# Informasjonssikkerhet og etikk – hvordan henger dette sammen DRI 1001 15.11.2005

## Informasjonssikkerhet og etikk hører dette sammen?

DRI 1001 15.11.2005

- **Hva** er informasjonssikkerhet
- **Hvorfor** informasjonssikkerhet – **hvilke** trusler har vi og hvilke verdier bør vi beskytte
- **Hvor** og **hvordan** kan vi sikre oss – noen eksempler
- Sikkerhet og etikk - noen sammenhenger
- Eksempler på etiske retningslinjer
  - Universitetets IT-reglement
  - DND og ACM

Pensumstoff

- Braadland, kap. 7
- http://www.usit.uio.no/it/reglement/it-reglement.html



## Oppgave

- Hva er etter deres mening de tre viktigste sikkerhetstruslene truslene dere kan bli utsatt for
- Hvilke 3 sikkerhetstiltak (eller flere) mener dere er særlig viktig
- Mener dere sikkerheten på Universitetets datanett og maskiner er god nok ?



## Definisjon av informasjonssikkerhet

- Beskyttelse mot brudd på *konfidensialitet*, *integritet* og *tilgjengelighet* for informasjonen og også for det informasjons-systemet informasjonen inngår i.

Sagt på en annet måte

- Robuste og effektive informasjonssystemer, som gir *korrekt informasjon* til *rette personer* til *rett tid*



## Hva betyr dette i praksis

- *Konfidensialitet*
  - Sikkerhet for at kun autoriserte brukere får tilgang til informasjonen.
- *Integritet*
  - Sikkerhet for at informasjonen er fullstendig, nøyaktig og gyldig.
- *Tilgjengelighet*
  - Sikkerhet for at informasjonen er tilgjengelig for autoriserte brukere til rett tid.

## Viktige begreper knyttet til informasjonssikkerhet (2)

- *Autentisering*
  - Benyttes for å bevise at en bruker er den brukeren han eller hun utgir seg for å være.
- *Autorisasjon*
  - Benyttes for å gi en bruker tilgang til kun den informasjonen eller til det informasjonssystemet han eller hun skal ha tilgang til.
- *Ikke-benekting (nonrepudiation)*
  - Benyttes for at en bruker ikke senere skal kunne nekte for at det er han eller hun som har utført handlingen.



## Hvorfor bør dere tenke på informasjonssikkerhet

- Dere vil ha stadig mer av deres "verdier" tilgjengelig på nettet
  - Økonomiske forhold , personopplysninger (f eks. helseopplysninger) , annen informasjon dere er *avhengig* av eller er viktig for dere
- Krav om generell *tilgjengelighet*, men også økende *avhengighet*
- Sikkerhetshendelser som virus, spam, tyveri med mer kan skape store problemer for dere eller andre dere samhandler med
- Dette bører også oss privatpersoner mer enn før
  - Økonomiske forhold
  - Helseopplysninger
  - Andre typer følsomme opplysninger

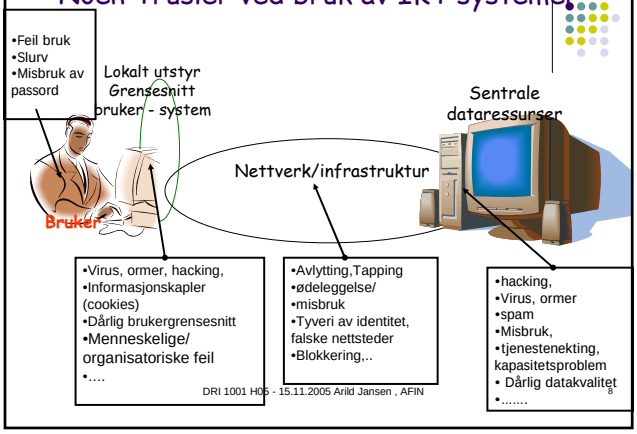


## Trusselbildet

- Sitat (Aristoteles) – "det er sannsynlig at noe usannsynlig vil skje"
- Den teknologiske utviklingen skaper uunngåelig utilsiktede og uønskede virkninger
- *Truslene* øker i antall og kompleksitet. *Trusselbildet* for den enkelte endrer seg stadig.
- Større informasjonssystemer og spesielt informasjonsinfrastrukturer har svakheter som gjør dem *sårbare* for kjente eller ukjente trusler.



## Noen Trusler ved bruk av IKT systemer



## Noen problemområder og trusler

- På lokalt utstyr:
  - Virus, ormer, hacking, informasjonskapler (cookies)
  - Dårlig brukergrensesnitt som skaper 'unødvendige' feil
  - Menneskelige/organisatoriske feil
- I infrastrukturen
  - Avlytting, ødeleggelse/misbruk
  - Tyveri av identitet, falske nettsteder,
  - Trådløse nett innebærer spesielle sikkerhetsproblemer
- "På sentrale ressurser
  - Virus, ormer, hacking,.tjenestenekting, kapasitetsproblemer, ..
  - Data- og informasjonskvalitet knyttet til både tekniske og organisatoriske forhold

