Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 7. Übung im SoSe 2007:
Risiko-Bewertung & -Behandlung

7.1 Risikotabelle

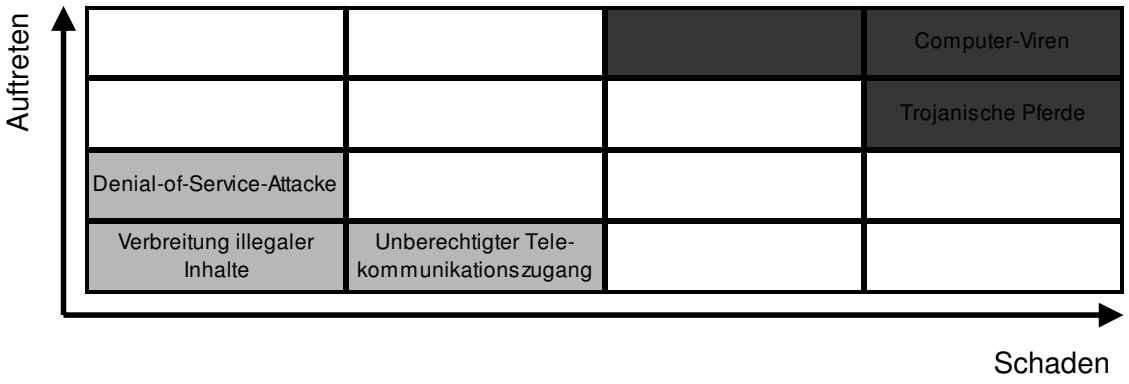
Rg.	Bedrohung	Auftreten	Schaden	Risiko
1	Computer-Viren	9	6	54
2	Trojanische Pferde	4	6	24
3	Denial-of-Service-Attacken	2	4	8
4	Unberechtigter Telekommunikationszugang	1	5	5
5	Verbreitung illegaler Inhalte	1	4	4

7.2 rangbezogene Risikotabelle

Bedrohung	Wert	**Auftreten**	Rang	Wert	**Schaden**	Rang
Computer-Viren	9	=>	1	6	=>	1
Trojanische Pferde	4	=>	2	6	=>	1
Denial-of-Service-Attacken	2	=>	3	4	=>	4
Unberechtigter Telekommunikationszugang	1	=>	4	5	=>	3
Verbreitung illegaler Inhalte	1	=>	4	4	=>	4

Rg.	**Bedrohung**	**Auftreten**	**Schaden**	**Risiko**
1	Computer-Viren	1	1	1
2	Trojanische Pferde	2	1	2
3	Denial-of-Service-Attacken	3	4	12
3	Unberechtigter Telekommunikationszugang	4	3	12
5	Verbreitung illegaler Inhalte	4	4	16

7.3 Risiko-Portfolio



7.4 Notfall-Vorsorge-Konzept

Notfall = Beeinträchtigung der Verfügbarkeit bei Safety
Notwendige Inhalte:

- Verzeichnis der IT-Systeme & Vernetzung (→ Netzwerkplan)
- Anforderungen an die Verfügbarkeit (→ Prioritätensetzung)
- Verantwortlichkeiten (→ Sicherheitsbeauftragter, CERT)
- Wiederanlaufplan & Notfallübungen
- Redundanzkonzept (Technik & Daten)

Hinweise:

→ Ergebnis fließt sinnvollerweise in ein Notfall-Handbuch ein
→ Regelmäßige Revision erforderlich
→ maßgeblich für die Architektur von IT-Systemen!
→ mittelständisches Unternehmen benötigt i.d.R. die zwingenden und zügig umzusetzenden Maßnahmen nach BSI-Grundschutz

Notfall-Vorsorge-Konzept nach BSI-Grundschutz (1)

