Sikkerhet SLA

Felles retningslinjer for sikkerhet gjeldende for alle Braathe Gruppen Tjenester

1 Om sikkerhet

Et stadig økende digitalt trusselbilde tilsier at Leverandøren har et ensartet sett med retningslinjer, virkemidler og tiltak for å kunne sikre forsvarlig drift som gjelder alle tjenester.

2 Dekningsområde

Sikkerhet SLA gjelder for alle tjenester levert av Leverandøren med mindre det er angitt unntak eller tillegg i den enkelte Tjenestebeskrivelse for den spesifikke tjeneste. Dekningsområde omfatter:

- Tjenester som er produsert på eller fra Leverandørens lokasjoner
- 3. parts tjenester, utstyr, programvare og konfigurasjoner som er levert som del av en løpende tjeneste fra Leverandøren
- Kundens eget utstyr og programvare som er underlagt driftsavtale med Leverandøren. Omfatter både utstyr som er plassert på Leverandørens lokasjoner og på Kundens lokasjoner.
- Kundens eget utstyr og programvare som benyttes på en slik måte at det kan påvirke sikkerheten til ovennevnte.

3 Leverandørens rettigheter og plikter

Leverandøren skal til enhver tid etterstrebe å sikre Tjenester som leveres i henhold til gjeldende lovgivning, velkjente kilder for sikkerhetsinformasjon, underleverandørenes anbefalinger (Best Practice) og industrinormer.

3.1 Evaluering av trusselbildet

Leverandøren skal ha rutiner i henhold til sikringstiltak som angis i Tillegg A i ISO 27001 standarden for å være løpende informert om sårbarheter og trusselsituasjonen.

3.2 Leverandørens hendelseshåndtering

Leverandøren skal så snart som praktisk mulig gjøre en selvstendig risiko- og sårbarhetsvurdering når det foreligger ny informasjon om sårbarheter og trusselsituasjon. Risikovurderingen vil ligge til grunn for å beslutte tiltak.

3.3 Tiltaksplikt og -rett ved hendelse

Leverandøren er pliktig å vurdere, og om nødvendig iverksette tiltak ut fra sin risikovurdering. Leverandøren har også med utgangspunkt i sine vurderinger rett til å iverksette tiltak. Tiltak skal stå i rimelig forhold til Leverandørens trussel- og risikovurderinger.

Leverandøren er ikke ansvarlig for direkte eller indirekte kostnader eller ulemper for Kunden i forbindelse med tiltak begrunnet i sikkerhet. For tjenester som inkluderer oppetidsgaranti eller -forventning er nedetid i forbindelse med sikkerhetstiltak unntatt fra oppetidsberegning.

3.4 Sårbarhetsanalyser

Leverandøren skal utføre regelmessige sårbarhetsanalyser for sine tjenester.

3.5 Varsling ved Sikkerhetsavvik

Leverandøren skal snarest informere dersom det er observert avvik eller hendelser som kan ha sikkerhetsmessig innvirkning på Kundens systemer og data. Manglende varsling er likevel ikke til hinder for å iverksette tiltak.

3.5.1 Kundededikerte systemer

Ved sikkerhetshendelse og tiltak begrenset til en Kundes dedikerte systemer vil varsling skje ved at det opprettes en sak i Leverandørens saksbehandlingssystem. Saken adresseres til Kundens avtaleansvarlig og/eller teknisk ansvarlig.

Ved akutte hendelser vil Leverandøren også søke å varsle Kunden via telefon til ovennevnte kontaktpersoner.

3.5.2 Felles systemer

Ved sikkerhetshendelse som kan berøre flere Kunder, eller alle Kunder, skal Leverandøren varsle dette via statusmelding på Leverandørens web-baserte statussider.

3.6 Sårbarheter i Kundens utstyr og programvare

Leverandøren kan oppfordre Kunden til å oppgradere utstyr og programvare, operativsystemer og enheter som Kunden råder over, dersom det er dokumentert kjente sårbarheter, eller at utstyr/programvare er passert End of Life dato og ikke lengre er støttet eller mottar sikkerhetsoppdateringer fra produsent.

