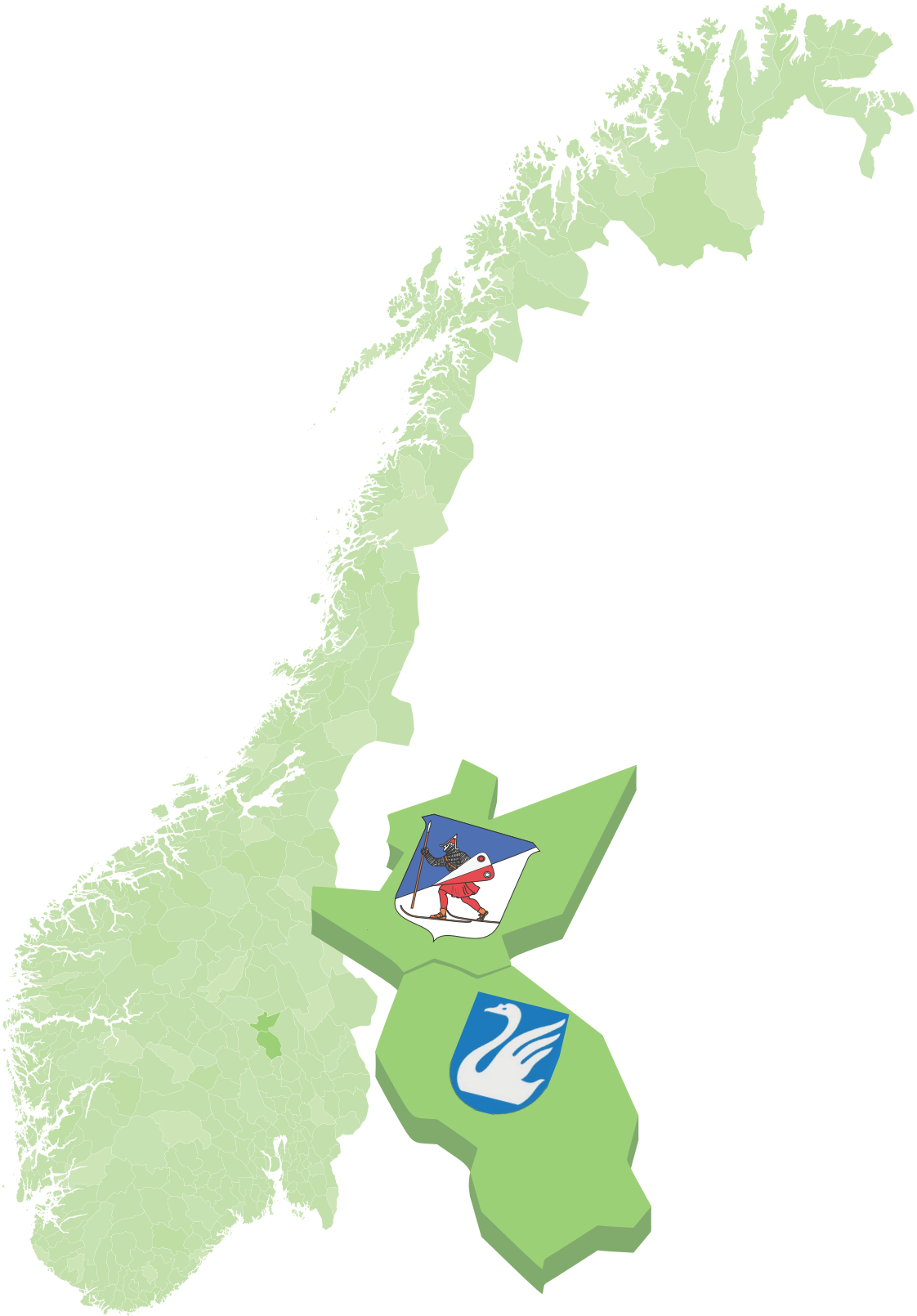
NorSIS
Norsk senter for informasjonssikring

Kommune CERT

–utredning av behov og muligheter

VEDLEGG



INNHOLD

Vedlegg A

Intervjuer med kommuner og interkommunale driftsselskaper

Det er blitt foretatt intervjuer med seks kommuner og to interkommunale selskaper. Representativt utvalg har blitt delt inn i små (færre enn 10.000 innbyggere), middels store (mellom 10.000 og 100.000 innbyggere) og store (flere enn 100.000 innbyggere).

Liten kommune 1:

Status i dag på informasjonssikkerhetsarbeidet og eventuelle mangler og behov

Kommunen er tilknyttet Helsenett og overvåkes av HelseCSIRT og er fornøyde med det. IT-lederen i kommunen oppga «et temmelig romslig IP-segment» til HelseCSIRT som nå dekker alle kommunens offentlige adresser. Samarbeidet med HelseCSIRT har bidratt til å avdekke sikkerhetshull blant underleverandører til kommunen.

IT-lederen ser ingen umiddelbare mangler med løsningene som tilbys i dag, men sier også at «det ikke hadde gjort noe» med en egen CERT for kommunesektoren.

Kjennskap til CERT-funksjoner

Kommunen er tilknyttet HelseCSIRT og drifter også et kraftverk som er tilknyttet KraftCERT. Kommunen mottar meldinger fra HelseCSIRT, og IT-sjefen er på mailinglisten til NorSIS.

Forventninger til en CERT-funksjon

Kommunen forventer at CERT-en overvåker trafikken, varsler ved trusler eller angrep og informerer om kjente forsøk på å utnytte svakheter og sårbarheter. Kommunen ønsker i tillegg rådgivning om hvordan den kan forebygge mot trusler og angrep og konkret løse utfordringer.

Meldinger fra HelseCSIRT kommer i dag på e-post og gjennom supportsystem til den som har vakt. HelseCSIRT har i tillegg fått vaktnummeret til kommunen for å varsle i særlig kritiske situasjoner. HelseCSIRT har ikke benyttet denne muligheten, men kunne/burde ha gjort det ved ett tilfelle før sommeren 2015.

Forslag til CERT-tjenester

IT-lederen mener overvåking, varsling og informasjon er de viktigste tjenestene. Det å avdekke og unngå trusler krever stor innsikt, noe kommunene sjelden har tilstrekkelig av.

På spørsmål om det er behov for opplæring og kompetanseutvikling, bekrefter han at det er et «uttømmelig behov for kunnskap». Han mener at behovet er størst sentral (IT-leder/-avdeling), og at ansvaret for å informere på brukernivå ligger hos IT-ansvarlige i den enkelte kommune. IT-lederen nevner behov for kompetanse og råd om brannmurer spesielt. Han har erfart at kommuner enten setter dette ut til underleverandører eller gjør det selv med «venstre hånd». Det synes ikke IT-leder er godt nok.

Mulige aktører til å ivareta CERT-funksjon
HelseCSIRT dekker allerede mye av kommunens behov.

Antatte suksesskriterier ved etablering av et CERT
En kommuneCERT bør være enkel å forholde seg til og ha et enkelt grensesnitt mot kommunen. Den bør også ha mulighet for å legge inn profiler av kundene, for å vite hvilke systemer den enkelte kunden har og hvilke ressurser den rår over til å håndtere trusler.

Videre er informasjon om sikkerhet og trusler viktig, også på ledernivå. CERT-en bør bidra til å styrke forankringen av sikkerhet helt opp til rådmannen.

Kommunen har hatt god dialog med HelseCSIRT, men kunne ønske seg en CERT som er en enda sterkere pådriver for samarbeid mellom kommunene.

Liten kommune 2:

Status i dag på informasjonssikkerhetsarbeidet og eventuelle mangler og behov
Kommunen føler sikkerheten er godt ivaretatt som den er gjennom å være tilsluttet interkommunalt samarbeid om IKT-tjenester.

Kjennskap til CERT-funksjoner
IKT-ansvarlig har ikke kjennskap til CERT fra før. Han mener å ha mottatt noen e-poster om HelseCSIRT eller NorCERT, men vet ikke hva disse tilbyr.

Forventninger til en CERT-funksjon
Det er ikke spesielle forventninger til en CERT-funksjon, da IKT-ansvarlig føler at sikkerhet er godt ivaretatt gjennom den løsningen de har. Han får videreformidlet varslinger fra IKT-samarbeidet, og gjør selv software-oppdateringer lokalt når dette er nødvendig. Han stoler på at andre trusler håndteres sentralt. IKT-samarbeidet har kontroll på brannmuren og utfører også on-site støtte når det er påkrevet.

Forslag til CERT-tjenester
IKT-ansvarlig nevner meldinger om trusler og hendelser som viktig, men han får dette dekket gjennom IKT-samarbeidet kommunen er del av. Han mener varslingene er viktigere for IKT-samarbeidet enn for kommunen selv.

Han opplever selv å være konstant presset på tid og har derfor liten mulighet til å delta i nettverk eller dialog i regi av en CERT. Det er i tilfelle noe som IKT-samarbeidet må ta del i.

Mulige aktører til å ivareta CERT-funksjon
IT-leder kjenner ikke til aktører som det er naturlig at kan ivareta en CERT. Han mener at han ikke ville ha stolt på en privat aktør og foretrekker en statlig aktør.

