

Indikatorer for informasjonssikkerhet

Versjon 1.0

Dato: 01.04.2004

KITH Rapport 08/04

ISBN 82-7846-225-9

KITH-rapport

KITH
INFORMASJONSTEKNOLOGI
FOR ET BEDRE HELSEVESEN

TITTEL

Indikatorer for informasjonssikkerhet

Postadresse
**Sukkerhuset
N-7489 Trondheim**

Forfatter(e):

Magnus Alsaker

Besøksadresse
Sverresgt 15

Oppdragsgiver(e)

Sosial- og Helsedirektoratet

Telefon
+47 - 73 59 86 00

Telefaks
+47 - 73 59 86 11

e-post
firmapost@kith.no

Foretaksnummer
959 925 496

ISBN

Dato

Antall sider

Kvalitetssikret av

Gradering

82-7846-225-9

01.04.2004

51

Bjarte Aksnes

Åpen

Godkjent av:

Jacob Hygen, adm. direktør

Rapportnr:

08/04

Sammendrag

Denne rapporten omhandler hvordan en kan benytte seg av indikatorer for måling av informasjonssikkerheten i en helsevirksomhet. Formålet med bruk av indikatorer er at de ansvarlige for informasjonssikkerheten på en enkel måte kan følge med hvordan tilstanden utvikler seg.

Rapporten beskriver hva en indikator er og hvordan et system for indikatorer for informasjonssikkerhet kan utvikles og tas i bruk i en virksomhet. Videre beskrives det hvilket informasjonsgrunnlag som kan danne basis for indikatorer og det beskrives konkrete eksempler på aktuelle indikatorer. Det beskrives også hvordan indikatorene kan presenteres for at det skal være enkelt å se hvordan tilstanden for informasjonssikkerheten utvikler seg over tid.

Til slutt gis det et konkret eksempel på hvordan et enkelt indikatorsystem for informasjonssikkerhet kan se ut, og det gis råd og anbefalinger rundt hvordan dette kan tas i bruk.

Innholdsfortegnelse

Innholdsfortegnelse	3
1. Indikatorer for informasjonssikkerhet	4
1.1. Eksempler.....	5
2. Hva er en indikator	7
2.1. Indikatorer for informasjonssikkerhet	8
2.2. Relevant informasjon	9
2.3. Utvelgelse av indikatorer	10
2.4. Metoder for innsamling av data.....	10
2.5. Presentasjon av resultat	11
2.6. Frekvens for måling av indikatorer	12
3. System for indikatorer	14
3.1. Suksessfaktorer	15
3.2. Stegene i innføringen	16
4. Aktuelle måleindikatorer	20
4.1. Menneskelige faktorer	20
4.2. Tekniske faktorer	25
4.3. Organisasjons- og holdningsfaktorer (strukturelle og kulturelle forhold).....	28
4.4. Prosesser og prosedyrer	35
4.5. Statistiske faktorer.....	40
5. Anbefalinger	47
6. Referanser	48
Vedlegg A: Eksempel på indikatorsystem	49

1. Indikatorer for informasjonssikkerhet

KITH ønsker å utvikle indikatorer for informasjonssikkerhet som kan benyttes for å kommunisere status for informasjonssikkerhet innenfor helseforetak (lokale og regionale) og andre helsevirksomheter. Bruk av indikatorer vil kunne gjøre det lettere å følge utviklingen på sikkerhetsområdet jevnlig og iverksette nødvendige tiltak, samt å sammenligne seg med tilsvarende virksomheter.

Målgruppen er primært de som har interesse av å følge med på hvilken tilstand som informasjonssikkerheten til en virksomhet befinner seg i. De som til daglig håndterer informasjonssikkerhet er ikke i den primære målgruppen, men også denne gruppen vil kunne ha mye nytte av å bruke indikatorer. Målgrupper vil kunne være:

- Ledelsen i helsevirksomheter (for eksempel HF eller RHF)
- Helsemyndigheter (for eksempel Sosial- og Helsedirektoratet)
- Publikum
- Ansatte i helsevesenet

Formålet med bruk av indikatorer er å:

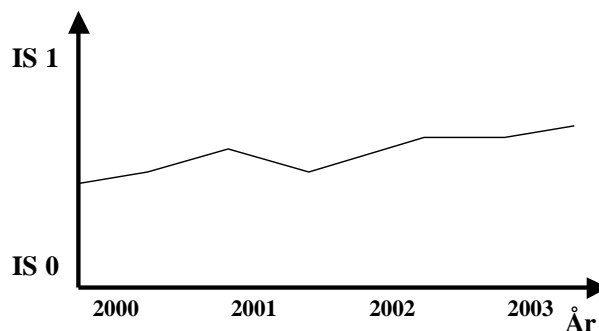
- Synliggjøre tilstand og/eller endringer for informasjonssikkerheten til en helsevirksomhet
- Få informasjonssikkerhet på dagsorden hos ledelsen
- Gi tilbakemeldinger på hvordan informasjonssikkerheten er
- Gjøre det mulig å sammenligne flere ulike helsevirksomheter

Målet er at de ansvarlige for informasjonssikkerheten ved helseforetak (dette er toppledelsen til en helsevirksomhet) på en enkel og grei måte skal kunne holde følge med i hvordan informasjonssikkerheten utvikler seg.

Målet med indikatorer er ikke å kunne "henge ut" de virksomheter som viser tegn til dårlig informasjonssikkerhet. Indikatorene skal være en hjelp til å kunne måle hvordan tilstanden til informasjonssikkerheten er og hvordan den utvikler seg. Indikatorene skal også kunne være til hjelp for å kunne gjøre de aktuelle tiltak som eventuelt er nødvendige for at informasjonssikkerheten skal bli tilfredsstillende.

1.1. Eksempler

Figur 1 nedenfor viser et eksempel på hvordan en kan tenke seg at informasjonssikkerheten blir målt og presentert over tid. "IS 0" betyr at indikatorene viser dårlig sikkerhet, mens "IS 1" betyr at indikatorene viser god sikkerhet.

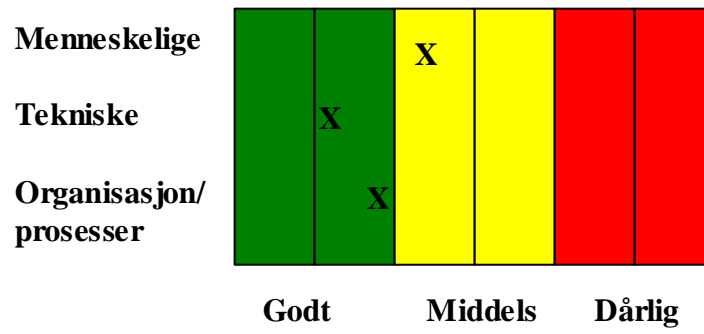


Figur 1: Eksempel på utvikling av informasjonssikkerheten hos et HF

Hva som er god og dårlig informasjonssikkerhet må defineres av den aktuelle organisasjon. God sikkerhet i en organisasjon er kanskje bare middels sikkerhet i en annen organisasjon. Kravene til informasjonssikkerhet vil for eksempel avhenge av type virksomhet, IT-systemer, hvor mye sensitiv informasjon som behandles, og lov- og regelverk som gjelder for den aktuelle virksomhet.

Ved å få til en oversikt over sikkerhetsnivået kan de ansvarlige for informasjonssikkerheten lettere både følge med på hvordan informasjonssikkerheten er, og sette inn nødvendige tiltak ved behov for det. Ved å gå nærmere inn på de enkelte indikatorene og se på hvilke indikatorer som eventuelt trekker opp eller ned, vil en også kunne finne ut hvilke områder som er årsak til god eller dårlig informasjonssikkerhet. En vil da lettere kunne sette inn de tiltakene som bidrar til at informasjonssikkerheten kommer på det nivået som er ønskelig.

Figur 2 nedenfor viser et eksempel på hvordan indikatorer fordelt på ulike kategorier kan gi et mer nyansert bilde av informasjonssikkerheten i en virksomhet. Her er indikatorene delt inn i gruppene menneskelige, tekniske og organisasjon. En slik oversikt kan være med på hjelpe ledelsen hos et helseforetak å se på hvilke områder hvor informasjonssikkerheten ikke er god nok og må forbedres. I dette eksemplet er fargekodene grønn, gul og rød brukt for å visualisere det sikkerhetsnivået som indikatoren gir (rødt = dårlig informasjonssikkerhet, grønn = god informasjonssikkerhet).



Figur 2: Eksempel på resultater fordelt på ulike områder

2. Hva er en indikator

Ved bruk av indikatorer for informasjonssikkerhet er det viktig at en benytter informasjon som er egnet til dette formålet. Det beskrives her hva en indikator er og hvilken informasjon som kan danne grunnlag for indikatorer for informasjonssikkerhet.

En indikator skal "indikere", det vil si angi eller måle retning i forhold til egenskaper eller dimensjoner en ønsker å måle. En indikator er altså en målbar størrelse som sier noe om tilstanden på et gitt område. I valget av hvilke indikatorer som anbefales brukt er det hensiktsmessig å vurdere den enkelte indikator i forhold til en del kriterier for hva som kjennetegner en god indikator.

Her kan det nevnes [4]:

- ❑ **Validiteten** sier noe om i hvilken grad indikatoren virkelig måler sentrale egenskaper ved den dimensjon som ønskes belyst (for eksempel informasjonssikkerheten i et helseforetak). Det er altså overensstemmelsen mellom indikator og dimensjon som fokuseres og hvor relevant eller representativ indikatoren er for det man ønsker å måle. Når denne sammenhengen og relevansen er helt åpenbar brukes ofte begrepet "face validity".
- ❑ **Påliteligheten eller reliabiliteten** er knyttet til muligheten for å innhente de ønskede data og kunne gi indikatoren dens korrekte verdi. For å sikre påliteligheten er det viktig å ha standardiserte rutiner for registrering og rapportering av data. Indikatorer består ofte av flere størrelser som relateres til hverandre i form av teller og nevner.
- ❑ **Definisjon av nevneren** er like viktig som å kunne definere og identifisere telleren. Dersom en skal lage en indikator for antall helsevirksomheter som har brannmur installert, så er det relevant samtidig å undersøke hvorvidt helsevirksomheten har tilknytning til Internett eller ikke (fordi en brannmur kun er viktig dersom en har til tilknytning til et eksternt nettverk).
- ❑ **Diskrimineringsvevnen** til en indikator viser til dens evne til å finne observerbare forskjeller mellom enhetene. Et eksempel på en indikator med dårlig diskrimineringssevne vil være å måle antall husholdninger med telefon som en indikator på forskjeller i levekår, da så å si alle husholdninger i dag har telefon uansett inntektsnivå.
- ❑ **Datatilgjengelighet** er svært viktig i forhold til å kunne begrense ressursinnsatsen til datainnsamling, og spesielt når de samme data skal hentes inn rutinemessig. Å samle inn separate data manuelt blir over tid svært ressurskrevende.

2.1. Indikatorer for informasjonssikkerhet

Det fins mange og forskjellige mulige indikatorer en kan bruke for å måle tilstanden for informasjonssikkerheten. Vi vil prøve å dele de inn i ulike hovedområder:

- ❑ **Menneskelige** - dette er forhold som går på menneskelige faktorer som kan påvirke informasjonssikkerheten
- ❑ **Tekniske** - dette er forhold som går på hvilke tekniske faktorer som finnes i helsevirksomheten for å ivareta informasjonssikkerheten
- ❑ **Organisasjon og holdninger** (strukturelle og kulturelle forhold) - dette er forhold som går på hvordan organisasjonen som helhet håndterer informasjonssikkerheten
- ❑ **Prosesser og prosedyrer** (for eksempel sikkerhetsstyring, avvikshåndtering) - dette er forhold som går på hvilke prosedyrer/rutiner/prosesser som finnes for å ivareta informasjonssikkerheten
- ❑ **Statistikk** - dette er informasjon som viser ulike tall på hvordan informasjonssikkerheten er, for eksempel antall virusangrep som forårsaket negative konsekvenser.

