Klassifisering av IKT-sikkerhetshendelser[1]

1 Formål med klassifisering av IKT-sikkerhetshendelser

Klassifisering av hendelser gjøres for å kunne kommunisere effektivt og presist om en hendelse mens hendelseshåndteringen pågår og for å etablere et konsistent statistisk grunnlag å basere analyser og tiltak på.

2 Klassifisering av IKT-sikkerhetshendelser

Klassifiseringen er basert på en internasjonal taksonomi fra eCSIRT.net-prosjektet[2]. Engelske navn fra eCSIRT-taksonomien står i parentes.

Klassifisering	Beskrivelse/eksempler
A. Uautorisert tilgang til informasjon (Information Content Security)	Vellykket uautorisert tilgang til informasjon eller funksjoner på systemer eller tjenester. Resultatet kan være kompromittering av konfidensialitet, integritet og/eller tilgjengelighet. Dette dekker også tilgang til informasjon under overføring.
B. Kompromittering (Intrutions)	Vellykket uautorisert tilgang til system eller tjeneste. Ingen tegn til aktivitet på målet.
C. Forsøk på kompromittering (Intrusion Attempts)	Forsøk på kompromittering av systemer eller tjenester ved for eksempel å lure autorisasjonssystemet, gjette passord, utnytte sårbarheter i systemet eller feil i oppsett. Mye brukt metode er også å lure legitime brukere til å starte skadelig programvare på interne systemer.
D. Tjenestenekt (Availability)	I denne typen angrep blir systemet bombardert med så mye trafikk at tjenester går ned eller blir mindre responsive.
E. Svindel (Fraud)	Bruk av ressurser for å tjene penger, for eksempel misbruk av domenenavn eller epostadresser. Salg eller installasjon av materiale beskyttet av copyright. Bruk av andres identitet.
F. Rekognosering/ informasjonsinnsamling (Information Gathering)	Informasjonsinnsamling om målet via for eksempel åpne kilder, skanning av nettverksinfrastruktur og tjenester som er åpne mot Internett, sniffing på nettverkstrafikk, sosiale nettverk eller direkte kontakt for eksempel via telefon.
G. Støtende innhold (Abusive Content)	Spam eller reklame fra parter som ikke har innhentet tillatelse til utsendelse. Plaging, trusler eller forfølgelse via digitale kanaler. Distribusjon av barnepornografi eller forherligelse av vold.

[1] Vedlegg 5 «Klassifisering av IKT-sikkerhetshendelser» vil på sikt erstattes av et vedlegg som redegjør for rapporteringsformatet av IKT-sikkerhetshendelser, der klassifisering av hendelser er ett av elementene. Nasjonal sikkerhetsmyndighet vil arbeide sammen med sektorvise responsmiljøer i tiden fremover for å videreutvikle rapporteringsformatet.

[2] For videre lesning - https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies

3 Kategorisering av mål

Mål refererer til hvem som er utsatt for en hendelse og hvor hendelsen inntreffer. Mål er delt inn i følgende kategorier:

1. *[3]Tverrsektorielt (virksomheter fra flere sektorer er involvert)
2. *Sektor (flere virksomheter fra samme sektor er involvert)
3. *Virksomhet (kun en involvert virksomhet)
4. Tverrsektorielt (som tverrsektorielt ovenfor)
5. Sektor (som sektor ovenfor)
6. Virksomhet (som virksomhet ovenfor)
7. Privatperson (en/flere privatpersoner, uten spesiell knytning til virksomhet)

3.1 Målsektor

For å oppnå presise valg av målkategori må virksomheten og sektoren selv identifisere hvilke mål som tilhører virkeområdet til rammeverk for håndtering av IKT-sikkerhetshendelser. Identifiseringen bør skje gjennom risiko- og sårbarhetsanalyser i virksomhet og sektor, og er et sektoransvar. Slike virksomheter bør tydelig fremkomme av sektorens aktørkart. Figuren nedenfor lister opp departementene, som selv må vurdere samfunnsområder - knyttet til virkeområdet til rammeverk for håndtering av IKT-sikkerhetshendelser.

Departement	**Sektor**	**(Avgrensede) samfunnsområder**
Arbeids- og sosialdepartementet (ASD)		Avhengig av vurdering av/i sektor
Barne- og likestillingsdepartementet (BLD)		Avhengig av vurdering av/i sektor
Finansdepartementet (FIN)	SRM (FinansCERT)	Finans
Forsvarsdepartementet (FD)	SRM (BKI/MilCERT)	Forsvar
Helse- og omsorgsdepartementet (HOD)	SRM (HelseCERT)	Helse
Justis- og beredskapsdepartementet (JD)	SRM (JustisCSIRT)	Justis
Klima- og miljødepartementet (KLD)	SRM (MiljøCERT)	Miljø
Kommunal- og moderniseringsdepartementet (KMD)		Avhengig av vurdering av/i sektor
Kulturdepartementet (KUD)		Avhengig av vurdering av/i sektor
Kunnskapsdepartementet (KD)	SRM (UNINETT CERT)	Forskning og høyere utdanning Meteorologiske tjenester
Landbruks- og matdepartementet (LMD)		Avhengig av vurdering av/i sektor

[3] * = Med kritisk infrastruktur og/eller kritiske samfunnsfunksjoner.

Nærings- og fiskeridepartementet (NFD)		Avhengig av vurdering av/i sektor
Olje- og energidepartementet (OED)	SRM (KraftCERT)	Kraft Andre – avhengig av vurdering av/i sektor
Samferdselsdepartementet (SD)	SRM (NkomCSIRT)	Ekom Andre – avhengig av vurdering av/i sektor
Utenriksdepartementet (UD)		Avhengig av vurdering av/i sektor
Statsministerens kontor (SMK)	N/A	

4 Vurdering av alvorlighetsgrad ved IKT-sikkerhetshendelser

Gjennom vurdering av en IKT-sikkerhetshendelse oppnås en kortverdi som enkelt kan rapporteres eller benyttes i oversiktsbilder. Eksempelvis vil kompromittering i flere virksomheter innen en sektor, uten at kritisk infrastruktur eller kritiske samfunnsfunksjoner er involvert, gi verdien B5. Denne benevnelsen bør benyttes ved rapportering av IKT-sikkerhetshendelser.

Vurdering av alvorlighetsgrad kan variere fra virksomhet til virksomhet og mellom sektorer, blant annet fordi digital hendelseshåndtering er knyttet til virksomhetens verdier og funksjon. Metoden i dette vedlegget kan være et godt utgangspunkt for vurdering av alvorlighetsgrad. I en vurdering av alvorlighetsgrad er også faktorer som situasjon og trusselaktør relevant, hvis dette er kjent.