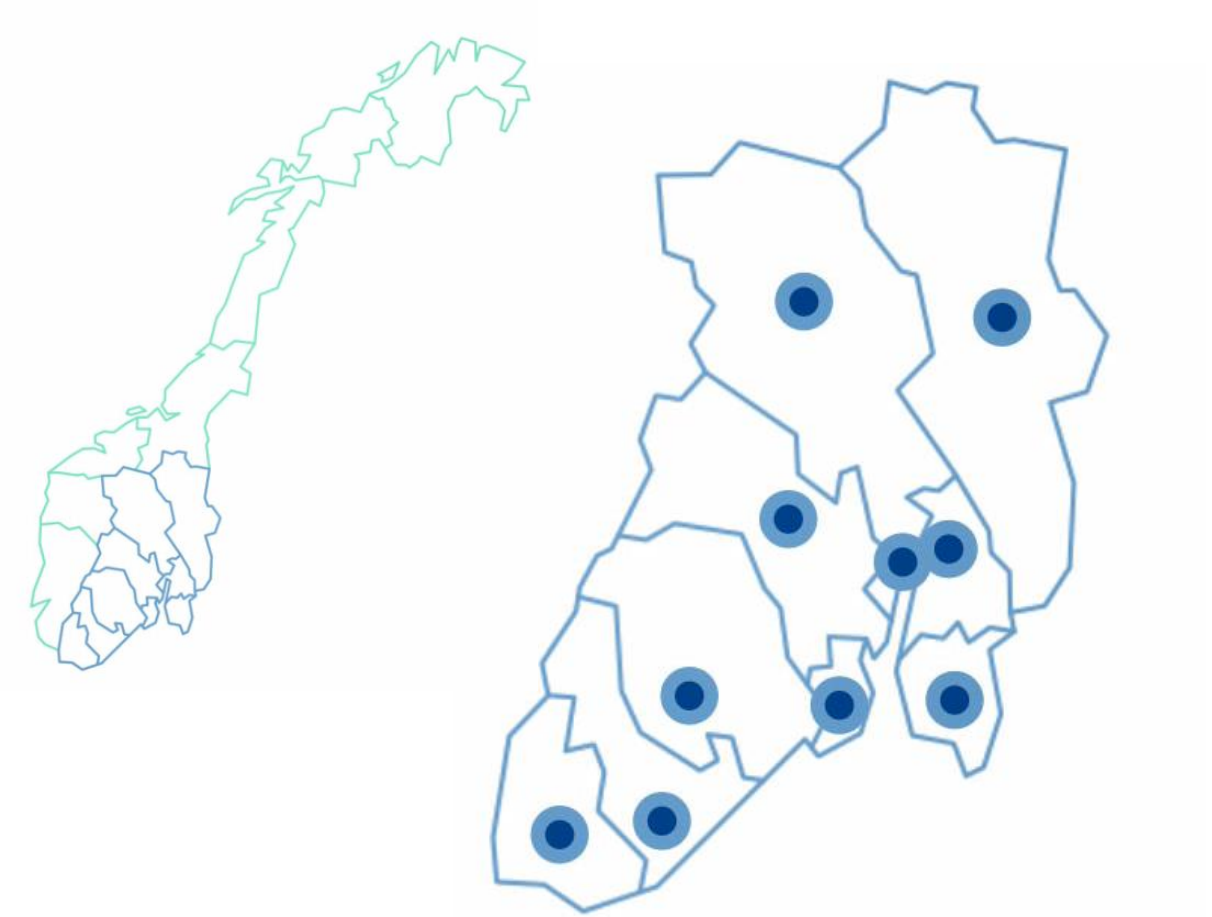
Angrepet mot Helse Sør-Øst

Norsk sykehus- og helsetjenesteforening

2019-06-06

HELSE SØR-ØST

Om Helse Sør-Øst



- Helse Sør-Øst består av elleve helseforetak, hvorav ni leverer pasientbehandling
- Helseregionen leverer spesialisthelsetjenester til rundt tre millioner innbyggere
- Budsjett på cirka 80 milliarder kroner/år
- I underkant av 80 000 medarbeidere
- Regionen har en stor, svært kompleks og driftskritisk IKT-portefølje.
- Gode og likeverdige helsetjenester til alle som trenger det, når de trenger det.