Forhold som går på organisasjon og prosesser/prosedyrer kan være vanskelige å skille og ofte vil det ikke være noen klart svar på hvor en indikator skal grupperes. Det er heller ikke viktig om en indikator plasseres i den ene eller andre gruppen. Det som er viktig er at en velger indikatorer som dekker et "bredt" område innenfor informasjonssikkerheten, og som fanger opp kritiske faktorer for informasjonssikkerheten for den aktuelle virksomhet.

2.1.1. Krav til indikatorer for informasjonssikkerhet

Et av hovedmålene med å benytte indikatorer er kunne sammenligne hvordan informasjonssikkerheten er mellom ulike helsevirksomheter. For å kunne få til dette er det viktig at de indikatorer som blir valgt har egenskaper slik at dette er realiserbart. Dette betyr blant annet at:

- Indikatorene bør være lite ressurskrevende å måle, dette gjelder både tid og innsats som kreves for å samle inn data
- Måling av indikatorene (innsamling av data) må kunne repeteres jevnlig
- Indikatorene bør være slik at en de er målbare (må være kvantifiserbare), en kan ikke bruke indikatorer som i for stor grad avgjøres ved vurdering, synsing eller andre subjektive mål.

Subjektive vurderinger vil også vanskelig la seg forene med å kunne få resultater som er sammenlignbare mellom helsevirksomheter.

- Indikatorene bør kunne måles hos ulike virksomheter, uavhengig av virksomhetens størrelse og form
- En verdi for en gitt indikator bør gi omtrent samme ”resultatscore” hos ulike helsevirksomheter, dette er viktig for at sammenligninger mellom ulike helsevirksomheter skal kunne bli reell.
- Indikatorene må kunne vise en utvikling over tid, og fortelle oss dersom noe endrer seg (blir bedre eller verre)
- Bare prosesser som er ”formelle” og/eller standardiserte bør danne grunnlag for indikatorene. Dette er viktig for at målingene skal kunne gjentas over tid og for at kvaliteten på selve målingene skal holde et jevnt godt nivå.

2.2. Relevant informasjon

Indikatorer for informasjonssikkerhet er et relativt nytt fagfelt, og det finnes lite informasjon om hvordan en skal bruke slike indikatorer.

Undersøkelser om datakriminalitet har ofte spørsmål som går på hvordan informasjonssikkerheten er i en virksomhet. Dette er kanskje noe som kan brukes som indikatorer for målinger av informasjonssikkerhet. Risikovurderinger og sikkerhetsrevisjoner er andre metoder som kan brukes som utgangspunkt for å finne egnede indikatorer for måling av informasjonssikkerheten.

Problemet med de nevnte metodene er at de kan være ganske omfattende å gjennomføre og at de ikke umiddelbart egner seg for jevnlig målinger av informasjonssikkerheten. En mulig strategi er å finne de elementer som lett lar seg måle og som er kvantifiserbare for å kunne gi målbare resultater.

Manglende menneskelig og kulturelt fokus

Mange undersøkelser til nå har i stor grad kun har fokus på tekniske faktorer. Andre relevante faktorer som mennesker, organisasjon og holdninger har i mindre grad vært belyst i faget informasjonssikkerhet. Kufås og Mølman (2003) sier at en må i sterkere grad fokusere på menneskelige og organisatoriske faktorer for å få et helhetsbilde av forhold som påvirker informasjonssikkerheten i en virksomhet.

Problemet med menneskelige faktorer med tanke på utvikling av indikatorer er at de i utgangspunktet er lite egnet for målbare enheter. Det er vanskelig å lage ”enkle” kvantitative målemetoder for hvordan ansatte for eksempel håndterer vedlegg i e-post eller hvor nøye de er med å håndtere sensitiv informasjon. For å få dette til må det gjerne formes som en slags

brugerundersøkelse hvor et større utvalg av de ansatte deltar. Dette krever som regel mer ressurser enn tekniske indikatorer en kan hente ut fra et IT-system.

Kufås og Mølman (2003) har utviklet et verktøy for å måle ”Informasjonssikkerhet, mennesker og kultur”. Verktøyet består av en rekke spørsmål hvor en skal ”rangere” hvordan en ivaretar informasjonssikkerheten. En usikkerhet med slike verktøy er at den enkelte ansatte må vurdere sitt eget forhold til informasjonssikkerhet. Svakheten kan da være at de ansatte beskriver situasjonen bedre eller dårligere enn den egentlig er, enten med vilje eller fordi de tror det faktisk er sånn. Det at mennesker utgjør en risiko for informasjonssikkerheten, gjør at også menneskelige forhold må vurderes når en skal danne seg et totalbilde av informasjonssikkerheten. Selv om verktøy for å gjøre dette kanskje krever mer ressurser og er mer omfattende enn rene kvantitative indikatorer.

2.3. Utvelgelse av indikatorer

En kan tenke seg to måter å angripe på når en finne egnede indikatorer. Den ene er en ”top-down” tilnærming, mens den andre er en ”bottom-up” tilnærming.

Top-down

En top-down tilnærming vil si at en tar til med det konkrete målet som en skal oppnå, dette kan være å redusere antall virusangrep med negative følger. Deretter må en finne aktuelle indikatorer som kan si noe om den utviklingen en ønsker å følge og om hvordan en skal måle den enkelte indikator.

Bottom-up

En bottom-up tilnærming vil si at man starter med en konkret indikator, for eksempel andelen med kjente sårbarheter som blir funnet på servere ved å gjøre en test. Deretter må en definere hvordan en kan følge utviklingen (eksempelvis antall kjente sårbarheter funnet). Tilslutt må en se på hvordan den aktuelle indikatoren kan være med på å nå de målsetninger som en har for det overordnede sikkerhetsstyringsprogrammet.

2.4. Metoder for innsamling av data

Metodene for innsamling av datagrunnlag bør være enkle og ikke for tidkrevende å gjennomføre. Dette er viktig dersom en i praksis skal kunne gjøre jevnlig målinger av informasjonssikkerheten i en helsevirksomhet. Metodene for datainnsamling bør også kunne gjennomføres på samme vis fra gang til gang for å sikre at data blir samlet inn på samme grunnlag.

Aktuelle metoder for innhenting av datagrunnlag er:

- ❑ Spørreskjemaer (for eksempel lagt ut på Intranett)
- ❑ Samtaler/intervjuer
- ❑ Automatiske og elektroniske metoder for datainnsamling (datalogger, oversikt over oppetid på systemer)

2.5. Presentasjon av resultat

Presentasjonen av indikatorene er viktig for å få frem de resultater som indikatorene viser. Flere ting er viktige med presentasjonen:

1. At resultatene faktisk sier noe om informasjonssikkerheten i helsevirksomheten slik at ledelsen vet hva dette betyr og kan gjøre de nødvendige tiltak
2. At resultatene viser en utvikling
3. At resultatene blir presentert slik at de kan sammenlignes mellom helsevirksomheter

Informasjonssikkerhetstall (IS-tall)

En mulighet er at resultatene samlet sett gir en tallverdi som sier noe om informasjonssikkerheten.

Figur 1 viser presentasjon av et slikt tall som ligger mellom null og en. Null vil da si at informasjonssikkerheten er svært dårlig, men en vil si at informasjonssikkerheten er svært god.

Eksempelvis kan det tenkes at et helseforetak kan komme ut med en total IS-indikator på 0,82 - noe som kan være meget bra, mens et annet helseforetak kommer ut med en total IS-indikator på 0,63 - noe som ikke er fullt så bra.

For å fastsette et slikt IS-tall mellom 0 og 1 kan for eksempel spørsmål som besvares med ja/nei brukes for å utvikle et slikt tall.

Et alternativ er å lage ulike tall som tilsvarer H-tall ved HMS undersøkelser. H-tallet vil si antall skader med fravær per million arbeidstimer, og forteller oss noe om sikkerhetsnivået på en arbeidsplass. For informasjonssikkerheten vil dette for eksempel kunne være antall feilsendinger av sensitiv informasjon per 100 ansatte.

”Karakterskala”

En annen mulighet er å gi en helsevirksomhet ulike karakterer på ulike områder slik som Figur 2 viser. En er også her avhengig av at indikatorene gir klare verdier som enkelt kan måles.

Mulige problemer med slik ”karaktersetting” er hvordan en skal vekte for eksempel ulike mangler eller feil som en finner. Skal eventuelt alle indikatorer telle like mye når resultatet bestemmes.

Statistikker

En del resultater er aktuelle å presentere som statistikker. Dette er indikatorer som ikke gir noe klar svar (for eksempel ja eller nei), men som heller sier noe frekvensen av en del faktorer. Dette kan eksempelvis være:

- ❑ Antall ulykker/feilbehandlinger per 1000 pasienter som skyldes feil i informasjonssystemer
- ❑ Antall feilsendinger per 100 ansatt av sensitiv informasjon
- ❑ Antall virusangrep/hackerangrep med negative konsekvenser for virksomheten
- ❑ Kostnader som følge av hendelser/ulykker som har skjedd
- ❑ % av IT som benyttes til informasjonssikkerhet
- ❑ Antall rapporteringer om brudd på informasjonssikkerheten per 100 ansatt

2.6. Frekvens for måling av indikatorer

Hvor ofte indikatorer blir målt avhenger av hvilke indikatorer som blir brukt, hvordan de blir samlet inn og hvor ofte ledelsen i helsevirksomheten ønsker at målinger skal skje.

Valg av indikatorer

Hvor lette indikatorene er å måle vil i praksis påvirke hvor ofte de blir målt. Dersom indikatorene er vanskelig å måle og krever mye ressurser vil dette sannsynligvis kunne føre til målinger ikke blir gjort så ofte som kanskje ønskelig.

Innsamlingsmetode

Dersom metodene som brukes for innsamling av data tar lang tid og kanskje også innebærer manuelle prosedyrer vil dette kunne føre til at innsamlingen tar så mye tid og ressurser at hyppigheten blir mindre enn ønskelig. Data som kan hentes inn elektronisk og også automatisk vil gjøre at datainnsamlinger vil gå raskere og enklere.

Når innsamlingsmetode velges, må det være valget av indikatorene som avgjør dette. Det primære er å bruke de indikatorene som egner seg til å gi svar på de spørsmål som ledelsen i helsevirksomheten har. Dette bør i utgangspunktet være viktigere enn hvordan dataene blir samlet inn.

Ledelsens ønsker

Ønsker fra ledelsen til helsevirksomheten om hvor ofte informasjonssikkerheten skal måles vil påvirke frekvensen for hvor ofte målinger blir gjort. Dersom ledelsen finner at

informasjonssikkerheten ikke er tilfredsstillende ønsker de kanskje å øke frekvensen av målinger. Dersom ledelsen er fornøyd med resultatene og de siste målinger ikke viser noen tegn til svakhet vil kanskje ledelsen ikke føle like stort behov for målinger.

Det vil imidlertid også være et viktig poeng å fortsette med samme frekvens på målingene også når ledelsen ser at resultatene er bra. En grunn til dette er for å forsikre seg om at nivået på informasjonssikkerheten holder seg like bra. Arbeid med informasjonssikkerhet er en prosess som må skje hele tiden fordi nye trusler dukker opp og helsevirksomheten selv endrer seg over tid. En annen grunn er at en så raskt så mulig ønsker å oppdage når informasjonssikkerheten endrer seg i negativ retning slik at en kan sette inn de aktuelle tiltak.

Dersom en har gjort tiltak for å bedre informasjonssikkerheten ønsker en å se om tiltakene får den effekten som en ønsker. Da kan det være at en øker frekvensen på målingene for å følge med i utviklingen etter at tiltak er gjort for å bedre informasjonssikkerheten.

