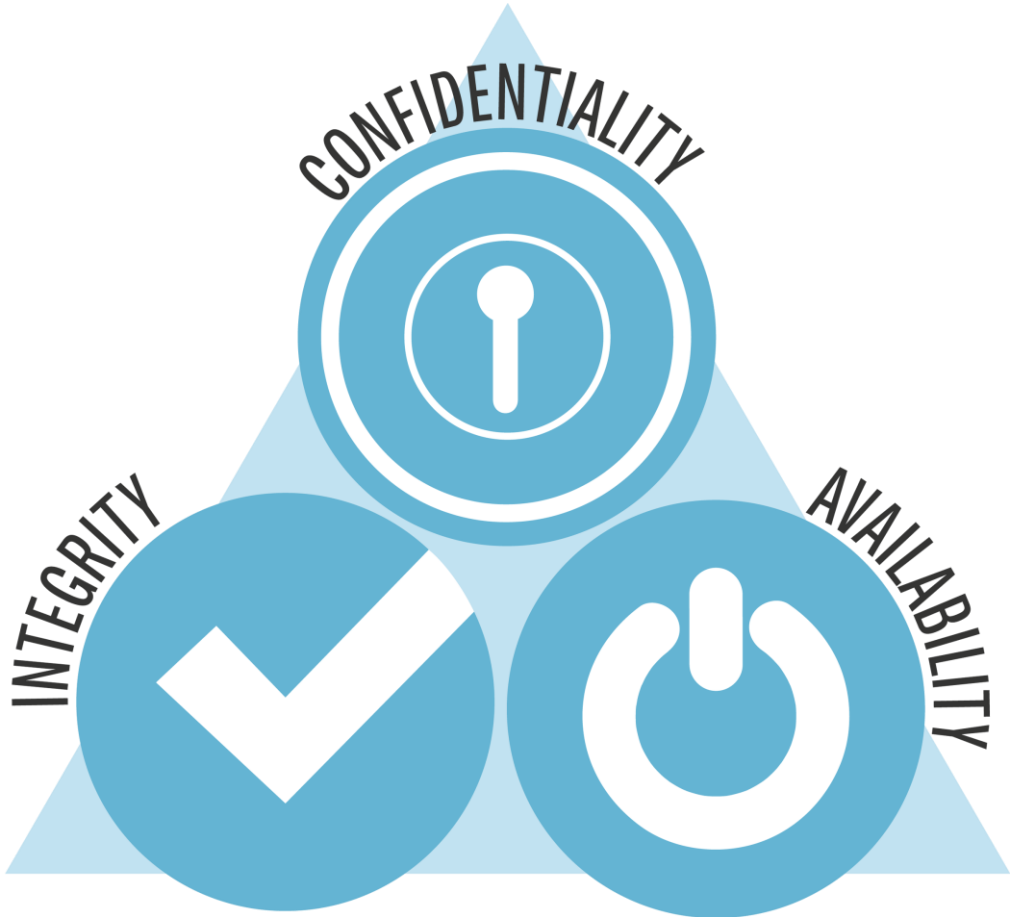
IT-sikkerhed

CIA modellen og trusler

CIA modellen



CIA modellen

- Confidentiality – fortrolighed:

  Kun personer, der er autoriserede til det, kan læse data

- Integrity - integritet:

  Kun personer, der er autoriserede til det, kan ændre i data

- Availability – tilgængelighed:

  Når, alle autoriserede brugere ønsker det, er data tilgængelig

Eksempel - bankkonto

Bankkonto: herunder kreditkortoplysninger og saldo

- Confidentiality – fortrolighed:
  Kun kunden og banken kender kreditkortoplysninger og saldo

- Integrity - integritet:
  Saldoen er korrekt – så saldoen ændrer sig kun, hvis der er blevet indsat eller hævet penge på kontoen

- Availability – tilgængelighed:
  Kunden og banken kan indsætte, hæve penge og tilgå saldoen, når der er brug for det

Øvelse – cold dog'en

- Et firma sælger hotdogs. Chefen udtænker nu *cold dog'en*. Den kolde hotdog skal lanceres i firmaets pølsevogne inden for et år. Indtil da er opfindelsen en forretningshemmelighed. Firmates chef lægger en tekst-fil med en beskrivelse af cold dog'en på firmaets hjemmeside, så de ansatte kan lære, hvordan cold dog'en tilberedes.

