Data Security H1: Inleiding

Inhoud

[Algemene begrippen 3](#_Toc466206110)

[Meet your enemy 3](#_Toc466206111)

[Management & wetgevende context 3](#_Toc466206112)

[Aspecten van beveiliging 4](#_Toc466206113)

# Algemene begrippen

* CIA triad
  + Confidentiality
    - Data is beperkt tot geautoriseerde gebruikers
    - Toegankelijk in verschillende vormen:
      * Data wordt verzonden (in transit)
      * Data wordt opgeslagen (at rest)
      * Data wordt verwerkt in een applicatie (in use)
  + Integrity
    - Data mag enkel aangepast worden door geautoriseerde gebruikers
    - Data tussen zender & ontvanger mag niet aangepast worden
  + Availability
    - Data moet steeds beschikbaar zijn
* Strategie voor beveiliging
  + Preventive
    - Firewalls, beperken fysieke toegang, backup, salting,...
  + Corrective
    - Bugfix, updaten van vulnerable software,...
  + Detective
    - IPS, virusscan, audit,...
* Terminologie
  + Vulnerability: kwetsbaarheid, heeft altijd een uniek nummer (CVE-2016-XXXX)
  + Exploit: toont aan hoe een vulnerability misbruikt kan worden

# Meet your enemy

* Externe aanvallers
  + Hackers
  + Professionele organisaties: crimineel & veiligheidsdiensten (overheid)
  + Verschuiving: professioneler & toegankelijker
* Interne aanvallers
  + Legitieme gebruikers
    - Slechte bedoelingen: data theft, wraakt,...
    - Goede bedoelingen: VB: slechte wifi dekking oplossen met eigen access point
  + Mobiele apparaten
    - Diefstal, verlies
    - Data buiten gecontrolleerde omgeving
  + Leveranciers

# Management & wetgevende context

* Risicoanalyse
  + Risico’s inschatten & beperken voor infrastructuur, data, gebruikers, applicaties
  + Inzicht in verantwoordelijkheid
* Policies
  + Information security policy: waarom & hoe IT-systemen gebruikt mogen worden
  + Information protection policy: de gevoeligheidsniveaus van informatie, wie er toegang tot heeft, en op welke manier de informatie verspreid mag worden
  + Password policy
  + Email policy
  + Information audit policy: hoe/wanneer/wat geaudit moet worden
* International security management frameworks
  + ISO27001
    - Standaard die de richtlijnen bevat om zelf een set van policies te ontwikkelen 🡪 kan dus toegepast worden op elk bedrijf
    - Inhoud:
      * Beleidsmatig, organisatorisch, bedrijfsmiddelen, personeel, fysiek, communicatie & operatie, toegangscontrole, systeem- en softwareontwikkeling & onderhoud, continuïteit, regelgeving
  + PCI-DDS
    - Payment Card Industry - Data Security Standard
    - Checklist van praktische regels waaraan een bedrijf moet voldoen dat credit card informatie gebruikt
  + Common Criteria

# Aspecten van beveiliging

* Onveilige protocollen: http, pop, smtp,...
* Foute implementaties: heartbleed, misbruik functionaliteit
* ‘Layer 8’ (OSI) (=users): social engineering, phishing, malafide emails,...
* Layer 7 (=applicatieniveau): XSS, SQLi, gevoelige data via foutmeldingen
* Layer 2/3/4: sniffen van netwerkverkeer, ARP spoofing/poisoning/...
* Layer 1 (=fysieke laag): fysieke diefstal van gegevens, ongeautoriseerde toegang tot computer of datalokaal, aangepaste firmware op routers/printers/switches/...