IT - Sicherheit 1 Zusammenfassung

Sassan Asnaashari

Kapitel 1 Begriffe

- Vertraulichkeit:
  - Zugriff auf Informationen ist auf autorisierte Personen begrenzt. Nicht autorisierte Personen können auf die Informationen nicht zugreifen.
- Integrität:
  - Informationen dürfen nur von Personen verändert werden, die dazu autorisiert sind. Strengere Auslegung: Die Informationen müssen korrekt, konsistent und vor Manipulation geschützt sein.
- Verfügbarkeit:
  - Autorisierte Personen und Systeme können auf die Informationen und Ressourcen zugreifen, wenn diese benötigt werden

Weitere Begriffe

Ein `Asset` (muss man beschützen) hat eine `Verwundbarkeit/Schwachstelle` diese verursacht eine `Bedrohung`, welche auf den `Asset` wirken kann.

Die `Security Control` schützt den `Asset` verändert die `Bedrohung` und reduziert das `Risiko` (welches die `Bedrohung` bewertet).

- Bewertung von Schwachstellen druch CVSS.
- Security Controls : Deterrent(verringern), Preventive(entfernen von Schwachstellen), Detective(Erkennen und Loggen), Corrective(verringern des Schadens), Compensationg(Security Control, welches an der Stelle eines andern verwendet wird)
- Asset: Das was beschützt werden muss(Mensch, System, Organisation)
- Risiko: Kombination aus Warscheinlichkeit des Auftretens,Auswirkung, häufig (Bewertung meist schwer, daher: gering, mittel, hoch reicht)
- Angriff: passiv(sniffing[Daten unautorisiert lesen]), aktiv([Daten verändern, Komponenten verändern, oder Verfügbarkeit beeinträchtigen[denial of service attack])
- Verwundbarkeit" durch CVEs versehen bewertet durch CVSS
- Bedrohung: Arten, Quelle
- Arten von Schwachstellen:
  - Buffer Overflow
  - Fehlende Prüfung von Eingabedaten
  - SQL Injection: Injezieren von Schadcode
  - Race Condition: gerade bei multi-thread Programmen oder verteilten Systemen
  - Unsichere Dateioperationen (zb zeitliche Veränderung der DAten)
  - Fehlende/unzureichende Zugriffskontrollen
  - Organisitorische Schwachstellen

Kapitel 2 Bewertungskriterien/Zugangskontrolle

Bewerungskriterien

- Wie sicher muss das System sein?
- Messen von Sicherheit

```
-> Dies führt zu Bewertungskriterienkatalog (TSEC Trusted Computer
System Evaluation Criteria)
* A – D von formaler Beweis bis kein/minimaler Schutz
* Sensitivklassen eines Objekts / Sensitivklassen eines Subject ( Bis
wie weit darf ich zugreifen)
```

Zugriffskontrolle

- Discretionary Access Control:
  - Objekte sind Subjekten zugeordnet, diese entscheiden selber über Zugriffskontrollen (Betriebssystem)
  - Mandatory Access Control:
    - Zugriffsbegrenzung anhand definierter Regeln
    - Security Police bilden die Menge aller Zugriffsregeln
    - Nutzer können die Regeln nicht ändern
    - SE Linux, AppArmor

Sicherheitsmodelle

- Bell-LaPadula Sicherheitsmodell (Fokus Vertraulichkeit) (Einstufung (hängt an Datei) vs Clearance(hat eine Person [Ermächtigung]))
  - Auf einer Ebene `lesen und schreiben` erlaubt
  - `Read Down` erlaubt lesen von unten
  - `No Read Up` verbietet lesen als geheim von streng geheim
  - `Write Up` erlaubt schreiben nach oben
  - `No Write Down` soll verhindern, dass der Account Streng geheim nur für streng geheime Angelegeneheiten genutzt wird.
- Biba Sicherheitsmodell (Fokus Integrität)
  - Erlaubt Lesen und Schreiben auf einer Integritätseinstufung
  - Lesen von Informationen deren Einstufung über der Ermächtigung liegt
  - Schreiben von Informationene deren Einstufnug unterhalb der eigenen Ermächtigung liegt
  - Verbietet Lesen von Informationen deren Einstufung unterhalb der eigenen Ermächtigung liegen
  - Schreiben von Informationen mit Einstufung oberhalb der eigenen Ermächtigung
- Separation of Duties (Mehrer Personen sind an Zugriffskontrollen beteiligt, Bei Gefahr Austausch oder rotierendes System)

- Least Privilege (Nur so viel KOntrolle wie nötig für die Aufgabe)
- Identifikation

Kapitel 3

ISO 9000/1

- Wir halten uns an unsere Vorgaben und haben diese dokumentiert

ISO/IEC 15408 : Common Creteria

- Was erfüllt werden soll in PP
- Wie werden eigenschaften erfüllt : TOA
- Es werden `Produkte` zertifiziert

Warum nicht immer EAL 7:

- sehr aufwendig
- nicht mgl
- oft ausreichend untere Studen zu nehmen
- Kosten und Dauer im Blick haben

ISO 27001 : Infromation Security Managment Systems

- Es werden keine `Produkte` sondern `Systeme`(Organisatorisches System)
- Kontext der Organisation verstehen (Womit wird Geld verdient)
- Erwartungen -> defenierne
- Scope (was ist mit drin, was nicht)
- Anhang A: sind die Security Controls -> darum muss man sich `konkret` kuemmern

Kapitel 4 Kryptographie

- überall vorhanden

Vorgehen

```
1. Handschake
2. Record Layer
```

Symmetrische Verschlüsselung

- m und k müssen geheim gehalten werden
- der ganze Rest auf Folie 5
- gerade die Algorithmen nicht!!! Die sind mgl bekannt

One time Key vs Multi use key

- OTK wird einmal genutzt

- MUK wird für mehrere Dokumente genutzt

Hauptaufgaben von Krypto

```
1. Sicherer Schlüsselaustausch
2. Sichere Kommuniktation
3. Verfügbarkeit ist `nicht` garantiert
```

Weitere Aufgaben

```
Digitale Signatur
Anonyme Kommunikation
... Folie 10
```

Allgemeines Vorgehen

1. Exakte Definition und Modellierung der Bedrohung
2. Vorschlag einer Konstruktion (Algorithmus, Protokoll, Nachrichten)
3. Beweis, dass der Bruch der Konstruktion bei der Bedrohung aus (1) identisch ist mit der Lösung eines zugrundeliegenden, schwierigen Problems

Historische Verfahren

- Ersetzungstabellen
- Ceasar Chiffre
- Vigener Chiffre
- Rotor basierte Verfahren (Enigma)