Risiko- og Sårbarhetsanalyse (ROS) for Sensedesk Assist

Sist oppdatert: 05.01.2025

1. Introduksjon

1.1 Formål med ROS-en

Dette dokumentet har som formål å:

- Identifisere og analysere potensielle trusler og sårbarheter knyttet til Sensedesk Assist-appen.
- Vurdere risikoer med hensyn til sikkerhet, integritet, tilgjengelighet og konfidensialitet i systemet.
- Beskrive eksisterende tiltak samt foreslå ytterligere risikoreduserende tiltak for å minimere sannsynligheten og konsekvensene av eventuelle sikkerhetshendelser.

1.2 Omfang

ROS-en omfatter alle aspekter av Sensedesk Assist, inkludert:

- Applikasjonens arkitektur og tekniske komponenter.
- Kommunikasjonskanaler og tilkoblingsinfrastruktur.
- Autentisering og autorisasjon.
- Drift, logging og overvåking.
- Eventuelle eksterne tjenesteleverandører og tredjepartsintegrasjoner.

---

2. Systembeskrivelse

2.1 Om Sensedesk Assist-appen

- **Plattform:** Windows-basert applikasjon.
- **Utviklingsrammeverk:** .NET 8.
- **Funksjonalitet:** Fjernstyring av andre Windows-PC'er og servere, med mulighet for support, vedlikehold og feilsøking.

- **Autentisering:** Brukere autentiserer seg som gjest via Entra ID.
- **Kommunikasjon:** All dataflyt foregår over HTTPS/TLS 1.2 med ende-til-ende-kryptering.
- **Infrastruktur:** Kommunikasjonen går via våre IIS relay-servere lokalisert i Norge, benytter .ASHX/SSE-teknologi, og benytter kun port 443.

2.2 Systemarkitektur og dataflyt

1. **Autentisering og tilkobling:**
   Brukeren logger inn via Entra ID og etablerer en sikker tilkobling.
2. **Dataoverføring:**
   Kommunikasjonen mellom klienten og den fjernstyrte enheten går gjennom krypterte kanaler med ende-til-ende-kryptering via våre relay-servere.
3. **Logging og overvåking:**
   Sesjonsdata, tilkoblingslogger og autentiseringsinformasjon samles inn for sikkerhets- og feilsøkingsformål.

---

3. Identifisering av Eiendeler og Verdier

For å sikre en helhetlig ROS er det viktig å identifisere hvilke ressurser og eiendeler som skal beskyttes:

- **Brukerautentisering og -autorisering:**
  Entra ID-integrasjonen som håndterer tilgang til systemet.
- **Kommunikasjonskanaler:**
  All dataoverføring skjer via HTTPS/TLS 1.2, som er kritisk for å ivareta konfidensialitet og integritet.
- **Relay-servere:**
  IIS-serverne i Norge som fungerer som mellommenn for dataoverføring.
- **Applikasjonsdata og logging:**
  Data knyttet til fjernstyringssesjoner, tilkoblingslogger, feilmeldinger og systemhendelser.
- **Klient- og serverkomponenter:**
  Selve applikasjonsklienten og den eksterne kontrollenhetene som styres via appen.

---

4. Trusselvurdering

4.1 Potensielle trusler

- **Uautorisert tilgang:**
  Risiko for at uvedkommende får tilgang til systemet dersom autentiseringsmekanismene kompromitteres.
- **Man-in-the-Middle-angrep:**
  Risiko for avlytting eller manipulering av data under overføringen, til tross for kryptering.
- **DoS/DDoS-angrep:**
  Risiko for tjenestenekt gjennom overbelastning av relay-servere eller applikasjonen.
- **Systemfeil og sårbarheter:**
  Programvarefeil, sårbarheter i .NET-rammeverket eller i konfigurasjonen av IIS-serverne.
- **Misbruk av fjernstyringsfunksjonaliteten:**
  Risiko for at en autorisert bruker med ondsinnede intensjoner utnytter funksjonaliteten for å skade eller få uautorisert tilgang til systemer.
- **Tredjepartsintegrasjoner:**
  Risiko knyttet til eksterne leverandører eller tjenester som kan introdusere sårbarheter.

---

5. Sårbarhetsvurdering

5.1 Identifisering av sårbarheter

- **Autentisering og autorisasjon:**
  Mulige svakheter i Entra ID-integrasjonen eller konfigurasjonsfeil som kan gi uautorisert tilgang.
- **Kryptering:**
  Selv om TLS 1.2 er robust, er det viktig å overvåke for eventuelle implementasjonsfeil eller manglende oppdateringer som kan kompromittere krypteringen.
- **Software og oppdateringer:**
  Sårbarheter i .NET-plattformen, operativsystemet eller IIS-konfigurasjoner som kan utnyttes hvis ikke regelmessig oppdatert.

- **Logging og overvåking:**
  Manglende eller utilstrekkelig logging kan hindre rask oppdagelse av mistenkelig aktivitet.
- **Nettverksinfrastruktur:**
  Sårbarheter i relay-serverne, for eksempel feilkonfigurerte brannmurer eller utilstrekkelig beskyttede tjenester.

