Rammeverk for håndtering av IKT-sikkerhetshendelser
—prinsippskisse

SCENARIO 1: Uautorisert tilgang til informasjon, forsøk på eller vellykket kompromittering av IKT-systemer hos en virksomhet

Er kritisk infrastruktur og/eller kritiske samfunnsfunksjoner rammet eller i fare for å rammes?

Ja

Varsle sektorvise responsmiljø (SRM)

- SRM varsler NSM
- Virksomhet utfører tiltak for å gjenopprette sikker tilstand på systemene, evt. i samarbeid med ekstern avtalepart og/eller SRM
- Virksomhet informerer overordnet myndighet
- Virksomhet varsler politiet for bistand innenfor politiets fullmakter og/eller for å anmelde
- SRM bistår eventuelt virksomhet i sin hendelseshåndtering, og koordinerer håndteringen i sektor og mot NSM

Nei

Virksomhet håndterer hendelsen internt, evt. i samarbeid med ekstern avtalepart

Virksomhet varsler evt. SRM for råd og veiledning om håndtering av hendelsen

Virksomhet anmelder forholdet til politiet

Politiet kan be NSM om informasjon om tekniske indikatorer etc. i forbindelse med en etterforskning. NSM kan dele informasjonen med politiet etter samtykke fra virksomhet

NSM

- Bistår SRM/ virksomheter med analyser, koordinerer informasjonsdeling og utarbeider nasjonalt situasjonsbilde som beslutningsgrunnlag til strategisk ledelse
- Leder og deltar i FCKS
- Rapporterer til JD, FD, lederdepartement, FCKS, SRM, virksomheter tilknyttet VDI, evt. andre berørte virksomheter

PST

- Innhenter informasjon om personer og grupper som kan utgjøre en trussel, utarbeider analyser og trusselvurderinger samt etterforsker
- PST deltar i FCKS
- Rapporterer til JD, lederdepartement og FCKS

POLITIET (KRIPOS)

- Bistår i gjenopprettelse av sikker tilstand gjennom håndtering av konsekvenser og bruk av tvangsmidler og/eller maktbruk for å stanse angrep
- Sikrer tekniske spor, gjør beslag, pågripelser og etterforskning
- Rapporterer til JD, lederdepartement og evt. til berørte virksomheter

SEKTORDEPARTEMENT

- Samhandler med SRM for å etablere situasjonsbilde for egen sektor
- Vurderer behov for å iverksette tiltak i egen sektor
- Rapporterer til regjeringen eller lederdepartement

FCKS

- Koordinerer håndtering av hendelser under senterets arbeidsområde
- Utøver vurderinger av hendelser i innledende fase av håndtering
- Understøtter partenes operative oppgaveløsing
- Anbefaler håndterende part om hvilke spor og eventuelle tiltak som bør gjennomføres

Etter at **angrepet er stanset** og sikker **tilstand gjenopprettet**, bør virksomheter som har vært angrepet alltid gjøre følgende:

- Anmelde forholdet til politiet, dersom dette ikke allerede er gjort
- Rapportere hendelsen til NSM i henhold til rammeverk vedlegg 5 "vurdering av IKT-sikkerhetshendelser"
- Evaluere virksomhetens håndtering av hendelsen og justere prosedyrer/beredskapsplanverk i henhold til læringspunkter

SCENARIO 2: Uautorisert tilgang til informasjon, forsøk på eller vellykket kompromittering av IKT-systemer som tilhører privatpersoner

Er det grunn til å tro at personen(e) er rammet som følge av at de besitte samfunnskritiske posisjoner, har tilgang til gradert informasjon eller på annen måte kan knyttes til kritisk infrastruktur eller kritiske samfunnsfunksjoner?

Ja

Gå til Scenario 1

Nei

Personen varsler Datatilsynet når det har skjedd en uautorisert utlevering av personopplysninger som krever konfidensialitet, tilsiktet eller utilsiktet

Personen anmelder forholdet til sitt lokale politikontor

Politiet kan be NSM om informasjon om tekniske indikatorer etc. i forbindelse med en etterforskning. NSM kan dele informasjonen med politiet etter samtykke fra virksomhet