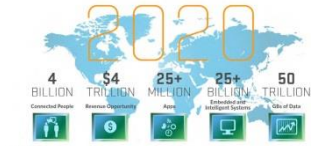
Sykehuspartner HF leverer IKT-tjenestene i Helse Sør-Øst

- Sykehuspartner har rundt 1 500 ansatte fordelt på flere lokasjoner i regionen
- Sykehuspartner drifter over 60 000 arbeidsflater, fordelt på rundt 12 000 servere.
- Helseregionen forvalter en applikasjonsportefølje på rundt 2 000 applikasjoner.
- Sykehuspartner har et 24/7 driftssenter kan i løpet av kort tid mobilisere 50 vaktlag bestående av mer enn 260 medarbeidere, også innenfor informasjonssikkerhet.
- Driftssenteret har i løpet av de fem siste årene håndtert 17 millioner alarmer, opprettet 100 000 feilrettingssaker og eskalert 30 000 hendelser til vaktlag.
- Sykehuspartner antispam-filter stopper mellom 150-300 millioner spammeldinger i måneden.

IKT er en kritisk tjeneste for helsesektoren

Patient Services and The Empowered Patient

The Internet of Things

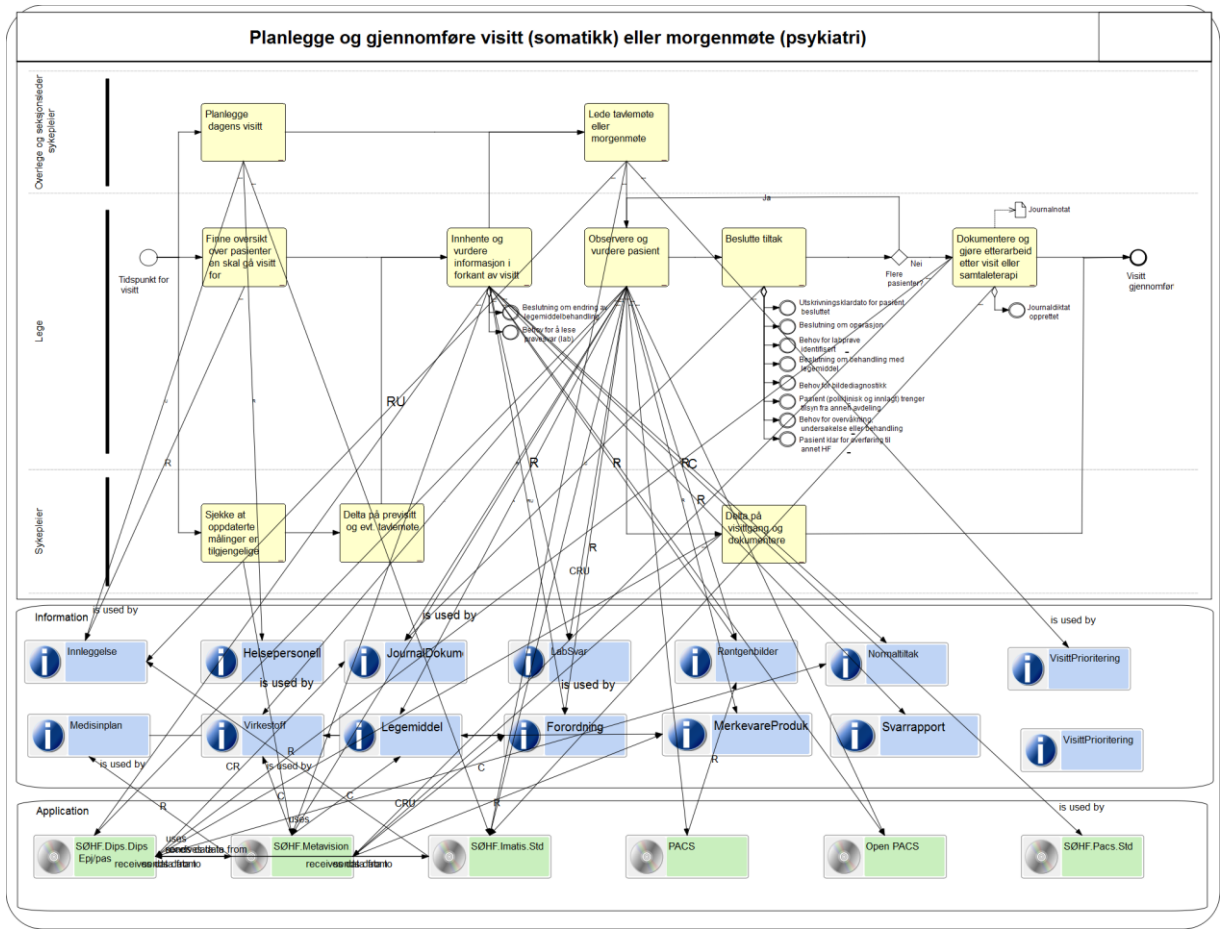


Digitalization

Mobility and Cloud Services

Big Data

Digitale sårbarheter gir ekte konsekvenser



Arbeidsprosesser som tidligere var manuelle blir nå automatiserte, og systemer som tidligere stod avlåst og alene står nå helintegrert og tilgjengelig 24/7

Når våre digitale verdier blir truet, gir det ekte konsekvenser for pasientene våre.

Disse sårbarhetene må håndteres.

