Nasjonal sikkerhetsmyndighet

Sist oppdatert: 2015-05-19

Åpenhet om IKT-hendelser - nasjonale anbefalinger

Anbefalinger om åpenhet rundt IKT-hendelser

Innledning

Norske virksomheter opplever stadig flere dataangrep. Både olje- og energibransjen, norske banker, myndigheter og industriselskaper har tidligere opplevd dataangrep, og dataspionasje.

Deling av informasjon er viktig for å sette virksomhetene i bedre stand til å forebygge, avdekke og håndtere slike hendelser. NSM har, som det nasjonale fagmiljøet for IKT-sikkerhet, på oppdrag fra Justis- og beredskapsdepartementet, utarbeidet anbefalinger for hvordan offentlige og private virksomheter bør vurdere åpenhet om IKT-hendelser. Anbefalingene er laget i samarbeid med Direktoratet for forvaltning og IKT (Difi), Norsk senter for informasjonssikring (NorSIS), Politidirektoratet (POD) og Næringslivets sikkerhetsråd (NSR).

Når en virksomhet vurderer åpenhet vil det være en rekke kryssende hensyn, men NSMs klare anbefaling er at åpenhet innenfor forsvarlige rammer vil ha stor samfunnsmessig nytte. Gjennom deling av informasjon legger virksomheten også til rette for selv å kunne motta bistand til håndtering av hendelsen. Deling av informasjon om hendelser tilrettelegger for læring og bedre forebygging, både i egen virksomhet og hos andre.

Ulike kategorier for åpenhet

Åpenhet kan inndeles i tre ulike kategorier.

1. Enkelte hendelser kan være underlagt en lovbestemt *rapporteringsplikt*, og åpenheten vil da bestå i at virksomheten rapporterer hendelsen til et eller flere myndighetsorganer.
2. Åpenhet kan bestå av målrettet *deling* av informasjon med berørte aktører, og slik være en forutsetning for en god håndtering.
3. Åpenhet vil kunne omfatte en *offentliggjøring* av hendelsen for eksempel i media.

Nedenfor følger anbefalinger knyttet til hvordan virksomheter bør forholde seg til de ulike åpenhetskategoriene.

Rapportering og anmeldelser

Flere regelverk stiller krav til rapportering av IKT-hendelser. Dette gjelder for eksempel:

- rapportering til NSM om hendelser av betydning for rikets sikkerhet eller vitale nasjonale sikkerhetsinteresser, i henhold til sikkerhetsloven.
- rapportering til Datatilsynet ved IKT-hendelser som har medført uautorisert utlevering av personopplysninger, i henhold til forskrift til personopplysningsloven.
- rapportering til ulike tilsynsmyndigheter, i henhold til regelverk innenfor den enkelte sektor.

Tilsynsmyndigheter må ha et best mulig bilde av sikkerhetstilstanden for både å kunne videreutvikle sikkerhetstiltak og gi råd og veiledning til virksomhetene. Virksomheter som er utsatt for IKT-hendelser bør

også rapportere/anmelde disse til politiet for å muliggjøre etterforskning og eventuell straffesaksforfølging. Mørketallsundersøkelsen fra NSR og NSMs erfaring indikerer at det i dag er en underrapportering av hendelser.

Det er derfor viktig at virksomheter underlagt slik rapporteringsplikt følger opp denne, og samtidig vurderer anmeldelse til politiet der dette er relevant. Dette vil komme både egen, og andre virksomheters sikkerhet til gode. Slik rapportering bør skje så raskt som mulig og i henhold til bestemmelser i gjeldende sektorregelverk.

Deling

Formålet med deling av informasjon om IKT-hendelser er å sette andre virksomheter og myndighetene i stand til å forebygge, avdekke og håndtere hendelser.

Når en hendelse inntreffer bør virksomheten eller driftsleverandør varsle og dele informasjon så raskt som mulig for å bidra til en best mulig operativ håndtering av hendelsen. Rask deling er påkrevd for at informasjonen skal ha verdi for mottaker.

