Sikkerhets-problemer

- Innbrudd/Uautorisert tilgang til informasjon
  - Avsløre informasjon og offentliggjøre den
  - Stjele informasjon uten å gi seg til kjenne
  - Forfalske/endre informasjon
- Forfalska informasjon, for eksempel om identitet
  - Avsender/mottaker er ikke den han/hun gir seg ut for å være (IP-spoofing, pakkesniffing)
- 'Denial-of-service'/Tjenesteavbrudd
  - Å 'jamme' et system slik at det ikke virker
- Virus, ormer og trojanske hester
- Driftsavbrudd, brann, katastrofer osv.

Sikkerhet – flere aspekter:

- Autentisitet
- Autorisasjon (+ tilgangskontroll)
- Tilgjengelighet
- Integritet
- Konfidensialitet
- 'Non-repudiation'/sporbarhet
- (driftssikkerhet)

Autentisering/autorisasjon

- Brukerautentisering
- Sesjonsautentisering (web: cookies)
- Autentisering vha:
  - Noe man vet (brukernavn, passord)
  - Noe man har (smartkort, mobil)
  - Noe man er (biometrisk autentisering)
- Norske løsninger for sikker pasient-fastlege-kommunikasjon over Internett:
  - PasientLink fra Nasjonalt Senter for Telemedisin
  - MedAksess fra Deriga

Kryptering

- To hovedtyper:
  - Symmetriske: Begge parter har same nøkkel som er hemmelig for alle andre. Denne brukes til både kryptering og dekryptering.
  - Assymmetriske: Det brukes en nøkkel til kryptering og en annen til dekryptering; det er en matematisk sammenheng mellom disse to. Alle har både en kjent (offentlig) nøkkel og en hemmelig (privat). (Døme: PGP, RSA)
- Assymmetriske nøkler: Basert på matematiske 'en-veis-funksjoner': det skal være tilnærmet umulig å finne privat nøkkel ut fra offentlig nøkkel.
- Tildeling av offentlige nøkler blir gjort av TTP (Trusted Third Party, Tiltrodd Tredjepart), institusjoner som 'alle' stoler på. Utstedelse av sertifikater, drift av katalogtjenester og sperresystem (Posten/ErgoGroup)
- PKI = Public Key Infrastructure

Kryptering sikrer konfidensialitet og autentisitet

1. Sender krypterer med sin private nøkkel (signering)
2. Sender krypterer med mottakers offentlige nøkkel (kryptering)

Transmisjon (overføring)

3. Mottaker dekrypterer med sin eigne private nøkkel (dekryptering)
4. Mottaker dekrypterer med senders offentlige nøkkel (verifisere signatur)

PKI / 'Digital signatur'

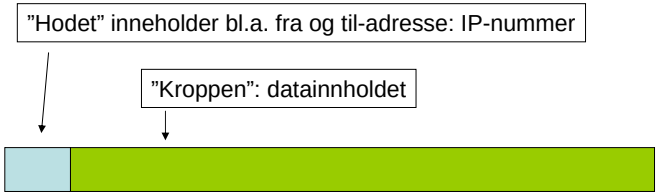
- Fra www.norskhelsenett.no:
  - "Du "stempler" dokumenter med halvparten av et unikt merke. Den andre halvparten er i en offentlig katalog. Siden ingen andre har en halvpart som passer, er ditt merke identifisert. På liknende måte kan du forsegle en konvolutt med mottakers offentlige merke som en del av låsen. Ved å legge sin private del i låsen går konvolutten opp. PKI gir en sikkerhetsmekanisme for sikring av infrastruktur, informasjonsutveksling og tilgang til systemer."

PKI / 'Digital signatur'

- PKI ønskes brukt for meldingsutveksling generelt (epikriser, labsvar, journalinfo, meldinger til sentrale registre), samt annen kommunikasjon mellom helsearbeidere.
- Det finnes både virksomhetssertifikat og personlig sertifikat. Personlig sertifikat er nødvendig når handlingen krever autorisasjon (resept, sykemelding)
- Mai 2003: Rikstrygdeverket, SHdir og Legeforeningen: offisiell åpning av standard-løsning for digital signatur for helsesektoren og trygdeetaten. (I første omgang legeerklæringer og sykemeldinger til RTV, + resept)
- (Lov om elektroniske signaturer)

IP : Internet Protocol

Trafikk på Internett består av mange små 'datapakker':



Et IP-nummer: 129.240.68.70

IP-nummer + portnummer: 129.240.68.70:80

Brannmurer

- Rutere og maskiner som er konfigurert for å håndheve en sikkerhetspolicy
- På nettverkslaget kan en ruter filtrere IP-pakker:
  - Stopper pakker basert på IP-adresse (kilde og eller mål), evt. også portnummer. To varianter:
  - Alt som ikke er tillatt er forbudt
  - Alt som ikke er forbudt er tillat
- Applikasjonlaget: Application gateway eller proxy:
  - Pakker ut IP-pakkene og analyserer innholdet. Mulighet for logging og alarm, kan ha ekstra sikkerhet og autentisering.
  - Screened host, screened sub-net, dual-homed gateway