Hvilke *verdier* beskytter vi?

Verdiene våre inkluderer:

- Ivareta den digitale helsehjelpen
- Beskytte person- og helseopplysninger
- Forskningsdata
- Utstyr, maskinvare og programvare
- Avtaler og kontrakter
- Omdømme
- Lønn

Varsling, rutiner og kommunikasjon

9.1: SPHF i beredskap, varsler HF og HSØ RHF, samt øvrige regionale IKT-leverandører. HSØ RHF varsler HOD.

13.1: HSØ RHF i beredskap

12.2: Siste møte i Hdirs kriseutvalg

8.1: SPHF hendelses-håndtering. Bistand fra HelseCERT og NorCERT

14.1: Møte i Hdir kriseutvalg – HOD gir fullmakt til Hdir

16.2: HSØ RHF avslutter beredskap, HOD trekker Hdirs koordineringsfullmakt

2.3: SPHF avslutter beredskap

Tiltak i Helse Sør-Øst etter dataangrepet

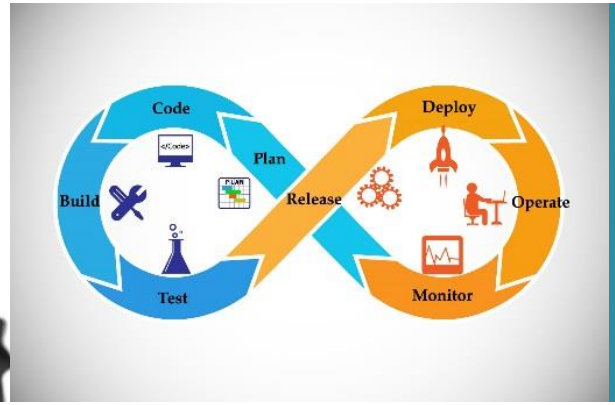
HELSE SØR-ØST

Informasjonssikkerhet er ikke bare teknologi

Kultur og holdninger

Organisasjon

Styring og prosesser



Teknologi

Informasjonssikkerhet og personvern-prosjektet: leveranseområder

Styrket tilgangsstyring

- Skal sikre rett tilgang til rett person til rett tid, og stenging av tilgang når behovet opphører
- Sporbarhet
- Økt bruk av automatisering

Personvern

- Bidra til at personvernet til ansatte og pasienter blir ivaretatt
- Dette har en indirekte effekt også for helseforetakene som databehandlingsansvarlige