Anbefalt frekvens

Hver enkelt helsevirksomhet må selv velge den frekvensen for målinger av informasjonssikkerheten som de selv mener er hensiktsmessig. Målinger av informasjonssikkerheten bør stort sett foretas kvartalsvis eller månedlig. I en startfase kan målinger foretas oftere enn en gang i måneden, kanskje så ofte som ukentlig dersom dette er hensiktsmessig. Som nevnt ovenfor vil valg av indikatorene og hvilke innsamlingsmetoder som blir brukt være med på å avgjøre hvor ofte det vil være hensiktsmessig å kunne gjøre målinger.

3. System for indikatorer

Det er flere elementer som er viktige når en helsevirksomhet skal planlegge og iverksette et system som innebærer indikatorer for måling av informasjonssikkerheten. I dette kapitlet vil vi forsøke å gi en beskrivelse av viktige faktorer ved innføring av indikatorer.

Fire grunnpillarer er viktige [1] dersom en virksomhet skal kunne innføre et system for måling av informasjonssikkerheten.

1. **Forankring hos ledelsen** - dette er viktig dersom en skal greie å innføre et system for måling av informasjonssikkerheten på en god måte. God forankring hos ledelsen viser at virksomheten tar sikkerheten på alvor og at dette er en viktig sak for virksomheten. Å få avsatt ressurser til å innføre systemet er også avhengig av at ledelsen støtter prosjektet.
2. **Sikkerhetspolicyer og prosedyrer** - en forutsetning for å kunne gjøre målinger av informasjonssikkerheten er at det finnes prosedyrer og policyer som sikrer at en kan iverksette ulike tiltak i forhold til hvordan en håndterer informasjonssikkerheten i virksomheten. Uten policyer og/eller prosedyrer kan det være vanskelig å finne gode indikatorer som kan benyttes til å måle informasjonssikkerheten.
3. **Kvantifiserbare målinger** - å finne frem til kvantifiserbare målinger som gjør at en får gode data om informasjonssikkerheten er en kritisk faktor for indikatorsystemet . Uten godt datagrunnlag er det svært vanskelig å innføre et system for måling av informasjonssikkerheten.
4. **Resultatorienterte analyser av målingene** - denne delen gjør bruk av dataene som blir samlet og frembringer resultatene som sier noe om hvordan informasjonssikkerheten er i en virksomhet.

I praksis vil det være vanskelig å innføre et system for målinger av informasjonssikkerheten dersom virksomheten ikke har satt dette i system (rutiner, prosedyrer) fra før. Dersom en virksomhet for eksempel mangler sikkerhetspolicyer, ikke har utført risikovurderinger, ikke har antivirusprogramvare installert, mangler katastrofeplaner eller mangler faste rutiner for sikkerhetskopiering, så vil det være vanskelig å kunne innføre et system med indikatorer uten at noe mer blir gjort. Det at virksomheten mangler rutiner/prosedyrer for det som er nevnt ovenfor, vil

i seg selv være et tydelig tegn på informasjonssikkerheten ikke er slik den bør være. I slike tilfeller vil indikatorer i så måte være unødvendig for å kunne si noe om informasjonssikkerheten.

For å få best mulig effekt ut av et system med indikatorer må virksomheter derfor ha et visst grunnlag for hvordan de håndterer informasjonssikkerheten. En virksomhet bør ha gjort visse grep for hvordan den håndterer informasjonssikkerheten, for eksempel bør dette innebære rutiner, prosedyrer eller dokumentasjon.

På den annen side kan innføring av et system med indikatorer for måling av informasjonssikkerheten gjøre at en virksomhet får på plass en ting som har manglet fra før. Dette vil i midleritid kanskje kreve at virksomheten (med ledelsen i spissen) tar et lite ”skippertak” og går grundig gjennom hvordan virksomheten håndterer informasjonssikkerheten.

3.1. Suksessfaktorer

Det er en rekke faktorer som påvirker hvordan et målesystem for informasjonssikkerhet vil fungere. I kapittel 2.1.1 er det listet opp krav til hvordan selve indikatorene bør være dersom de skal fungere som ”måleenheter”. I tillegg er det også andre faktorer som er viktige.

Organisasjonsmessige forhold

De som på en eller annen måte har et eierskap (interesse, ansvar, myndighet) til informasjonssikkerheten bør involveres i en prosess med å innføre et indikatorsystem i en organisasjon. Som nevnt tidligere er spesielt viktig at ledelsen er med i denne prosessen. Dersom det allerede finnes andre enheter i en organisasjon som er ansvarlige for lignende målinger eller prosesser (dette kan for eksempel være HMS, service) så bør disse trekkes med prosessen med å planlegge og innføre systemet for måling av informasjonssikkerheten.

Håndterbart system

Det er viktig at systemet som planlegges innført ikke blir for stort og uhåndterlig. Det er vanskelig å gi noen eksakte anbefalinger, men i en innføringsperiode bør ikke antall indikatorer overstige 15-20. Dette tallet kan godt være mindre, men en må ha mange nok indikatorer til at systemet som helhet gir meningsfulle pekepinner på hvordan informasjonssikkerheten er. Som et eksempel på et indikatorsystem er det i vedlegg A skissert et forslag med totalt 11 ulike indikatorer.

Etter at virksomheten har brukt målesystemet en stund kan en godt legge til flere indikatorer dersom en finner dette hensiktsmessig. Uansett er det trolig bedre å ha få og gode indikatorer, enn å ha mange indikatorer som er dårlige og som gir dårlige svar. Ved valg av indikatorene kan

kriteriene som er beskrevet i begynnelsen av kapittel 2 være lurt å benytte seg av.

Datahåndtering

For å sikre kvaliteten og validiteten til dataene, er det viktig at standardiserte metoder brukt i forbindelse med innhenting og bearbeiding av måledataene. Dette sikrer at data brukt i forskjellige målinger er basert på det samme ”grunnlaget”, slik at resultater er sammenlignbare mellom forskjellige målinger.

For en organisasjon som tar i bruk indikatorer for å måle informasjonssikkerheten må en også huske på at det ikke er sikkert at alle indikatorer til enhver tid vil gi meningsfulle resultater. En organisasjon bør derfor ikke stole fullt ut på indikatorene uansett hvilke resultater de gir, eller at indikatorene gir alle svar eller tegn på det som er viktig i forhold til informasjonssikkerheten i en organisasjon.

Indikatorene som er tatt i bruk på en god måte bør i midlertidig kunne peke på hvordan informasjonssikkerheten utvikler seg i en organisasjon.

3.2. Stegene i innføringen

Her beskrives det kort hvordan en innføring av indikatorer for informasjonssikkerhet kan foregå.

Identifisere interessenter

Første fase i en innføring vil være å samle de personer som har et forhold til informasjonssikkerheten i en organisasjonen. Egentlig er alle i en organisasjon å regne som interessenter i forhold til informasjonssikkerheten fordi alle ansatte på en eller annet måte et ansvar for å ivareta informasjonssikkerheten i organisasjonen.

Likevel vil det være personer (eller roller) i en organisasjon som er viktigere i forhold til ansvar og myndighet for informasjonssikkerheten. Dette vil typisk kunne være IT-drifts ansvarlig, ledelsen i organisasjonen (for et helseforetak er det direktøren som er den øverste ansvarlige for informasjonssikkerheten) eller ansatte med et spesielt ansvar for informasjonssikkerhet.

Definere mål og formål

Fase to er å finne frem til og beskrive formålet og målet med systemet for måling av informasjonssikkerhet. Formålet er hva et slikt system skal oppnå på lengre sikt for virksomheten, dette kan for eksempel være at vi skal bli kjent som en virksomhet med god håndtering av informasjonssikkerheten.

Målet med indikatorene vil være det konkrete de skal oppnå, dette kan eksempelvis være at antall feilsendinger av sensitiv informasjon ikke skal være mer enn to tilfeller per 100 ansatte innenfor et tidsrom på et år.

Policyer, veiledninger og prosedyrer

Fase tre blir å beskrive hvordan sikkerhetskontroller bør blir implementert. Dette kan skje gjennom policyer, veiledninger eller prosedyrebeskrivelser som er utarbeidet og tilpasset for den enkelte organisasjon.

Vurdering av systemet for sikkerhetsprogram

I fase fire bør en vurdere systemet som en planlegger å innføre for indikatorene. Her bør alle indikatorer som er aktuelle vurderes for å finne de beste indikatorene. Her bør mest mulig relevant informasjon fremskaffes rundt hver indikator.

Implementering og bruk av indikatorene

I denne fasen bør en velge ut indikatorene som skal implementeres og eventuelt beskrive disse nærmere dersom det er behov for det. Selve bruken av indikatorene kan beskrives gjennom følgende seks trinn:

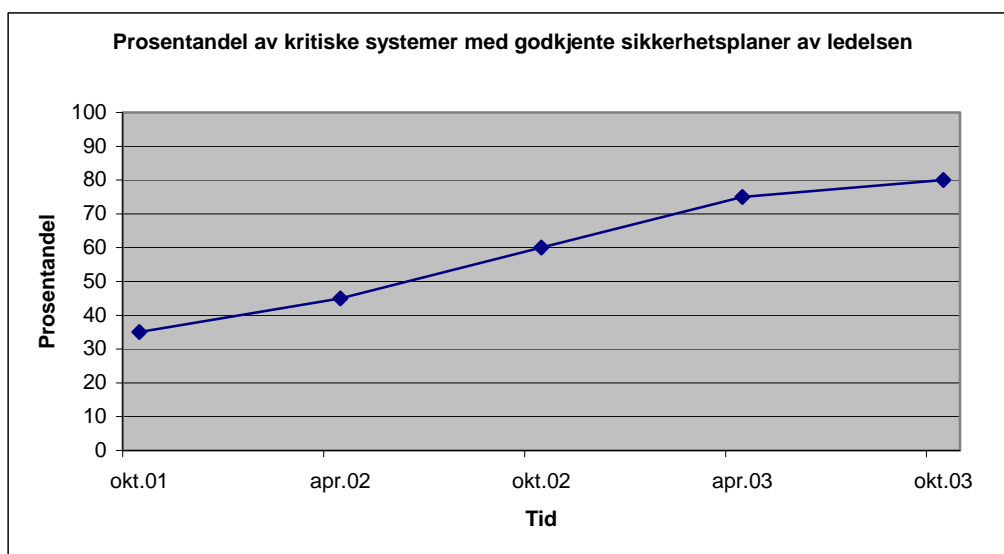
1. Forbered for datainnsamling
2. Innsamling av data
3. Identifiser rettende tiltak
4. Planlegg rettende tiltak
5. Utfør rettende tiltak

Analysere resultater

Siste fasen er å vurdere hvordan systemet fungerer og om en er fornøyd med de resultatene som systemet gir. Dersom en ikke er fornøyd med resultatene som målesystemet oppnår må en vurdere om det er nødvendig å gå tilbake og eventuelt endre på policyer/retningslinjer eller om andre indikatorer bør brukes. Når det snakkes om resultater av indikatorene menes det ikke om de viser om informasjonssikkerheten er bra eller ikke.

3.2.1. Definerings av målkriterier

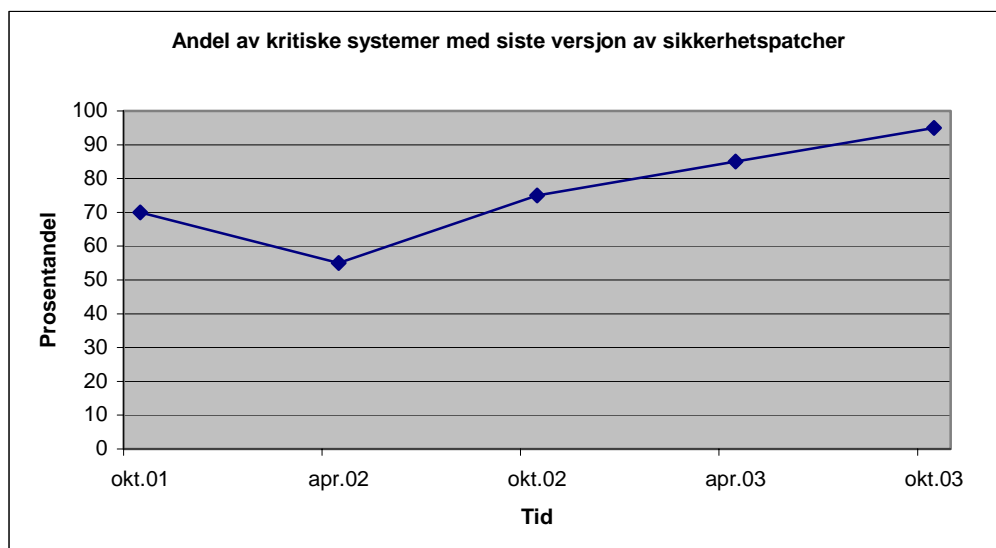
En viktig faktor for et system til måling av informasjonssikkerhet er å definere hvordan indikatorene skal måles. En del indikatorer vil sannsynligvis måle hvilke "sikkerhetsmekanismer" som er tilstede i en virksomhet, og det naturlige vil være å måle prosentvis hvor mange mekanismer som er implementert. Dette vil kunne gi en god pekepinn på hvilke sikkerhetsmekanismer som er implementert i en virksomhet og målet vil som regel være 100 %. Figuren under viser et eksempel på en indikator som måler implementeringsgraden av en sikkerhetsmekanisme.



