestand, Stücklisten, Bestandsliste) sind regelmäßig auszulagern

# Infrastruktursicherheit

## Zutritt Firmengelände/Gebäude/Rechenzentrum

- Die Anzahl und Lage der Zugänge zum Firmengebäude sollte in einem Plan festgehalten werden

- Zur Sicherung des Geländes/Gebäudes sollten geeignete Überwachungssysteme (Kameras, Pförtner, Alarmanlage) installiert werden

- Die Schlüsselliste sollte regelmäßig überarbeitet und an die veränderten Gegebenheiten angepasst werden

- Die Schließanweisung für Pförtner und Wachdienst sollte stets aktuell gehalten werden

## Zutritt und Ausstattung Telekommunikationsraum

- Der Raum sollte permanent verschlossen gehalten werden

- Die in den Raum hineinführenden Kabelschächte sollten durch geeignete Baumassnahmen gegen Manipulation und Sabotage geschützt werden

- Zusätzlich sollte eine Abschottung der Türen und Mauerdurchbrüche gegen Feuer und Rauch vorhanden sein

## Zutritt und Ausstattung Rechenzentrum

- Das Rechenzentrum sollte permanent verschlossen gehalten werden

- Der Kreis der Schlüsselinhaber sollte möglichst klein gehalten werden, Zutritt ist in der Regel lediglich Mitarbeitern der IT-Abteilung zu gewähren

- Die Türen und Mauerdurchbrüche sollten gegen Einbruch, Sabotage, Feuer und Rauch gesichert sein

- Das Rechenzentrum sollte mit Rauchsensoren und einer geeigneten Löscheinrichtung ausgestattet sein

- Im Rechenzentrum und in den umliegenden Räumen dürfen keine Brandlasten (Papier, ausgemustertes DV-Equipment) gelagert werden

## Einbruchsicherung Firmengebäude und RZ

- Das Gebäude ist durch geeignete Maßnahmen (Pförtner, Wachdienst, Kameraüberwachung, Alarmanlage, Bewegungsmelder) gegen unbefugten Zutritt von außen zu schützen. Das gilt insbesondere außerhalb der regulären Arbeitszeiten

- Nach Feierabend ist sicherzustellen, dass alle Fenster und Türen verschlossen sind

## Brandschutz und Alarmierung Firmengebäude

- Die Reihenfolge und Art der Alarmierung der zuständigen Personen und Institutionen (Pförtner, Wachdienst, Bereitschaftsmitarbeiter, Feuerwehr) sollte durch technische Maßnahmen (Alarmanlage, Störmeldekontakte) und organisatorische Regelungen festgesetzt werden

- Es sollten regelmäßige Brandschutzübungen unter Einbeziehung der Mitarbeiter und der Feuerwehr durchgeführt werden

- Die vorhandenen Brandschutzmaßnahmen (Brandschutztüren, Feuerlöscher, Rauchmelder, Fluchtwege, Löscheinrichtung) sollten regelmäßig überprüft werden

- Im Brandfall gefährliche Stoffe sollten besonders gekennzeichnet werden und in einen Plan aufgenommen werden

- Beachtung sonstiger möglicher Katastrophen (z. B. Hochwasser)

## Notstromversorgung

- Eine Notstromversorgung für alle Bereiche (RZ, Verwaltung, Produktion) sollte unter dem Gesichtspunkt der Aufrechterhaltung des Geschäftsbetriebs vorgehalten werden

- Die Verfügbarkeit und Dauer der Verfügbarkeit ist zu untersuchen und zu dokumentieren

## Verkabelungspläne

- Die Verkabelungspläne sollten folgende Informationen enthalten:
    - Lage und Zugänge der Kommunikationsleitungen (Telefon, WAN)
    - Kabelführung und Art der DV Vernetzung
    - Installierte Versorgungsleitungen (Strom, Wasser)

# Krisenmanagement

## Krisenstab

- Der Krisenstab setzt sich aus den Mitgliedern der wichtigsten Abteilungen inkl. Öffentlichkeitsarbeit zusammen und regelt die Zuständigkeiten im Krisenfall

## Aufgaben im Krisenfall

- Der Krisenstab steuert die Informationspolitik gegenüber Kunden, Lieferanten, Presse und Versicherungen

- Ferner ist er für die Information der Mitarbeiter zuständig (Was ist passiert, Konsequenzen)

- Die Einsatzsteuerung der Mitarbeiter sollte zentral erfolgen, darunter fällt die Festlegung der Arbeitszeiten und die Rückholung von Mitarbeitern aus dem Urlaub

- Der Wiederanlauf muss gesteuert werden, z. B. durch Entscheidungen bzgl. der Beschaffung von Maschinen, Gebäuden, Material sowie des Einsatzes von Fremdpersonal

# Rechenzentrum/Rechenzentrumsbetrieb

## Dokumentation Hardware

- Bestandslisten und Rechnungskopien der Hardware sollten zusätzlich in Papierform oder auf einem Datenträger vorliegen

- Eine Aufstellung der Sicherungsmedien (Geräte, Bänder und deren Lagerort) sollte ebenfalls auf Papier oder Datenträger zu erstellt werden

- Das gilt ebenfalls für die technische Infrastruktur der RZ (Klimaanlage)

- Die Dokumentationen sind außerhalb des Firmengeländes zu lagern

## Dokumentation Software

- Die Einstellungen der RZ Komponenten (Router, Switche etc.) sollten außerhalb des Firmengeländes aufbewahrt werden. Das gleiche gilt auch für Konfigurationen (Firewall, Virenscanner)

- Eine Auflistung der Hard- und Softwarelieferanten und Dienstleister sollte ständig aktuell gehalten werden

## Wiederanlaufpläne

- Die Reihenfolge der Recoverymaßnahmen sollte in einer Prioritätenliste hinterlegt und im Katastrophenfall abgearbeitet werden

- Es sollte für jeden Server ein Wiederanlaufplan erstellt werden

- Die Kontrolle der Durchführbarkeit ist regelmäßig in geeigneter Form (Test mit neuer Hardware, Servicerechenzentren) durchzuführen

# Allgemeine Hinweise

Die in dieser Veröffentlichung dargestellten Hinweise erheben kein Anspruch auf Vollständigkeit oder Richtigkeit. Auch können für entstehende Fehler oder Schäden bei der betrieblichen Umsetzung im Zusammenhang mit den dargestellten Tipps keine Rechtsansprüche an die Verfasser oder den Initiator abgeleitet werden. Trotz aller Sorgfalt können sich Informationen inzwischen verändert haben. Eine Haftung oder Garantie für die Aktualität, Richtigkeit und Vollständigkeit der zur Verfügung gestellten Informationen kann daher nicht übernommen werden.



# Literatur


- Betriebliche Unterlagen, Sicherheitsanweisungen, Betriebsvereinbarungen der Netzwerkpartner

- Bundesamt für Sicherheit in der Informationstechnik (August 2004):

  Leitfaden IT-Sicherheit, 2004, IT-Grundschutz kompakt, Bonn, Bundesamt für Sicherheit in der Informationstechnik

- IT-Grundschutzhandbuch, CD-Version März 2005, Bonn, Bundesamt für Sicherheit in der Informationstechnik


# Weiterführende Informationen

Weiterführende Informationen sind u.a. erhältlich bei:

- Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de
- Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien, http://www.bitkom.org
- etc...