Informasjonen som deles bør være så detaljert at mottaker kan iverksette nødvendige egenbeskyttelsestiltak basert på informasjonen. Mangel på detaljert informasjon om en hendelse bør likevel ikke være til hinder for deling. Informasjon som ikke er detaljert vil også kunne være av verdi for andre ved å synliggjøre at IKT-angrep foregår, og kunne bidra til å sette sammen et helhetsbilde som flere kan nyttiggjøre seg av.

Informasjon bør deles med sektorvise responsmiljøer, slik at andre virksomheter som kan være berørt blir varslet. Informasjon bør også deles med Norsk senter for informasjonssikring (NorSIS). Gjennom NorSIS vil informasjon kunne tilrettelegges og formidles til små og mellomstore virksomheter som ikke er knyttet til et sektorvis responsmiljø.

Videre bør informasjonen deles bredt med politi og med andre relevante offentlige myndigheter. Deling av informasjon bør skje i så stor utstrekning som mulig. Det er ingen absolutte begrensninger for informasjonsdeling utover hva som følger av lovbestemt taushetsplikt. Der politiet har etablert en etterforskningssak, eller et tilsynsorgan har en sak til behandling, bør deling skje etter samråd med disse. Der statlige aktører kan stå bak, og saken håndteres av EOS-tjenestene, bør en eventuell informasjonsdeling skje i tett samarbeid med disse.

Gjennom deling av informasjon legger virksomheten til rette for også selv å kunne motta bistand til håndtering av hendelsen.

Det er også viktig at erfarte hendelser deles for å tilrettelegge for læring og bedre forebygging både i egen virksomhet og hos andre. Erfaringer fra håndtering av hendelser bør derfor i etterkant deles med både de overnevnte aktører, samt bransjeorganisasjoner og relevante interesseorganisasjoner.

Justis- og beredskapsdepartementet (JD), i samarbeid med Forsvarsdepartementet (FD), er i ferd med å etablere en struktur for håndtering av IKT-hendelser. Dette skjer gjennom en målrettet oppbygning av sektorvise responsmiljøer med relasjoner til sektorens virksomheter og NSM NorCERT. Dette er forankret i nasjonal strategi for informasjonssikkerhet med handlingsplan. Herunder er det utarbeidet en modell for

hvordan samarbeidet skal foregå mellom aktørene i strukturen.[1]Modellen forutsetter at virksomhetene deler informasjon med sitt sektorvise responsmiljø. Dette miljøet har ansvar for å tilrettelegge for informasjonsdeling, og videreformidle informasjon til og fra virksomhetene i sektoren.

De sektorvise responsmiljøene skal sikre at alle relevante aktører mottar korrekt varslingsinformasjon og settes i stand til å gjøre nødvendige tiltak. Miljøene vil ha en bistandsfunksjon mot virksomhetene og er også sektorens bindeledd mot NSM NorCERT. Der sektorvise responsmiljøer enda ikke er etablert, bør informasjon deles med NSM NorCERT og NorSIS.

Den endelige beslutning om å dele informasjon om IKT-hendelser, og sette betingelser for bruk av informasjonen, ligger hos den enkelte virksomhet. Deling av informasjon er ikke ensbetydende med at den gjøres allment kjent. Offentliggjøring av informasjon behandles nedenfor.

Offentliggjøring

Enkelte aktører(som Telenor, Statoil og Forsvaret) har de siste årene vært åpne om IKT-hendelser de har vært utsatt for, men fortsatt er det slik at IKT-hendelser i liten grad blir offentliggjort.

Offentliggjøring er viktig for å informere befolkningen og mindre virksomheter om forhold som kan påvirke forretningsdrift, offentlige tjenester og hverdagslivet. Media vil være en viktig kanal for å nå fram til innbyggerne og små og mellomstore bedrifter.