- Hvad betyder **C**onfidentiality, **I**ntegrity og **A**vailability i denne sammenhæng?

CIA modellen

Confidentiality – fortrolighed:
Kun personer, der er autoriserede til det, kan læse data

Integrity - integritet:
Kun personer, der er autoriserede til det, kan ændre i data

Availability – tilgængelighed:
Når, alle autoriserede brugere ønsker det, er data tilgængelig

Summe øvelse

CIA modellen ifm. kommunikation over netværk

[C] *fortrolighed*: Uvedkommende kan ikke opsnappe kommunikationen.

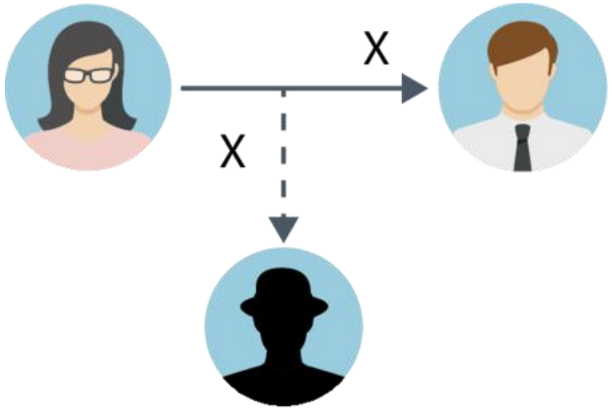
[I] *integritet*:

- *data-integritet*: Indholdet af en besked fra A til B kan ikke ændres under transporten over netværket.
- *autenticitet*: En uvedkommende aktør C kan ikke udgive sig for at være A eller B.
- *uafviselighed*: Hvis A sender B en besked, kan A ikke bagefter nægte det.

[A] *tilgængelighed*: Uvedkommende kan ikke afbryde A's og B's mulighed for at kommunikere.

[C] fortrolighed

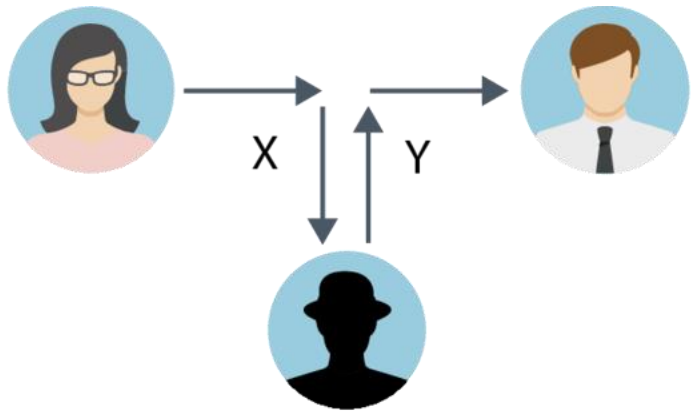
- Uvedkommende kan ikke opsnappe kommunikationen.



Aflytning:
Brud på fortrolighed

[I] integritet: data-integritet

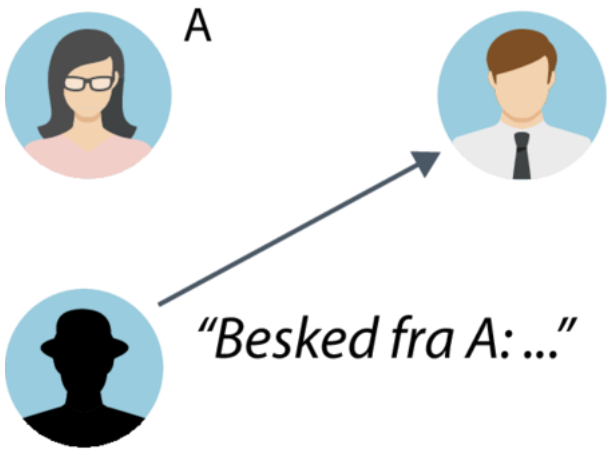
- Indholdet af en besked fra A til B kan ikke ændres under transporten over netværket.