---

6. Risikoanalyse

Merk: Ved bruk av Sensedesk Assist, ikke intern/»on prem» Sensedesk web-server (relay-servere hos Sense Data as).
Risikoene vurderes basert på sannsynlighet for hendelse og konsekvens ved realisering:

Risiko	**Sannsynlighet**	**Konsekvens**	**Risikonivå**
Uautorisert tilgang via kompromittert Entra ID	Lav–Moderat	Høy	Moderat–Høy
Avlytting/manipulering av data (Man-in-the-Middle)	Lav	Høy	Moderat
DoS/DDoS-angrep	Moderat	Moderat–Høy	Moderat
Utnyttelse av sårbarheter i applikasjonen	Moderat	Høy	Høy
Misbruk av fjernstyringsfunksjonalitet	Lav–Moderat	Høy	Moderat–Høy
Tredjepartsleverandører introduserer sårbarheter	Lav–Moderat	Moderat	Moderat

Merk: Risikonivået bør vurderes kontinuerlig gjennom oppdateringer, sikkerhetstesting og overvåkning.

Merk: Ved bruk av Sensedesk Assist, og «on prem» Sensedesk web-server

Risiko	**Sannsynlighet**	**Konsekvens**	**Risikonivå**
Uautorisert tilgang via kompromittert Entra ID	Lav	Høy	Moderat
Avlytting/manipulering av data (Man-in-the-Middle)	Lav	Høy	Moderat
DoS/DDoS-angrep	Lav	Moderat–Høy	Moderat
Utnyttelse av sårbarheter i applikasjonen	Moderat	Høy	Høy
Misbruk av fjernstyringsfunksjonalitet	Lav–Moderat	Høy	Moderat–Høy
Tredjepartsleverandører introduserer sårbarheter	Lav	Moderat	Moderat

7. Risikoreduserende Tiltak

7.1 Tekniske tiltak

- **Kryptering:**
  Opprettholde og regelmessig verifiser krypteringen (HTTPS/TLS 1.2) for å hindre avlytting og dataendring.
- **Autentisering:**
  Sørg for at Entra ID-integrasjonen er robust med multifaktorautentisering der det er mulig.
- **Brannmur og nettverkssikkerhet:**
  Begrens eksponering ved kun å åpne port 443. Implementer IDS/IPS (intrusion detection/prevention systems) for å oppdage angrepsforsøk.
- **Oppdateringer og patching:**
  Regelmessig oppdatering av operativsystemer, .NET-plattformen og IIS for å lappe kjente sårbarheter.
- **Logging og overvåking:**
  Implementer omfattende logging med sanntidsovervåking av sikkerhetshendelser, og sørg for at logger gjennomgås regelmessig.
- **Sikkerhetsarkitektur:**
  Utfør periodiske sårbarhetstester og penetrasjonstesting for å identifisere og avhjelpe svakheter i systemet.

7.2 Organisatoriske tiltak

- **Sikkerhetspolicyer og retningslinjer:**
  Etabler klare retningslinjer for IT-sikkerhet og prosedyre for håndtering av sikkerhetshendelser.
- **Opplæring:**
  Gi regelmessig opplæring til ansatte om sikkerhetsprosedyrer og bevissthet rundt potensielle trusler.
- **Beredskapsplan:**
  Utarbeid og test en beredskapsplan for rask respons ved sikkerhetshendelser eller systemfeil.
- **Tredjepartsavtaler:**
  Sørg for at eventuelle tredjepartsleverandører oppfyller de nødvendige sikkerhetskrav og har signerte avtaler som dekker risikohåndtering.

---

8. Anbefalinger og Videre Tiltak

- **Regelmessig sikkerhetsgjennomgang:**
  Gjennomfør periodiske revisjoner, sårbarhetstester og penetrasjonstester for å holde tritt med nye trusler.
- **Overvåkning i sanntid:**
  Implementer overvåkingssystemer som kan oppdage og varsle om mistenkelig aktivitet så tidlig som mulig.
- **Oppdateringsstrategi:**
  Etabler en robust strategi for patching og oppdatering av alle systemkomponenter for å minimere sårbarheter.
- **Kontinuerlig opplæring:**
  Sørg for at alle brukere og administratorer er oppdatert på beste praksis for sikkerhet, og at de er bevisste på potensielle trusler og hvordan de skal håndteres.

---

9. Konklusjon

Basert på analysen konkluderes det med at Sensedesk Assist-appen i dag har implementert flere viktige sikkerhetstiltak for å beskytte systemet mot kjente trusler. Samtidig finnes det risikoer, særlig knyttet til potensielle sårbarheter i autentiseringsløsningen, programvarekomponenter og infrastruktur. Ved å følge de anbefalte tekniske og organisatoriske tiltakene kan disse risikoene reduseres til et akseptabelt nivå. Det anbefales at ROS-dokumentasjonen revideres regelmessig og tilpasses ved nye teknologiske endringer eller oppdagede trusler.