Antatte suksesskriterier
Ingen spesielle.

Middels kommune 1:

Status i dag på informasjonssikkerhetsarbeidet og eventuelle mangler og behov

Det er udiskutabelt at det er behov for en CERT-funksjon for kommunene og fylkeskommunene i Norge. Det er et stort behov for en organisasjon som gir tydelige anbefalinger og målrettet IR-ISAC. I dag kan man knytte til seg eksterne leverandører, men for en enkelt kommune er dette særlig kostnadskrevende og man må ha tekniske ressurser for å iverksette tiltak knyttet til varsling.

Det er ikke etablert tilfredsstillende maler for kommunene i dag. Det er ikke sentralisert styring av hva man burde gjøre. Det ønskes maler for blant annet risikohåndtering. Malene som er utarbeidet hos Difi og Datatilsynet synes ikke praktiske nok, og man kan stille spørsmål om hvem som har utarbeidet disse. En gjetning går i retning av jurister.

Det mangler en struktur og krav til sikkerhet i kommunesystemer i dag.

Kjennskap til CERT-funksjoner

Ja i betydelig grad.

Forslag til CERT-tjenester

En CERT-funksjon bør fange opp det som skjer, slik at organisasjonen bidrar med kompetanseheving, policyer, varsling og struktur på sikkerhetsarbeidet.

Organisasjonen bør starte i det små, for deretter å eskalere. Det må etableres et grunnregime hvor det er behov for å definere hva som er mest kritisk å håndtere. Kan gjerne være en håndfull personer i starten og ved behov innhenter man ekspertise.

For kommunene vil det være snakk om varsling av universelle trusler, ikke fagspesifikke. Det er veldig sjelden man opplever fagspesifikke trusler. Oppdatering er fagsystemer er imidlertid viktig.

Forventninger til en CERT-funksjon

- E-post varsling til utpekte kontaktpersoner i hver kommune.
- Varsling med gode og enkle beskrivelser av tekniske tiltak, men også begrenset overvåking. Det kan være nyttig å sende ut bulletiner for eksempel ved tilfeller hvor Cryptolocker og diverse phishing-forsøk er særlig aktive.
- Logg og revisjonskrav – hva gjør man med logger for å ivareta korrekt forvaltning av lovverket. I dag mottas det forskjellig loggformat fra forskjellige leverandører. Det er ønskelig at det blir etablert formelle krav til leverandører og for eksempel logging.

Mulige aktører til å ivareta CERT-funksjon

- Difi har i dag ID –porten og Sikker digital post. De burde muligens hatt en tjeneste man kunne logge seg inn på hvor man kan se tiltak til sine nettløsninger, hvilken tilstand, er det nye versjoner etc. Difi burde komme med en standard på logger. I dag er det ikke krav, et loggregimeløsning etterspørres.
- KINS er en fin arena for å spre informasjon.

Antatte suksesskriterier

- Lære av HelseCSIRT. Deres varsler har gode, teknisk enkle løsningsforslag til alle trusler som sendes ut. Nærmest daglige varsler.
- Viktig å forplikte rådmennene tydelig på dokumentansvar og informasjonssikkerhet. Kommunene må abonnere på varsler og følge opp krav som settes av CERT-organisasjonen.

Middels kommune 2:

Status i dag på informasjonssikkerhetsarbeidet og eventuelle mangler og behov
Kommunen har et IT-samarbeid med tre andre kommuner. De er samarbeidende kommunene er små (<10.000 innbyggere). Kommunen har mulighet til å inngå leverandøravtale som sikrer kompetanse ved hendelser. Dette er ansett som veldig kostbart og er ikke inngått. Leverandører har stor makt og man stoler i stor grad på deres kompetanse. Lite krav blir stilt fra kommune til leverandør. Kommunen har etablert egne kanaler for hendelseshåndtering.

Kjennskap til CERT-funksjoner
Ja, kjenner begrepet og har kjennskap til vanlige funksjoner.

Forventninger til en CERT-funksjon
Gi råd om tekniske tiltak. Et eksempel er krav til logging. Viktig med varsler slik at man ta «tak» tidlig. Det viktigste er å få ut informasjon tidlig slik at kommunene kan agere eller hente inn ressurser som ivaretar det tekniske arbeidet.

Forslag til CERT-tjenester
Informasjonsutveksling av generelle trusler og hva man må tenke på når det gjelder hendelser. Etablere grunnkurs for de som skal ivareta hendelser i kommunene.

Stor kommune 1:

Status i dag på informasjonssikkerhetsarbeidet og eventuelle mangler og behov
Har en stor avdeling for IT-drift. Kommunen har egen direktør for IKT og egen sikkerhetsansvarlig. Informasjonssikkerhet er prioritert i kommunen.

Kjennskap til CERT-funksjoner
Ja i betydelig grad.

Forventninger til CERT-funksjon
En CERT-funksjon bør være navet for kommune-Norge. Kritiske systemer må vurderes, og varslinger og anbefalinger bør kunne fungere som en øyeåpner for kommunene der det finnes utfordringer.

Det bør også kunne forventes at CERT-funksjonen og involverte ressurspersoner skal fungere som et kompetansesenter for kommunene.

Forslag til CERT-tjenester
Større kommuner bør kunne hjelpe mindre omkringliggende kommuner som mangler ressurser ved hendelser. De kan også bidra med kompetanse ved tekniske tiltak som følge av varsling. CERT-en bør ha oversikt over hvilke ressurspersoner som kan benyttes og hvilken fagkompetanse de besitter.

Det er også viktig at det blir utarbeidet maler som kan benyttes av kommunene, et eksempel her er mal for verdivurdering.

Det bør være en forutsetning at sensornettverk etableres på sikt.

Antatte suksesskriterier
CERT-en må ikke bli en «silo-CERT» uten samarbeid med andre CERT-miljøer og NorCERT. Det er viktig å få rapporter fra de andre sektor-CERTene som har ansvar for enkelte fagenheter i kommunene, som helse og vann og avløp. HelseCSIRT overvåker Helsenettet og varsler de aktuelle enheter i kommunene. Det må etableres et sentralt nettverk som kan være raskt ute med «early warnings».

Stor kommune 2:

Status i dag på informasjonssikkerhetsarbeidet og eventuelle mangler og behov
Egen IT-driftsavdeling. Sikkerhetsansvarlig med flere medarbeidere. Informasjonssikkerhet blir prioritert høyt i kommunen. Drift og supportavtaler med leverandører som bidrar med ekspertise ved hendelser. Det vil være kostnadskrevende for mindre kommuner å ha leverandøravtaler på samme nivå.

Kjennskap til CERT-funksjoner
Ja i betydelig grad.

Forventninger til en CERT-funksjon
Informasjonsutveksling og håndtering av hendelser og sårbarheter i systemer bør ivaretas. Et kommune-CERT bør etableres. Et CERT bør være med å utvikle scenarioer slik at kommunene kan øve beredskap på relevante tema.

De bidrar gjerne med egen kompetanse inn i en ressurspool som kan benyttes ved kriser.

Forslag til CERT-tjenester
Kommunen ønsker og vil tilby en aktiv roll mot mindre kommuner da de er i besittelse av høy kompetanse på flere områder. Informasjonsutveksling er nødvendig i oppstartsfasen og heller utvikle tjenesten etter hvert som kompetanse og erfaring øker. Maler for risikostyring og klassifisering bør knyttes mot et CERT

Antatte suksesskriterier
Det er essensielt at man starter i det små og bygger sten på sten. Informasjonsutveksling bør være en tjeneste man starter med. Kommunene bør hjelpe hverandre til å bli gode og bidra med hjelp til hverandre når noe skjer.

Det er viktig å tilføre kompetanse med inngående kjennskap til sektoren. Informasjonsutveksling i første fase for deretter å utvikle kompetanse slik at man kan bidra til koordinering ved hendelseshåndtering.

Interkommunalt driftsselskap 1

Status i dag på informasjonssikkerhetsarbeidet og eventuelle mangler og behov
Generelt sett er det bra at noen tar tak i dette og utreder muligheten for felles løsninger i kommune-sektoren. Kommunene kjenner sikkerhetsutfordringene på kroppen, men har selv begrensede ressurser til å løse dem og trenger gode, felles løsninger.

IKT-samarbeidet får i dag dekket behovet for en CERT innenfor helsesektoren gjennom HelseCSIRT, som de føler gir god støtte og respons. Tilknytningen til HelseCSIRT dekker også deler av de administrative tjenestene, men her har IKT-samarbeidet supplert med andre løsninger for å ivareta sikkerheten.

Kjennskap til CERT-funksjoner

Lederen for IKT-samarbeidet har relativt god kjennskap til CERT-er gjennom tilknytningen til HelseCSIRT. De har også meldt seg inn i varslingsordningen til NorCERT, men er usikre på hva de kan forvente av denne ordningen. De har fått lite informasjon om NorCERT og opplever også informasjonen som vag.

