Sikkerhedstrusler i sundhedsvæsenet

- hvordan kan risiko og sårbarhed reduceres

Arne Tjemsland

Chefkonsulent

Secode Norge

arne.tjemsland@secode.com

+47 99282916

Bakgrunn

- Mørketallsundersøkelsen (Norge), noen relaterte eksempler:
  - » 50% av virksomhetene innen helse- og sosial vet ikke om de har vært utsatt for datainnbrudd eller datatyveri
  - » Sektoren bruker sikringsmekanismer som kryptering i langt mindre grad (bare 13%) enn andre sektorer (40%)
- Secode Norge har i en årrekke arbeidet med helseforetak og rådgivning knyttet til den Norske Personopplysningsloven.
  - » Et foregangssykehus (Ullevål Universitetssykehus): Kunde i mange år, eksempler siste år:
    - Status på sikkerhet - Risikoanalyse: IT-drift, hendelseshåndtering
    - Tiltak – rådgiver for definering og gjennomføring
    - Måling - Monitorerings- og overvåkingstjeneste for trafikk (IDS)
    - Måling - Analyse og implementering av løsning for å oppdage misbruk av EPJ

Sikkerhetstrusler i Sundhedsvesenet

SECODE
Controlling IT Security

- Risikobildet er meget sammensatt – 24 timer i døgnet
  - »Organisering
    - Ansvar, arbeidsoppgaver, vaktordninger, hendelseshåndtering
  - »Menneskers moral og handlinger
    - Interne handlinger: Nysgjerrighet, feil, likegyldighet osv.
    - Aktivitet (ondsinnet?) fra driftsleverandører og samarbeidspartnere
    - Ekstern ondsinnet aktivitet: innbrudd, kartlegging, virus,
  - »IT Tekniske svakheter, eksempler
    - Sårbarheter i Programvare
    - Konfigurering av programvare
    - Kompleksitet
    - Lite velegnede løsninger
    - Single point of failure (nettverk, systemer)
  - »Kompetanse
  - »Fysisk adgangsforhold osv
- Disse faktorene krever en helhetsbetraktet tilnærming (top-down)

Utfordringer

- EPJs omgivelser må håndteres integrert med IT-sikkerhet og på en slik måte at den operative drift understøttes
  - » EPJs operative drift:
    - Tilgjengelighet 24 t i døgnet, skiftordninger, dårlig tid, krav til effektivitet, liv og helse
  - » Lover og regler (Lov om behandling av personoplysninger)
    - Oppfylle lovens intensjon og relaterte regler
    - Rettigheter til registrerte personer, sikker forvaltning
  - » Organisasjonens kultur
  - » Tekniske omgivelser
  - » Behov for dokumentasjon vs operativ reduksjon av risiko
    - Dokumenter løser ikke behov for sikkerhet
    - Mennesker er ikke prosessorientert i sin tekning, men oppgaveorientert

Hvordan møter vi dette?

SECODE
Controlling IT Security

- Trusler og utfordringer kan kun møtes ut fra en helhetsbetraktning / balansert tilnærming
  - » Lav operasjonell risiko nås gjennom en kombinasjon av tiltak der tekniske tiltak bare er en del av virkemidlene
  - » Erfaring viser at det er avgjørende å identifisere de Digitale Verdier
    - For systemene som EPJ kommuniserer med / er avhengig av
    - Hvilket beskyttelsesbehov har EPJ og relevante tekniske delsystemer
      - Høy, Middels, Lav knyttet til Konfidensialitet, Tilgjengelighet, Integritet
      - Har man satt et mål (Loven) på det og valgt sikkerhetstiltak?
    - Eks: Erfaring fra Ullevål Universitetssykehus: EPJ har høyt beskyttelsesbehov (Høy) og krav til tilgjengelighet hele døgnet. Økonomimoduler har lavere krav til beskyttelse mot innsyn og tilgjengelighet
    - Tiltak iverksettes i henhold til beskyttelsesbehov gjennom balanserte tiltak

Omgivelser

SECODE
Controlling IT Security

- Til ettertanke:
  - »Er EPJ avhengig av services produsert utenfor EPJs sikkerhetsmessige kontroll?
    - Outsourcing
    - Utviklere
    - Konsulenter
    - Systemer
  - »Leverer EPJ informasjon/services til enheter/brukere utenfor EPJs kontrolldomene?
- Man bør definere sikkerhetsmessig kontroll domene

Hvordan møter vi dette?

SECODE
Controlling IT Security

- Organisering og ansvar er helt avgjørende
  - Ansvar fordelt på roller (IT, ledere, brukere, sikkerhet…)
  - Enklest mulig hverdag for brukere, men med tydelige ansvar
  - Oppfølging av IT-sikkerhet, logger osv
  - Rapportering og synliggjøring for virksomhetens ledelse
  - Integrert med budsjettprosesser
- Tekniske sikkerhetstiltak er en del av helheten
  - Systematisk understøtte brukernes og EPJs behov
  - Sikre tilgjengelighet
  - Ansvar for vedlikehold definert
  - Dagens sitat: EPJ er 20% teknikk og 80% organisasjon – teknikk får 80% av oppmerksomheten: Stemmer med våre erfaringer

Ta kontroll

SECODE
Controlling IT Security

- Helhetsbetraktede valg, gjennomføring og vedlikehold av IT-sikkerhetstiltak
  - »Kontinuerlig prosess
    - Definere beskyttelsesbehov
    - Bestemme ønsket sikkerhetsnivå
    - Analysere nåtilstand på risiko
    - Gjennomføre tekniske og organisatoriske/administrative tiltak
      - Forbedringsprosess
    - Måle/vedlikeholde sikkerhetsnivå

Ta kontroll

- Sikkerhetsmessig modenhetsnivå
- Restrisiko