NORMEN

Sikkerhets- og samhandlingsarkitektur ved intern samhandling (faktaark 20b)

Versjon 3.1

20.09.2018

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler retningslinjer for etablering av: - Standardisering av virksomhetens sikkerhetsfunksjoner ved intern samhandling - Sikkerhet ved samhandling i formaliserte arbeidsfellesskap Formålet med faktaarket er å gi virksomheten en sikkerhetsarkitektur som tilrettelegger for samhandling på en trygg måte.Retningslinjene kan benyttes ved innføring av nye IKT-systemer eller endringer i eksisterende systemer. Faktaarket har en teoretisk tilnærming og inneholder eksempler på blant annet sikkerhetsarkitekturer og soneinndeling i lokale nett.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er • Virksomhetens leder/ledelse • Sikkerhetsleder / sikkerhetskoordinator • IKT-ansvarlig • Databehandler • Leverandør
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen • Kapittel 5.5.3 Elektronisk samhandling
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Pasientjournalloven § 23 Internkontroll • Personvernforordningen artikkel 24 Den behandlingsansvarliges ansvar • Personvernforordningen artikkel 32 Sikkerhet ved behandlingen • Veileder for tilknytning til helsenettet • Tjenesteutsetting av kommunale helse- og omsorgstjenester (faktaark 46)

Sikkerhets- og samhandlingsarkitektur ved intern samhandling

1. Konfigurasjonsstyring

Følgende krav skal ivaretas ved etablering av intern samhandling:

- Virksomheten skal ha oversikt over og kontroll på alt utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger. Dette gjelder også utstyr ved hjemmekontor og mobilt utstyr
- Konfigurasjonen skal sikre at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt
- Konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, skal ikke settes i drift før følgende tiltak er gjennomført:

    - Risikovurdering som viser at nivå for akseptabel risiko oppfylles
    - Test som sikrer at forventede funksjoner er ivaretatt
    - Implementering som sikrer mot uforutsette hendelser
    - Ny konfigurasjon er dokumentert
    - Virksomhetens leder eller den ledelsen bemyndiger har godkjent endringen

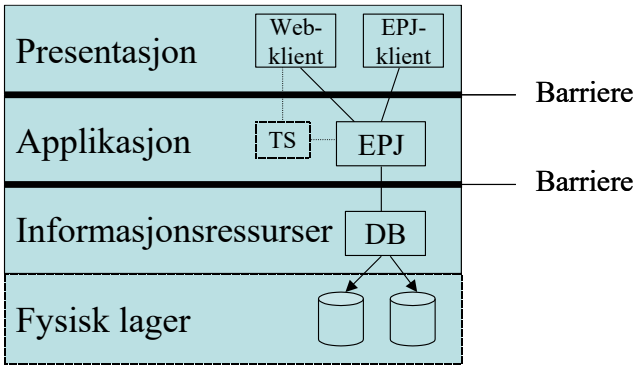
2. Sikkerhetsarkitektur for en tjeneste

Tabellen nedenfor illustrerer hvordan sikkerhetsarkitekturen kan beskrives i en lagdelt modell for hver enkelt tjeneste. Denne bør benyttes for å illustrere hvordan ulike tjenester og applikasjoner er bygd opp med tilhørende sikkerhetsmekanismer. Tabellen kan benyttes på tjenester innen egen virksomhet og for tilgang til tjenester levert gjennom Norsk Helsenett.

Lag	Eksempler på sikkerhetsmekanismer
Presentasjon (klient/arbeidsstasjon)	– Nettverksautentisering – Kryptering – Nettverkskontroll – Klientautentisering – Terminalløsninger
Applikasjon/ forretningslogikk	– Hendelsesregistrering i applikasjonen – Applikasjonsautentisering (for eksempel EPJ) og tilgangsstyring – Validering av felt og data
Informasjonsressurser (database)	– Transaksjonslogg og systemlogg – Låsemekanismer (read-only) – Tilgangsstyring til databasen – Integritetskontroll
Fysiske komponenter	– Redundans i teknologi – Fysisk sikring

Eksempel:

Figuren nedenfor illustrerer sikkerhetsarkitekturen for en EPJ-løsning. Presentasjonslaget viser frem den aktuelle informasjonen ved hjelp av en webklient (nettleser) eller en egen EPJ-klient. Klienten kommuniserer med en applikasjon (EPJ). Det er også mulig å benytte en terminalserverløsning (TS), som i realiteten betyr at all databehandling skjer i applikasjonslaget. Kommunikasjonen mellom presentasjon og applikasjon kan om nødvendig krypteres. I datanettverket kan det være sikkerhetsbarrierer. Selve applikasjonen (EPJ) kommuniserer med databasen (DB) som holder kontroll på alle dataelementene som er lagret i et fysisk lager. Det fysiske lageret kan være fordelt på ulike lagringssystemer eller servere.



