Datensicherheit, Übung 2

Henry Haustein

Aufgabe 1

Ja kann es. Angenommen eine Vorgabe der IT ist es, alle 6 Monate sein Passwort zu ändern. Da niemand Lust hat sich alle 6 Monate ein neues Passwort zu merken, fangen die Leute an, ihr Passwort mit einem Post-It an den Monitor zu kleben. Damit ist es aber ein leichtes für andere Personen, z.B. Reinigungskräfte, an das Passwort zu kommen.

Aufgabe 2

Angriffe entwickeln sich immer weiter, es werden neue Schwachstellen und andere Angriffsvektoren gefunden, gegen die man sich wappnen muss. Z.B. OpenSSL: Seit Jahren Open Source, aber trotzdem wurde HeartBleed erst vor wenigen Jahren entdeckt. Oder Log4Shell, ...

Aufgabe 3

Da es keine 100%ige Sicherheit gibt, bleibt immer ein Risiko. Risiko: nach Häufigkeit (Eintrittserwartung) und Auswirkung (Schadensmaß) bewertete Gefährdung eines Systems. Betrachtet wird immer die negative, unerwünschte und ungeplante Abweichung von Systemzielen und deren Folgen.

Aufgabe 4

Maßnahmenklassifikation nach Zielrichtung und Zeitpunkt (pre-loss vs. post-loss):

- vermeiden
- vermindern
- überwälzen
- selbst tragen

alternative Klassifikation nach Objektklassen

- Infrastrukturelle Maßnahmen
- Organisatorische Maßnahmen
- Personelle Maßnahmen
- Technische Maßnahmen

Aufgabe 5

Probleme

- Ermitteln von Wahrscheinlichkeiten schwierig (z.B. Motivation von Angreifern, ...)
- Abschätzen der Schadenshöhe schwierig (z.B. Folgekosten, ...)
- Ungenauigkeiten werden durch die Multiplikation verschärft

Aufgabe 6

Definition der Klassen von S_H und p_{St}. Akzeptanzlinie von Unternehmensführung festgelegt.

Aufgabe 7

Planung des Sicherheitsprozesses

- Ermittlung der Rahmenbedingungen, Formulierung der allgemeinen Sicherheitsziele
- Erstellung einer IT-Sicherheitspolitik

Aufbau einer Sicherheitsorganisation

- Gesamtverantwortung: Leitungsebene; mindestens ein Verantwortlicher (Informationssicherheitsbeauftragter)
- Verantwortlichkeit jedes Mitarbeiters

Umsetzung der Sicherheitsziele: IT-Sicherheitskonzept

- Erstellung eines IT-Sicherheitskonzepts: Analyse der Sicherheit, Auswahl und Begründung von Maßnahmen

Aufrechterhaltung der Sicherheit und Verbesserung

- Regelmäßige Überprüfungen (interne Audits zur Umsetzung der Sicherheitsmaßnahmen; Überprüfung der Rahmenbedingungen; Awareness-Maßnahmen)
- Nutzung der Ergebnisse für Optimierung und Verbesserung

Aufgabe 8

Anforderungsanalyse

- "Bestandsaufnahme": Objekte, die für den festgelegten Geltungsbereich relevant sind
- Schutzbedarfsfeststellung
- Gesetze, Verträge und unternehmensinterne Regelungen

Risikoanalyse: Risikobildungsmodell

- Risiko-Identifikation
- Risiko-Einschätzung
- Risiko-Bewertung

$\Rightarrow$ Festlegen der Maßnahmen

Aufgabe 9

Brute-Force-Angriff, Stehlen der Datenbank mit Nutzer-Passwort-Kombos, SQL-Injection (bei webbasierten Formularen)

Aufgabe 10

Ist der Fingerabdruck einmal kopiert bzw. in falsche Hände gelangt, lässt er sich nicht mehr ändern. Biometrische Merkmale sind höchst persönliche Merkmale, die auf gar keinen Fall in fremde Hände gelangen dürfen $\Rightarrow$ extrem hohe Sicherheitsanforderungen nötig!