Begrepsliste til bruk for rammeverk for håndtering av IKT-sikkerhetshendelser

Begrep	**Beskrivelse**
Alvorlig IKT-sikkerhetshendelse	Reelle uønskede tilsiktede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og/eller kritiske samfunnsfunksjoner.
BFF	Beredskapssystem for forsvarssektoren (se NBS)
Beredskapstiltak	Tiltak som iverksettes som respons på en reell hendelse eller trussel om hendelse for å øke sikkerhetsnivået, motstå uønskede hendelser og/eller for å kunne håndtere hendelsen effektivt dersom den inntreffer.
CERT	«Computer Emergency Response Team» er en koordinerende enhet for IKT-sikkerhet. CERT er en lisensbelagttittel. I Norge eksisterer ulike CERT-miljøer. NorCERT er det nasjonale CERT-miljøet. Se også CSIRT.
Comcheck	En kontroll som gjennomføres for å sikre at de oppgitte kommunikasjonskanalene er i drift.
CSIRT	«Computer Security Incident Response Team" er en koordinerende enhet for IKT-sikkerhet. CSIRT er ikke en lisensbelagt tittel.
Cyber	Benyttes om alt som er på internett og digitalt. Cyberspace refererer til en verden av sammenkoblede datasystemer og informasjonsressurser. Betegnelsen blir ikke benyttet i rammeverk for digital hendelseshåndtering, men sidestilles i denne sammenheng med betegnelsen «IKT».
Defensive operasjoner	Beskyttelse av egne systemer gjennom å logge, analysere, oppdage og håndtere IKT-sikkerhetshendelser.
Digital	Funksjoner som er bygget opp ved hjelp av det binære to-talls systemet, 0 eller 1 som refererer til av eller på/signal eller ikke signal. Det aller meste av datateknologi og informasjon på datamaskiner er digitalt.
Grunnsikring	Permanent funksjonalitet og beskyttelse for å gjøre systemer mindre sårbare for uønskede hendelser.
Hybride trusler	Systematisk og synkronisert bruk av flere virkemidler for å oppnå strategiske målsettinger med vesentlig skadepotesial.
Håndtering av IKT-sikkerhetshendelser	Defensive tiltak ved alvorlige IKT-sikkerhetshendelser for å stanse, gjenopprette sikker tilstand for berørte systemer, skadevurdere og skadebegrense.
IKT	IKT forstås her som alle systemer som utfører sin funksjon gjennom å sende, motta, lagre, prosessere og konvertere informasjon fra andre systemer.
IKT-sikkerhetshendelse	Situasjoner der IKT-systemer blir utsatt for tilsiktede handlinger.

IKT-sikkerhet	Beskyttelse av informasjon og systemer som er sårbare fordi de er koblet til, eller på annen måte er avhengig av IKT.
Integritet i IKT-systemer	Å sikre at IKT-systemer er korrekte, gyldige og fullstendige.
Konfidensialitet i IKT-systemer	Å sikre at IKT-systemer og informasjon i systemene bare er tilgjengelig for de som skal ha tilgang.
Krise	En ekstraordinær hendelse som rammer sivil samfunnssikkerhet og som krever at ekstraordinære tiltak iverksettes.
Kritisk infrastruktur	De anlegg og systemer som er nødvendige for å opprettholde samfunnets kritiske funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghet.[1]
Kritisk samfunnsfunksjon	De funksjonene som må opprettholdes i samfunnet for å sikre trygghet og basale fysiske behov for befolkningen.
Kryptering	Koding av informasjon slik at den blir uleselig for uvedkommende.
NBS	Nasjonalt beredskapssystem (NBS) består av Sivilt beredskapssystem (SBS) og Beredskapssystem for forsvarssektoren (BFF). NBS er et redskap for politisk styring og forankring av krisehåndteringsprosessen.[2]
Offensive operasjoner	Tiltak for å forstyrre, manipulere eller ødelegge en motstanders datasystemer (computer network attack, CNA), og/eller tiltak for å oppnå adgang til en motstanders datasystem, tappe det for informasjon og utnytte denne informasjonen (uten at motstanderen er klar over det) (computer network exploitation, CNE) som støtte til en militær operasjon.[3]
Responstid	Den tiden det tar fra en uønsket hendelse blir oppdaget, til man iverksetter det første tiltaket for å håndtere hendelsen.
Risiko	Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen (NS 5830:2012).
Risikobilde	En beskrivelse av risiko på et gitt tidspunkt. Innen forebyggende sikkerhet utgjør risikobildet en samlet vurdering av verdier, truslene mot disse og sårbarheter som eksisterer i forhold til truslene i en bestemt tidsperiode eller knyttet til en spesifikk hendelse (NS 5830:2012).
Risiko- og sårbarhetsanalyse (ROS)	En strukturert vurdering av 1) hvilke uønskede hendelser som kan komme til å skje, 2) sannsynlighet for at en uønsket hendelse vil inntreffe, 3) sårbarhet ved systemer, 4) hvilke konsekvenser hendelsen eventuelt vil få og 5) usikkerheten knyttet til vurderingene.[4]
SBS	Sivilt beredskapssystem (se NBS).
Sikkerhetspolitisk krise	En ekstraordinær hendelse som rammer statssikkerhet og som krever at ekstraordinære tiltak iverksettes, både i militær og sivil sektor. Se definisjon av *statssikkerhet.*
Skadevare (Malware)	Skadelig programvare (fra engelsk malicious software).
Skadevareanalyse	Analyse av det tekniske innholdet i skadevare.