Forventninger til en CERT-funksjon

Lederen for IKT-samarbeidet er veldig opptatt av mandatet til CERT-en. Det må være tydelig hva den skal dekke og hva kommunene eventuelt kan forvente. Det er ikke viktig at en kommuneCERT har spesiell kompetanse om kommunal forvaltning eller hvilke systemer og ressurser kundene rår over: «En IT-løsning er en IT-løsning. Komponentene er like overalt, og kommunenes IT-systemer er ikke verre enn andre systemer». Det er viktigere å vite hva CERT-en vil levere og at den holder det den lover.

Forslag til CERT-tjenester

Overvåking og varsling nevnes som de to klart viktigste tjenestene. Dette er tjenester som krever innsikt og kompetanse som kommunene ofte ikke har selv – og som med fordel kan samkjøres utenfor eget hus. Lederen for IKT-samarbeidet sier at han «er glad for tjenester som ligger utenfor huset, så lenge jeg vet hva jeg kan forvente og er trygg på leveransene».

IKT-samarbeidet opplever at de selv er gode på drift og håndtering av trusler og hendelser. De har god nytte av varslingene fra HelseCSIRT, som gjør at de kan reagere raskt når det trengs.

På spørsmål sier lederen at det ville være nyttig om CERT-en etablerer et ressurssenter eller forum for dialog om cybersikkerhet i kommunene, gjerne med årlige samlinger. I tillegg til deling av erfaringer og kompetanse, ser han på dette som viktig for å få innsikt i hvordan CERT-en jobber og at «tjenestene leveres på en skikkelig måte».

Mulige aktører til å ivareta CERT-funksjon

Generelt mener lederen at det vil gi legitimitet til ordningen om en sentral, offentlig aktør står bak. Han mener at KommIT/KS burde ha tatt tak i dette og er skuffet over at det ikke er gjort. En privat aktør er også mulig, men det vil ikke gi samme legitimitet.

Av andre aktører mener han Difi er i særposisjon til å utvikle og tilby en CERT-funksjon overfor kommunene. Det kan også være naturlig med en utvidelse av tilbudet fra NorCERT, men erfaringene med NSM så langt er at informasjonen er for knapp og vag om hva NorCERT leverer.

Antatte suksesskriterier

God informasjon og trygghet om leveransene er viktigst, i tillegg til faktorene som er nevnt over.

Interkommunalt driftsselskap 2

Status i dag på informasjonssikkerhetsarbeidet og eventuelle mangler og behov

IKT-samarbeidet er tilknyttet HelseCSIRT, som har satt opp en egen probe hos dem. Det gjør at HelseCSIRT fanger opp mer enn bare helsesektoren. De er godt fornøyde med dette samarbeidet og opplever at de får god nytte og gode råd fra HelseCSIRT.

På spørsmål om det er behov for en egen CERT for kommunesektoren, er lederen usikker. Han ser likevel nytteverdien av en CERT for andre deler av kommuneforvaltningen enn helsesektoren.

Kjennskap til CERT-funksjoner

Lederen har kjennskap til CERT gjennom samarbeidet med HelseCSIRT. IKT-samarbeidet abonnerer ikke på meldinger fra NorCERT og har heller ikke inngående kunnskap om hva de leverer.

Forventninger til en CERT-funksjon

Erfaringene fra samarbeidet med HelseCSIRT er at det er behov for å bli kjent raskt med hendelser og få råd om håndtering av dem. Forhåndsvarsling av trusler, oppdateringer og spesielle typer angrep er også viktig. Han nevner Cryptolocker som eksempel på god håndtering fra HelseCSIRT: Varslingen kom i tide, og HelseCSIRT delte effektivt rutiner og anbefalinger for håndtering av trusselen fra andre brukere av HelseCSIRT.

På spørsmål mener han at det også er behov for mer konkret og evt. onsite støtte i kommunene. De blir ofte maktesløse ved angrep og trenger krisehjelp. I dag må de gå til eksterne leverandører for å få slik hjelp.

Forslag til CERT-tjenester

Deteksjon og råd om håndtering av trusler og hendelser anses som de viktigste. På spørsmål sier lederen at det også er nyttig med dialog og samlinger om sikkerhet. Han mener dette er spesielt viktig og aktuelt for interkommunale samarbeid, mens kommunene i mindre grad har mulighet eller ressurser til å delta.

Mulige aktører til å ivareta CERT-funksjon

En nærliggende løsning er å utvide mandatet til HelseCSIRT.

Generelt sett bør CERT-en henges på eksisterende løsninger. Nasjonal styring anses også som viktig. Det gir én felles overbygning, kan bidra til å samle spisskompetanse og skaper trygghet om leveransene. En frittstående (privat) løsning anses som mindre troverdig og attraktivt.

Antatte suksesskriterier

Å skape trygghet om leveransene – hva CERT-en leverer og at den leverer godt – anses som viktigst. Den må unngå skremselspropaganda, men levere gode råd, vise kompetanse og bidra til å bygge nettverk, slik IKT-samarbeidet har erfart at HelseCSIRT gjør.

VEDLEGG B

Nasjonale og sektorvise CERTer i Norge

1. NSM NorCERT

Operasjonssenteret i Nasjonal sikkerhetsmyndighet, NSM NorCERT, er Norges nasjonale senter for håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.

NSM NorCERT er den viktigste arenaen for IKT-samarbeid, et nasjonalt samlingspunkt og en koordinerende enhet for IKT-sikkerhetshendelser. Vi er den operative delen av NSM, dedikert til cybersikkerhet og hendelseshåndtering.

Alvorlige dataangrep

NSM NorCERT håndterer alvorlige dataangrep mot samfunnsviktige virksomheter og informasjon. Operasjonssenteret i Nasjonal sikkerhetsmyndighet håndterer flere tusen saker i løpet av et år av disse var det i fjor 88 alvorlige (2014).

Nasjonalt sensornettverk

NSM NorCERT drifter og organiserer et nasjonalt sensornettverk på internett. Sensornettverket skal avdekke forsøk på datainnbrudd mot samfunnskritiske virksomheter på tvers av sektorer. Dette er kort fortalt en digital innbruddsalarm for AS Norge.

NSM NorCERT skal

- Forebygge alvorlige dataangrep mot samfunnsviktige virksomheter og informasjon
- Dele informasjon ved hjelp av spesialrapporter, foredrag og annen utadrettet virksomhet
- Koordinere respons til alvorlige IT-sikkerhetsangrep mot kritisk infrastruktur og informasjon
- Innhente informasjon om alvorlige sikkerhetstruende hendelser på Internett
- Koordinere tidlig sikkerhetsoppdatering av samfunnskritiske datasystemer
- Fokusere på deling av informasjon
- Til enhver tid ha et oppdatert nasjonalt IKT-risikobilde
- Hjelpe frem responsmiljøer i Norge
- Gi innspill til nasjonale beredskapssystemer og bistår beredskapsarbeidet

Hva er en CERT?

CERT-funksjonen er et kjent begrep internasjonalt. CERT står for Computer Emergency Response Team og er en koordinerende enhet for informasjonssikkerhet. Det faktum at digitale trusler har liten respekt for landegrenser betyr at gjensidig samarbeid mellom CERTer er ekstremt viktig.

Trusted Introducer

NSM NorCERT er sertifisert og akkreditert av Trusted Introducer (ekstern nettside).

RFC 2350: Expectations for Computer Security Incident Response at NorCERT (pdf)

2. UNINETT CERT

Eierskap og formål

Uninett organiserer CERT-funksjonen for universitet og høyskoler i Norge. Uninett startet opprinnelig i 1993 som et forskningsprosjekt i Sintef. Formålet ved oppstart var knyttet til drift. I 1995 ble informasjonssikkerhet også en tjeneste.

UNINETT CERTs hovedoppgave er å håndtere og koordinere sikkerhetshendelser som berører UNINETTs kunder. CERTet rådgir kundene i sikkerhetsspørsmål, gjennomfører trafikkovervåkning og varsler om uønskede hendelser.

Organisering

Uninett er organisert som et statlig eid AS. Eier er Kunnskapsdepartementet. Enkelte medlemsskap er obligatoriske gjennom statlig eierskap, men UNINETT har også frivillige medlemmer.

Det er til sammen 3 årsverk som betjener CERT-funksjonen. Det er flere av UNINETTs ansatte som bidrar med kompetanse, mens det er to som er fast ansatte i tjenesten.

Finansiering

Tjenesten dekkes i sin helhet av UNINETTs årlige tjenesteavgift.

Tjenester

UNINETT CERTs tjenester er tilgjengelig for alle som benytter UNINETT som internettleverandør (de som er tilknyttet forskningsnettet).