Baustein 1.3 Notfall-Vorsorgekonzept mit den Maßnahmen

- M 6.1 (A) Erstellung einer Übersicht über Verfügbarkeitsanforderungen
- M 6.2 (A) Notfall-Definition, Notfall-Verantwortlicher
- M 6.7 (A) Regelung der Verantwortung im Notfall
- M 6.8 (A) Alarmierungsplan
- M 6.13 (A) Erstellung eines Datensicherungsplans
- M 6.4 (B) Dokumentation der Kapazitätsanforderungen der IT-Anwendungen
- M 6.5 (B) Definition des eingeschränkten IT-Betriebs
- M 6.6 (B) Untersuchung interner und externer Ausweichmöglichkeiten
- M 6.11 (B) Erstellung eines Wiederanlaufplans
- M 6.14 (B) Ersatzbeschaffungsplan

Notfall-Vorsorge-Konzept nach BSI-Grundschutz (2)

Baustein 1.3 Notfall-Vorsorgekonzept mit den Maßnahmen

- M 6.3 (C) Erstellung eines Notfall-Handbuches
- M 6.9 (C) Notfall-Pläne für ausgewählte Schadensereignisse
- M 6.10 (C) Notfall-Plan für DFÜ-Ausfall
- M 6.12 (C) Durchführung von Notfallübungen
- M 6.15 (Z) Lieferantenvereinbarungen (optional)
- M 6.16 (Z) Abschließen von Versicherungen (optional)
- M 6.75 (Z) Redundante Kommunikationsverbindungen

Hinweise: (A) – (C) erforderlich für Zertifizierung

- (A) = vorrangige & unerlässliche Maßnahmen
- (B) = zügig umzusetzende Maßnahmen
- (C) = nachrangig umzusetzende Maßnahmen
- (Z) = für höheren Schutzgrad erforderlich

7.5 Entwurf einer Sicherheitsleitlinie

Notwendige Inhalte einer Sicherheitsleitlinie:

- Gründe für Sicherheitsleitlinie (→ Bedrohungslage + Schutzbedarfsanalyse = Risikobewertung)
- Festlegung der Sicherheitsziele (→ Mehrseitige IT-Sicherheit)
- Maßnahmen zur Durchsetzung (→ technische und organisatorische Maßnahmen)
- Festlegung der Verantwortlichkeiten

Hinweise:

→ zielt schwerpunktmäßig auf Security ab

→ maßgeblich für die IT-Sicherheit im laufenden Betrieb!

Mindestinhalt einer Sicherheits-leitlinie nach BSI-Grundschutz

- Der **Stellenwert der IT-Sicherheit** und die **Bedeutung der IT** für die Institution müssen dargestellt werden
- Die **IT-Sicherheitsziele** und der Bezug der IT-Sicherheitsziele zu den Geschäftszielen und Aufgaben der Institution müssen dabei erläutert werden
- Die Kernelemente der **IT-Sicherheitsstrategie** sollten genannt werden
- Die Leitungsebene muss allen Mitarbeitern aufzeigen, dass die IT-Sicherheitsleitlinie von ihr getragen und durchgesetzt wird. Ebenso muss es **Leitaussagen zur Erfolgskontrolle** geben
- Die für die Umsetzung des IT-Sicherheitsprozesses etablierte **Organisationsstruktur** muss beschrieben werden

information security policy nach ISO/IEC 17799

- Definition, Ziele, Umfang und **Bedeutung der Informationssicherheit**
- Verknüpfung des Informationssicherheitsmanagements mit der gesamten **Unternehmensstrategie** und die Aussage des Managements, bei der Verwirklichung der Informationssicherheit unterstützend tätig zu sein
- Formulierung eines **Rahmenwerks von Sicherheitsmaßnahmen**, das mit dem Risikomanagement fest verbunden ist
- zusammenfassende **Erläuterungen** zur Compliance, zu Schulungsmaß-nahmen, zur Gewährleistung der Geschäftskontinuität und zu den Folgen von Verstößen gegen Vorgaben der Sicherheitsleitlinie – unter Einbeziehung von security policies, Richtlinien, Standards und Anforderungen der Compliance
- Festlegung der **Verantwortlichkeiten**, auch für die Mitteilung von Sicherheitsvorfällen
- **Referenzen** auf konkrete und detailliertere security policies, Richtlinien und Dienstanweisungen