UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi
Datasikkerhet temavideo 7: Sikkerhet i og for nettverk

Kristin Skar
kritisk@ifi.uio.no

Nettverkssikkerhet

Nettverkssikkerhet: Sikkerhetstrusler

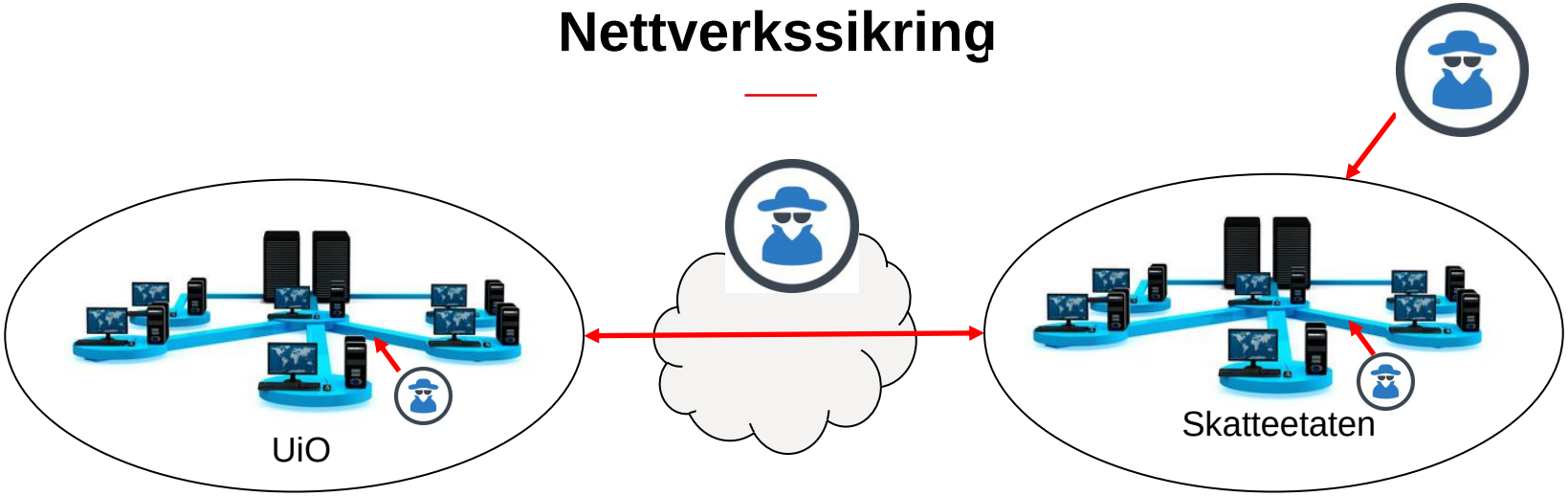
Trusler:

- På datatrafikk:
  - **Avlytting**: Uvedkommende lytter til nettverkstrafikk og får tak i konfidensiell informasjon. *Passivt angrep.*
  - **Data modifiseres** (Man in the Middle-angrep, MitM): Uvedkommende griper inn i kommunikasjonen og modifiserer data. *Aktivt angrep.*
  - **Forfalskning**: Uvedkommende sender ikke-autentiske meldinger eller later som de er en annen. *Aktivt angrep.*
- Tjenestenektangrep: Utilgjengelige ressurser
- Uautorisert bruk: Misbruk av ressurser

Berørte sikkerhetsmål:

- Konfidensialitet
- Integritet
- Autentisitet for opphav til data/melding.
- Tilgjengelighet

Nettverkssikring



Nettverkssikkerhet kan sies å bestå av følgende to hovedområder:

- Kommunikasjonssikkerhet: Beskytte data i transporten mellom virksomheter/endenoder.
- Skallforsvar: Beskytte en virksomhets dataressurser mot uautorisert tilgang fra omverdenen.

Kommunikasjonssikkerhet: Wifi vs kablede nettverk

Kommunikasjon i trådløse nett går via radiosignaler:

- «Hvem som helst» kan lytte til signalene.
- Radiosignaler følger ikke fysiske grenser (f.eks. bygninger, vegger, ol).
- Åpner for uautorisert nettverkstilgang uten fysisk tilgang til f.eks en bygning.

Andre utfordringer:

- Signalforstyrrelser (tilsiktet eller utilsiktet) kan føre til utilgjengelighet
- Falske aksesspunkter: En trådløs enhet vil koble seg til aksesspunktet med sterkest signal.
- Kompromitterte aksesspunkter, spesielt åpne nett/aksesspunkter.

Kommunikasjonssikkerhet: Wifi vs kablede nettverk

Kommunikasjon i kablede nett går via fysiske kabler:

- Avlytting krever fysisk tilgang, men er likevel fullt mulig.

Andre utfordringer:

- Ødelagt kabel (tilsiktet eller utilsiktet) kan føre til utilgjengelighet.
- Kompromittert nettverks-endepunkter (routere/switcher).
- Kompromitterte enheter på samme fysiske nettverk.

Kommunikasjonssikkerhet

Avlytting er svært enkelt

Løsning: Bruk sikre nettverksprotokoller

Skallforsvar

- Brannmur:
  - Slipper inn eller avvise trafikk inn i og/eller ut fra et nettverk basert på forhåndsdefinerte regelsett.
  - Brannmur fungerer som en *tilgangskontroll* for nettverket.
  - Kan være et dataprogram eller maskinvare laget for akkurat dette formålet.
- Innbruddsdeteksjon
  - Overvåker nettverkstrafikk, og kan detektere:
    - Både forsøk på og suksessfulle innbrudd
    - Datavirus og annen ondsinnet programvare
    - Tjenestenektangrep

Takk for i dag!

mn.uio.no/ifi