Datensicherheit, Zusammenfassung Vorlesung 4

Henry Haustein, Dennis Rössel

Was kann bzgl. der erreichbaren Sicherheit ausgesagt werden?

keine 100%ige Sicherheit möglich

Warum ist Sicherheit kein Zustand, sondern ein Prozess?

erreichtes Sicherheitsniveau ist nicht dauerhaft

Welche Aufgaben sind der Awareness bzgl. Sicherheit zuzuordnen?

Sensibilisierung, Schulung, Training

Welche Prinzipien sind beim Sicherheitsmanagement zu beachten?

Kombi aus technischen, organisatorischen, personellen und infrastrukturellen Maßnahmen

Was beinhalten IT-Sicherheitspolitik und IT-Sicherheitskonzept?

IT-Sicherheitspolitik:

- Charakterisierung des Unternehmens
- Geltungsbereich der Sicherheitspolitik
- Bedeutung der Sicherheit
- Gefährdungslage
- weitere Vorgaben
- Organisationsbeschluss und Verpflichtungserklärung

IT-Sicherheitskonzept:

- Anforderungsanalyse (Was?)
- Risikoanalyse (Wovor?)
- Festlegung der Maßnahmen (Wie?)

Was sind die wesentlichen drei Aufgaben bei der Erstellung eines IT-Sicherheitskonzepts?

IT-Sicherheitskonzept:

- Anforderungsanalyse (Was?)
- Risikoanalyse (Wovor?)
- Festlegung der Maßnahmen (Wie?)

Welche Schritte beinhaltet die Anforderungsanalyse?

Anforderungsanalyse

- Bestandsaufnahme: relevante Objekte
- Schutzbedarfsfeststellung
- Gesetze, Verträge und unternehmensinterne Regelungen

Wie entstehen allgemein Risiken (Risikobildungsmodell)?

Bedrohungen/Schwachstellen → gefährdende Ereignisse → Risiken

Mit welchen zwei Faktoren werden Risiken bewertet?

Eintrittswahrscheinlichkeit, möglicher Schaden

Wie können Maßnahmen zur Risikobewältigung nach der Zielrichtung bzw. dem Zeitpunkt ihrer Wirkung eingeteilt werden?

Maßnahmenklassifikation nach Zielrichtung und Zeitpunkt:

- vermeiden
- vermindern
- überwälzen
- selbst tragen

Was beinhaltet die Validierung der Maßnahmen?

Validierung der Maßnahmen

- Eignung
- Wirksamkeit
- Zusammenwirken
- Praktikabilität
- Akzeptanz

- Wirtschaftlichkeit
- Angemessenheit

Welche Fragen sind bei der Definition von Zugriffsberechtigungen zu klären?

Wer? Wann? Wo? Welche? Was? Warum?

Wie werden die Zugriffskontrollinformationen grundsätzlich verwaltet, welche vereinfachten Varianten (ACL, CL) gibt es?

allgemein: Zugriffskontrollmatrix, ACL (Access Control List), CL (Capability List)

Was ist das Prinzip bei RBAC, welche Aufgaben sind zu lösen?

Grundidee: Repräsentation einer bestimmten Aufgabe und der damit einhergehenden Zugriffsrechte durch eine Rolle

Aufgaben:

- Definition der Rollen und der zugehörigen Zugriffsberechtigungen
- Zuweisung der Rollen zu den Objekten

Welche prinzipiellen Möglichkeiten der Identifikation von Menschen durch IT-Systeme gibt es?

Was man ist (Biometrie), Was man hat (Dokument), Was man weiß (Passwort)