Følgende tjenester er tilgjengelig:

Håndtering av sikkerhetshendelser
- Koordinering
- Hindre ytterligere ødeleggelse og/eller økonomisk tap
- Assistanse i forbindelse med opprydding og gjenetablering av tjenester

Overvåking og varsling
- Identifisering av uønsket trafikk basert på et oppdatert trusselbilde
- Varsling om infiserte maskiner og annet misbruk

Forebyggende virksomhet
- Videreformidling av viktige sikkerhetsadvarsler som er spesielt relevante for sektoren
- Implementering og vedlikehold av sikringstiltak
- Utvikling av sikkerhetsarkitektur for sektoren
- Rådgivning

Kunnskapdepartementet har gitt UNINETT i oppgave å lede og etablere et sekretariat for informasjonssikkerhet i UH-sektoren i Norge

I tillegg til sekretariatet har UNINETT etablert et sikkerhetsforum for universiteter og høgskoler. Forumet skal være rådgivende innenfor området informasjonssikkerhet, beredskap og kontinuitet. Her skal man kunne dele erfaringer og skaffe seg kunnskap om hvordan man kan jobbe effektivt og praktisk innenfor informasjonssikkerhet og beredskap/kontinuitet1[1].

Samarbeid
Medlemsskap i nasjonale og internasjonale organisasjoner. Det synes avgjørende å ha et godt samarbeid med både nasjonale og internasjonale aktører.

UNINETT er akkreditert hos TI-Trusted Introducer[2]. Alle europeiske team kan registrere seg hos denne tjenesten og utveksle erfaring.

Sanksjoner
Uninett CERT har anledning til å stenge sider som er infiserte.

3. HelseCSIRT (Computer Security Incident Response Team)

Eierskap og formål
HelseCSIRT er opprettet som en del av Norsk Helsenett SF på oppdrag fra Helse- og omsorgsdepartementet. HelseCSIRT skal være helse- og omsorgssektorens felles kompetansesenter for informasjonssikkerhet. Senteret skal spre kompetanse om IKT-trusler og beskyttelsesmekanismer og kontinuerlig overvåke trafikken i helsenettet. Senteret skal samarbeide med NorCERT og andre nasjonale og internasjonale enheter[3].

HelseCSIRT skal være et ressurssenter for sektoren og skal være i god dialog med sektoren og ønsker at virksomhetene i sektoren bruker senteret og gir beskjed om hva de har behov for.

Organisering
Organisasjonen består av 9 ansatte og er en del av Norsk Helsenett SF. HelseCSIRT ledes av seksjonsleder Gunnar Johansen (pr. 1.9.2015).

Varsling skjer via e-post. Det er opprettet e-postlister for hvem som skal kontaktes ved hendelser.

1 Uninett.no

2 https://www.trusted-introducer.org/services/overview/norwegian.html

3 Kilde: HelseCSIRT

Tjenestetilbud
Forebygge, oppdage, varsle og bistå ved håndtering av hendelser. Primærområdet er helse- og omsorgssektoren i Norge.

Nasjonalt beskyttelsesprogram (NBP);
Sensornettverk i Helsenettet. Sensorene skal oppdage og varsle om hendelser samt sikre sporbarhet slik at man har loggdata som gjør at HelseCSIRT kan bistå på en best mulig måte når en hendelse har skjedd. Skanning av nettet gir også proaktive muligheter til å oppdage og stenge sårbarheter før de blir utnyttet. Varsling skal også skje om sårbarheter i utbredt programvare. Det er etablert system og rutiner for hendelseshåndtering og varsling til sektoren. HelseCSIRT gjennomfører etter anmodning, også inntrengningstesting mot sentrale virksomheter i spesialisthelsetjenesten. Organisasjonen henter inn trusselinformasjon, analyserer og deler informasjon i nettverket.

De som omfattes av nasjonalt beskyttelsesprogram (NBP) er virksomheter som er tilknyttet Norsk Helsenett. Dette er alt fra Helsedirektoratet, spesialisthelsetjenesten, regionale sykehusforetak til private og offentlige klinikker, tannleger, fastleger og apotek. Det er inngått avtale med 268 av 428 kommuner pr 1.9.2015

Medlemmene varsles via e-post. Varsling gjelder eksempelvis sårbarheter i utbredt programvare og patching.

HelseCSIRT har også fått i oppdrag å etablere et nasjonalt kompetanseforum for e-sikkerhet i helse- og omsorgssektoren. Forumet etableres med tanke på erfaringsutveksling, kompetansespredning og diskusjon rundt fremtidige løsninger og bruk av felleskomponenter. Første møtet ble avholdt 27. august i år.

«Kunnskaps- og erfaringsdeling er det vi ønsker skal komme ut av dette forumet» - Gunnar Johansen, seksjonsleder for HelseCSIRT[4].

Finansiering
HelseCSIRT finansieres med øremerkede midler over statsbudsjettet.

Samarbeid
Sektor-CERTene samarbeider sammen med nasjonalt CERT. Finner HelseCSIRT informasjon om eksempelvis phishingforsøk mot finansaktører så varsles FinansCERT, tilsvarende så varsles NSM NorCERT ved hendelser som faller inn under deres ansvar. HelseCSIRT har også utviklet godt og aktivt samarbeid med mange internasjonale CERTer og sikkerhetsorganisasjoner.

Sanksjoner
HelseCSIRT fører ikke tilsyn, de gir heller ikke informasjon til tilsynsførende myndighet. Hovedfokus er å holde helsenettet sikkert.

4. FinansCERT

Eierskap og formål
FinansCERT ble opprettet i 2013 etter en utredning gjennomført av finansbransjen. Pådrivere til etablering var NorCERT og Finanstilsynet, sammen med bransjen. Organisasjonen er en egen enhet eid av Finans Norge gjennom medlemmene. Medlemsmassen består av ca. 140 virksomheter innen finans og forsikring.

4 http://www.helsemedisinteknikk.no/Default.aspx?ID=171&Action=1&NewsId=5737&M=NewsV2&PID=520

FinansCERT skal bidra til effektiv håndtering av IT-sikkerhetshendelser i, eller rettet mot, banker og livselskaper. FinansCERT sin viktigste oppgave er å dele informasjon i næringen om hendelser, gjennomførte tiltak og skadeforebygging. FinansCERT skal bidra til å redusere finansnæringens tap fra cyber-kriminalitet.

Organisering
FinansCERT er organisert som et AS uten profittformål. Det er 4 ansatte. FNO bidrar med administrative tjenester. FinansCert ledes pr. 1. 9.15 av Morten Tandle.

Tjenester
FinansCERT skal ha oversikt over trusselbildet og varsle medlemmene. Det blir utarbeidet kvartalsvise rapporter basert på informasjonsinnhenting og analyse.

FinansCERT skal også koordinere finansinstitusjonenes arbeid ved hendelser. FinansCERT skal også bidra i øvelser og katastrofeplanlegging til medlemmene.

Prosessene i tjenestetilbudet basert på standard prosesser, kjent fra bl.a. SANS[5], med forebygging (kjenne til trusselbildet), oppdage og håndtere hendelser (skadebegrensning og retur til normalsituasjon), samt evaluering.

Varsling til medlemmene foregår via et eget sikret system for informasjonsdeling.

Finansiering
Medlemsavgift. Årlig budsjett blir foreslått og gjennomgått av FNO. Har et årlig budsjett på 10 mill. kroner.

Samarbeid
FinansCERT har samarbeid med flere organisasjoner og offentlige instanser. Samarbeidsavtalene er inngått med blant andre Datakrimenheten i Kripos og NorSIS.

Sanksjoner
FinansCERT har ikke noen myndighet ovenfor medlemmene, men har en rådgivende rolle. Er avhengig av å gi gode råd for å bli hørt.

Tilsyn med næringen utføres av Finansdepartementet og Finanstilsynet.

5. KraftCERT

Eierskap og formål
KraftCERT eies av Statnett, Statkraft og Hafslund Energi i fellesskap, med åpning for flere eiere. KraftCERT skal våre rådgivende instans for håndtering av informasjonssikkerhetshendelser med særlig fokus på beskyttelse av kontrollsystemer. Virksomheten skal inneha sikkerhetskompetanse og hendelseshåndteringskompetanse.

Organisering
KraftCERT er etablert som et ideellt AS, og har tre ansatte. Ledes av Margrete Raaum pr. 1.9.2015. Kraftselskap er underlagt kraftforsyningens beredskapsorgan (KBO). NVE kan involvere KraftCERT ved behov i forbindelse med beredskapshendelser.

5 https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses- 1791

Tjenester

ISAC (Informastion Sharing and Analysis Center) er en av tjenestene som KraftCERT skal tilby. Informasjon fåes blant annet fra ICS-CERT og andre partnere, både fra åpne og lukkede lister. ICS-CERT er tilknyttet DHS/US-CERT og er fokusert på kontrollsystemer og kritisk prosessindustri. I tillegg mottar KraftCERT varsler om trusler og angrep fra flere kilder, og dette deles igjen med medlemmene. Det sendes ut nyhetsbrev en gang i uken og varsler ved behov, uten forsinkelse.

Rådgivning foregår på flere måter. KraftCERT utarbeider best practices, enten på kjente problemstillinger i kontrollsystemindustri, eller på områder som blir identifisert som et behov hos medlemmene. KraftCERT arrangerer også kurs i hendelseshåndtering for sine medlemmer og har også planer om å både tilrettelegge for andre kurs for medlemmene og potensielt anbefale opplæringstiltak.