Eksempel: Sikkerhetsarkitekturen for en EPJ-løsning

3. Soneinndeling på lokalt nett

Soneinndeling benyttes for å skille ulike data i forskjellige logiske eller fysiske sikkerhetssoner. Hensikten med soneinndeling er å sikre at tilgang til de ulike sikkerhetssonene på en hensiktsmessig måte kan styres ut i fra hvem som skal ha tilgang til dem og fra hvor. Soneinndeling vil i tillegg kunne hindre at sårbarheter utnyttes på tvers av systemer og soner.

Det finnes en rekke sikkerhetsbarrierer som kan benyttes for å dele et nettverk eller en tjeneste opp i flere soner. Brannmurer er en mye brukt løsning for nettverk, men det er ingen føringer på hvilken teknologi som benyttes så lenge formålet om tilgangsstyring er oppfylt. For å vite at nødvendige tiltak er etablert skal det gjøres en risikovurdering.

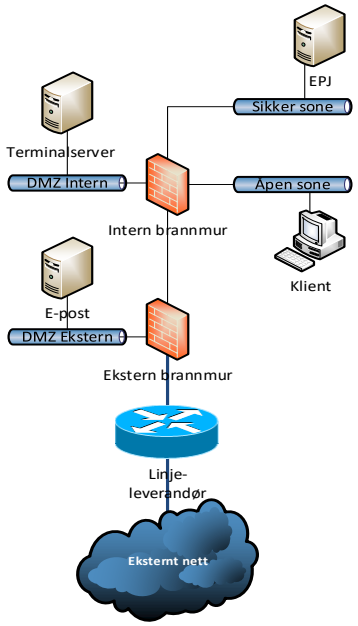
Eksempel på soneinndeling[1]:

Sone	Beskrivelse
Sikker sone	Sonen omtales også som lukket sone eller sensitiv sone. Her skal tjenester som inneholder helse- og personopplysninger plasseres. Flere mindre virksomheter opererer kun med sikker sone når de er tilknyttet helsenettet. Tilgangen inn mot sikker sone skal sikres med tanke på å hindre uautorisert tilgang. Ved lagdeling i en applikasjon (Se kapittel 1) kan Sikker sone deles ytterligere for å sikre Applikasjon og Informasjonsressurser ytterligere. Presentasjon plasseres da normalt i DMZ.
Intern sone	Sonen omtales også som åpen sone. Klienter og utstyr som ikke inneholder (lagrer lokalt) helse og personopplysninger. Utstyr som står i intern sone har gjennom sikkerhetsløsninger tilgang til andre soner som f eks
DMZ	Sonen(e) benyttes for å terminere trafikk inn eller ut mot andre soner som trenger sikring.

Eksempler

Nedenfor følger to eksempler på vanlig bruk av soner. I de fleste eksemplene er kunderuter fra Norsk Helsenett benyttet som indre brannmur, men kunden kan fritt sette opp dedikert brannmur i tillegg til kunderuteren.

<u>Soneinndeling på nettverksnivå, med bruk av flere soner:</u>



Eksempel: Soneinndeling på nettverksnivå, med bruk av flere soner

[1] Det er ikke et krav at virksomhets nettverk skal være basert på en to-sone-modell. Tilstrekkelig sikkerhet kan ivaretas på flere måter og må baseres på en risikovurdering.

Egenskaper:

- Oppsett med to brannmurer som sikrer trafikk mellom sonene
- DMZ-soner tilknyttet både ekstern og intern brannmur for terminering av trafikk inn mot eller ut fra henholdsvis sikker sone (EPJ) og åpen sone (E-post)
- Klienter har tilgang til sikker sone via terminalserver

<u>Bruk av virtualisering for å dele opp i ulike logiske soner:</u>

Eksempel: Bruk av virtualisering for å dele opp i ulike logiske soner

Egenskaper:

