IT - Security Forum #3

Das IT-Sicherheitskonzept

Andreas Wisler
Dipl. Ing. FH
GO OUT Production GmbH
wisler@goSecurity.ch

IT - Security Forum #3

Inhalt

- Einleitung
- Vorbereitung
- Anforderungen
- Vorgehen
- Inhalt eines Sicherheitskonzeptes
- Kontrolle
- Erweiterungen / Anpassungen

IT - Security Forum #3

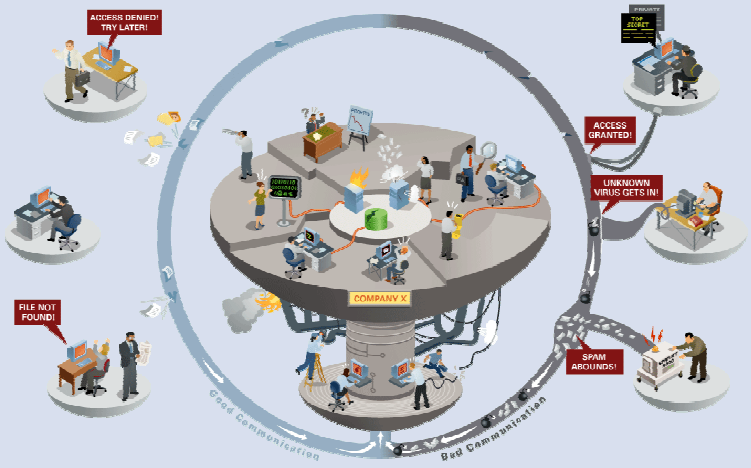
Einleitung

- Das IT-Sicherheitskonzept beschreibt die **notwendigen Massnahmen** zur Realisierung und Aufrechterhaltung des für das Unternehmen **angemessenen, definierten Sicherheits-niveaus**.
- Basierend auf dem IT-Sicherheitskonzept kann im Unternehmen ein angemessenes Sicherheitsniveau erreicht und bei **konsequenter Durchsetzung** der Massnahmen gehalten werden.
- Das IT-Sicherheitskonzept betrifft **alle Stufen.** (Geschäftsführung, IT-Leitung, Mitarbeiter)

3

IT - Security Forum #3

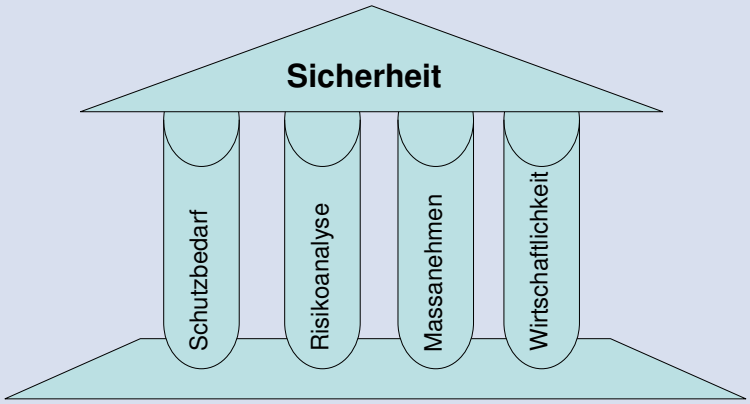
Wie sieht es heute aus?



4

Vorbereitung

- Schutzbedarf
- Risikoanalyse
- Massnahmenauswahl
- Wirtschaftlichkeit



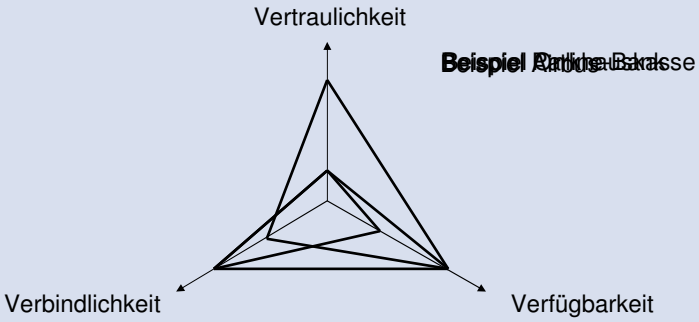
IT - Security Forum #3

5

Schutzbedarf

Was will ich schützen?

- Schutzziele:
  - Verfügbarkeit
  - Verbindlichkeit
  - Vertraulichkeit



IT - Security Forum #3

6

IT - Security Forum #3

Risikoanalyse

Wogegen muss ich mich schützen?

- Eine Risikoanalyse betrachtet, welche **Gefährdungen** auf ein System einwirken können und ab welchem Punkt die entstehenden **Schäden bedrohlich** wirken.

