Sikt
Kunnskapssektorens tjenesteleverandør

Vedlegg

Digitaliseringsstyret for høyere utdanning og forskning

Vedlegg 08A – Tjenesteoversikt, Cybersikkerhetssenter

Innledning

Dette vedlegget gir en uttømmende oversikt over tjenestene Cybersikkerhetssenteret vil levere.

Tjenestene er sortert i henhold til kategoriene i NSMs grunnprinsipper for IKT-sikkerhet (beskytte og opprettholde, oppdage, håndtere og gjenopprette), som det forventes at virksomhetene forholder seg til. Tjenester under rådgivning og kompetanseheving bidrar til virksomhetens arbeid med de organisatoriske og menneskelige sikkerhetsområdene. Dette omfatter eksempelvis personvern, ledelsessystem, sikkerhetsstyring, og beredskapsøvelser og disse tjenestene bidrar til et helhetlig og robust sikkerhetsarbeid.

Cybersikkerhetssenteret som obligatorisk fellestjeneste

Alle virksomheter som er tilknyttet forskningsnettet fra Sikt får Cybersikkerhetssenterets responsfunksjon som en del av leveransen. Dette er en koordinerende funksjon som ivaretar Sikt sine forpliktelser som nettleverandør og er kontaktleddet opp mot nasjonale sikkerhetsmyndigheter. Dette er en rolle Uninett CERT har hatt frem til nå, og som på grunn av fusjon til Sikt vil bli organisert under Cybersikkerhetssenteret.

Cybersikkerhetssenteret er utpekt som SRM av Kunnskapsdepartementet i overenstemmelse med gjeldende rammeverk for håndtering av IKT-sikkerhetshendelser og skal gjennom sitt mandat dekke alle KDs underliggende virksomheter. Som SRM er Cybersikkerhetssenteret en del av den nasjonale beredskapen og totalforsvaret.

Beskytte og opprettholde:

- Varsling og koordinering av hendelser og nettmisbruk (abuse) fra adresser i Forskningsnettet.
- Blokkering av trafikk mot IP-adresser med ondsinnet innhold
- Jevnlig informasjonsdeling om kjente trusler for kunnskapssektoren, inkludert større hendelser, som gjør sektoren i bedre stand til hendelseshåndtering

Oppdage:

- Tidlig varsling ved alvorlige sikkerhetshendelser som kan ha betydning for kunden
- Beredskapsvakt for innmelding av særlig alvorlige hendelser utenom ordinær arbeidstid.
- Kontinuerlig varsling av tekniske detaljer om kjente sårbarheter, trusler og trusselaktører (trusseletterretning)
- Ukentlig sårbarhetsscan og tilhørende rapport per virksomhet med oversikt over funn og anbefalte tiltak.

Håndtere og gjenopprette:

- Tilgang til informasjonsdeling og koordinering under større hendelser
- Bistand og rådgivning ved cyberangrep og andre alvorlige sikkerhetshendelser
- Beskyttelse mot og håndtering av tjenestenektangrep (DDoS)
- Tilgang til tillitsnettverk med deling av sensitiv informasjon via sikre kommunikasjonskanaler (forutsetter godkjent lokalt responsteam)
- Mulighet for å delta på møter som samler sektoren ved større hendelser, for å diskutere situasjonsforståelse og dele erfaringer (forutsetter godkjent lokalt responsteam)

Rådgivning og kompetanseheving:

- Tilgang til oppdatert informasjon via vår tette dialog med samarbeidspartnere nasjonalt og internasjonalt, inkludert sikkerhetsmyndigheter, sikkerhetsteam i andre sektorer, nordiske og europeiske forskningsnett, samt kommersielle leverandører.
- Tilgang til kompetansemiljø for IKT-sikkerhetsrelaterte spørsmål for alle nettkunder
- Kurs for etablering og drift av lokale hendelseshåndteringsteam
- Forum for autoriserte hendelseshåndteringsteam (IRT-forum)

Listen over tjenester er ikke uttømmende, og vil endres i takt med kundenes behov, og tilgjengelig kapasitet og kompetanse i Cybersikkerhetssenteret for forskning og utdanning.

Cybersikkerhetssenterets valgfrie fellestjeneste

Cybersikkerhetssenterets valgfrie fellestjeneste bygger på et bredt og tverrfaglig *sektorfellesskap* for informasjonssikkerhet og personvern, koordinert og fasilitert av Cybersikkerhetssenteret. Gjennom godt samarbeid og erfaringsutveksling i flere arenaer blir deltakerne bedre i stand til å ta tak i det lokale sikkerhetsarbeidet som må gjøres.

Den kan kjøpes av alle virksomheter i norsk kunnskapssektor (Gjelder også virksomheter utenfor universitet- og høgskolesektoren). Pakken kan kun kjøpes samlet og leveres uten lokal tilpasning.