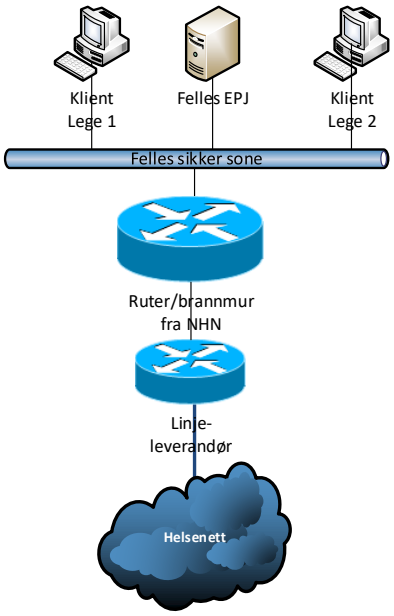
- Virtualiseringsteknologi benyttes for å lage logiske skiller mellom de ulike sonene som etableres på samme fysiske infrastruktur
- Sikkerheten i virtualiseringslaget vil kunne tilby tilstrekkelig sikkerhetsbarriere
- Virtualisering kan gjøres både på server og nettverk i en slik løsning

4. Samarbeid mellom virksomheter om behandlingsrettede helseregistre

Se tjenesteutsetting av kommunale helse- og omsorgstjenester (faktaark 46) og ”Veileder med avtaleeksempler ved samarbeid om felles journal”

Felles journalsystem følger de samme tekniske krav til sikkerhet som om nettverk og server hadde vært dedikert til kun en juridisk enhet.

Figuren nedenfor illustrerer bruk av felles sikker sone i virksomheter som samarbeider om behandlingsrettede helseregister (gruppepraksis med to leger):



Eksempel - Bruk av felles sikker sone i virksomheter som samarbeider om behandlingsrettede helseregister (gruppepraksis med to leger)

Egenskaper:

- Oppsett med en felles sikker sone
- Oppsett med kun en intern brannmur som sikrer Felles sikker sone
- Klienter og server i samme nett
- Forutsetter eksterne sikringsløsninger for tilgang til f. eks. Internett eller tilgang inn mot sikker sone fra eksterne nett

5. Delt lokalnett mellom ulike juridiske enheter

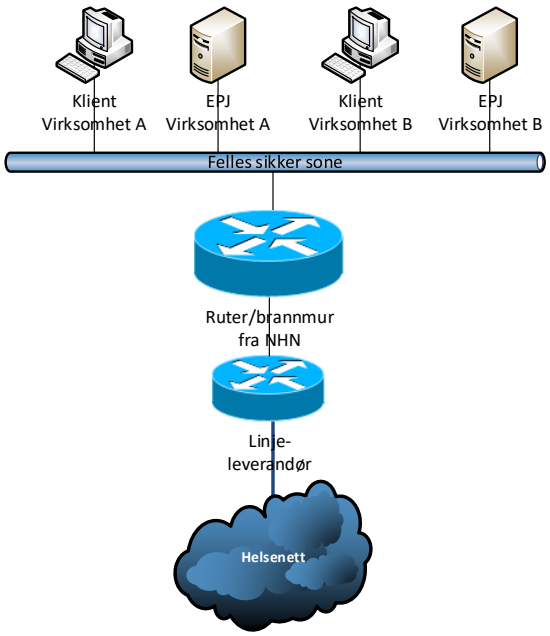
Så lenge virksomhetene har tiltak mot uautorisert tilgang til helse- og personopplysninger kan to ulike juridiske enheter dele lokalnett. Data fra de ulike virksomhetene skal holdes

logisk adskilt, noe som forutsetter sikring på server/applikasjonsnivå. Ved felles lokalnett forutsettes det at enhetene er underlagt et felles informasjonssikkerhetsregime og samordnet drift på felleskomponentene.

Noen anbefalte sikringsmekanismer for å sikre data:

- Gode prosedyrer og avtaler
- Passordbeskyttelse på servere/fagsystem
- Lokal brannmur på server
- Bruk av sertifikater på klient/serverkommunikasjon

<u>Eksempel på to juridiske enheter i felles lokalnett</u>



Eksempel: To juridiske enheter i felles lokalnett

Egenskaper:

- Virksomheten deler fysisk nett og har felles sikker sone
- Tilgangsstyring inn mot journalsystemet hindrer uautorisert tilgang mellom virksomhetene
- Oppsett med kun en intern brannmur som sikrer Sikker sone
- Klienter og server i samme nett
- Forutsetter eksterne sikringsløsninger for tilgang til f. eks. internett eller tilgang inn mot sikker sone fra eksterne nett

6. Sammenkobling av virksomhetens geografisk adskilte enheter

Ved sammenkobling av geografisk adskilte enheter forutsettes det at enhetene er underlagt et felles informasjonssikkerhetsregime. Når enhetene er sammenkoblet vil de fungere som et felles datanettverk. Sammenkoblingen stiller således ikke ytterligere krav til sikkerhet på klientsystemene.

Det stilles krav om:

- Kryptert datakommunikasjon over åpne nett
- Bruk av PKI-sertifikat og kryptering av samband skal være i samsvar med Kravspesifikasjon for PKI i offentlig sektor.