System	Gefährdung	Auswirkung	Kritisch
Webserver	Gross	Gering	Gering
ERP	Mittel	Gross	Gross
Mailserver	Mittel	Gross	Mittel
Telefon	Gering	Mittel	Mittel
CNC	Gering	Sehr Gross	Sehr Gross

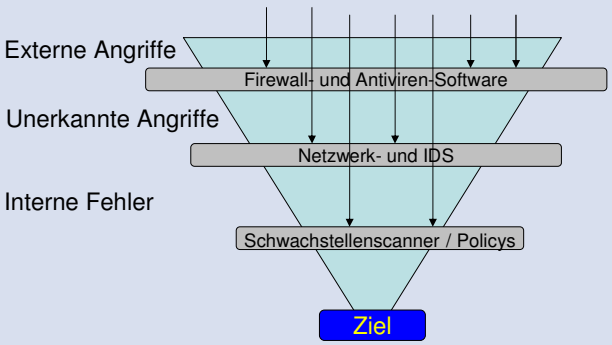
7

IT - Security Forum #3

Massnahmenauswahl

Wie kann ich einen wirksamen Schutz erreichen?

- Welche Massnahmen sind möglich?
- Welchen Teil der Gefährdung decken diese ab?
- Welche Bereiche werden tangiert?
- Was ist der Nutzen einer Massnahme?
- Können Massnahmen zusammengefasst werden?



8

IT - Security Forum #3

Wirtschaftlichkeit

Kann ich mir diesen Schutz leisten?

- Welchen Schaden kann eine Gefährdung maximal anrichten?
  - Einteilung in Kategorien
    - Niedriger bis mittlerer Schaden
    - Hoher Schaden
    - Sehr hoher Schaden
- Welche Restrisiken bleiben?
- Wie hoch ist die Eintrittswahrscheinlichkeit?
- Was kostet eine Massnahme?

System	Gefährdung	Auswirkung	Kritisch	Schaden
Webserver	Gross = 3	Gering = 1	Gering = 1	3 * 1 * 1 = 3
ERP	Mittel = 2	Gross = 3	Gross = 3	2 * 3 * 3 = 18
Mailserver	Mittel = 2	Gross = 3	Mittel = 2	2 * 3 * 2 = 12
Telefon	Gering = 1	Mittel = 2	Mittel = 2	1 * 2 * 2 = 4
CNC	Gering = 1	Sehr Gross = 4	Sehr Gross = 4	1 * 4 *4 = 16

9

IT - Security Forum #3

Vorgehen

- Bewertung der Ergebnisse
- Massnahmen ausarbeiten
- Kosten- und Aufwandschätzung
- Festlegen der Umsetzungsreihenfolge
- Festlegen der Verantwortlichkeiten
- Erarbeitung begleitende Massnahmen
- Schulung und Sensibilisierung

10

Inhalt eines Sicherheitskonzeptes

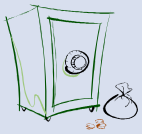
- Grundlage, Zweck
- Anforderungen
  - Funktionalität
  - Sicherheit
  - Benutzer
  - Administration
- Organisation
  - Zuständigkeiten
  - Pflege und Wartung des Konzeptes
- Sicherheit beim Personal
  - Stellenbeschreibung
  - Vertraulichkeitsvereinbarung
  - Ausbildung in Sicherheitsfragen
  - Reaktion auf sicherheitsrelevante Ereignisse
- Physische Sicherheit
  - Sicherheitsbereiche
  - Verkabelung

IT - Security Forum #3

11

Inhalt eines Sicherheitskonzeptes

- Betrieb von Systemen und Netzwerken
  - Operative Verfahren und Aufgaben
  - Planung und Abnahme
  - Verwaltung
  - Nutzung des Internets
  - Schutz vor böswilliger Software
  - Sicherheit beim elektronischen Datenverkehr
- Zugriffskontrolle
  - Benutzer
  - Betriebssystem
  - Anwendungen
  - Schlüsselverwaltung
  - Überwachung
  - Mobile Geräte
- Not-Organisation
  - Vorgehen
  - Ausweichmöglichkeiten
  - Verträge mit Drittfirmen
  - Schulung
  - Übungen / Kontrollen

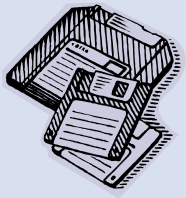


IT - Security Forum #3

12

Inhalt eines Sicherheitskonzeptes

- Anhänge
  - Gefährdungen, Restrisiken
  - Betrieb der Informatikstruktur
  - Nutzungsreglement (intern, extern)
  - Backup-Konzept und Backup-Plan
  - Firewall-Konzept
  - Akzeptierte Ausfallzeiten



IT - Security Forum #3

13

Kontrolle

- Verantwortlichkeiten
- Rechte und Pflichten
- Umsetzung
- Anpassungen notwendig?

IT - Security Forum #3

14

IT - Security Forum #3

Anpassungen

- Vorgehen
- Genehmigung (Durch wen?)
- Überprüfung
- Kommunikation

15

IT - Security Forum #3

Zusammenfassung

- Vorbereitung sehr wichtig
- Verantwortlichkeiten klären
- Gefährdungen festhalten
- Massnahmen bestimmen
- Umsetzungskontrolle
- Schulung und Sensibilisierung
- Regelmässige Kontrolle

16