Figur 3: Eksempel på indikator som viser "implementeringsgrad"

Det at en sikkerhetsmekanisme er implementert vil i ikke si det samme som at informasjonssikkerheten er god. Selv om det gjøres backup er det ikke sikkert at rutine for dette er godt nok (for eksempel ved at ingen har hovedansvaret eller at det ikke gjøres regelmessig). En bør i tillegg til implementeringsgraden av sikkerhetsmekanismer også se på hvordan de ulike mekanismene fungerer. Dette kan være vanskeligere siden en her må finne kvalitative målkriterier som kan si hvordan informasjonssikkerheten er.

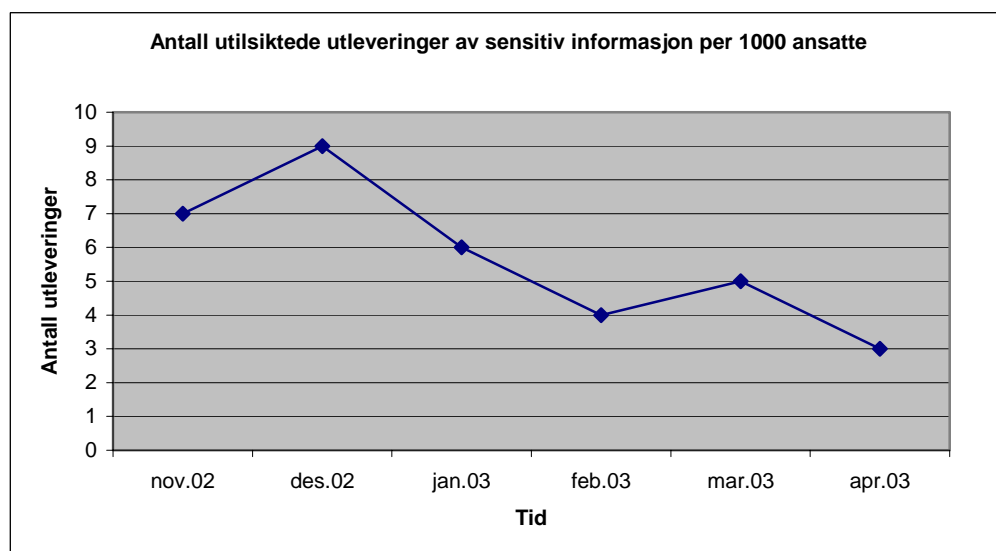
Figuren under viser et eksempel på en kvantitativ indikator som sier noe om hvor gode rutiner det finnes for å oppdatere systemer med oppdatert sikkerhetsprogramvare.



Figur 4: Eksempel på indikator som viser en "kvalitativ" utvikling

I tillegg kan det være en interessant faktor å se på hvilke negative hendelser som skjer i forhold til informasjonssikkerheten. Dette er hendelser som kanskje det kan være vanskelig å koble sammen med manglende sikkerhetsrutiner, men som likevel kan gi et godt inntrykk av hvordan organisasjonen som helhet håndterer informasjonssikkerheten.

Figuren under viser antall hendelser med utilsiktet utlevering av sensitiv informasjon.



Figur 5: Eksempel på indikator som viser en "statistisk" utvikling

4. Aktuelle måleindikatorer

Som beskrevet tidligere er det forskjellige typer informasjon som kan være grunnlaget for indikatorer. Her gis det en oversikt over mulige faktorer som kan fungere som indikatorer for informasjonssikkerhet. Å benytte alle indikatorene beskrevet vil føre til svært mange faktorer i et indikatorsystem. Hver virksomhet må derfor selv velge ut de indikatorene de finner mest hensiktsmessige å benytte i forhold til egen organisasjon.

Å benytte alle indikatorene beskrevet i dette kapitlet vil føre til et stort og kanskje uhensiktsmessig system for indikatorer. Hver virksomhet bør derfor selv velge ut de indikatorene (kan eksempelvis starte med de 10-15 mest aktuelle) som de mener er mest hensiktsmessige. En virksomhet kan godt starte innenfor et område (for eksempel indikatorer som omhandler tekniske faktorer) som de velger å prioritere i en oppstartsfasen.

Faktorene er delt opp i følgende hovedgrupper:

- Menneskelige faktorer
- Tekniske faktorer
- Organisasjons- og holdningsfaktorer
- Prosesser og prosedyrer
- Statistiske faktorer

En del av indikatorene kan godt passe inn under flere av hovedgruppene og det kan være gråsoner mellom oppdelingen av gruppene. Med å plassere indikatorene i ulike grupper vises det at det flere forskjellige forhold som spiller inn på informasjonssikkerheten. Informasjonssikkerhet er sådan et komplekst felt hvor mange faktorer med ulike egenskaper til sammen utgjør den samlede ”summen” av informasjonssikkerhet.

4.1. Menneskelige faktorer

Menneskelige faktorer kan bli vanskelige å måle på en effektiv og lite ressurskrevende måte. Mulige alternativer å spørre en person om hva den mener om hvordan tilstanden er; et annet

alternativ er å spørre mange personer. Faren er at enten blir det den subjektive vurderingen foretatt av bare en enkelt person, eller så blir det fort ressurskrevende å samle inn dataene.

4.1.1. ”kvantifiserbare” menneskelige faktorer

Nedenfor har vi listet opp en del spørsmål [3] som kan være aktuelle å bruke for måling av informasjonssikkerheten.

- Kjenner du til ”Lov om behandling av personopplyninger” som trådte i kraft 1 januar 2001?
- Loven pålegger helseforetaket å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Er du kjent med de tiltak som skal sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger ved helseforetaket?
- Er du kjent med lovens definisjon av ”sensitive personopplysninger”?
- Vet du hvem som er hovedansvarlig for informasjonssikkerheten ved Helseforetaket?
- Er du kjent med ditt ansvar for informasjonssikkerhet?
- Er du kjent med gjeldende prosedyrer for informasjonssikkerhet ved helseforetaket?
- Vet du hvor disse finnes (er tilgjengelig)?
- Er du kjent med taushetspliktens omfang og konsekvenser ved brudd på denne?
- Bytter du passord annenhver måned?
- Låner du bort ditt passord til en kollega?
- Har du skrevet ned ditt/dine passord på en ”huskelapp” ?
- Er du kjent med ditt ansvar for bruk og oppbevaring av nøkkel/adgangskort?
- Hvis du mister nøkkelen/adgangskortet; vet du hvor du skal melde fra?
- Melder du fra?
- Eller låner du nøkkelen /adgangskortet til en kollega?
- Når du skal fratrukke stillingen vet du hvor/til hvem du skal levere nøkkelen/adgangskortet?
- Låser du ned dokumenter inneholdende pasientopplysninger før du forlater arbeidsplassen?
- Kjenner du til om eksternt servicepersonell skriver under taushetserklæring?
- Hvis en elektriker skal utføre en jobb i journalarkiv, slipper du han inn ?
- Låner du bort nøkkelen/adgangskortet til eksternt servicepersonell?

Spørsmålene ovenfor kan alle besvares med ja eller nei, og kan således inngå i en ”kvantitativ” måling ved at en for eksempel setter opp andelen av ja/nei svar som er gitt.

4.1.2. "Kvalitative" menneskelige faktorer

En annen tilnærming enn kvantitative menneskelige faktorer er å utvikle indikatorer som i større grad enn bare fange opp ja/nei sier noe mer om hvordan mennesker til daglig håndterer informasjonssikkerheten. En kan godt si at de kvantitative faktorene listet opp i kapittel 4.1.1 forteller noe om *kunnskapsnivået* mennesker besitter om temaet informasjonssikkerhet, mens kvalitative faktorer forteller noe om hvordan mennesker i *praksis* bruker denne kunnskapen.

Nedenfor er det listet opp noen forslag til kvalitative faktorer som kan benyttes [7]:

- Tenker du sikkerhet ved bruk av Internett?
- Hvor nøye er du med ved håndtering av vedlegg i e-post?
- Hvordan nøye er du med håndtering av sensitiv informasjon?
- Hvordan vil du beskrive at du følger virksomhetens sikkerhetsregler?
- Er temaet informasjonssikkerhet noe som blir diskutert mellom de ansatte, og mellom de ansatte og ledelsen?
- Hva er hensikten med de prosedyrer og regler for informasjonssikkerhet som finnes i virksomheten?

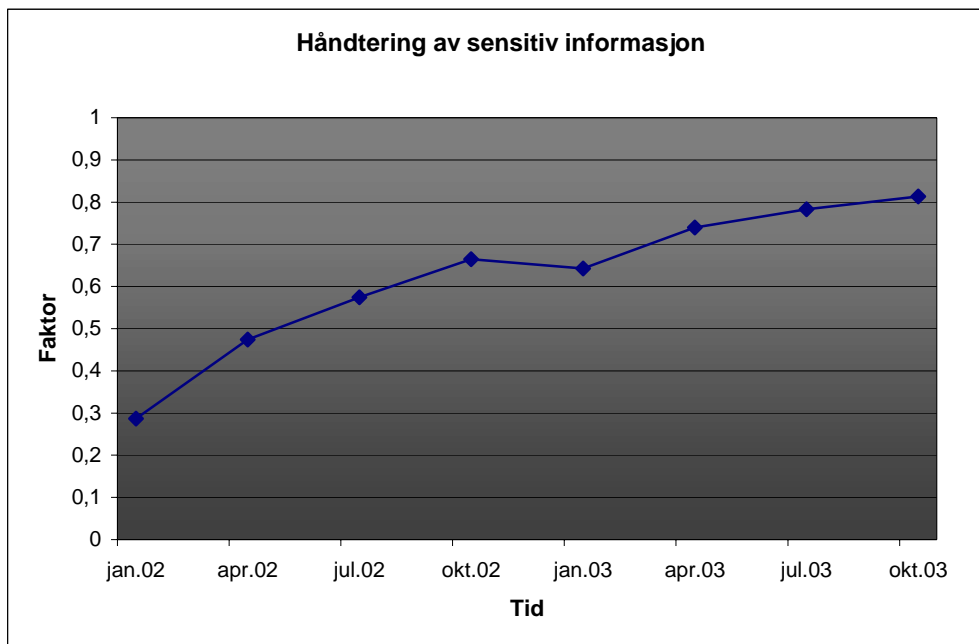
I tabellen under er det vist hvordan menneskelige faktorer kan brukes i et system indikatorer. Fargeskalaen benyttet i øverste rad henviser til hvor kritisk det tilhørende svaralternativet er. Her er fargene rød, gul og grønt benyttet med henblikk på graden av alvorlighet. Dersom svaralternativ merket med rød farge er det som best beskriver virksomheten bør det gjøres strakstiltak på dette området. Dersom gult svaralternativ passer best bør virksomheten være ekstra på vakt og følge med dette området, men grønt svaralternativ betyr at virksomheten fungerer bra på dette området.