IR (Incident Response) skal i utgangspunktet utføres inne i selskapene, men KraftCERT vil fungere rådgivende overfor selskapene, bistå med konkrete råd eller også utrykning ved større hendelser. Man har i utgangspunktet inngått rammeavtale med mnemonic (MIRT) om garantert respons ved større hendelser om nødvendig. Selve utrykningen av MIRT ved hendelser dekkes av det enkelte medlem. Rammeavtalen gjelder også administrative og fagsystemer, ikke bare kontrollsystemer.

KraftCERT har inngått en rammeavtale med mnemonic om SOC-tjenester (Security Operations Center). Avtale mellom medlemmene om overvåking internt i nettet må inngås i tillegg, for de selskaper som ønsker det. Kraftselskaper er underlagt strenge krav til overvåking i nettet (tilsyn føres av NVE). For de selskaper som har VDI sensor vil KraftCERT også bistå med håndtering av de varsler dette avstedkommer.

Hvert selskap har oppgitt ønsket kontaktpunkt for hhv administrative henvendelser og hendelser. Varsling skjer via e-post, SMS eller telefon per i dag, men en portal for utveksling av data står klar i løpet av oktober.

Finansiering

Driften er finansiert av medlemsavgifter, og et eventuelt overskudd blir ført tilbake inn i selskapet.

Det er garantert for driften de tre første årene.

Samarbeid

KraftCERT har samarbeid med blant annet kontrollsystemspesifikke CERTer som ICS-CERT, JPCERT/CC (Japan) CERT.at Østerrike) og TR-CERT (Tyrkia). Disse teamene arbeider alle for å redusere risiko innenfor og på tvers av alle sektorer knyttet til kritiske infrastruktur som opererer industrielle kontrollsystemer KraftCERT har også direkte avtaler om varsling hos leverandører av kontrollsystemer og deltar i internasjonale arbeidsgrupper for sikring og incident response i kontrollsystemer. KraftCERT arbeider også tett med det norske sikkerhetsmiljøet, ikke minst NorCERT.

Vedlegg C

CERT-organisasjoner internasjonalt, et utvalg

First International, som er et internasjonalt nettverk for alle etablerte CERTer i hele verden, har bidratt til å få kontakt med flere miljøer internasjonalt. Disse miljøene har i større og mindre grad tjenester mot lokale myndigheter.

1. CERT-IST i Frankrike.

Eierskap og formål
Virksomheten er privat og uavhengig og er ikke en nasjonal CERT. Deres kundegruppe består av alt fra små og store virksomheter og innen mange bransjer og er en multisektor-CERT.

Organisering
Organisasjonen ble etablert i 1999 og ledes av Martine Giralt. De er fire ansatte.

Tjenester
Kundene tilhører alt fra sykehus og militære til transportører og retail. Med så differensiert kundemasse må virksomheten ha tilpassede tjenester til denne gruppen. Dette gjøres ved at kundene abonnerer på tjenester som er tilpasset deres organisasjon og systemer. Eksempelvis er kontrollsystemer (SCADA) en abonnementsgren.

CERT-IST har en privat/offentlig webside. Det er viktig å definere opp riktige profiler for kunder. Eksempelvis hvilken infrastruktur og applikasjoner som benyttes. Medlemmene får e-post med varsler utfra valgte profil.

Organisasjonen har en daglig overvåking av media og nyheter, og plukker ut de som er mest relevante. Nyhetsbrevet de sender ut daglig er tospråklig; fransk og engelsk.

Et annet tjenesteområde er å rådgivning og bistand med hendelseshåndtering, også kun ved mistanke om hendelse. Dette dreier seg om hjelp til alt fra etterforskning, teknisk støtte ved datainnbrudd til deteksjon av skadevare.

Finansiering
Medlemmene betaler en årlig avgift, hvor tjenesten de mottar er rådgivning og varsling.

Samarbeid
I Frankrike møter alle CERT-ene sammen med myndighetscerten, CERT-FR. CERT- FR deler ikke informasjon med de andre CERTene da de kun ivaretar kritisk infrastruktur og myndighetskontorer.

2. TWN-CERT

Organisasjon og eierskap
TWNCERT er den nasjonale CERT-funksjonen i Taiwan. TWNCERT er internt i Taiwan kjent som ICST (Institute for Computer Sciences). TWNCERT og tilhørende funksjoner er myndighetseid.

Tjenester
ICST har en egen webside (http://www.icst.org.tw). Deres ISAC, kalt G-ISAC har et varslingssystem til både offentlig og privat sektor. Varsel sendes ut til alle offentlige etater samt private sektorer om de nyeste truslene og sårbarhetene.

Foruten å samle informasjon fra andre cyber-sikkerhetsorganisasjoner, har TWNCERT sitt eget Honeynet, en Botnet tracer og overvåkingssystemer.

All informasjon som blir samlet inn fra nevnte kilder legges ut på nettsiden. Dette gjelder de generelle trusler og sårbarheter. Informasjonen som er spesifikk for offentlige etater sendes direkte til etatene. Privat sektor eller ISP (Internet Service Provider) relatert info vil bli sendt via G-ISAC og ordinært varslingssystem.

3. CERT-FI

Organisasjon og eierskap
Nasjonal CERT og myndighetseid. Formålet er å sikre infrastruktur, ikke bare kritisk infrastruktur.

Tjenester
Som den nasjonale CERT fra Finland NCSC-FI bidrar de med koordineringstjenester, fasilitering av andre CSIRTs, systemadministratorer og netteiere.

CERT-FI publiserer også informasjon om aktuelle sikkerhetsrisikoer, sårbarheter, veiledninger og varsler på deres offentlige hjemmeside. I tillegg produseres sektorspesifikke rapporter til telekommunikasjonsleverandører, kritiske infrastruktur-leverandører og sentrale myndigheter[6].

4. CERT-UK

Organisasjon og eierskap
Nasjonal CERTi Storbritannia og er myndighetseid. Myndighetene har også etablert flere Warps (ISAC) som tilhører National Help Service (NHS).

En del av CERT-UT er Cybersecurity Information Sharing Partnership (CISP). Dette er en felles satsning mellom industri og regjering med det formål å dele informasjon om cybertrusler og sårbarheter for å øke bevissthet og forståelse som på sikt vil bidra til å redusere konsekvenser for britiske bedrifter.

6 https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert- fi/rfc2350.html

Tjenester

CERT-UK har fire hovedoppgaver som følge av Storbritannias Cyber Security Strategy:

- Leder håndtering av nasjonale cyber-sikkerhetshendelser
- Støtter kritisk infrastruktur med håndtering av cyber sikkerhetshendelser
- Fremme forståelse av cyber-sikkerhet på tvers av industri, akademia og offentlig sektor
- Er et internasjonalt kontaktpunkt for koordinering og samarbeid mellom de nasjonale CERTene.

Det er også etablert lokale Warnings, Advisory and Reporting Point (WARP) og disse er nå en del av Senter for beskyttelse av nasjonal infrastruktur (CPNI). Warp medlemmene kan være fordelt på sektor, bransje eller geografi. Warpmedlemmer kan motta og dele oppdatert informasjon om cybertrusler og sårbarheter og slik bidra til og dele beste praksis.

Vedlegg D

KS; eKommunekartlegging 2014

KOMMUNESEKTORENS ORGANISASJON
The Norwegian Association of Local and Regional Authorities

Tre elementer i digitaliseringsarbeidet i kommunal sektor

- ✓Digitaliseringsstrategi for kommunesektoren 2013-2016
- ✓KS' interessepolitiske posisjoner på digitaliseringsområdet
- ✓KommIT: Program for IKT-samordning i kommune-sektoren 2012-2015

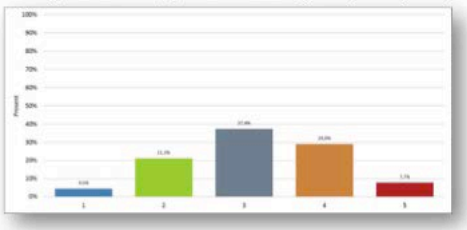
KS KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

«En samordnet kommunal sektor leverer digitale tjenester som gir innbyggere og næringsliv et reelt digitalt førstevalg»

KS KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

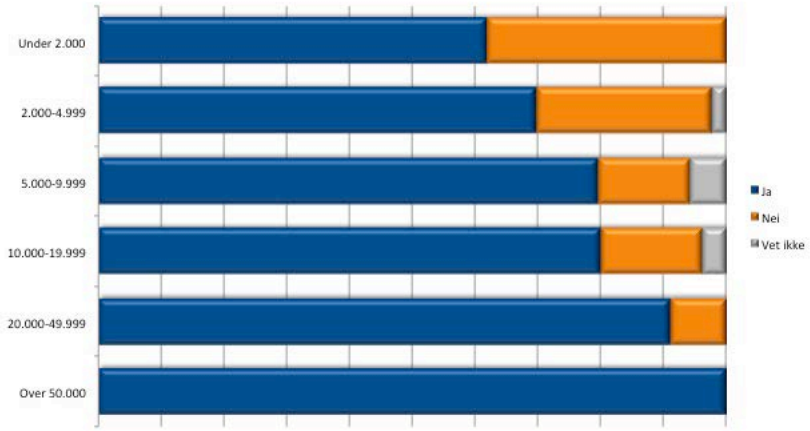
eKommunekartleggingen og målkort

I hvilken grad har kommunen/fylkeskommunen satt seg inn i Digitaliseringsstrategi 2013-2016 for kommuner og fylkeskommuner?