Sikkerhet: mer enn teknologi

- Det viktigste elementet er en sikkerhetspolicy
  - Sikkerhetsmål
  - Sikkerhetsstrategi
  - System for avvikshåndtering
  - System for revisjon (vedlikehold og oppdatering)
- Brukaropplæring, sikkerhetskultur
- Risikovurdering og sårbarhetsanalyser
  - Risiko = sannsynlighet x konsekvens
- Nye risiko-områder med ny teknologi
  - Trådløse nett
  - PDA-bruk (lette å miste)

Reguleringer og retningslinjer for informasjonssikkerhet i helsevesenet

- Flere lover regulerer IT-systemer:
  - Personopplysningsloven (POL, gjeldende frå 1.1.2001). §§ 13 og 14 stiller krav til system for å ivareta informasjonssikkerheten. Grunnleggende mål: beskytte den enkelte mot at personvernet blir krenka
  - Personopplysningsforskriften (POF) §3-5: Sikkerhetsrevisjon
  - Helseregisterlova (frå 1.1.2002) omhandler elektronisk behandling av helseopplysninger (§ 16 og 17 informasjonssikkerhet) Grunnleggende mål: forsvarlig og effektiv helsehjelp uten at personvernet vert krenka.
  - Forskrift om pasientjournal (1.1.2001)
  - Helsepersonell-lova: Dokumentasjonsplikt, ikke fokus på sikkerhetsproblematikk
  - Arkivlova (NOARK-standarden): arkivering og langtidslagring. Journalen er definert som fagarkiv og ikke saksarkiv, dvs. ikke underlagt de strengeste kravene.

Sentrale begreper:

- Sensitive opplysninger, innbefatter bl.a. helseopplysninger
- Meldeplikt versus konsesjonsplikt
  - Dersom registeret innehold sensitiv informasjon er det i utgangspunktet konsesjonspliktig
  - Men registre som er hjemla i lov er unntatt, de er 'bare' meldepliktige (deriblant journalsystem)
  - Registre i blodbanker, forskningregistre, donorregistre er konsesjonspliktige
- Behandlingsansvarlig: den som har bestemmelsesrett over personopplysningene. Er ansvarlig for å etablere systemer og skal kunne dokumentere disse. (Direktør i helseforetaka)

Informasjonssikkerhet i helseforetak

- Sikkerhetsaspektet er sentralt i lovene:
- I personopplysningslovens § 14, Internkontroll, pålegges den behandlingsansvarlige å etablere ..”planlagte og systematiske tiltak som er nødvendig for å oppfylle kravene”. Dvs. et styringssystem (også Helseregisterloven § 17)
- Utdjupa i Personopplysningsforskriften (pof) kapittel 2-4: risikovurdering er pålagt
- Helsevesenet: bransjenorm for sikkerhet er utarbeidet.

Informasjonssikkerhet i helseforetak (2)

- (Operativt) ansvar hos ledelsen ved foretaket (direktør), driftsansvar kan ligge hos andre
- Sikkerhetsledelse:
  - Definere mål og strategier
  - Beskrive ansvars- og myndighetsforhold
  - Etablere internkontroll-systemer, inkl. risikovurderinger, sikkerhetsrevisjoner

Informasjonssikkerhet i helseforetak (3)

- Krav
  - Foretaket skal ha oversikt over personopplysninger
  - Risiko og sårbarhetsanalyser skal gjennomføres
  - Sikkerhetsrevisjoner skal gjennomføres
  - System for avvikshåndtering skal være implementert
  - Internkontrollsystem skal være etablert

Driftssikkerhet

- Scenarier:
  - Kabelbrudd, strømbrudd, brann, vannskade, svikt i kjølesystem, diskkrasj, svikt ifbm. oppgraderinger, manglende sikkerhetskopieringer
- Løsninger:
  - Redundante løsninger (doble sett kabler, speila disker osv.), alarmsystem, rutiner

Gråsoner rundt journalen?

Lovgivning og standardisering har tatt utgangspunkt i visjonen om den ene, 'altomfattende' journalen, ikke i dagens virkelighet med mange løst sammenkoblede systemer (jfr. CSAM)

Papirjournalen var definert fysisk, mens grensene rundt den elektroniske journalen er mindre definerte.

- Hva med systemene som leverer data til EPJ?
- Hva med de systemene som EPJ innholder en peker/link til?
- Hva med systemene som blir brukt i parallell med EPJ?

Eksempler på problemer avdekket i fbm. Datatilsynets kontroller

- Journalsystemet er meldepliktig, men var ikke meldt.
- Dokumenterte system for internkontroll forelå ikke
- Ikke akseptabel kontroll med system for autorisasjon og tilgang
- Ledelsen hadde ikke tilstrekkelig oversikt over forskningsprosjekt som brukte opplysninger fra EPJ
- Mangelfull systematisk oversikt over nettverk og systemkonfigurasjon
- Kunne ikke dokumentere risikovurdering, sikkerhetsmål, sikkerhetsstrategi og sikkerhetsrevisjoner
- Ansvars- og myndighetsforhold ikke avklart
- Kunne ikke dokumentere tilfredsstillende sikring av konfidensialitet