KRAVSPESIFIKASJON

Anskaffelse Sikkerovervåkningstjeneste (SOC)

Innhold

1. Innledning

1.1. Bakgrunn

IT-tjenesten for kommunene Melhus og Skaun (ITMidt) leverer tjenester til alle kommunens innbyggere, og benytter nødvendige nettjenester som krever høy oppetid og god sikkerhet. Disse tjenestene er både interne og eksterne, men fellesnevneren er at de for mange av brukerne benytter internett som bærer. Det er et strategisk mål at disse tjenestene kan driftes på en forsvarlig måte som både møter krav fra bestiller og forventningene fra sluttbruker.

1.2. Mål og omfang

ITMidt ønsker å anskaffe en døgnkontinuerlig (24/7/365) tjeneste for sikkerhetsovervåking og støtte til hendelseshåndtering av sikkerhetshendelser i Kundens IT-miljø. Dette innebærer å inngå et samarbeid med en Leverandør som leverer en MDR-tjeneste som ivaretar sikkerhetsovervåking, sårbarhetskontroll og -oppfølging og hendelseshåndtering, hvor Leverandøren også skal gi Kunden rask tilgang på spisskompetanse for bistand ved større sikkerhetshendelser. Det forventes få en proaktiv overvåking og håndtering av sårbarheter, og ikke bare reaktiv håndtering ved større uønskede hendelser.

1.3. Oversikt over dagens løsninger i ITMidt

Tekst	
Sikkerhetsverktøy hos Kunden i dag	- XDR - EDR
Volum og frekvens	- 2-300 Gb pr dag + økende - EPS – 2.500 gjennomsnitt
Enheter/endepunkt (servere, klienter, etc.)	- 200+ servere - 5000+ klienter
Oppbevaringstid	- Hot retention: 30 dager - Alerts and incidents hot retention: 180 dager

2. Utfylling av kravspesifikasjonen

Tabellen nedenfor inneholder krav til leveranse og tjenester. Kravene er delt inn to kategorier:

A-krav

A-Krav er absolutte krav som må oppfylles. A-krav vurderes som «oppfylt» eller «ikke oppfylt». Manglende oppfyllelse av a-krav vil føre til avvisning.

B-krav

Viktige krav som beskriver Kundens behov og ønsker. Oppfyllelse av B-krav vil bli evaluert under tildelingskriteriet «Kvalitet».

C-krav

Ønskelige opsjonskrav som beskriver Kundens behov og ønsker. Oppfyllelse av C-krav vil bli evaluert under tildelingskriteriet «Kvalitet».

Dersom leverandøren ønsker å bruke en eller flere underleverandører til å utføre deler av leveransen skal det oppgis i bilag 2. Leverandør må også opplyse om hvilke deler av kontrakten som underleverandør skal utføre.

Dersom det etter Leverandørens mening er åpenbare feil eller uklarheter i Kundens kravspesifikasjon, skal Leverandøren påpeke dette i Mercell.

3. Overvåking og trusselvurdering

- Alle kravene besvares i med ja/nei/forbehold + en beskrivelse av løsning. Manglende beskrivelse i dette dokumentet kan føre til redusert poengscore.

- Maksimal lengde på beskrivelse bør være ca 750 tegn om ikke annet er oppgitt. Lengre beskrivelse enn dette kan føre til redusert poengscore.

Oppdragsgivers krav				Leverandørens svar
#	Beskrivelse av kravet	Krav kode	Oppfylt Ja/Nei	Løsningsbeskrivelse (kommentar ved nei til kravpunkt)
3.1.	Leverandøren skal ha en organisasjon og et sikkerhetsovervåkingssenter som leverer tilbudte tjenester hele døgnet, alle dager i året (24/7/365)	A		
3.2.	Beskriv hvordan organisasjonen er oppbygget for å håndtere sine tjenester 24/7/365 • Organisering 1./2./3. linje Kompetanse i de forskjellige linje-nivå	B		
3.3.	Leverandøren skal sørge for kontinuerlige trussel vurderinger rettet mot det norske markedet. Beskriv hvordan leverandøren holder seg oppdatert på den norske og globale trusselsituasjonen, eks. samarbeid med norske myndigheter.	B		
3.4.	Leverandøren bes beskrive hvordan analyse, trusseloppdagelse og trusseletterretning gjennomføres, og at det legges vekt på å beskrive følgende områder: • Analyser, korrelering og datasammenslåing av loggdata fra Kunden med øvrig informasjon som Leverandøren har tilgang til • Leverandørens interne læring og deling av informasjon om Kunden generelt, samt operative hendelser og tilstander	B		