Spørsmål	I	II	III	IV	V
1. Hvordan er rapportering og håndteringen av uønskede hendelser?	Det finnes ikke noe formelt system for rapportering av hendelser. Kun større hendelser som medfører skader blir "brannslukket" der og da.	Ledelsen påpeker at hendelser skal rapporteres, men det er ingen som følger det opp i praksis. Det er tilfeldig hvilke hendelser som blir meldt, og det finnes ingen faste rutiner for oppfølging.	De ansatte rapporterer stort sett hendelser som skjer, og de blir stort sett fulgt opp. Det er imidlertid ikke noe formelt system rundt slik at en kan lære av de hendelsene som skjer.	De ansatte er flinke til å rapportere om hendelser som skjer. IT-avdelingen setter i verk både strakstiltak og forebyggende tiltak.	Det er en god rapporteringskultur hos de ansatte. Alle hendelser blir fulgt opp av IT-avdelingen og det blir gitt tilbakemeldinger for å bevisstgjøre de ansatte.

Spørsmål	I	II	III	IV	V
2. Hvordan håndterer de ansatte sensitiv informasjon?	De ansatte tenker sjelden på at de håndterer sensitiv informasjon.	Ingen faste rutiner for håndtering av sensitiv informasjon. Det går "stort sett" bra!	Vi har brukerpolicy for behandling av sensitiv informasjon som alle er informert om. Ingen konkret kontroll om de ansatte følger policyen, men dette tas opp med jevne mellomrom. Vi har ikke opplevd noen negative hendelser.	De ansatte er i stor grad bevisste. Låser alltid PC-en når de går bort og lar ikke utskrifter ligge og slenge.	De ansatte er svært bevisste og tar alle forholdsregler. Alle er bevisste med sensitiv informasjon både i papirform og elektronisk. Både ledelsen og de ansatte er flinke til å "bevisstgjøre" andre om dette.
3. Hvordan blir informasjonssikkerhet inkludert i planlegging og gjennomføringen av prosjekter?	Dette er så å si aldri noe tema. Tar det etter hvert som behov oppstår.	Tas som regel inn på slutten og er ikke det som har mest fokus.	Blir alltid vurdert, men kanskje ikke med størst prioritet. Har ikke alltid fokus på egne behov, men mest på å oppfylle lov- og regelverk.	Det blir alltid vurdert i startfasen og alle vet at det er en viktig faktor.	Informasjonssikkerhet blir alltid behandlet gjennom hele perioden. Alle har forståelse for at dette er svært viktig og kritisk faktor.
4. Hvilke vaner har de ansatte ved bruk av e-post?	Tar imot og videresender e-post med vedlegg ukritisk uten å tenke på sikkerheten. Tenker aldri på at en e-post kan havne på avveie.	Tenker sjelden på innholdet i en e-post. Sender ofte sensitiv informasjon på e-post.	Benytter sikkerhetsfunksjoner i e-post systemet. Er kritisk når en sender sensitiv informasjon.	Er forsiktige med e-post som har vedlegg eller e-post fra ukjente. Sender sensitiv informasjon med kryptering.	De ansatte tar alle forholdsregler ved e-post. Sender alltid sensitiv informasjon kryptert og sjekker alle vedlegg for virus.

Tabell 1: Bruk av menneskelige faktorer i et indikatorsystem.

I tillegg til bruk av fargekoder kan også gis poeng for de ulike svaralternativene dersom en ønsker å fremstille det for eksempel ved hjelp av en graf som viser en utvikling over en tid. Eksempelvis kan de fem svaralternativene gis henholdsvis 0, 0.25, 0.5, 0.75 og 1 poeng.



Tabell 2: Graf som viser utvikling over tid

Tabellen over viser hvordan utviklingen av menneskelige indikatorer kan fremstilles grafisk dersom en velger å benytte poeng for å beskrive tilstanden. Her vises det de ansattes holdning til håndtering av sensitiv informasjon (spørsmål 2 i Tabell 1 ovenfor). I grafen er det også brukt farger som går fra rød til grønn for å vise hvor kritisk tilstanden er.

De menneskelige faktorene kan med sammenligning med andre indikatorer for å gi fylligere og utfyllende informasjon. Dersom alle ansatte sier de håndterer vedlegg i e-post svært forsiktig og det samtidig er tekniske indikatorer som viser at det har komnt flere virus fra vedlegg i e-post, kan dette for eksempel være tegn på at ansatte ikke har fått god nok opplæring i bruk av e-post.

Ulike kategorier

Det er ikke gjort noen oppdeling av de ulike menneskelige faktorene som er tatt med i eksemplene ovenfor. Ved større undersøkelser rundt temaet "mennesker, kultur og informasjonssikkerhet" er det kanskje hensiktsmessig å dele inn aktuelle spørsmål i ulike kategorier. Kufås og Mølman (2003) har i sitt verktøy brukt følgende inndeling:

- Atferd
- Kunnskap og holdninger
- Policy og ledelse
- Inkludering og læring
- Ansvarsfordeling

- Prosedyrer og formalisering
- Analyser, vurderinger og revisjon
- Bevissthet og menneskelige relasjoner

4.2. Tekniske faktorer

Tekniske faktorer er forhold som går på hvilke tekniske faktorer som finnes i helsevirksomheten for å ivareta informasjonssikkerheten

4.2.1. Anti-virus programvare

Kritisk faktor	Er anti-virus programvare installert og aktivert slik at virusskanning foregår automatisk?
Delspørsmål	
Måleenhet	Prosentdelen med systemer som har automatisk virusdeteksjon
Formål	Å måle risikoen knyttet til kjente virus
Formel	Antall systemer med automatisk virusskanning / Antall systemer totalt
Frekvens	Kvartalsvis eller halvårlig
Beskrivelse av indikator	<p>Automatisk virusskanning gjør at virussjekk blir utført regelmessig og at oppdateringer av antivirusprogramvaren skjer automatisk. Dersom en stor andel av systemene ikke har automatisk virussjekk er risikoen større for at virus kan infiltrere systemet og gjøre til skader. PC-er, servere og e-post system bør som minstekrav inngå i indikatoren.</p> <p>Målet for denne indikatoren er at 100 % av systemene har automatisk virusdeteksjon.</p>

4.2.2. Sårbarheter

Kritisk faktor	Blir systemer jevnlig testet med tanke på kjente sårbarheter, og blir oppdateringsprogramvare (sikkerhetspatcher) installert
Delspørsmål	Blir det benyttet automatiske verktøy for sårbarhetsskanning?

Måleenhet	Prosentdelen med systemer som har siste versjon av oppdateringsprogramvare installert
Formål	Å måle risikoen som er knyttet til sårbarheter som allerede er kjente.
Formel	Antall systemer med oppdaterte programvare / Antall systemer totalt
Frekvens	Månedlig
Beskrivelse av indikator	<p>Sikkerhetspatcher blir gitt ut for ulike programvaresystemer for å rette opp sikkerhetsmessige feil eller mangler i systemet som er funnet. Mange datainnbrudd utnytter nettopp svakheter som allerede er kjente og hvor systemene ikke er oppdatert med siste versjon av sikkerhetspatcher. Mange datainnbrudd kunne ha blitt unngått ved å hatt oppdaterte sikkerhetspatcher.</p> <p>Målet for denne indikatoren er at 100 % av alle systemer har installert siste versjon av sikkerhetspatcher.</p>

4.2.3. Felles brukeridenter og passord

Kritisk faktor	Finnes det systemer som har felles brukeridenter og passord ved helsevirksomheten?
Delspørsmål	
Måleenhet	Antallet felles brukeridenter og passord som finnes
Formål	
Formel	<p>Antallet felles brukeridenter og passord som finnes / Antall systemer totalt.</p> <p><i>Alternativt: antall unike brukeridenter som finnes / antall brukeridenter totalt</i></p>
Frekvens	

Beskrivelse av indikator	<p>Felles brukeridenter og passord gjør at mange brukere kan logge seg inn i systemer uten at en har kontroll med hvilken bruker det er som gjorde innloggingen. Bruk av felles brukeridenter og passord gjør at det er vanskelig å oppdage dersom uautoriserte tilganger til et system benytter seg av felles brukeridenter og passord.</p> <p>Målet er at 0 % av systemene har felles brukeridenter og passord som kan benyttes av vanlige brukere.</p>
---------------------------------	---

4.2.4. Brannmurer

Kritisk faktor	Finnes brannmur (dersom en har tilgang til Internett) og blir denne jevnlig kontrollert og ev. konfigurert for å være optimal
Delspørsmål	Finnes det kvalifisert personale som jevnlig (daglig/ukentlig) kontroller brannmur?
Måleenhet	Ja/nei
Formål	Å finne ut hvor godt brannmuren blir vedlikeholdt og om det finnes nok kunnskaper om teknologien.
Formel	
Frekvens	Kvartalsvis
Beskrivelse av indikator	Brannmuren er kritisk med tanke på å ha kontroll over datakommunikasjonen som går in/ut av virksomhetens nettverk. En god fungerende brannmur krever at den vedlikeholdes og konfigureres slik at den fungerer optimalt.

4.2.5. Testmiljø

Kritisk faktor	Finnes det et testmiljø hvor kritiske oppgraderinger eller endringer blir testet og godkjent før implementering
Delspørsmål	
Måleenhet	Andelen kritiske oppgraderinger eller endringer som blir kjørt i et testmiljø

Formål	Å finne ut risikoen knyttet til kritiske endringer eller oppgraderinger som blir gjort.
Formel	Antall kritiske oppgraderinger eller endringer som blir godkjent i et testmiljø / antall kritiske oppgraderinger eller endringer totalt som gjøres
Frekvens	Årlig eller halvårlig (eventuelt kvartalsvis for store virksomheter)
Beskrivelse av indikator	Ved å prøve ut kritiske endringer eller oppgraderinger i et testmiljø vil en finne ut eventuelle uventede konsekvenser ved den aktuelle oppgraderingen/endringen, dette kan være andre systemer som påvirket. En vil også kunne finne eventuelle feil i de oppgraderingene/endringene som blir gjort. Målet for denne indikatoren er at 100 % av alle kritiske endringer eller oppdateringer blir prøvd ut i et testmiljø før de blir implementert.

4.3. Organisasjons- og holdningsfaktorer (strukturelle og kulturelle forhold)

Organisasjonsfaktorer er forhold som går på hvordan organisasjonen som helhet håndterer informasjonssikkerheten

4.3.1. Risikovurderinger

Kritisk faktor	Blir risikovurderinger av informasjonssikkerheten utført jevnlig og dokumentert, og blir dette utført når systemer, organisasjon eller andre forhold endrer seg
Delspørsmål	
Måleenhet	Frekvensen for hvor ofte risikovurderinger blir utført.
Formål	Å finne ut hvor ofte risikovurderinger blir utført.
Formel	Antall kritiske systemer det er utføres risikovurderinger for / Antall kritiske systemer totalt sett
Frekvens	Årlig eller halvårlig

Beskrivelse av indikator	Risikovurderinger skal identifisere de ulike truslene mot informasjonssikkerheten i en virksomhet. Truslene endre seg over tid og nye trusler dukker opp for eksempel som en følge av virksomheten er i endring.
---------------------------------	--

Oppfølging av risikovurderinger

Kritisk faktor	Sørger de ansvarlige for informasjonssikkerhet ved virksomheten at det blir gjort nødvendige tiltak med de truslene som ble vurdert til å ha en høy risiko ved siste risikovurdering.
Delspørsmål	
Måleenhet	Antall trusler med høy risiko
Formål	Å finne ut om virksomheten har gjort noe med de truslene som har en høy risiko.
Formel	Antall trusler med høy risiko som det ikke det er gjort noe med siden siste risikovurdering er utført
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Trusler som er vurdert til å ha høy risiko er tegn på at informasjonssikkerheten ikke er som den bør være. For trusler med høy risiko må det sette inn tiltak slik at risikoen blir akseptabel. Målet med indikatoren er at alle trusler som hadde høy risiko ved siste risikovurdering er endret slik at risikoen er akseptabel for virksomheten.

