Vedlegg L

SKJEMA FOR VARSLING AV DIGITALE ANGREP

INFORMASJON OM VIRKSOMHETEN	
Navn virksomhet:	
Org.nr.:	
Vakttelefon:	
Firma epost:	
Nettside:	
Hvilken sektor(er) tilhører virksomheten:	

INFORMASJON OM MELDER	
Ditt navn:	
Din rolle:	
Mobil:	
E-post:	***Et ikke-kompromittert system*** *som korrespondanse kan sendes til*
Din virksomhets e-post	*For referanseformål - vil ikke bli brukt til korrespondanse*
Evt. annen kontaktperson:	

INFORMASJON OM HENDELSEN	
Beskrivelse av hendelsen:	
(a) Hendelsens natur	
(b) Når oppstod hendelsen	
(c) Antall brukere som potensielt er berørt	
(d) Geografisk utbredelse	
(e) Omfanget av evt. avbrudd i tjenester/ leveranser	
(f) Årsaken til hendelsen	
(g) Mulige konsekvenser for Forsvaret	
(h) Mulige økonomiske og samfunnsmessige	

konsekvenser	
Er meldingen kun til informasjon eller ønskes råd/assistanse:	
Allerede iverksatte tiltak:	
Antatt påvirkning:	[Ingen/liten/moderat/stor/katastrofal/ukjent]
Kan data være stjålet, endret eller slettet?	
Kan det foreligge brudd på personopplysningssikkerhet for Forsvarets personell:	
Status på hendelsen:	[Akkurat oppdaget/pågående undersøkelser/gjenopprettet kontroll/gjenopprettet funksjoner/avsluttet sak]
Andre som er varslet om hendelsen:	[Konsulentselskaper/Datatilsynet/Kripos/andre myndigheter]

SIGNATUR	
Sted /dato:	
Signatur:	

HVOR SKAL MELDINGEN SENDES	
Mottaker:	***MILCERT***
E-post:	*Cyfor.css.kontakt@mil.no (ugradert)* *ressurs_001074@mil.no (gradert BEGRENSET)*
Adresse:	*Jørstadmovegen 600, 2625 Fåberg*
Telefon:	*+47 61 10 3812 (dagtid 0730-1530)*
Kopi til:	***NSM Nasjonalt cybersikkerhetssenter (NCSC)***
E-post:	*cert@ncsc.no (ugradert)* *ncsc-hh@nsm.nb-nett.no (gradert BEGRENSET)*
Telefon:	*02497 (+47 23 31 07 50) (Døgnbemannet)*
Web:	*https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter*

OM MILCERT OG HÅNDTERING AV INFORMASJON

Cyberforsvaret ved Cyberforsvarets cybersikkerhetssenter (CSS) ivaretar den sektorvise responsfunksjonen for alvorlige digitale angrep mot forsvarssektoren (MilCERT). MilCERT skal bidra til å beskytte Forsvarets operasjoner mot digitale angrep. Videre skal MilCERT bidra til å iverksette ekstraordinære beskyttelses- og håndteringstiltak for å hindre eller stoppe digitale angrep, redusere skaden og håndtere konsekvensene av digitale angrep.

Ved varsling til MilCERT vil denne, sammen med berørte enheter i sektoren, vurdere i hvilken grad hendelser kan få konsekvenser for forsvarssektorens virksomhet. Dette skal sikre at det gjøres nødvendige skadevurderinger for forsvarssektoren og at det ytes bistand til koordinering og håndtering av hendelsen i sektoren. MilCERT kan også bidra til å hindre eller begrense videre spredning av en digital trussel i samarbeid med NSM NCSC.

Informasjon som deles med MilCERT, skriftlig eller muntlig, behandles konfidensielt. Dette gjelder uavhengig av om informasjonen er merket eller uttalt å være konfidensiell/fortrolig eller ikke. Alle ansatte i MilCERT har taushetsplikt om forhold de blir kjent med gjennom MilCERT sin virksomhet. Informasjon som gjelder hendelser vil bare gjøres tilgjengelig for personell i MilCERT med et tjenstlig behov for tilgang. Dersom informasjon om hendelser utgjør innsideinformasjon, vil informasjonen bli behandlet i samsvar med Forsvarets instruks for håndtering av innsideinformasjon.

OM NCSC OG HÅNDTERING AV INFORMASJON

Nasjonal sikkerhetsmyndighet (NSM) ved Nasjonalt cybersikkerhetssenter (NCSC) ivaretar den nasjonale responsfunksjonen for alvorlige digitale angrep og det nasjonale varslingssystemet for digital infrastruktur (VDI). NCSC skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot digitale angrep, herunder Forsvaret.

Ved varsling til NCSC kan NCSC yte bistand til koordinering og håndtering av hendelsen. NCSC kan også bidra til å hindre eller begrense videre spredning av en digital trussel.

Informasjon som deles med NCSC, skriftlig eller muntlig, behandles konfidensielt. Dette gjelder uavhengig av om informasjonen er merket eller uttalt å være konfidensiell/fortrolig eller ikke. Alle ansatte i NSM har taushetsplikt om forhold de blir kjent med gjennom tjenesten. Informasjon som gjelder hendelser vil bare gjøres tilgjengelig for personell i NSM med et tjenstlig behov for tilgang. Dersom informasjon om hendelser utgjør innsideinformasjon, vil informasjonen bli behandlet i samsvar med NSMs instruks for håndtering av innsideinformasjon.

NSM er en del av EOS-tjenestene og underlagt kontroll fra Stortingets kontrollutvalg for etterretnings- overvåknings- og sikkerhetstjenestene (EOS-utvalget). Utvalget inspiserer NSM flere ganger årlig.