Offentlighet om IKT-hendelser vil ha stor samfunnsmessig nytte. Gjennom proaktiv offentliggjøring synliggjøres behovet for god sikkerhet, og hva som faktisk skjer på internett. Dette vil bidra til økt sikkerhetsbevissthet både hos virksomhetene og i samfunnet. Større grad av offentlighet om hendelser vil også bidra til å vise at for eksempel dataangrep kan ramme alle virksomheter i offentlig og privat sektor, og således å avmystifisere dette. En stor grad av offentlighet rundt IKT-hendelser vil legge til rette for en åpenhetskultur og gjøre det enklere for andre virksomheter å informere om hendelser hos seg. Gjennom offentliggjøring blir det også lettere å oppnå aksept og forståelse for behovet for god informasjonssikkerhet i offentlige og private virksomheter og i samfunnet som helhet.

På den annen side må offentliggjøring av informasjon om IKT-hendelser praktiseres på en slik måte at taushetspliktbestemmelser ivaretas. De samfunnsmessige fordeler av offentliggjøring må også vurderes opp mot mulige negative konsekvenser, for eksempel om offentlighet kan utnyttes av trusselaktører til handlinger som kan ha store negative konsekvenser. Offentliggjøring bør heller ikke skje der dette kan være ødeleggende for en forsvarlig håndtering av saken.

Til hjelp til gjennomføring av vurderingen

Det er den enkelte virksomhet selv som må beslutte om man vil gå offentlig ut med en IKT-hendelse.
Nedenfor følger noen råd til støtte for virksomhetenes vurdering:

- Er hendelsen eller elementer av denne av en slik karakter at allmenheten bør kjenne til dette?
- Kan offentliggjøring bidra til å forebygge hendelser i andre virksomheter?

[1] Skriv fra JD til departementene av 18.11.14

- Ønsker virksomheten selv å gå offentlig ut eller er det mest hensiktsmessig at bransje- eller interesseorganisasjon eller sektorvise responsmiljø brukes som kanal for å unngå unødig eksponering av den aktuelle virksomhet?
- Risiko, og eventuelt skadepotensiale knyttet til offentliggjøring, må vurderes før en hendelse offentliggjøres.
- Det bør vurderes om sårbarheter som førte til hendelsen fortsatt kan utnyttes.
- Det bør generelt sett utvises større varsomhet med offentliggjøring mens en hendelse pågår, herunder hvor detaljert informasjon som kan offentliggjøres, enn rundt informasjon om en avsluttet hendelse.
- Ved offentliggjøring av tilsiktede hendelser bør det utvises varsomhet slik at detaljer om virksomhetenes og myndighetenes håndtering av hendelsen ikke eksponeres på en uønsket måte.
- Ved håndtering av hendelser der fremmede stater antas å stå bak bør offentliggjøring skje etter samråd med EOS-tjenestene.
- Offentliggjøring bør ikke skje der dette kan skade muligheten for effektiv håndtering av hendelsen, eller politiets etterforskning.
- Er virksomheten i tvil om hendelsen bør offentliggjøres eller ikke, kontakt ekspertmiljøer som for eksempel egen sektor CERT, NorCERT eller NorSIS for å motta råd og veiledning.

Vurdering av åpenhet som en del av øvelser

IKT-hendelser bør være en integrert del av virksomheters øvelser i krisehåndtering. Virksomhetene anbefales å øve håndtering av IKT-hendelser som del av scenarier hvor målsettingen er å opprettholde drift og tjenesteleveranse. Åpenhet om IKT-hendelser bør inngå som et moment i slike øvelser for å bygge erfaring knyttet til vurderinger rundt dette.

Kontaktpunkter

NSM kan kontaktes for spørsmål knyttet til disse anbefalingene. Det vises også til internettsidene til Næringslivets Sikkerhetsråd (nsr-org.no) og Norsk senter for informasjonssikkerhet (norsis.no).