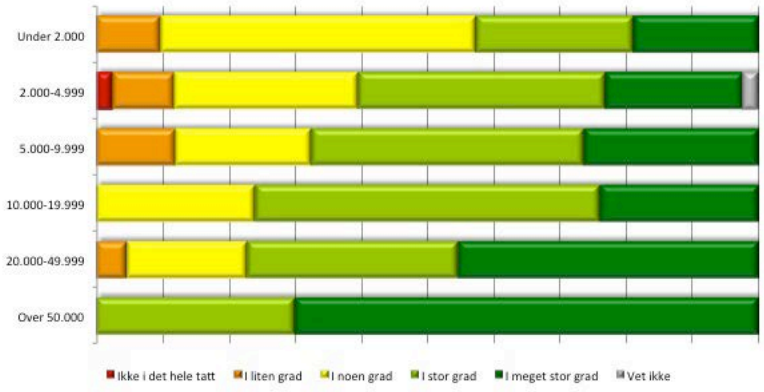
1	Ikke i det hele tatt
2	I liten grad
3	I noen grad
4	I stor grad
5	I meget stor grad

43: Har kommunen/fylkeskommunen en egen strategi for informasjonssikkerhet?



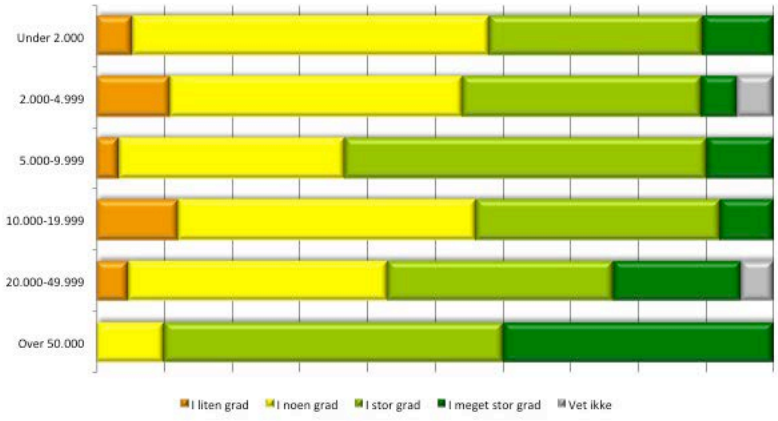
KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

44: I hvilken grad har kommunene/fylkeskommunen utarbeidet egne retningslinjer for informasjonssikkerhet?



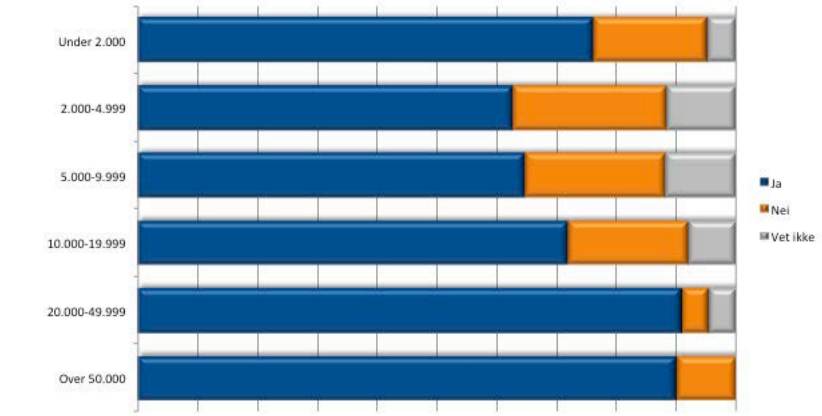
KS KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

45: I hvilken grad er ledelse og ansatte kjent med kommunens/fylkeskommunens retningslinjer for informasjonssikkerhet?



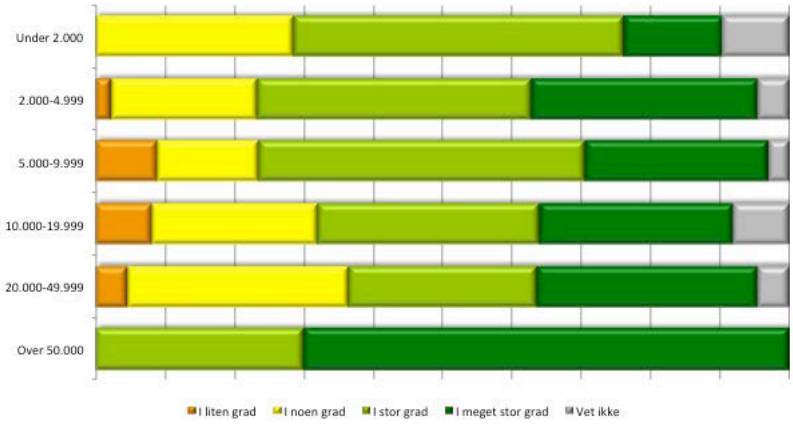
KS KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

46: Er det utarbeidet rutiner for å inngå databehandleravtale med andre som behandler personopplysninger på vegne av kommunen/fylkeskommunen?



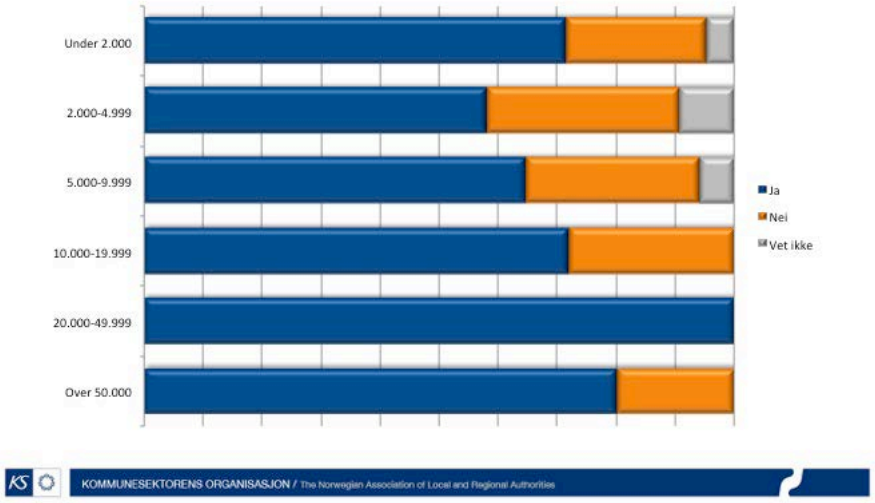
KS KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

47: I hvilken grad er kommunens/fylkeskommunens internkontroll- og styringssystem forankret i øverste administrative ledelse?

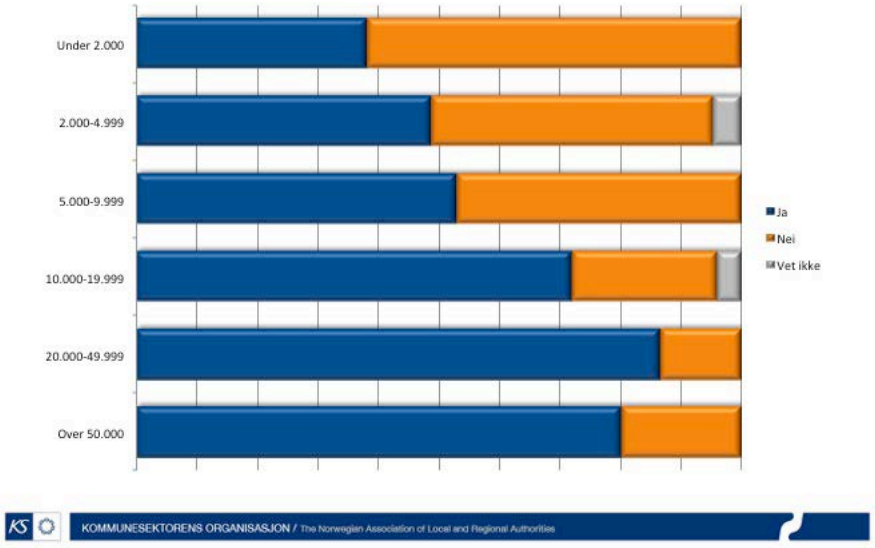


KS KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

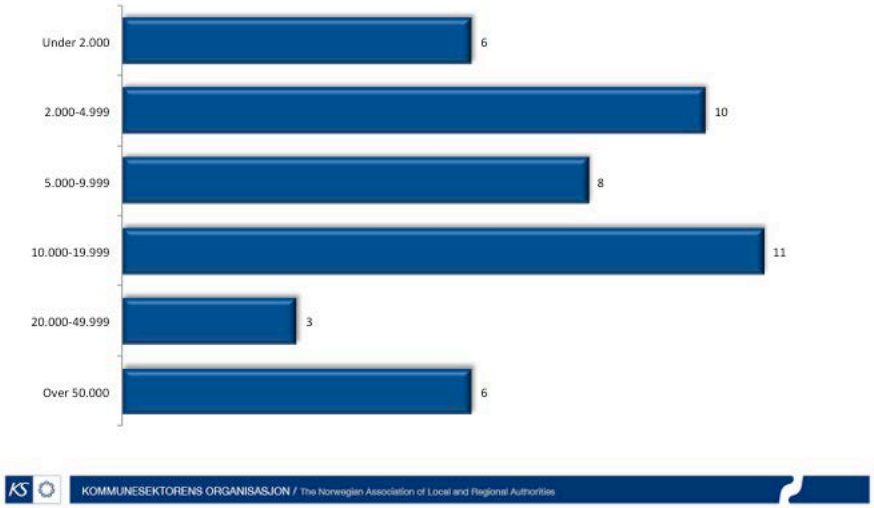
48: Behandler kommunen/fylkeskommunen alle sensitive personopplysninger i sikret sone?