4.3.2. Sikkerhetsplaner

Kritisk faktor	Er sikkerhetspolicyer i virksomheten godkjent av ledelsen
Delspørsmål	
Måleenhet	Andel av sikkerhetspolicyer godkjent av ledelsen
Formål	Å finne ut om ledelsen i virksomheten har godkjent de overordnede sikkerhetspolicyene som finnes.

Formel	Antall sikkerhetspolicyer godkjent av ledelsen / antall sikkerhetspolicyer totalt
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Sikkerhetspolicyer i en helsevirksomhet bør være godkjent av ledelsen. Det er viktig at ledelsen godkjenner slike planer for å vise viktigheten av dette for virksomheten. Målet for denne indikatoren er at 100 % av sikkerhetspolicyene i virksomheten er godkjent av ledelsen.

Godkjente sikkerhetsplaner

Kritisk faktor	Har kritiske systemer godkjente sikkerhetsplaner
Delspørsmål	
Måleenhet	Prosentandelen med systemer med sikkerhetsplaner som er godkjent
Formål	Å finne ut om det finnes planer for hvordan en håndterer kritiske systemer for eksempel dersom det skjer feilsituasjoner eller at en må gjøre en omstart av et system.
Formel	Antall kritiske systemer med sikkerhetsplaner som er godkjente / antall sikkerhetsplaner totalt som finnes for kritiske systemer
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	At kritiske systemer har godkjente sikkerhetsplaner er viktig for unngå at feil, stans eller andre hendelser fører til unødig at systemet ikke er fungerende. Målet for denne indikatoren er at 100 % av de kritiske systemene har godkjente sikkerhetsplaner.

Oppdatering av sikkerhetsplaner

Kritisk faktor	Blir sikkerhetsplaner for kritiske systemer endret og holdt oppdaterte
Delspørsmål	

Måleenhet	Gjennomsnittsalderen for sikkerhetsplaner
Formål	Å finne ut hvor oppdaterte og ”passende” sikkerhetsplanene er til hvordan systemene faktisk er.
Formel	Antall kritiske systemer hvor sikkerhetsplaner er oppdaterte siste 6, 12 og 24 måneder / antall sikkerhetsplaner totalt
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Like viktig som å utforme sikkerhetsplaner er det holde dem ved like og oppdatere dem når det er ting som endrer seg. Målet for denne indikatoren er at 100% av sikkerhetsplanene blir vedlikeholdt og endret/oppdatert jevnlig.

4.3.3. Katastrofeplaner

Kritisk faktor	Finnes det katastrofeplaner for kritiske systemer (og operasjoner/prosedyrer)
Delspørsmål	
Måleenhet	Prosentandelen av kritisk systemer som har en katastrofeplan
Formål	Å finne ut om det har blitt lagt planer for katastrofesituasjoner i virksomheten.
Formel	Antallet kritiske systemer med katastrofeplaner / antall totalt kritiske systemer
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Katastrofeplaner kan hjelpe til med å redusere konsekvensene og opprettholde drift ved en eventuell katastrofesituasjon. Målet for denne indikatoren er at 100% av alle kritiske systemer er beskrevet i katastrofeplaner.

Oppdatering av katastrofeplaner

Kritisk faktor	Blir katastrofeplaner testet og oppdatert når det skjer endringer i virksomheten (systemer, avdelinger, personer, ...).
Delspørsmål	

Måleenhet	Prosentandelen av kritisk systemer hvor katastrofeplanen er testet
Formål	Å finne ut om virksomheten tester ut de katastrofeplanene de har.
Formel	Antallet katastrofeplaner som har blitt testet og oppdatert siste år/ antall katastrofeplaner totalt
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Målet med denne indikatoren er at alle katastrofeplaner blir testet/oppdatert med jevne mellomrom.

4.3.4. Sikkerhetsorganisasjon

Kritisk faktor	Finnes det en sikkerhetsorganisasjon i virksomheten ved at det er definert klare roller og ansvarsområder i forhold til informasjonssikkerhet.
Delspørsmål	
Måleenhet	Ja/nei
Formål	
Formel	
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	En sikkerhetsorganisasjon er et tegn på at en virksomhet tar informasjonssikkerhet virkelig på alvor og at den formelt har en egen enhet som skal håndtere dette. Målet med denne indikatoren er at det finnes en fungerende sikkerhetsorganisasjon i virksomheten.

4.3.5. Hovedansvarlig for informasjonssikkerhet

Kritisk faktor	Er det klart hvem som er hovedansvarlig for informasjonssikkerheten i virksomheten
Delspørsmål	
Måleenhet	Ja/nei

Formål	Å finne ut om virksomheten har klart definert hvem som har ansvaret for informasjonssikkerheten.
Formel	
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Målet med denne indikatoren er at det finnes en person i virksomheten som er hovedansvarlig for all informasjonssikkerhet i virksomheten.

4.3.6. Opplæring

Kritisk faktor	Blir det gitt opplæring i for eksempel av og påloggingsprosedyrer, bruk av passord og håndtering av avvikssituasjoner (for eksempel stans i IT-systemer)
Delspørsmål	
Måleenhet	Ja/nei
Formål	Å finne ut om virksomheten gir tilstrekkelig opplæring til ansatte for at de på en forsvarlig måte skal kunne ivareta informasjonssikkerheten i det daglige arbeidet.
Formel	Antall ansatte som har fått tilstrekkelig opplæring innen informasjonssikkerhet / totalt antall ansatte
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Opplæring er en forutsetning for at den "vanlige" ansatte i sitt daglige arbeide skal kunne ivareta informasjonssikkerheten. Opplæring bør først og fremst gis ved ansettelse, men også gjennom at alle ansatte kjenner til policyer, hvem de skal rapportere til og lignende. Målet med denne indikatoren er at 100% av de ansatte har fått tilstrekkelig opplæring/kunnskap for å ivareta informasjonssikkerheten.

4.3.7. Kompetanse

Kritisk faktor	Har personene som jobber med informasjonssikkerhet formelle kvalifikasjoner, opplæring, kurs eller annet som gjør at de har nødvendige kunnskaper til å oppfylle ansvar/arbeidsoppgaver.
Delspørsmål	
Måleenhet	Prosentandelen med personer som jobber med informasjonssikkerhet som har nødvendig kompetanse
Formål	
Formel	Antall personer med nødvendig kompetanse som jobber med informasjonssikkerhet / antall personer totalt som jobber med informasjonssikkerhet
Frekvens	Kvartalsvis eller halvårlig
Beskrivelse av indikator	De som til daglig jobber med og har ansvar for informasjonssikkerhet bør ha en eller annen form for ”formell” kompetanse. Dette er viktig for at de på en god måte skal ivareta de arbeidsoppgaver og det ansvaret de har. Målet er at 100% av de som jobber med og har ansvar for informasjonssikkerheten har nødvendig kompetanse.

4.3.8. Medieoppslag

Kritisk faktor	Negative medieoppslag om dårlig og eller manglende informasjonssikkerhet i virksomheten
Delspørsmål	
Måleenhet	Antall negative medieoppslag
Formål	Å finne ut om det er noen negative medieoppslag om forhold rundt informasjonssikkerhet i virksomheten.
Formel	Antall negative medieoppslag siste år eller halvår.
Frekvens	Årlig eller halvårlig

Beskrivelse av indikator	<p>Medieoppslag er isolert sett ikke så veldig interessant eller en god indikator. Det som kan være interessant er å se på hvordan antallet medieoppslag samsvarer med det som de andre indikatorene gir uttrykk.</p> <p>Målet med denne indikatoren er at det skal være ingen negative medieoppslag og at eventuelle medieoppslag ”stemmer” overens med hvordan det faktisk er.</p>
---------------------------------	--

4.4. Prosesser og prosedyrer

Prosesser og prosedyrer er forhold som går på hvilke prosedyrer/rutiner/prosesser som finnes for å ivareta informasjonssikkerheten (for eksempel sikkerhetsstyring eller avvikshåndtering).

4.4.1. Rapporteringssystem

Kritisk faktor	Finnes det formelle prosedyrer for å rapportere hendelser som angår informasjonssikkerheten
Delspørsmål	
Måleenhet	Andel systemer som benytter formelle prosedyrer
Formål	Å finne ut om det finnes et system hvor en kan rapportere avvik som angår informasjonssikkerheten.
Formel	Antall kritiske systemer hvor en benytter rapportering av avvik / antall kritiske systemer totalt som finnes
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	<p>Er rapporteringssystem er viktig for at de som er ansvarlige for informasjonssikkerheten får vite om de hendelsen som skjer i de ulike systemene.</p> <p>Målet med denne indikatoren er at det benyttes et rapporteringssystem for alle systemer.</p>

4.4.2. Datalogger

Kritisk faktor	Finnes det faste rutiner for sjekk av datalogger og skjer dette jevnlig
Delspørsmål	
Måleenhet	Prosentdelen av datalogger som blir sjekket jevnlig
Formål	Å finne ut om dataloggene jevnlig blir kontrollert.
Formel	Antallet datalogger som jevnlig blir sjekket / Antallet datalogger totalt
Frekvens	Kvartalsvis eller månedlig
Beskrivelse av indikator	<p>At det finnes faste rutiner for kontroll av dataloggene og at dette blir gjort jevnlig er viktig for å kunne oppdage hendelser som har skjedd i nettverket.</p> <p>Målet med denne indikatoren er at 100% av dataloggene har faste rutiner for kontroll og at disse blir fulgt jevnlig.</p>

4.4.3. Sikkerhetsrevisjon og testing

Kritisk faktor	Utføres sikkerhetsrevisjoner jevnlig
Delspørsmål	
Måleenhet	Frekvensen for sikkerhetsrevisjoner
Formål	Å finne ut om sikkerhetsrevisjoner blir utført.
Formel	Antallet kritiske systemer hvor revisjon har blitt utført siste året / antall kritiske systemer totalt
Frekvens	Årlig
Beskrivelse av indikator	<p>Sikkerhetsrevisjoner skal avdekke sikkerhetsbrudd som har oppstått, men også forebygge og forhindre at sikkerhetsbrudd skjer i fremtiden.</p> <p>Målet med denne indikatoren at sikkerhetsrevisjoner utføres jevnlig (for eksempel hvert 2. år)</p>

4.4.4. Sikkerhetskopiering

Kritisk faktor	Tas det backup av viktige systemer (filer og prosedyrer) og blir dette dokumentert
Delspørsmål	
Måleenhet	Prosentdelen av systemer som har faste rutiner for sikkerhetskopiering av kritiske filer og operasjoner
Formål	Å finne ut om det er gode nok backup rutiner for viktig informasjon som finnes i virksomheten.
Formel	Antallet kritiske filer som har faste rutiner for sikkerhetskopiering / Antallet kritiske filer som krever sikkerhetskopiering
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Målet for denne indikatoren er at 100% av viktige systemer, filer og prosedyrer blir tatt tilstrekkelig sikkerhetskopier av.

Offsite lagring

Kritisk faktor	Lagres taper med sikkerhetskopier offsite på sikret sted
Delspørsmål	
Måleenhet	Andelen av backup taper (måned- eller uketaper) for viktige systemer (filer og prosedyrer) som lagres offsite
Formål	
Formel	Antall av backup taper for viktige systemer som lagres offsite / antall viktige systemer totalt
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Målet for denne indikatoren er at 100% av backup tapene (måned- eller uketaper) blir lagret på et sikkert sted utenfor virksomheten. Dette er viktig for eksempel ved en brann dersom en skal få tilgang til dataene.