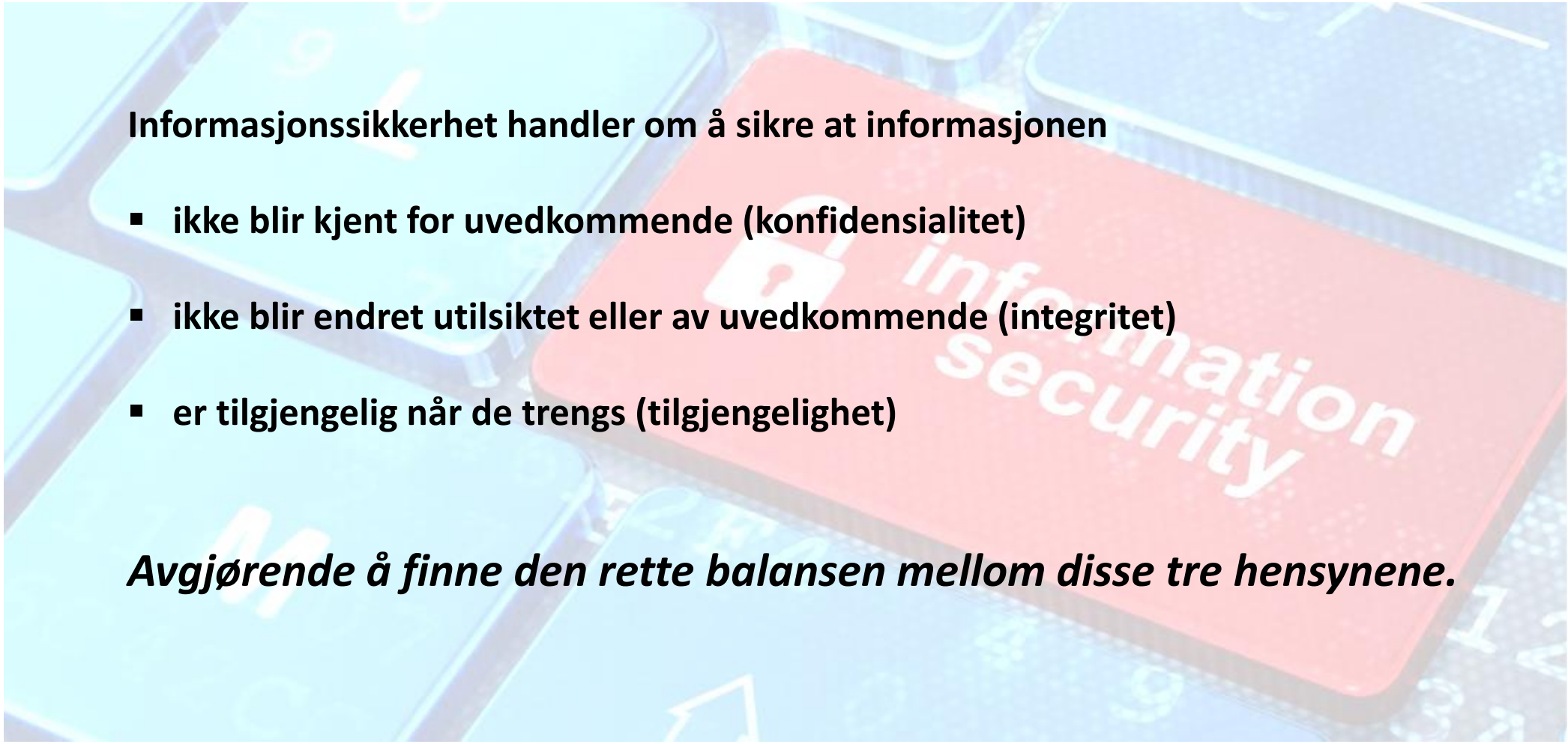
Sikkerhetsplattform

- Øke deteksjonsevne
- Redusere angrepsflate
- Øke responskapabilitet
- Styrke SP sin evne til å håndtere dataangrep

Risiko

- Felles risikoakseptkriterier i regionen
- Effektivisert ROS-prosess
- Forbedret risikostyring internt i Sykehuspartner

Informasjonssikkerhet – prinsipper



Informasjonssikkerhet handler om å sikre at informasjonen

- **ikke blir kjent for uvedkommende (konfidensialitet)**
- **ikke blir endret utilsiktet eller av uvedkommende (integritet)**
- **er tilgjengelig når de trengs (tilgjengelighet)**

Avgjørende å finne den rette balansen mellom disse tre hensynene.