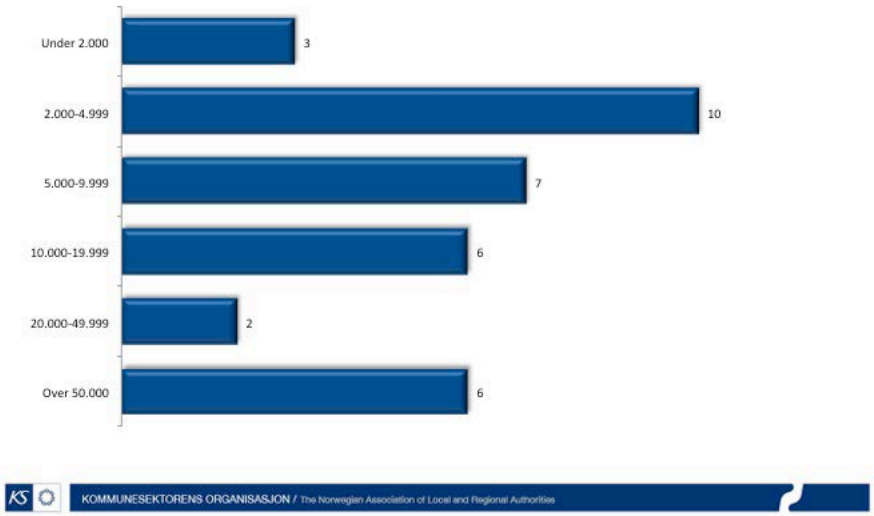
49: Har kommunen/fylkeskommunen tatt i bruk skytjenester?



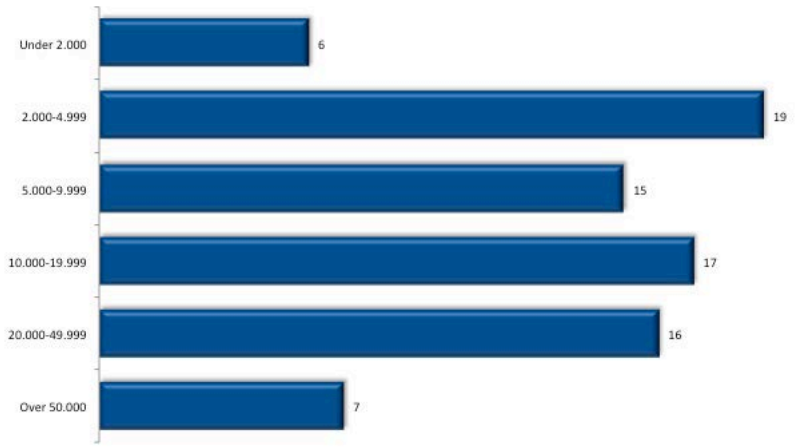
50: Infrastruktur-/lagringstjenester (f.eks. Dropbox, Skydrive/ Onedrive, Google Drive)



50: Standardapplikasjoner (f.eks. Ms Office 365, Google apps, web-basert epost)

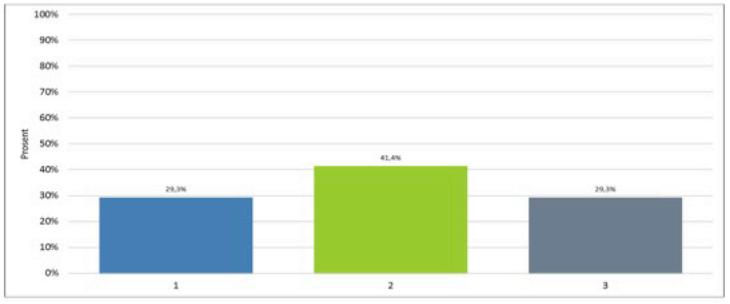


50: Web-baserte plattformer/fagsystemer (f.eks. Fronter, It's learning)



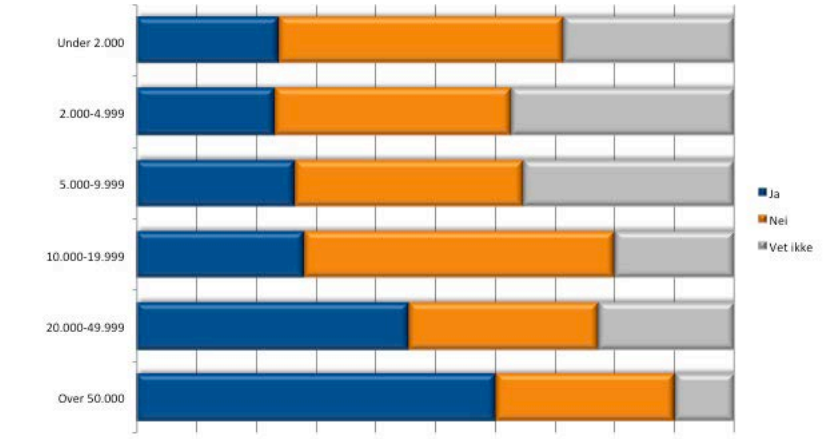
Personvern, taushetsplikt og informasjonssikkerhet

Er det gjennomført grundige sikkerhets- og sårbarhetsanalyser for de skytjenester som er tatt i bruk?



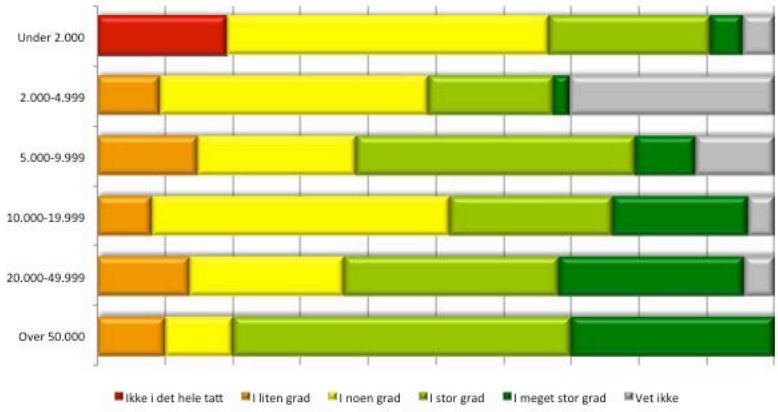
Ja	29,3%
Nei	41,4%
Vet ikke	29,3%

51: Er det gjennomført grundige sikkerhets- og sårbarhetsanalyser for de skytjenester som er tatt i bruk?



KS KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

64: I hvilken grad har kommunen/fylkeskommunen lagt til rette for opplæring i Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren?



KS KOMMUNESEKTORENS ORGANISASJON / The Norwegian Association of Local and Regional Authorities

VEDLEGG E

KINS – innspill Kommune CERT

KINS
Kommunal Informasjonssikkerhet

INNSPILL FRA KINS ANG. KOMMUNE CERT

De fleste kommuner/fylkeskommuner bruker tilnærmet de samme IT verktøy, både fagsystemer og operativsystemer/databaser. De har også i stor grad en IT infrastruktur (nettverk, servere, klienter, virtualisering. etc) basert på lik teknologi.

KINS ser derfor et stort behov for en felles døgnåpen Kommune CERT, som kan holde seg oppdatert og raskt varsle kommunene om svakheter/sårbarheter/trusler i så vel fagsystemer som standard programvare og teknologi.

Et Kommune CERT må også kunne stille opp på kort varsel for å bistå kommuner som f.eks er rammet av et større virus-angrep eller andre kritiske problemer. En CERT bør også kunne drive rådgivning ang IT sikkerhet, og f.eks gjennomføre penetrasjonstesting på oppdrag. Det er også naturlig at CERTen holder god kontakt med leverandører, både av viktige fagsystemer og hyllevare-leverandører, som Microsoft, Apple, Google, Cisco, Checkpoint, m.fl. Et Kommune CERT må være med i den nasjonale beredskapsorganisasjonen.

