Braathe AS
Nærumveien 24, 1580 Rygge / Org.nr. 981 933 311 MVA
69 01 30 00 / post@braathe.no / www.braathe.no

EOSL Policy for IaaS i Braathe Cloud

Formål

Formål med End Of Service Life Policy er et overordnet rammeverk for leveranser når utstyr og systemer går forbi End Of Service Life (EOSL) som definert nedenfor. EOSL har som konsekvens at man må identifisere og håndtere økt risiko, gjøre nødvendige tiltak, samt ta forbehold og begrensninger for at drift av systemene skal kunne fortsette innenfor rammer som er akseptable for Kunden og Leverandøren.

Leverandøren bistår Kunden så langt forsvarlig med å utvikle løsninger for EOSL drift dersom det vil bety betydelig ulempe for Kunden å bytte system eller oppgradere til støttet system. I noen tilfeller vil det dessverre ikke være mulig å komme til noen løsning ut fra systemets beskaffenhet og oppgradering/bytte vil være eneste farbar vei. Bistand i forbindelse med EOSL implementering leveres i henhold til Tjenestebeskrivelse «Timebasert Konsulenttjenester».

EOSL Policy

Leverandørens definisjon «End Of Service Life» (EOSL)

Når operativsystem, applikasjoner, programvare, utstyr eller komponenter ikke lengre mottar nødvendige tekniske- og sikkerhetsoppdateringer, eller andre forhold som kan påvirke muligheten for å drifte systemet i henhold til kjent beste praksis og med akseptabelt risikonivå.

I industrien benyttes ofte begreper som End of Life, End of Support med mere. Leverandørens EOSL definisjon forstås som synonymt med slike begreper. Som regel annonseres status og EOSL datoer av opprinnelig produsent eller annen ansvarlig instans, for eksempel Open Source kildekodeansvarlig.

Risikobilde

Fra og med produktets EOSL dato utgjør nye og eksisterende sårbarheter en stadig økende risiko for kompromittering da disse ofte ikke vil bli rettet eller risikoredusert på annen måte. Kompromittering utgjør en videre risiko for sideveis bevegelse til Kundens andre systemer og videre til Leverandørens fellessystemer og plattformer.

EOSL Tiltak

Primært tiltak er ***alltid*** å oppgradere systemer til versjoner som fortsatt er støttet og mottar tekniske- og sikkerhetsoppdateringer fra Produsent. Vi anbefaler derfor våre Kunder ***på det sterkeste*** til å oppgradere i god tid før EOSL dato.

Kostnader ved nødvendige versjonsoppgraderinger, systembytte eller andre nødvendige tiltak dekkes av Kunden i henhold til gjeldende avtaler og betingelser.

I noen tilfeller kan oppdatering eller systembytte være krevende for Kunden. I denne situasjonen vil risikoreduserende tiltak måtte iverksettes:

- Drift av EOSL systemer flyttes bort fra Leverandørens felles plattformer til Kundededikert plattform
    - Se Tjenestebeskrivelse «Dedicated IaaS Platform»
- Reduksjon av angrepsflate

    - For eksempel fjerning fra Internett
    - Analyse og gjennomgang av trafikk til og fra systemet
    - Lukking/blokkering av unødvendige portåpninger
- Isolering av system
- Endring av bruksmønster for system
- Andre nødvendige tiltak

Tiltaksliste over er nødvendigvis ikke uttømmende.

Leverandøren skal varsle anbefalte EOSL tiltak i rimelig tid og legge til rette for prosess i samråd med Kunden.

Etablering EOSL tiltak

Undersøkelser forarbeid, design og implementering av EOSL tiltak utføres i henhold til Tjenestebeskrivelse «Timebasert Konsulenttjeneste». Slike prosjekter kan være omfattende og medføre driftsavbrudd på systemer og delsystemer under implementering.

Det tas forbehold om at videre utvikling i risikosituasjonen vil kunne føre til behov for ytterligere tiltak.

Leverandørens plikter

Leverandøren skal varsle Kunden i rimelig tid når EOSL datoer er kjent. Normalt vil dette gjelde versjoner av Operativsystemer, men kan også gjelde serverapplikasjoner dersom informasjonen er fritt tilgjengelig for Leverandøren.

Kundens plikter

Kunden plikter å etterkomme rimelige EOSL anbefalinger og krav fra Leverandøren. Slike anbefalinger og krav kan også omfatte tiltak som nevnt over, nødvendige endringer og innstramminger i Kundens tilganger og 3. parts leverandørers tilganger, driftsrutiner med mere.

Kunden har et forhøyet aktsomhetskrav ved aksess til, og bruk av EOSL systemer. Kundens brukere og eventuelle 3.part som får tilgang til EOSL systemer skal om nødvendig gjennomgå opplæring og følge opp sikringstiltak og rutiner som etableres.

Kunden har et selvstendig ansvar for å kjenne til EOSL tidspunkt for sine egne 3.parts systemer som er installert på systemer driftet av Leverandøren, eller i direkte kontakt med systemer driftet av Leverandøren på vegne av Kunden. Kunden skal varsle Leverandøren skriftlig i rimelig tid før kommende, eller ved passert EOSL dato når dette blir kjent for Kunden.

Forbehold og begrensninger

Leverandørens anbefalte Sekundære Tiltak er av ***risikoreduserende og skadebegrensende*** karakter og utgjør på ingen måte garanti mot at kompromittering kan skje.

Tiltakene er å anse som midlertidige og kan til enhver tid endres dersom endring i risikovurdering tilsier dette.

Leverandøren forbeholder seg uansett rett til å stenge ned, suspendere eller terminere drift av EOSL system dersom Kunden ikke retter seg etter anbefalte tiltak, misligholder sin aktsomhetsplikt, eller det oppstår en videre forhøyet risiko for kompromittering. Suspendering eller terminering skal normalt varsles skriftlig med minimum 10 virkedager. Dersom det oppstår akutt forhøyet risiko basert på Leverandørens vurdering, kan likevel nedstenging og suspendering iverksettes uten nærmere varsel. Se ellers Sikkerhet SLA som publisert på Leverandørens nettsted.

Tiltak iverksatt av Leverandøren endrer ikke Kundens forpliktelser, eller grunnlag for oppsigelse.