Information Security Fundamentals

Patrick Bucher

Inhaltsverzeichnis

1 Einführung

- Was ist Sicherheit?
  - "Sicherheit gibt es nicht": nichts ist 100%-ig sicher
  - Manipulation und unbefugten Zugriff verhindern
  - vermeiden von unerlaubter Verwendung
  - Redundanz (Doppelspurigkeit) haben
  - vermeiden von Datenverlust
  - Wahrung der Privatsphäre (Vorsicht: Privacy ist nicht das gleiche wie Security!)
    - persönliche Daten
    - besonders schützenswerte Daten (z.B. Patientendaten)
- Sicherheit bietet einen Schutz:
  - gegen Unbefugte
  - vor Verlust (Geld oder Leben)
  - *gegen Bedrohungen* (von aussen)
  - *vor Verletzlichkeiten* (von innen)

Wenn eine Bedrohung auf eine Verletzlichkeit trifft, gibt es ein *Ereignis*.

Grundkategorien der Sicherheit (und was man im Bereich der Sicherheit dagegen macht):

1. Bedrohung
   - eliminieren
   - vermindern
   - versichern
   - tragen

    - (durch Gesetzgebung beschränkt zu bekämpfen)
2. Verletzlichkeit
3. Ereignis

- Gegen Verletzlichkeiten kann man besser Massnahmen ergreifen als gegen Bedrohungen.
- Was ist ein Risiko?
  - Eintretenswahrscheinlichkeit
  - Schadensausmass
  - Rtot=Summe von Ew*SA
  - Wie finde ich alle Bedrohungen und alle Verletzlichkeiten, die zu einem Ereignis führen?
    * mithilfe von Standards und Frameworks

Definition von Sicherheit:

- Confidentiality (Vertraulichkeit)
- Integrity (Integrität)
- Availability (Verfügbarkeit)

Im Netzwerk:

- Non-Repudiation (Nicht-Abstreitbarkeit)
- Tracability (Nachverfolgbarkeit)
  - Forensik
- Auditability (Auditierbarkeit)
  - GoV (Grundzüge ordentlicher Verarbeitung)
- Authentication (Authentifizierung)
- AAA (Triple-A)
  - Authentication (wer?)
  - Authorisation (darf was?)
  - Accounting (wird wie berechnet?)

Eintretenswahrscheinlichkeit	Student/Firma
wöchentlich	4
monatlich	3
jährlich	2
zehnjährlich	1

Schadensausmass	Student

1000 4 1000..100 3 100..10 2 <10 1

Schadensausmass Firma >100’000 4 10’000..100’000 3 10’000..1’000 2 <1’000 1

Eintretenswahrscheinlichkeit mit Schadensausmass multiplizieren!

2 Kryptologie 1

2.1 Arten der Kryptoanalyse

Bei bekannten Verfahren:

- Brute-Force
- Ciphertext-Only

Bei unbekannten Verfahren:

- Known-Plaintext: (Beispiel: Ein Telegramm ist immer mit “Heil Hitler” unterschrieben)
- Chosen-Plaintext: Die Möglichkeit, einen Klartext durch das Krypto-Verfahren und dem gesuchten Schlüssel zu verschlüsseln.
- Chosen-Ciphertext: Man kann beliebige Cyphertexte entschlüsseln lassen, kennt aber den Key nicht.

zu Folie 12: Geburtstagsparadox!

zu Folie 16:

- Electronic Codebook (ECB)
- CBC: Output eines Blockes fliesst (mittels XOR) in die Chiffrierung mit ein
  - sicherer
  - fehleranfälliger (jeder Fehler wirkt sich auf den nächsten Block aus, wegen XOR jedoch nicht auf den gesamten Rest (doppelt gedreht))