	• Operativt samarbeid med sektorvise responsmiljøer i Norge eller andre norske eller internasjonale responsmiljøer. Trusseljakt Med trusseljakt menes å lete etter trussel aktører i Kundens IT-miljø basert på indikatorer eller på hypoteser			
3.5.	Beskriv hvordan Leverandøren kan levere tjeneste for sårbarhetsskanning av Kundens IT-miljø	C		
3.6.	Leverandøren skal levere tjeneste for overvåkning av logger fra hele kundens IT-miljø (datasenter og sky)	A		
3.7.	Beskriv typisk ansvarsfordeling mellom SOC og Kunden ved håndtering av alarmer • Varslingskanaler • Fleksibilitet i varslingssystemet • Automatisk hendelseshåndtering (isolering av endepunkter, IP-filtrering med mer) Garanterte varsling-/responstider	B		
3.8.	Leverandøren skal ha hendelseshåndteringsteam tilgjengelig med respons-garanti. Beskriv evnen til å levere støtte til Kunden innenfor følgende områder ved større hendelser: • Hendelsesledelse • Hendelseshåndtering	A		
3.9.	Som en del av hendelseshåndteringsteamet skal det opprettes månedlige statusmøter for oppdatering om aktuell status: • Gjensidig deling av erfaring og opplevelser • Endringer i trusselbildet • Sårbarheter (både generelle og spesifikke for kundens miljø) • Forberedende vurderinger	B		

3.10.	Leverandør må kunne stille ressurser on-site avhengig av hendelse, situasjon og behov	A		
3.11.	Leverandøren skal kunne bistå med • Lede håndtering av hendelsen • Identifisere hendelsen • Isolering av skade/skadebegrensning • Utrydde fremmede elementer relatert til hendelsen • Bistand til gjenoppretting av tjenesteleveranse til normal drift i samarbeid med kunde og evt. tredjepart (teknisk personell knyttet til enhver tid gjeldende IT-konsulentavtale) • Forensics og analyse (hva har skjedd) • Levering av rapport over hendelsen og på følgende håndtering (inkl. anbefaling for å redusere risiko for gjentakelse.	B		
3.12.	Leverandør skal levere periodiske hendelsesrapporter. Rapportene skal som minimum utarbeides pr. måned, kvartalsvis og år. Disse skal inneholde bl.a., men ikke uttømmende; • Overordnet rapport med vurdering av sikkerhetssituasjonen og oppsummering av viktige forhold (fra bl.a. tema under) • Oversikt/ tall med ulik kategorisering over events identifisert og antall events med ulik behandlingsstatus • Oversikts/tall over antall hendelser kategorisert på spesifisert måte og antall med ulik behandlingsstatus	A		

	• Oversikt/tall identifiserte sårbarheter av ulike kategorier, alder siden identifisert og status på tidligere identifiserte sårbarheter • Forslag til prioritering av sårbarheter og tiltak på sårbarheter • Oversikt over trender på type events, hendelser, trusler, etc. som Kunden skal være oppmerksomme på • Statusrapport fra trusselovervåkning generelt og for ITMidt spesielt Rapportene skal benyttes henholdsvis månedlige operative møter, og kvartalsvise strategiske møter.			
3.13.	Leverandøren bør ha kundetilpasset "dashboard" via web-basert portal	B		
3.14.	Muligheter for kunde-tilpassede rapporter	B		
3.15.	Beskriv om / hvordan leverandøren kan arbeide med Kunden for å sikre at Kunden har en sikkerhetsarkitektur som gir en fornuftig beskyttelse av de tjenester Kunden leverer	B		
3.16.	Beskriv om / hvordan leverandøren kan bistå Kunden i å sikre at denne har tilstrekkelig oppdatert kompetanse på IT-sikkerhet, både i IT-divisjonen og generelt	C		
3.17.	Leverandøren skal kunne bistå med rådgivning (fast og ad-hoc)	A		

