

UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

Temavideo 1 uke 1: Sikkerhet

Kristin Skar
kritisk@ifi.uio.no

Sikkerhet?







Sikkerhet?

Safety

Security

Certainty



“Sikkerhet kan defineres som en tilstand; fravær av uønskede hendelser eller frihet fra fare og frykt. Denne tilstanden er imidlertid ikke statisk, men påvirkes av endringer i faktorer som trussel og farer, sårbarhet og verdi”

Store norske leksikon, snl.no



Refleksjon

Hva kan være
“*en verdi*”?

(gi eksempler)

Verdier

Hva som er en verdi handler om *hva som er viktig for noen i et gitt tilfelle.*

- Hva er viktig for deg?
- Hva er viktig for en virksomhet?
- Hva er viktig for samfunnet?

Oppsummert

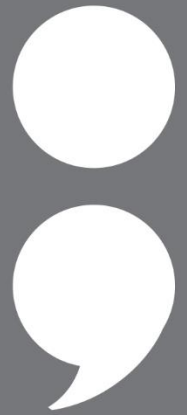
– vil beskytte *verdier* mot skade og ødeleggelse
– hva som er *en verdi* kan variere stort
– bekymringen er *skadelige hendelser,* tilsiktet eller utilsiktet

Hva som utgjør en trussel vil dermed være svært situasjonsbetinget.

Sikkerhet i en digital hverdag

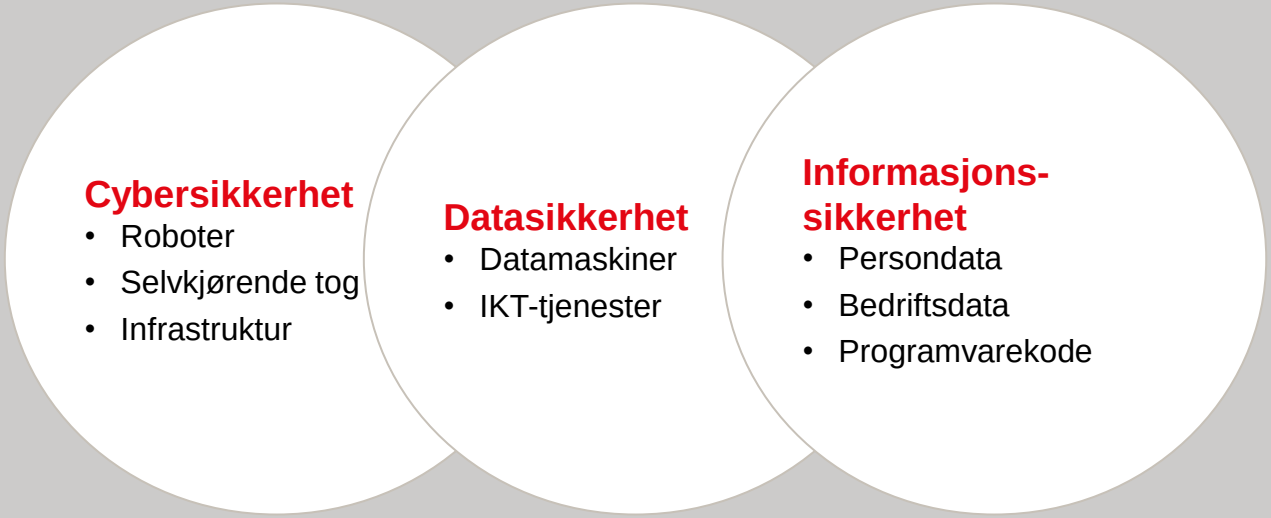






UiO : Institutt for informatikk

Digital sikkerhet
Flere begreper – samme betydning?





Refleksjon:

Datakriminalitet: Konsekvens for deg?

Nye tjenester, nye trusler



«Digitalisering (innføring av digital teknologi) er viktig, men like viktig er det at sikkerheten holder tritt med utviklingen»



Digitale trusler stadig økende:

- Datakriminalitet
- Sabotasje
- Industrispionasje
- Etterretning



Kilder:

https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde/

https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

Dataangrep: Hvem?

En tusselaktør er…

- den som kan tenkes å utføre en potensielt skadelig handling.
- Hvilke trusselaktører man bekymrer seg for er situasjonsbetinget.

Men hvem *er* trusselaktørene?

- Sporadiske «hackere»
- Aktivister
- Kriminelle
- Virksomheter
- Nasjonalstater

Dataangrep: Hvorfor?

- Økonomisk vinning/gevinst: Utpressing, svindel, utnytte kontoinformasjon
- Uautorisert tilgang til forretningshemmeligheter, forskning, mm.
- Svekke konkurrenter, virksomheter, stater
- Tilgang til konfidensiell informasjon som kan brukes til å påvirke politiske prosesser, til sabotasje eller militær maktutøvelse

- Ideologi (hacktivisme)
- Anerkjennelse
- Nysgjerrighet, snoking?

Dataangrep: Tilfeldig? Målrettet?



Konklusjon: Økende behov for digital sikkerhet

- Hurtig innovasjon i nye IT-produkter og -tjenester skaper også nye sårbarheter og insentiver for angrep:
  - Kriminalitet følger nye tjenester og nye forretningsmodeller
  - Stadig flere tjenester er eksponert online
- Forbrukere rangerer ny teknologi framfor sikker teknologi
- Sikkerhet ignoreres ofte når utviklere har tidspress
- Hurtig utvikling av mer effektive angrepsverktøy
- Økende antall trusler

Takk for i dag!

mn.uio.no/ifi

