Krav for anskaffing av IoT-einingar og -system

Dette dokumentet inneheld tekniske krav til utstyr, tenester og system som skal plasserast i kommunale bygg. Leverandørar av slike system skal dokumentere at krava er oppfylt for å bli prekvalifisert i innkjøpsprosessar.

Dokumentasjon av kommunikasjonsbehov
Det skal leverast ei skisse over utstyret med kommunikasjonsbehov over kommunens nettverk. Dette skal minimum innehalde avsendar, mottakar, protokoll og portnummer. For enklare løysingar kan dette leverast i tekst- eller tabellform.

Eksisterande nettverksinfrastruktur skal nyttast
Leverandør kan ikkje etablere eigen infrastruktur eller eigne kommunikasjonskanalar inn til bygget. Alt utstyr som skal "på nett" skal koplast i kommunens eksisterande infrastruktur – enten kabla eller trådlaus - etter følgjande retningslinjer:

- *DHCP skal nyttast - statiske IP-adresser er ikkje tilletne. Utstyret må lyde innstillingane det får servert med DHCP, og kan t.d. ikkje nytte andre DNS-tenarar.*
- *Alt utstyr skal støtte både IPv4 og IPv6.*
- *Utstyr som nyttar Power-over-Ethernet (PoE) skal hente straum frå kommunens eksisterande svitsjar – bruk av "injector" og liknande er ikkje tillete.*
- *Alt utstyr skal som minimum merkast med namn, leverandør og kontaktinformasjon til leverandør.*

Førehandsinnmelding av utstyr
Leverandør skal melde inn alt utstyr som skal monterast før installasjon. Dette skal rapporterast inn vha. skjemaet "Innmelding av IoT-einingar".

Utstyr skal oppdaterast
Alt utstyr skal oppdaterast minimum ein gong per år. Dette inkluderer firmware, drivarar og operativsystem. Ved særleg alvorlege tryggleikshol og oppdateringar frå produsent skal det gjennomførast oppdatering raskt og utanom dei ordinære intervalla, og systemeigar skal varslast om slike alvorlege trugsmål.

Dokumentasjon av prosess for risiko- og sårbarheitsstyring
Leverandør skal dokumentere at dei har ein strukturert prosess for sårbarheitsstyring på plass. Dette inkluderer praksis som å ha god passordhandtering, gjennomføre regelmessige sikkerhetsvurderingar, implementere sårbarheitsskanning og prosedyrer for å rette opp identifiserte sårbarheiter umiddelbart.

Ekstern kommunikasjon skal krypterast
Dersom heile eller delar av løysinga skal kommunisere med noko som er utanfor kommunens interne nettverk – t.d. ei offentleg nettsky – skal denne trafikken være kryptert med DTLS/TLS 1.2.

Intern styringstrafikk skal krypterast
Ukrypterte protokollar som Telnet eller HTTP skal ikkje nyttast for å konfigurere utstyr.

Bruk av unike passord
Passord som blir brukt i løysinga skal ikkje være dei samme som hos andre kundar. Det skal heller ikkje nyttast standardpassord frå produsent. Alle passord skal delast med systemeigar.

Single Sign-On
Alle løysingar eller påloggingsmekanismer som støttar SAML, OpenID Connect, RADIUS eller LDAP skal nytte ein av desse for pålogging med brukarar frå Active Directory. For web-portalar og andre løysingar der sluttbrukar eller systemeigar sjølv skal logge på, er dette eit absolutt krav.

Bruk av dedikerte servicekontoar

Alle tenester skal ha kvar sin dedikerte servicekonto – normalt er denne registrert i Active Directory. Behov for servicekontoar skal meldast inn før installasjon.

Leverandørtilgang for fjerninstallasjon og -drift

Fjerntilgong blir gitt via app.ssikt.no. SSIKT tilbyr forskjellige løysingar gjennom denne, alt etter systemleverandørens behov. Desse behova må meldast inn før installasjon, samt namn, telefonnummer og tittel på alle personar som skal ha tilgang til å fjerndrifte løysinga. Det blir ikkje etablert leverandørspesfikke VPN-løysingar og liknande.