Ændring af besked:
Brud på data-integritet

[I] integritet: autenticitet

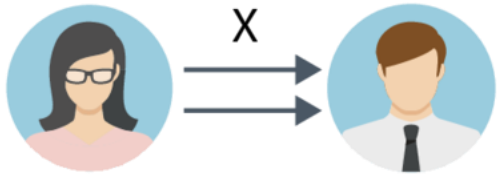
- En uvedkommende aktør C kan ikke udgive sig for at være A eller B.



Falsk afsender:
Brud på autencitet

[I] integritet: uafviselighed

- Hvis A sender B en besked, kan A ikke bagefter nægte det.

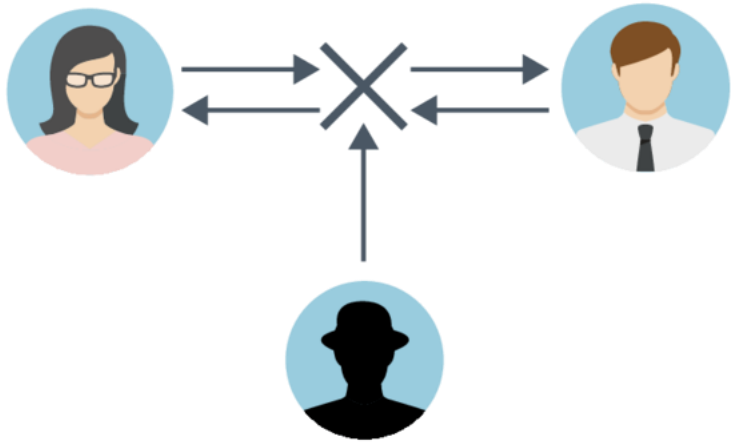


"Jeg har aldrig sendt beskeden x"

Afsender afviser at have sendt besked:
Brud på uafviselighed

[A] tilgængelighed

- Uvedkommende kan ikke afbryde A's og B's mulighed for at kommunikere.



Afbrydelse af forbindelse:
Brud på tilgængelighed

Øvelse Trusler ifm. kommunikation over netværk

1) Undersøg hvad den trussel, som I får udleveret på papir, dækker over (søg på nettet)

2) Tænk samtidig over hvilke aspekter i CIA modellen, der er truet

CIA modellen

[C] *fortrolighed*:

- Uvedkommende kan ikke opsnappe kommunikationen.

[I] *integritet*:

- *data-integritet*: Indholdet af en besked fra A til B kan ikke ændres under transporten over netværket.
- *autenticitet*: En uvedkommende aktør C kan ikke udgive sig for at være A eller B.
- *uafviselighed*: Hvis A sender B en besked, kan A ikke bagefter nægte det.

[A] *tilgængelighed*:

- Uvedkommende kan ikke afbryde A's og B's mulighed for at kommunikere.

Quiz og byt: Trusler

I får til start alle et kort, hvorpå der står en trussel

```
while(læreren siger til){
   • I vifter med kortet for at signalere, at I er ledige
   • I mødes to og to – man forklarer på skift det
     begreb, som står på ens kort
   • Man stiller opklarende spørgsmål til hinanden
   • Man bytter kort
}
```

Øvelse (dokumenteres i logbogen)

Trusler ifm. kommunikation over netværk

Forklar hvad følgende trusler dækker over og hvilke aspekter i CIA modellen, der er truet

- Packet sniffing
- Spoofing og phishing
- Replays
- DoS og DDoS
- Malware
- Spyware
- Ransomware
- CEO-fraud
- Trojansk hest
- Computerorm

CIA modellen

[C] *fortrolighed*:

- Uvedkommende kan ikke opsnappe kommunikationen.