4. Andre krav

Oppdragsgivers krav		Leverandørens svar

#	Beskrivelse av kravet	Krav kode	Oppfylt Ja/Nei	Løsningsbeskrivelse (kommentar ved nei til kravpunkt)
4.1.	Leverandøren skal ha dokumenterte rutiner for 1) Drift av sine løsninger 2) Oppdage feil og flaskehalser	B		
4.2.	Erfaring - Leverandøren skal minimum hatt 5 kunder på tilbudt leveranse de siste 3 år (tilsvarende kunde-segment)	A		
4.3.	Gi en kort beskrivelse av Leverandørens nåværende posisjon i markedet innenfor området som omfattes av avtalen	B		
4.4.	Leverandøren bes beskrive hvilke rammeverk denne forholder seg til med hensyn til ulike aspekter av cybersikkerhet. Herunder også hvilke kilder som benyttes for å motta trusselinformasjon.	B		
4.5.	Beskriv kort hvilke planer Leverandøren har for å videreutvikle tjenestene i tråd med utviklingen i markedet	B		
4.6.	Beskriv kort hvilke kompetansehevende tiltak Leverandøren har for sine ansatte	B		
4.7.	Tjenesten bør tilby en web-basert kundeportal	B		
4.8.	Løsningen skal kunne håndtere økt antall logger/datamengder, beskriv hvordan løsningen skalerer både teknisk og kostnadsmessig/økonomisk	B		
4.9.	Løsningen skal være skalerbar, og må være fleksibel i konfigurasjon	A		
4.10.	Ved kontraktens avslutning, skal det være mulig for Kunden å eksportere all relevant data. Leverandøren skal yte bistand til Kunden dersom Kunden ønsker å avslutte hele eller deler av avtalen. Leverandøren skal legge til rette for at Kundens data	A		

	blir overført til Kunden eller til tredjepart utpekt av Kunden			
4.11.	Hvordan utøver Leverandøren forbedringsvurdering av egen løsning/tjeneste	B		
4.12.	Leverandøren bes beskrive planlegging av etableringsfasen og hvilke aktiviteter som skal gjennomføres for å etablere tjenesten	B		
4.13.	Innsamlede logger og data lagres og behandles i Norge	A		
4.14.	Bekreft om det er ressurser fra andre land enn Norge som har tilgang til innsamlede logger/data. Hvis Ja, beskriv hvilke land	B		
4.15.	Beskriv hvordan Leverandøren sørger for god informasjonssikkerhet i tjenesten, som blant annet • Styringssystem for informasjonssikkerhet (ISMS), eks. ISO27001:2022 • Ekstern verifikasjon av informasjonssikkerhet i virksomheten, eks. SOC2 type 2 rapport • Bruk av anerkjente rammeverk for IKT sikkerhet, eks. NSM Grunnprinsipper for IKT sikkerhet eller NIST Cybersecurity Framework 1.1 • Rutiner for hendelseshåndtering og sårbarhetsstyring, inkludert varslingsrutiner til Kunden • Risiko i leverandørkjeden • Håndtering av risiko ved planlagte endringer og oppdukkende sikkerhetshendelser • Dataseparasjon for Kundens data opp mot andre kunders data i Leverandørens systemer og kommunikasjonsløsninger • Tilgangsstyring	B		

	• Informasjonssikkerhets- og personverntiltak for Kundens informasjon ved overføring, lagring og behandling • Sikkerhet ved integrasjoner mellom Kundens og Leverandørens datamiljø • Dataflyt og hvor Kundens data overføres, lagres og behandles • Mulighet for sletting av loggdata og andre data når Kunden ber om det Rutiner for fysisk sikkerhet og personalsikkerhet			
4.16.	Beskriv hvordan Leverandør og løsningen etterlever GDPR	B		
4.17.	**Opsjon produkter og tjenester** Det skal være mulig å kjøpe andre tilhørende produkter eller tjenester. List opp de mest relevante produkter og tjenestene med priser i denne besvarelsen.	C		

5. Administrativt

Oppdragsgivers krav				Leverandørens svar
#	Beskrivelse av kravet	Krav kode	Oppfylt Ja/Nei	Løsningsbeskrivelse (kommentar ved nei til kravpunkt)
4.18.	**Møter:** Det skal kunne holdes driftsmøter hvert halvår. Leverandøren er ansvarlig for innkalling samt å skrive referat. I møtene skal driftsituasjonen siste måned samt produserte rapporter på oppetid og kvalitet gjennomgås.	B		
4.19.	**Tilleggstjenester:** Leverandøren skal oppgi priser for tilleggstjenester som eksempelvis konsulent-tjenester og rådgivingstjenester.	B		

4.20.	**Fakturering:** Fakturen skal gjenspeile de ulike tjenestene som er levert. Betaling skal skje månedlig og fakturaen må støtte EHF.	B		
4.21.	**Fakturering:** Fakturering skal skje i henhold til Staten standardavtale for drift (SSA-D)	B		
4.22.	**Fakturering:** **I kontrakten skal det stilles krav om bruk av elektronisk faktura i godkjent standardformat.**	A		
4.23.	**GDPR** Om nødvendig skal det inngås databehandleravtale i henhold til GDPR	B		