Testing av backup rutiner

Kritisk faktor	Blir rutiner for sikkerhetskopiering testet
Delspørsmål	Blir det gjennomført "restore" tester for å se om data kan bli gjenskapt
Måleenhet	Andel av viktige systemer hvor "restore" funksjon er testet
Formål	Å finne ut om de rutiner for sikkerhetskopiering som finnes fungerer slik at data kan gjenskapes dersom det er nødvendig.
Formel	Antall viktige systemer hvor restore funksjon er testet / antall viktige systemer totalt
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Å teste rutineene for sikkerhetskopiering er nesten like viktig som å utføre backup jobber. Dersom ikke tapte data kan gjenskapes fra backup tapene er det liten vits i å utføre sikkerhetskopieringen. Målet med denne indikatoren er at 100% av alle rutinen er testet og godkjent at de fungerer på en god måte.

4.4.5. Adgangskontroll

Skrivere i åpne områder

Kritisk faktor	Finnes skrivere i "åpne" områder som det kan skrives ut journalnotater, sykemeldinger, resepter eller annen informasjon som inneholder pasientopplysninger
Delspørsmål	
Måleenhet	Prosentandelen skrivere som kan brukes til pasientinformasjon som står i avgrensede områder
Formål	Å finne ut om pasientinformasjon kan havne på steder hvor det er ingen kontroll med hvem som befinner seg.
Formel	Antall skrivere som brukes til pasientinformasjon som står i avgrensede områder / antallet skrivere totalt som kan brukes til pasientinformasjon
Frekvens	Årlig eller halvårlig

Beskrivelse av indikator	Målet med denne indikatoren er at 100% av skrivere som brukes til pasientopplysninger står i avgrensede områder.
---------------------------------	--

Kontroll av servicepersonell

Kritisk faktor	Er det kontroll med eksternt servicepersonells adgang til områder hvor pasientinformasjon oppbevares/forvaltes (for eksempel ekspedisjonen, områder med Pc-er)?
Delspørsmål	
Måleenhet	Ja/nei
Formål	Å hindre at servicepersonell får adgang til sensitiv informasjon uten noen form for kontroll.
Formel	
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Servicepersonell kan være en trussel mot sikkerheten dersom de ferdes "fritt" i områder hvor sensitiv pasientinformasjon er tilgjengelig. Også uvedkommende som gir seg ut for å være servicepersonell (kalt "social hacking"), eller annet type personell, kan være en risikotrussel i slike sammenhenger.

4.4.6. Dokumentasjon

Kritisk faktor	Finnes det dokumentasjon om hvordan kritisk hardware/software skal bli brukt.
Delspørsmål	
Måleenhet	Prosentandelen med kritisk hardware/software hvor det finnes dokumentasjon
Formål	
Formel	Antall kritisk hardware/software systemer med dokumentert / antall kritisk hardware/software systemer totalt
Frekvens	Årlig eller halvårlig

Beskrivelse av indikator	Målet med denne indikatoren er at 100% av kritisk hardware/software systemer er godt dokumentert. Det kan medføre en stor risiko dersom ikke finnes dokumentasjon av for eksempel en applikasjon eller et system. Oppdateringer eller sikkerhetspatcher blir ofte forsømt når det ikke finnes dokumentasjon.
---------------------------------	--

4.4.7. Fysisk sikkerhet

Kritisk faktor	Har rom eller områder med servere, backup maskiner eller annet kritisk utstyr fysisk adgangskontroll (dør er låst, nøkkelkort eller lignende)
Delspørsmål	
Måleenhet	Prosentandelen med rom eller områder med kritisk utstyr som er avlåst
Formål	
Formel	Antall rom eller områder med kritisk utstyr som er avlåst / antall rom eller områder totalt med kritisk utstyr
Frekvens	Halvårlig eller kvartalsvis
Beskrivelse av indikator	Målet med denne indikatoren er 100%. Dersom kritisk utstyr står åpent tilgjengelig kan dette medføre en stor risiko i at uvedkommende kan få tilgang til for eksempel en server.

4.5. Statistiske faktorer

Statistiske faktorer er informasjon som viser ulike tall på hvordan informasjonssikkerheten er, for eksempel antall virusangrep som forårsaket negative konsekvenser for helsevirksomheten.

4.5.1. Ressurser brukt på informasjonssikkerhet

Kritisk faktor	% av IT budsjett brukt på informasjonssikkerhet
Delspørsmål	

Måleenhet	Prosentdel av IT-budsjett som brukes på informasjonssikkerhet
Formål	
Formel	Andel av IT-budsjett som brukes på informasjonssikkerhet / totalt IT-budsjett
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	<p>Må ses i sammenheng med andre faktorer. Dersom en bruker mye ressurser på IT-sikkerhet, men de andre indikatorene viser dårlige resultat er det et tegn på at det arbeidet som legges ned ikke er av god nok kvalitet. Kan også være vanskelig å definere hva som brukes til informasjonssikkerhet og hva som ikke brukes til det.</p> <p>Denne indikatoren har ikke noe klart mål. En god tendens vil være at en mindre andel brukes på sikkerhet, mens at de andre indikatorene viser at informasjonssikkerheten er bra.</p>

Personell innenfor IS

Kritisk faktor	Andel av personell som jobber med informasjonssikkerhet
Delspørsmål	
Måleenhet	Prosentandel av årsverk som jobber med informasjonssikkerhet
Formål	
Formel	Antall årsverk som jobber med informasjonssikkerhet / antall årsverk totalt
Frekvens	Årlig eller halvårlig
Beskrivelse av indikator	Denne indikatoren sier noe om hvor mye arbeid som legges ned i arbeidet med sikkerhet.

4.5.2. Rapportering

Kritisk faktor	Antall rapporteringer om brudd på informasjonssikkerheten per 100 ansatt
Delspørsmål	
Måleenhet	Antall brudd på informasjonssikkerheten

Formål	
Formel	Antall rapporteringer om brudd på informasjonssikkerheten per 100 ansatte
Frekvens	Kvartalsvis eller månedlig
Beskrivelse av indikator	<p>Denne indikatoren vil generelt si noe om hvor mange sikkerhetsbrudd som foregår i en organisasjon.</p> <p>Målet for indikatoren er at det blir rapportert så få brudd som mulig. En forutsetning er at et velfungerende rapporteringssystem ligger i bunn og blir benyttet når et brudd blir oppdaget.</p> <p>Målet for denne indikatoren er at færrest mulig tilfeller av sikkerhetsbrudd blir meldt (i et velfungerende rapporteringssystem).</p>

4.5.3. Virusangrep

Kritisk faktor	Antall virusangrep stoppet
Delspørsmål	
Måleenhet	Prosentandel av virusangrep som ble stoppet
Formål	
Formel	Antall virusangrep stoppet / antall virusangrep totalt
Frekvens	Månedlig
Beskrivelse av indikator	<p>Denne indikatoren vil si hvor godt virksomhetens antivirusprogramvare fungerer.</p> <p>Målet for denne indikatoren er at 100 % av virusangrepene blir stoppet.</p>

Virus på PC-er

Kritisk faktor	Virus ikke stoppet, dvs. kommet inn på PC, men isolert der
Delspørsmål	
Måleenhet	Prosentandel av virus ikke stoppet

Formål	
Formel	Antall virusangrep ikke stoppet, men isolert på PC / antall virusangrep totalt
Frekvens	Månedlig
Beskrivelse av indikator	Denne indikatoren sier noe om hvor mange virusangrep som kom inn på PC-er, men som ble isolert der ikke fikk noen konsekvenser. Målet for denne indikatoren er at 100 % av virusangrepene som kommer inn på PC blir isolert der.

4.5.4. Ondsinnet kode i nettverk

Gule hendelser

Kritisk faktor	Antall "gule" hendelser i nettverket. Dvs. uønsket, ondsinnet aktivitet hvor vi ikke er sårbare.
Delspørsmål	
Måleenhet	Prosentandelen gule hendelser i nettverket
Formål	
Formel	Antall gule hendelser i nettverket
Frekvens	Månedlig
Beskrivelse av indikator	Denne indikatoren vil vise hvor mye ondsinnet aktivitet som foregår i nettverket til virksomheten. Dettet kan være at virusangrep legger igjen en trojansk hest eller at noen utenfra utnytter svakheter i nettverket og kommer seg inn. Målet er at så få "gule" hendelser som mulig skjer i nettverket.

Oransje hendelser

Kritisk faktor	Ant. "oransje" hendelser i nettverket. Dvs. ondsinnet, avansert/målrettet aktivitet hvor vi er sårbare.
Delspørsmål	

Måleenhet	Prosentandelen oransje hendelser i nettverket
Formål	
Formel	Antall oransje hendelser / antall hendelser totalt
Frekvens	Månedlig
Beskrivelse av indikator	Denne indikatoren vil vise hvor mye ondsinnet aktivitet som foregår i nettverket til virksomheten. Dettet kan være at virusangrep legger igjen en trojansk hest eller at noen utenfra utnytter svakheter i nettverket og kommer seg inn. Målet er at så få "oransje" hendelser som mulig skjer i nettverket.

Røde hendelser

Kritisk faktor	Ant. "røde" hendelser. Aktivitet som indikerer at maskin/tjeneste er kompromittert.
Delspørsmål	
Måleenhet	Prosentandelen røde hendelser i nettverket
Formål	
Formel	Antall røde hendelser / antall hendelser totalt
Frekvens	Månedlig
Beskrivelse av indikator	Denne indikatoren vil vise hvor mye ondsinnet aktivitet som foregår i nettverket til virksomheten. Dettet kan være at virusangrep legger igjen en trojansk hest eller at noen utenfra utnytter svakheter i nettverket og kommer seg inn. Målet er at så få "røde" hendelser som mulig skjer i nettverket.

4.5.5. Nedetid på systemer

Kritisk faktor	Nede tid på kritiske systemer
Delspørsmål	
Måleenhet	Andel nedetid målt i timer per måned
Formål	

Formel	Nedetid for systemet i timer per måned / totalt antall timer per måned som systemet er i drift
Frekvens	Månedlig
Beskrivelse av indikator	Dette bør måles på ulike systemer som for eksempel EPJ, PAS, RIS, PACS, e-post og ev. andre viktige systemer i virksomheten. Nedetid på de ulike systemene vil være en kritisk faktor fordi dvs. at systemene ikke er tilgjengelige og ikke kan benyttes. Andelen nedetid kan måles per uke eller per måned. Et viktig punkt er at lite nedetid en måned ikke gjør at en kan ha mer nedetid neste måned. En kan altså ikke "samle" opp liten nedetid på systemene for å bruke dette når systemene eventuelt får større periode med nedetid.

4.5.6. Feilsendinger av sensitiv informasjon

Kritisk faktor	Antall feilsendinger per 100 ansatt av sensitiv informasjon
Delspørsmål	
Måleenhet	Antall feilsendinger av sensitiv informasjon
Formål	
Formel	Antall feilsendinger med sensitiv informasjon per 100 ansatte
Frekvens	Månedlig
Beskrivelse av indikator	Antall feilsendinger av sensitiv informasjon vil gi en pekepinn på hvordan den "vanlige" ansatte håndterer sensitiv informasjon. Feilsendinger vil kunne være rene "uhell" som skjer og som ikke noen kan lastes for. Ofte vil det i midlertidig feilsendinger kunne være at en ikke har gode nok holdninger til sensitiv informasjon. Målet med indikatoren er at så få feilsendinger som mulig skjer.

4.5.7. Glemt passord

Kritisk faktor	Antall glemt passord
Delspørsmål	
Måleenhet	Antall glemt passord

Formål	
Formel	Antall glemte passord
Frekvens	Månedlig eller kvartalsvis
Beskrivelse av indikator	<p>Denne indikatoren kan være litt tvetydig. Ingen glemte passord kan tyde på at passordene er svært enkle eller at de kan være skrevet ned. Dette vil kunne gjøre at det er enkelt for uvedkommende å finne ut passord for å komme inn på ulike systemer. Ingen meldinger om glemte passord kan også være et tegn på at noen "låner" passord eller benytter felles brukeridenter dersom dette finnes.</p> <p>Mange glemte passord vil direkte føre til at det er mange situasjoner hvor personale ved virksomheten ikke får logget seg inn på IT-systemene. Dette fører til dårligere tilgjengelighet og kan være alvorlig for eksempel i en kritisk situasjon.</p>

5. Anbefalinger

Her kommer anbefalinger for de som ønsker å ta i bruk indikatorer for måling av informasjonssikkerheten.