3.6.1 Opphevelse av SLA og stenging av Kundetjenester

Dersom kunden ikke etterkommer skriftlige sikkerhetsoppfordringer innen rimelig tid, kan Leverandøren iverksette følgende tiltak ut fra situasjonens alvorlighet:

- Suspensjon av tjenestens SLA og øvrige leveranser under tjenesten
- Endring av system og/eller konfigurasjon
- Stenging av tilganger og systemer

Leverandøren skal sende skriftlig varsel til Kundens Avtaleansvarlig, med rimelig frist utfra situasjonens alvorlighetsgrad, før tiltak iverksettes. Tiltak gjelder inntil forholdet er brakt i orden. Tiltak av sikkerhetsmessig karakter fritar ikke Kunden fra betalingsplikt for den berørte tjenesten.

3.7 Tiltak

Tiltak ansees nødvendig når det foreligger sikkerhetsavvik i form av kjente feil og mangler på utstyr, programvare eller konfigurasjoner som er angitt i «Common Vulnerabilities and Exposures» (CVE) systemet, andre velkjente kilder for sikkerhetsinformasjon, systemet/løsningen er i motstrid med produsentens sikkerhetsråd og/eller god sikkerhetspraksis.

Tiltak utløses så snart Leverandøren er kjent med sikkerhetsmangelen og etter at Leverandøren har gjort sin risikovurdering.

Aktuelle tiltak kan omfatte, men er ikke begrenset til:

- Rådgivning av kunden
- Hasteroppdatering – Utføres vanligvis i samråd med Kunde(ne) og utenfor kjernetid
- Nødoppdatering – utføres umiddelbart og uten nærmere varsel. Se ellers kapittel «Ekstraordinære Trusselsituasjoner» nedenfor
- Nedstenging av tilganger og systemer
- Isolering av systemer

- Midlertidige tilgangsmetoder for å omgå trussel

Tiltakene skal ha rimelig tidsramme for utførelse, gjenåpning av eventuelt nedstengte tilganger skal skje så snart forholdet er avklart og trusselen ansees redusert til et akseptabelt nivå

4 Kundens Forpliktelser

Kunden er forpliktet til å gi sine brukere tilstrekkelig opplæring vedrørende IT-Sikkerhet. Leverandøren kan bidra med retningslinjer og opplæringsmateriale på forespørsel.

Kunden aksepterer Leverandørens retningslinjer for brukernes tilgang og benyttelse av systemene, og skal iverksette Leverandørens rimelige tilrådinger selv om disse oppleves av Kunden og deres brukere å medføre ulempe og/eller kostnader.

Kunden er forpliktet til å holde eget utstyr og programvare som er omfattet av denne «Sikkerhet SLA», oppdatert på et sikkerhetsmessig forsvarlig nivå.

4.1 Varsling av sikkerhetsavvik fra Kunden

Dersom Kunden har observert, eller har mistanke om avvik i sikkerhet i henhold til den leverte Tjenesten, skal Kunden uten unødig oppholde melde dette til Leverandøren.

Avviksmelding skal sendes til Leverandørens saksbehandlingssystem support@braathe.no og skal angis med «Sikkerhetsavvik» i begynnelsen av emnelinjen.

Dersom det er en akutt situasjon, skal kunden kontakte Leverandøren umiddelbart pr. telefon til Leverandørens support/vakttelefon og det skal angis «Sikkerhetsavvik».

Dersom det konstateres faktisk og akutt sikkerhetsavvik er Kunden fritatt fra Vaktgebyr for slik henvendelse.

5 Ekstraordinære trusselsituasjoner

Dersom det oppstår alvorlige sikkerhetstrusler mot Leverandøren eller Kunden som antas å kunne påføre vesentlig skade, kan Leverandøren iverksette alle rimelige tiltak for å sikre sine og Kundens systemer inkludert stenging av hele eller deler av Tjenestene uten nærmere varsel.

Dersom et slikt sikkerhetstiltak iverksettes skal Leverandøren uten opphold søke å avklare situasjon og gjenopprette tilganger, så snart dette ansees forsvarlig.

Leverandøren skal i rimelig tid etter tiltaket er iverksatt søke å informere Kunden med relevant informasjon.

Etter sikkerhetstiltak er gjennomført og systemer og tilganger er gjenopprettet, skal Leverandøren på forespørsel sende skriftlig rapport vedrørende tiltaket til Kunden, eller publisere en slik rapport på sine nettsider. Rapporten skal også sendes til relevante myndigheter i rimelig tid etter hendelsen er over i de tilfeller dette er aktuelt.