[I] *integritet*:

- *data-integritet*: Indholdet af en besked fra A til B kan ikke ændres under transporten over netværket.
- *autenticitet*: En uvedkommende aktør C kan ikke udgive sig for at være A eller B.
- *uafviselighed*: Hvis A sender B en besked, kan A ikke bagefter nægte det.

[A] *tilgængelighed*:

- Uvedkommende kan ikke afbryde A's og B's mulighed for at kommunikere.

SQL injections

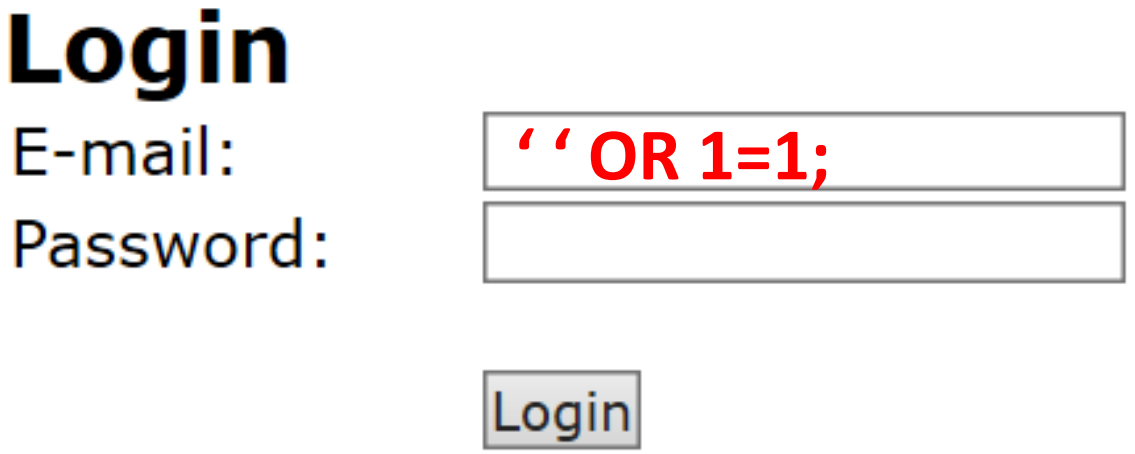
- Webside med login formular:

- SQL kode som tjekker i databasen:

```
SELECT bruger_id FROM bruger_database WHERE
brugernavn='$bruger' AND kodeord='$kodeord';
```

SQL injections

- En hacker taster nu:



- Det giver:

```
SELECT bruger_id FROM bruger_database WHERE
brugernavn=' ' OR 1=1; AND kodeord='';
```

Script injection

- Injection af et script:

Script injection hos Bahne

- [Artikel i Version 2, den 29. novmeber 2019]

DON’T DO THIS AT HOME!

Brevkassespørgsmål til cyberhus.dk:

Hej cyberhus. Jeg vil lige høre om det er tilladt at sql injecte en side bare for at se om det er muligt og så ikke gøre noget ved det? Evt. ringe til admin på siden?

Svar:

SQL Injection er stærkt ulovligt og det eksempel du har opstillet med at teste og ringe til admin, ville i bund og grund svare til at slå en person, for at teste om det gør ondt. SQL Injection er ikke ulovligt hvis det mislykkedes, men hvis det lykkedes dig at bryde ind på andres systemer (.. i denne sag SQL databasen), vil det være overtrædelser af flere lovgivninger og kan reelt give en fængselsstraf, hvis admin laver sag mod dig.

Tænk på hvordan det vil være i den fysiske verden…

- Er det lovligt at prøve at bryde ind i min nabos hus – bare for at se om det kan lade sig gøre? Så vil jeg bagefter kontakte ham og fortælle hvor svaghederne er…

Ej vel!