KITH har utarbeidet et konkret forslag til indikatorsystem for informasjonssikkerhet. Systemet er vist i Vedlegg A, og er også tilgjengelig i Microsoft Excel-format ved å kontakte KITH. Systemet består av til sammen 11 indikatorer som er delt inn i 4 ulike kategorier.

Indikatorene som er valgt er kvalitativt beskrivende indikatorer. Indikatorene er et utvalg gjort av KITH, men hver enkelt virksomhet må selv velge ut de indikatorene som de finner mest hensiktsmessige. De valgte indikatorene kan imidlertid danne et godt grunnlag for å starte opp med et system for indikatorer.

Konkrete råd og anbefalinger

Her følger noen konkrete råd for bruk av indikatorer i en virksomhet:

- Få med ledelsen ved utprøving av et indikatorsystem. Dette er viktig med tanke på å få nok ”tyngde” for å få et velfungerende system.
- Velg i første omgang ut noen få områder hvor det finnes et godt informasjonsgrunnlag for å kunne lage gode indikatorer. Det er viktig at en begynner med noen få gode indikatorer, og ikke tar med for mange indikatorer i første omgang. Indikatorsystemet kan heller over tid bygges ut til å dekke større deler av den totale informasjonssikkerheten i virksomheten.
- Prøv å få med indikatorer som gir et helhetlig bilde av virksomheten, dvs. indikatorer som dekker både det tekniske, organisasjonen og menneskene.
- Prøv å fremstill indikatorene slik at det er enkelt å følge med på utviklingen av indikatorene.
- Få de aktuelle involverte personer til å forstå at indikatorer ikke handler om kontroll eller overvåking, men at formålet er å bedre informasjonssikkerheten i virksomheten. Dette er viktig dersom indikatorene skal kunne gi korrekte data spesielt på hvordan menneskelige indikatorer fungerer (ansatte vil kanskje føle seg fristet til å gi et bedre bilde enn virkeligheten, men da vil ikke indikatorene fungerer som en pekepinn).
- Prøv å benytt resultatet av indikatorene konkret i det praktiske arbeidet med å forbedre informasjonssikkerheten i virksomheten. Dette forutsetter midlertidig at virksomheten føler seg trygg på at indikatorene gir et korrekt bilde av hvordan informasjonssikkerheten faktisk fungerer i virkeligheten.

6. Referanser

- [1] *“Security Metrics Guide for Information Technology Systems”*, NIST (National Institute of Standards and Technology), Special Publication 800-55. Oktober 2002
- [2] *“Workshop on Information Security System Scoring and Ranking”*, Applied Computer Security Associates. Mai 21-23, 2001
- [3] *”Veileder for å ivareta informasjonssikkerhet”*, Sosial- og Helsedirektoratet i samarbeid med INFOSEC Norge AS, November 2002
- [4] *”Indikatorer for årlig måling av utviklingen i helsenett og elektronisk samhandling”*, Samarbeidsforum for elektronisk samhandling i helsesektoren. Forprosjektrapport 2000
- [5] *“A Guide to Security Metrics”*, SANS Info Sec Reading Room, Juli 2001
(<http://www.sans.org/rr/audit/metrics.php>)
- [6] *“Implementing an Effective IT Security Program”*, SANS Info Sec Reading Room, August 2002 (http://www.sans.org/rr/audit/IT_sec.php)
- [7] Ivar Kufås, Roy Are Mølmann: *“Informasjonssikkerhet og innsideproblematikk”*, ROSS - Risiko og sårbarhetsstudier ved NTNU, 2003. ISBN: 82-7706-204-4.

Vedlegg A: Eksempel på indikatorsystem

Vedlegg A viser eksempel på et system for indikatorer for måling av informasjonssikkerhet.

Indikatorene er oppdelt i fire grupper med til sammen 11 indikatorer. Indikatorene er spørsmål med tilhørende fem ulike svaralternativer. Alle indikatorene kan gis poeng slik at de kan fremstilles grafisk for enklere å vise tilstanden. Der svaralternativer er benyttet er disse fargelagt med rødt som betyr "kritisk", gult som betyr "pass på", og grønt som betyr "velfungerende".

De fem svaralternativene kan gis poeng, for eksempel på en skala fra 0 til 1 poeng hvor beste svar gis 1 poeng mens dårligste svar gis 0 poeng. Dette vil da med 11 indikatorer gi en totalsum mellom 0 og 11 poeng. Alternativt kan en ta gjennomsnittet av poengsummen for indikatorene. På denne måten kan indikatorene fremstilles grafisk og vise en utvikling over tid.

Under vises indikatorsystemet. Indikatorsystemet er også tilgjengelig i Excel-format ved å kontakte KITH.

Indikatorer for informasjonssikkerhet

Menneskelige faktorer	I	II	III	IV	V
1. Hvordan er rapportering og håndteringen av uønskede hendelser?	Det finnes ikke noe formelt system for rapportering av hendelser. Kun større hendelser som medfører skader blir "brannslukket" der og da.	Ledelsen påpeker at hendelser skal rapporteres, men det er ingen som følger det opp i praksis. Det er tilfeldig hvilke hendelser som blir meldt, og det finnes ingen faste rutiner for oppfølging.	De ansatte rapporterer stort sett hendelser som skjer, og de blir stort sett fulgt opp. Det er i midlertidig ingen som prøver å lære noe av de hendelsene som skjer.	De ansatte er flinke til å rapportere om hendelser som skjer. IT avdelingen setter i verk både strakstiltak og forebyggende tiltak.	Det er en god rapporteringskultur hos de ansatte. Alle hendelser blir fulgt opp av IT-avdelingen og det blir gitt tilbakemeldinger for å bevisstgjøre de ansatte.
2. Hvordan håndterer de ansatte sensitiv informasjon?	De ansatte tenker sjelden på at de håndterer sensitiv informasjon.	Ingen faste rutiner for håndtering av sensitiv informasjon. Det går "stort sett" bra!	Vi har brukerpolicy for behandling av sensitiv informasjon som alle er informert om. Ingen konkret kontroll om de ansatte følger policyen, men dette tas opp med jevne mellomrom. Vi har ikke opplevd noen negative hendelser.	De ansatte er i stor grad bevisste. Låser alltid PC-en når de går bort og lar ikke utskrifter ligge og slenge.	De ansatte er svært bevisste og tar alle forholdsregler. Alle er bevisste med sensitiv informasjon både i papirform og elektronisk. Både ledelsen og de ansatte er flinke til å "bevisstgjøre" andre om dette.
3. Hvordan blir informasjonssikkerhet inkludert i planleggingen og gjennomføringen av prosjekter som involverer sensitiv informasjon?	Dette er så å si aldri noe tema. Tar det etter hvert som behov oppstår.	Tas som regel inn på slutten og er ikke det som har mest fokus.	Blir alltid vurdert, men kanskje ikke med størst prioritet. Har ikke alltid fokus på egne behov, men mest på å oppfylle lov- og regelverk.	Det blir alltid vurdert i startfasen og alle vet at det er en viktig faktor.	Informasjonssikkerhet blir alltid behandlet gjennom hele perioden. Alle har forståelse for at dette er svært viktig og kritisk faktor.
Tekniske faktorer	I	II	III	IV	V
1. Er antivirus installert og aktivert slik at virusskanning foregår automatisk? Dette bør omfatte alle PC-er arbeidsstasjoner som er tilknyttet et nettverk, servere og e-post.	Vi har ikke noen form for virusskanning	Antivirus er installert, men det foretas ikke automatisk virusskan	Viruskan blir gjort automatisk, men usikkert om antivirusprogramvaren er oppdatert.	Viruskan blir gjort automatisk, og antivirusprogram-varen er alltid oppdatert med siste versjon.	Viruskan blir gjort automatisk, og antivirusprogram-varen er alltid oppdatert med siste versjon. De ansatte skanner også alle filer som er usikre på.
2. Gjennomføres det jevnlig sårbarhetsskanning av datanettverket med bruk av egnede verktøy?	Virksomheten utfører ikke noen form for sårbarhetstester.	Virksomheten har utført det en gang i forbindelse med en kontroll av sikkerheten. Usikkert om hvorvidt testen ble fulgt opp.	Virksomheten utfører sårbarhetstesting av og til, men resultatene blir ikke fulgt opp systematisk.	Virksomheten utfører sårbarhetstesting årlig. Alle funn av kritisk karakter blir systematisk fulgt opp og forbedret.	Virksomheten utfører sårbarhetstesting minst to ganger årlig eller ved større endringer i nettverket. Alle funn blir systematisk fulgt opp og forbedret.
3. Er brannmur installert og vedlikeholdt (forutsetter at en har Internett-tilkobling)?	Virksomheten har ikke brannmur	Brannmur er installert, men den er ikke endret eller vedlikeholdt siden installasjonen.	Brannmuren blir vedlikeholdt "nå og da", men vi har ikke tilstrekkelig kompetanse til å gjøre dette godt nok.	Brannmuren blir vedlikeholdt jevnlig av personer med nødvendig kompetanse.	Brannmuren blir vedlikeholdt jevnlig og kontrollert daglig av personale med riktig kompetanse. Brannmuren blir ansett som kritisk for sikkerheten i virksomheten.

Figur 6: Del 1 av indikatorsystemet

Organisasjon	I	II	III	IV	V
1. Risikovurderinger	Vi har ikke foretatt risikovurderinger.	Det har blitt foretatt en risikovurdering, men den er sannsynligvis ikke aktuell nå lenger.	Risikovurderinger blir utført "nå og da", men ikke årlig. Det er ikke alltid det gjøres noe med de risikoene som identifiseres.	Risikovurderinger gjøres årlig og de aktuelle risikoer blir fulgt opp med nødvendige tiltak.	Risikovurderinger gjøres minst årlig eller når store endringer krever det. Aktuelle risikoer blir fulgt opp med de nødvendige tiltak.
2. Oppdatering av sikkerhetsplaner for kritiske systemer	Inge kritiske systemer har sikkerhetsplaner.	Vi har planer for de fleste kritiske systemer, men de er ikke oppdaterte.	Alle kritiske systemer har en sikkerhetsplan, med de blir ikke systematisk oppdatert. Kun IT-ansvarlig som er kjent med planene.	Alle kritiske systemer har sikkerhetsplaner som blir oppdatert jevnlig. Planene er kjent, men ikke formelt godkjent av ledelsen.	Alle kritiske systemer har sikkerhetsplaner. Planene er testet og godkjent av ledelsen. Planene blir oppdatert jevnlig eller når endringer krever dette.
3. Katastrofeplaner	Det finnes ingen katastrofeplaner.	Det finnes en katastrofeplan, men den er verken testet eller godkjent av ledelsen.	Det finnes en katastrofeplan som er testet en gang. Den blir ikke oppdatert jevnlig.	Katastrofeplanene er testet og blir oppdatert jevnlig.	Katastrofeplanene blir både oppdatert og testet årlig, eller når endringer krever dette. Planene er godkjent av ledelsen.
Diverse					
1.Hvordan fungerer backup rutiner	Det tas ikke backup.	Det tas backup av de mest kritiske systemene.	Det tas backup av alle data, men har ikke testet rutiner for gjenoppretting.	Det tas backup av alle data og rutiner for gjenoppretting testes jevnlig.	Det tas backup av alle data og rutiner for gjenoppretting testes jevnlig. Kritiske data blir lagret på forsvarlig sted.
2. Gjennomsnittlig nedetid på EPJ og PAS målt pr måned det siste året.	Nedetid mer enn 7 ½ time pr måned. Tilsvarer oppetid < 99%.	Nedetid mellom 3 og 7½ time pr måned.	Nedetid mellom 1½ og 3 timer pr måned.	Nedetid mellom 45 min og 1½ time pr måned.	Nedetid mindre enn 45 minutter pr måned. Tilsvarer oppetid >99,9 %

Figur 7: Del 2 av indikatorsystemet