KINS ser også at det hadde vært formålstjenelig å opprette et Norsk Kommune Nett (NKN) på samme måte som Norsk Helse Nett. Enkelte kommuner blir i dag delvis overvåket av - og får varslinger fra - NHN/Helse-CERT. Men dette gjelder bare de kommuner som er med i et beskyttelses-program, og bare for «Sikker sone».

Et lukket Kommune-nett kan overvåkes av KommuneCERT, og ha felles sikrede åpninger mot leverandører og spesielt Internett. Dermed kan en mengde angrep som i dag rammer hver enkelt kommune, som for eksempel DDOS angrep, lukes vekk ved gatewayene, uten å forstyrre produksjonen i kommunen så mye. *Et Kommune CERT må altså kunne detektere og motvirke angrep mot det lukkede kommune-nettet.*

Kommune CERT bør organiseres som et eget selskap, finansiert av det offentlige.
Det bør bygge på erfaringer fra kommune-Norge i dag, og eventuelt legges til et eksisterende bra fagmiljø.
Kommune CERT bør være en pådriver innen standardisering for kommunal IT, og koordinere aktiviteter på tvers av kommuner.

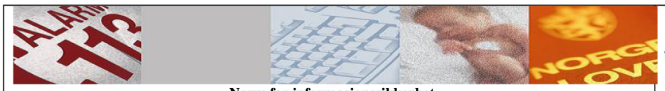
KINS har nylig opprettet et lukket *KinsFORUM*, for sine medlemmer. *Dette kan raskt og rimelig videreutvikles til å bli et «varslings-CERT» for kommuner*, basert på varsler fra Helse-CERT, Telenor CERT, og andre. Dette vil trolig kunne gjennomføres med noen få ekstra årsverk, for eksempel tilknyttet IT sikkerhetsavdelingen i Bærum kommune, eller andre kommuner med fokus på IT sikkerhet. KINS kan i tilfelle utgjøre et styre for virksomheten, eventuelt sammen med andre aktører.

Konklusjon:
KINS anbefaler at det skaffes midler til å videreutvikle KinsFORUM til å bli et fungerende «varslings-CERT» G-ISAC for alle kommuner og fylkeskommuner. Dette kan etter hvert gradvis videreutvikles til å omfatte etableringen av et lukket Kommune Nett, og fulle CERT funksjoner, som beskrevet ovenfor.

Med hilsen
Stein Fotland Leder KINS

VEDLEGG F

Norm for informasjonssikkerhet –faktaark nr. 8



Utgitt med støtte av: Helsedirektoratet

Avviksbehandling

Støttedokument
Faktaark nr 8
Versjon: 4.0
Dato: 12.2.2015

Formål	Formålet med avviksbehandling er å: • Håndtere sikkerhetsbrudd på en systematisk måte • Gjenopprette normaltilstanden etter et sikkerhetsbrudd • Vurdere endringer i sikkerhetsarbeidet for å hindre fremtidige sikkerhetsbrudd • Sikre at Datatilsynet varsles ved uautorisert utlevering av helse- og personopplysninger		
Ansvar	Den enkelte medarbeider er ansvarlig for å rapportere avvik. Virksomhetens ledelse er ansvarlig for å behandle avvik og iverksette tiltak.		
Gjennomføring	Ved avvik fra etablerte sikkerhetstiltak og prosedyrer.		
Omfang	Alle virksomheter som behandler helse- og personopplysninger skal ha prosedyrer for håndtering av avvik.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☒ Forskningsansvarlig ☒ Prosjektleder forskning ☒ Sikkerhetsleder	☒ Ansatt / medarbeider ☒ Forsker ☒ Personvernombud	☒ IKT-ansvarlig ☒ Databehandler ☐ Leverandør
Hjemmel	• Personopplysningsforskriften § 2-6		
Referanser	• Norm for informasjonssikkerhet, kap 6. 3 Avvikshåndtering • Faktaark 41 - Skadereparasjon når data har blitt utilsiktet utlevert		

Avvik er brudd på etablert regelverk og prosedyrer som skal sikre konfidensialitet, integritet og tilgjengelighet. For å sikre at regelverket følges skal det etableres avviksbehandling slik at årsak til avviket, korrigerende tiltak og rapportering blir dokumentert.

En prosedyre for avvikshåndtering må spesielt:
- Definere en fast mottaker av avviksmeldinger
- Beskrive hvordan avviksmeldingen håndteres hos mottaker
- Beskrive hvem som er ansvarlig for håndteringen
- Gi veiledning i hva som er et avvik (for eksempel: utskift kommer på feil skiver, bærbart utstyr blir stjålet, papirjournal ligger åpent tilgjengelig, bruker går fra arbeidsstasjonen usikret, bruker låner ut brukernavn og passord til andre, brukers tilgang blir ikke fjernet ved fratredelse, helse- og personopplysninger blir sendt i usikret e-post, autorisert bruker får ikke tilgang, urettmessig tilegnelse av taushetsbelagte opplysninger {snoking}, urettmessig bruk av nødrettstilgang)
- Gi eksempler på hva som ikke er et avvik; bruker får ikke logget på PC, planlagt nedetid for systemet, planlagt oppdatering av systemet
- Melde avvik som skyldes eksterne kommunikasjonsparter til ekstern part, samt sørge for at ekstern part gir tilbakemelding om oppfølging av avviket

Prosedyren bør inneholde:
- Hvordan og til hvem avvik skal rapporteres
- Identifisere årsaken til avviket
- Planlegge og gjennomføre tiltak for å hindre gjentagelse
- Samle inn og sikre hendelsesregistre og eventuelle andre bevis
- Kommunikasjon med brukere som berøres av eller er involvert i gjenopprettingen
- Plassere ansvar for å lukke avviket

Det anbefales å benytte et felles avvikssystem i virksomheten. Da er det er viktig å kunne skille avvik mellom ulike områder (for eksempel medisinsk sikkerhet, personellsikkerhet (HMS), informasjonssikkerhet).

Eksempel på forløp av avviksbehandling kan være:

Nr	Aktivitet	Beskrivelse
1.	Oppdage og rapportere avviket	Avvik kan avdekkes på ulike måter: - Ansatte oppdager at informasjon er kommet på avveie, IKT-driftspersonell avdekker sikkerhetsbrudd som manglende tilgang, uautorisert tilgang osv - Melding om avvik kan også komme fra databehandler eller gjennom automatiske varslingsfunksjoner. Alle ansatte har plikt til å melde fra om avvik - Avvik rapporteres iht prosedyre. I større virksomheter kan det være naturlig at en sikkerhetskoordinator eller lignende rolle utpekes som mottaker av avviksrapporten og som ansvarlig for å iverksette strakstiltak. - I forbindelse med elektronisk samhandling er det viktig at store virksomheter klargjør for kommunikasjonsparter hvem som skal varsles og hvem som har ansvar for å følge opp avvik som er relatert til samhandlingen
2.	Iverksette strakstiltak	- Nødvendige strakstiltak, dvs. tiltak for å stoppe avviket og begrense skadeomfanget må iverksettes så raskt som mulig - Strakstiltakene bør besluttes av den som er ansvarlig for å håndtere avviket i samarbeid med eventuelt berørte parter og annen nødvendig kompetanse, f.eks. IKT-driftsavdeling - Opplysninger om hva som er besluttet og av hvem, hva som er utført og av hvem skal dokumenteres på avviksskjema. Eksempler på strakstiltak er å stenge tjenester i nettverket og stenge brukerkontoer
3.	Samle inn og sikre hendelsesregistre og eventuelle andre bevis	- Tekniske spor, hendelsesregistre o.l. som kan bidra til å klargjøre årsakssammenheng for avviket bør samles inn så raskt som mulig - Hvis avviket kan medføre politianmeldelse bør relevante komponenter (IKT-systemer, hendelsesregistre, osv.) beskyttes mot endringer (frakobles nettverk, speilkopieres, mv.) for å kunne benyttes som evt. bevismateriale
4.	Korrigerende tiltak	- Korrigerende tiltak er de mer langsiktige endringene som gjennomføres som konsekvens av avviket - De korrigerende tiltakene skal fjerne/redusere årsaken til avvikene og kan innebære mer omfattende endringer i IKT-systemer, organisasjonen og prosedyrer - Iverksetting av korrigerende tiltak bør også innebære en vurdering av strakstiltakene som er innført og hvorvidt disse skal opprettholdes eller endres
5.	Vurdering av tiltak	- Tiltakene som er innført bør vurderes etter en tid. Det bør vurderes om tiltakene har vært hensiktsmessige, hvorvidt de er effektive for å hindre sikkerhetsbrudd og om de har hatt utilsiktede konsekvenser som eksempelvis mangelfull tilgang til systemer, redusert funksjonalitet i IKT-systemene, mv. Denne vurderingen bør være en del av ledelsenes årlige gjennomgang av informasjonssikkerheten - Har avviket vært omfattende bør det gjennomføres en risikovurdering for å avklare om etablerte tiltak er tilstrekkelige. - Ved uautorisert utlevering av helse- og personopplysninger skal Datatilsynet varsles. Videre kan virksomhetens ledelse vurdere om den registrerte (pasient, pårørende, osv) skal informeres.

www.norsis.no