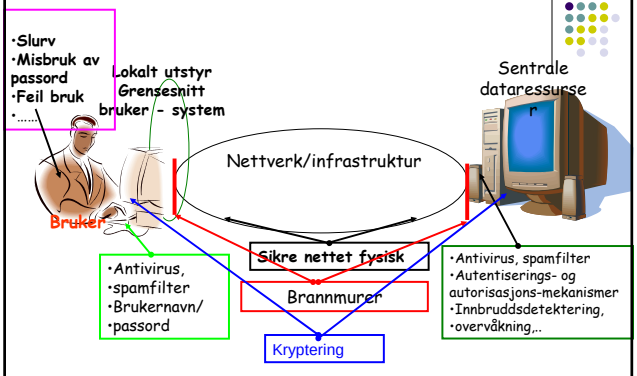


## Internett og sikkerhet

- Internett protokollene ble opprinnelig laget med tanke på en kommunikasjon basert på åpenhet og fleksibilitet, og *ikke med tanke på sikkerhet*.
- De første sikkerhetshendelser ble oppdaget fra midten og mot slutten av 1980-tallet.
- I dag skal "alle" bruke Internett til "alt".
- Vår bruk av Internett blir overvåket, både "lovlig" av programvareselskaper og tjenesteleverandører og ulovlig av alt fra nysgjerrige til organiserte kriminelle
- Med bakgrunn i den voldsomme økningen i bruk av Internett, er det utrolig viktig å "*tenke*" *sikkerhet*.



## Eksempler på tiltak






## Eksempler på tekniske tiltak

- Brannmur
- VPN (Virtual Private Network)
- Antivirus, spamfilter
- Autentiserings- og autorisasjonsmekanismer
- Innbruddsdetektering, overvåkning,..
- PKI (Offentlig nøkkel infrastruktur) og elektronisk signatur
- Filtrering av nettsider,
- Ulike personvernøkende teknologier

## Eksempel på en enkel sikkerhets- og sårbarhetsanalyse

- Hvilke **verdier** vil jeg beskytte
  - Menneskeliv /helse, økonomi, informasjon,…
- Hvilke **trusler** kan inntreffe
  - Innbrud, hacking, virus, misbruk, dårlig datakvalitet ,…
- Hva er **sannsynligheten** for at disse trusler finner sted
- Hva er **konsekvensene** (”skadekostnad”)
  - **Risikokostnad** = skadekostnad * skadefrekvens
- Hvilke **tiltak** bør/må vi iverksette



## Sikkerhet, etikk og moral

Etikk: ”teori om rett og moral”, dvs. noen generelle, overordnede ”regler” eller retningslinjer (bud) som styrer ens atferd

Handler om hva som er rett og galt og hvorfor

Prinsipper for å handle riktig

Plikt-etikk og konsekvensetikk: Forholdet mellom etikk og loven

*Er alle handlinger som **ikke** er **ulovlig** også gode handlinger?*



## Litt generelt om etiske retningslinjer

Forskningsetiske retningslinjer

- http://www.etikkom.no/retningslinjer

NITOs etiske retningslinjer

- http://www.nito.no/article.asp?ArticleID=7468&Rank=1&SubRank=2&txtRank=Om+NITO&txtSubRank=Etikk

Etiske regler for leger

- http://www.legeforeningen.no/index.db2?id=485
- Etiske retningslinjer for Statens petroleumsfond
- http://odin.dep.no/fin/norsk/tema/statens_petroleumsfond/p30005696/retningslinjer/bn.html



## Eksempler på etiske spørsmål

- Individets rettigheter
  - Personvernet (er lovregulert, men også gråsoner)
  - Overvåkning av pasienter som ikke kan ta vare på seg sjøl (senil demente, psykiske pasienter ), kriminelle
  - Rett til å kontrollere epost
- Opphavsrett – hva er akseptable rettigheter og beskyttelse
- Dataspill med voldelig innhold
- Bruk av Internett
- Maktforhold, f eks. kontroll/overvåkning i arbeidslivet

## Noen etiske ' dilemmaer;

- Lese en feilsendt epost
- Låne bort eller låne et passord
- Prøve å knekke en kode for å demonstrere svakheten i et program eller passordsystem
- Legge ut "mykporno" på UiO's nettsider



UiO's IT-reglement

- http://www.usit.uio.no/it/reglement/it-reglement.html
- UNINETTs etiske retningslinjer for bruk av nettet http://www.uninett.no/publikasjoner/unot/94-007.html

Den Norske Dataforening

- http://dataforeningen.no/?module=Articles;action=Article.publicOpen;ID=2636
- http://dataforeningen.no/?module=Articles;action=Article.publicOpen;ID=2370

ACM

- http://www.acm.org/constitution/code.html



## Konsekvensetikk og pliktetikk

| Etisk grunnsyn | Fokus | Kriterier |
|---|---|---|
| Konsekvensetikk | **Resultatene** Hvilke effekter – positive eller negative | **Verdier** Hva/hvem rammer de |
| Pliktetikk | **Handlingene** Er de ulovlige eller bare lite ønskelige? | **Normer** Hva er "riktige" og "gale" handlinger |



## Etisk vurdering – mulig framgangsmåte

- Analyser den konkrete 'problem, f eks, hendelse
  - Hva er hendt, hvem er berørt,, teknologiske fakta
- Etisk standpunkt
  - Hvilket etisk problem berøres
  - Hvilke etisk norm/prinsipp kan anvendes
  - Ta et standpunkt
- Løsningstrategi
  - Alternative løsninger
  - Velg en løsning og begrunn denne
- Iverksett løsningen –
- Case: Lese andres epost

***Hva er akseptabel risiko og hvordan bestemmer vi den?***

- *Vi må stille spørsmålet om hvor stor risiko er vi villig til å ta; og hvem bør eller skal bære kostnadene ved dette. Vi kan ikke uten videre akseptere at forvaltning og næringsliv i samfunnets interesse utvikler nye løsninger hvor det er borgerne som må bære "kostnadene" når noe går galt.*