[1] St.meld. nr. 22 (2007-2008) «*Samfunnssikkerhet»,* og DSBs rapport *«Samfunnets kritiske funksjoner»* (2016).

[2] NBS er gradert, og defineres derfor her på et overordnet nivå.

3 Fra Forsvarsdepartementets Cyberretningslinjer (2014)

[4] DSB (2014): Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen

Samfunnssikkerhet	Ivaretagelse av sivilbefolkningens liv, helse og trygghet, og sikre sentrale samfunnsfunksjoner og viktig infrastruktur mot angrep og annen skade.[5]
Statssikkerhet	Sikkerhetsbehov knyttet til statens eksistens, suverenitet og integritet. Når statssikkerheten er truet kan det legitimere innsats av mange eller alle statens tilgjengelige ressurser. Slike trusler vil ofte ha sikkerhetspolitiske aspekter.
Sårbarhet	Manglende evne til å motstå en uønsket hendelse eller opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning (NS 5830:2012).
Tilgjengelighet i IKT-systemer	Å sikre at IKT-systemer er tilgjengelig innenfor de tilgjengelighetskrav som er satt.
Tjenestenekt-angrep (DoS, DDoS)	Et internettangrep som overbelaster en server ved at stor trafikk rettes mot serveren. Hensikten er å hindre normal tilgang fra ordinære brukere.
Trussel	Mulig uønsket handling som kan gi en negativ konsekvens (NS 5830:2012).
Trusselaktør	En kjent eller ukjent aktør (person, organisasjon, land eller annen) som forbindes med en trussel (NS 5830:2012).
VDI	Varslingssystem for digital infrastruktur består av sensorer utplassert hos virksomheter som ansees som en del av kritisk infrastruktur i Norge. VDI driftes av NSM[6] og er en frivillig ordning basert på åpenhet og tillit mellom NSM og virksomheten.
Verdi	Ressurs som hvis den blir utsatt for en uønsket påvirkning vil ha en negativ konsekvens for den som forvalter eller drar fordel av ressursen (NS 5830:2012).
Verdivurdering	En analyse og vurdering som har til hensikt å identifisere hvilke objekter og hvilken type informasjon som er så viktige for virksomheten at de må skjermes.
Virksomhet	Betegnelse for en organisatorisk enhet som eksempelvis kan være et departement, et direktorat, en etat, en organisasjon eller et privat foretak. For dette rammeverket må det skilles mellom departementet som sekretariat for politisk ledelse, departementet som en virksomhet som skal ivareta egen sikkerhet, og departementet som overordnet ansvarlig for sikkerhet i egen sektor.

[5] FD og JD (2015): «*Støtte og samarbeid – en beskrivelse av totalforsvaret i dag».*
[6] www.nsm.stat.no.