Beskytte og opprettholde:

- Tilgang til oppdaterte sperrelister som blant annet kan brukes i utbredte sikkerhetsprodukter som Windows ATP Defender og Cisco Umbrella.
- Fri bruk av sentrale DNS-servere som til enhver tid har oppdaterte sperrelister
- Tilgang til mal for modenhetsvurdering på IKT-sikkerhetsområdet basert på anerkjente rammeverk.
- Ubegrenset antall tjenersertifikater, personsertifikater og kodesigneringssertifikater

Oppdage:

- Tilgang til sentral database over trusler, inkludert detaljert informasjon og relaterte hendelser. Databasen brukes til å lage våre sperrelister, og blir kontinuerlig fornyet gjennom registreringer fra sektoren og data fra andre sektorer og internasjonale partnere som europeiske forskningsnettverk.
- Lagring av og innsyn i egne logger fra fellestjenester iht. avtaler
- Sensor tilkoblet virksomhetens nettilknytning som avdekker trusler og angrepsforsøk. Varsling og tilgang gjennom sikre kanaler.

Håndtere og gjenopprette:

- Tilgang til historiske data i forskningsnettet for å kunne ettergå tekniske spor

Rådgivning og kompetanseheving:

- Tilgang til fagfellesskap:
  - Forum for informasjonssikkerhetsansvarlige (CISO-forum)
  - Forum for juridiske tema innen informasjonssikkerhet og personvern *(kommer)*
- Utvikling og vedlikehold av beste praksis-dokumenter i samarbeid med fagfellesskapene
  - Etablering og videreutvikling av ledelsessystem for informasjonssikkerhet og personvern.
  - Risikovurdering og risikostyring
  - Klassifisering av informasjon
  - Kunnskapsbase for beredskapsøvelser med verktøysamling (dreiebok, scenarioer, mm) for gjennomføring av egne øvelser
  - Oppdaterte tiltakskort som beskriver hva som må gjøres ved alvorlige hendelser
  - Nye beste praksiser etter sektorens behov
- Tilgang til rammeavtaler på sikkerhetstjenester og produkter og mulighet til å påvirke anskaffelser av på vegne av kunnskapssektoren. Verktøyene er valgfrie å ta i bruk og det vil påløpe tilleggskostnader i form av lisenser.
  Aktuelle eksempler:
  - Risikostyringsverktøy
  - Passordhåndteringsverktøy
- Materiell til opplæring og bevisstgjøring av studenter og ansatte for å forbedre sikkerhetskultur, inkludert sikkerhetsmåneden oktober.

Listen over tjenester er ikke uttømmende, og vil endres i takt med kundenes behov, tilgjengelig kapasitet og kompetanse i Cybersikkerhetssenteret for forskning og utdanning.

Cybersikkerhetssenterets valgfrie tilleggstjenester

Alle i UH-sektoren har samme kjernevirksomhet, lovverk og felles krav fra Kunnskapsdepartementet (KD). For å møte de ulike prioritetene for virksomhetene i sektoren, tilbyr vi disse tilleggstjenestene.

Beskytte og opprettholde:

- Bistand til gjennomføring av modenhetsvurdering på IKT-sikkerhetsområdet med rapport til bruk for operativ og strategisk oppfølging.
- Bistand til å vurdere sikkerheten hos tjenesteleverandører ved tjenesteutsetting

Oppdage:

- Oppdragsbasert analyse av virksomhetens loggdata (engangsanalyse og/eller kontinuerlig analyse)

Håndtere og gjenopprette:

- Bistand til utarbeidelse av kontinuitets- og beredskapsplaner
- Bistand til planlegging og gjennomføring av beredskapsøvelser

Rådgivning og kompetanseheving:

- Bistand ved innføring og videreutvikling av ledelsessystem for informasjonssikkerhet og personvern
- Etterlevelsesrevisjon av ledelsessystem for informasjonssikkerhet og personvern
- Bistand til kartlegging av informasjonsverdier
- Bistand til kontroll med kunnskapsoverføring (eksportkontroll)
- Bistand til gjennomføring av risikovurderinger
- Bistand til utarbeidelse av databehandleravtaler
- Deltagelse i årlig sektorøvelse innen informasjonssikkerhet
- Tilgang til delte risikovurderinger (*kommer*)
- Annen bistand innen informasjonssikkerhet og personvern
- Kurs gjennomført av senteret eller samarbeidspartnere:
    - Gjennomføring av risikovurderinger
    - Informasjonssikkerhet og personvern for ledere
    - Utarbeide databehandleravtaler
    - Grunnleggende logginnsamling og analyse
    - Hendelseshåndtering i MS365
    - Gjennomføring av personvernkonsekvensvurdering (DPIA)

Listen over tjenester er ikke uttømmende, og vil endres i takt med kundenes behov, tilgjengelig kapasitet og kompetanse i Cybersikkerhetssenteret for forskning og utdanning.