Beredskap ved cyberhendelser

- Helse Sør-Øst har mye (og god) erfaring med å håndtere hendelser, også innenfor cyberdomenet.
- Viktig at også fremtidige hendelser følger de overordnede prinsippene for beredskap.

Det er kun Sykehuspartner som kan normalisere hendelser i Sykehuspartners infrastruktur

Forutse – Forhindre – Oppdag - Handle

Vårt mål er å etablere en repeterende, selvforsterkende, effektiv og lærende prosess hvor vi kan:

- forutse trusler,
- forhindre utnyttelse av sårbarheter,
- oppdage angrep,
- håndtere hendelser som oppstår

Deteksjon er vesentlig – analyseplattformen avgjørende

› I Helse Sør-Østs regionale sikkerhetsstrategi er deteksjon sentralt:

4.2.16 Egenskaper ved tekniske sikkerhetskontroller

En forutsetning for enhver fungerende sikkerhetsorganisasjon er deteksjon.
Virksomheten skal ha nettsentriske kontroller som identifiserer sikkerhetshendelser, korrelerer loggdata og sikrer spor når sikkerhetshendelser oppstår.

› Har styrket vår evne til å avdekke sikkerhetstruende aktivitet og uønsket trafikk i systemene gjennom å innføre en analyseplattform i Helse Sør-Øst. I tillegg til å dekke internett-trafikk dekker den i stor grad intern trafikk og endepunkter.
Denne vil videreutvikles både i omfang og i analyseevne

Hva kan vi og andre lærte

Lærdommer og anbefalte tiltak

1) Det finnes aktører som kan ønske å gjøre betydelig skade i spesialisthelsetjenestens IKT-systemer. Dette må inn i aktuelle trussel-, verdi- og risikovurderinger, samt også beredskapsplanverk.

2) Rutine for beslutning om å ta ned kritisk viktige systemer under tidspress må formidles og jevnlig øves på, for alle som vil bli involvert i slike beslutninger.

Lærdommer og anbefalte tiltak

3) Etter revisjon bør IKT-relaterte hendelser, inkludert dataangrep, øves på i beredskapsorganisasjonen på samme måte som for andre typer beredskapshendelser. Både som mindre skrivebordøvelser og som fullskala hendelser, i samarbeid med relevante eksterne samarbeidspartnere.

4) Det bør gjøres et arbeid knyttet til håndtering av kommunikasjon og informasjon internt og eksternt i saker med spesielle utfordringer på dette området. Det gjelder eksempelvis når det er begrenset med informasjon (lite tilgjengelig) og/eller stor usikkerhet, og saker der informasjonen lovmessig er begrenset i henhold norsk lov.

Lærdommer og anbefalte tiltak

5) Hendelsen bør benyttes til en felles gjennomgang med relevante nasjonale myndigheter og andre samarbeidspartnere om hvordan denne type hendelser best kan håndteres med spesielt fokus på samarbeid, rolle- og oppgavefordeling.

Lærdommer og anbefalte tiltak

6) «Fix the basics» – se til NSMs fire grunnleggende sikkerhetstiltak

7) God deteksjon er nødvendig for å håndtere en hendelse

8) Verifiser at backup-systemer også fungerer i krisesituasjoner

9) Kompetanse og kapabilitet i og rundt egen organisasjon er viktig, bruk f.eks. sektorens CERT-miljø for å heve eget sikkerhetsnivå

10) Skjerm det operative responsmiljøet under en hendelse