

IoT-säkerhet: Det här bör du tänka på när du planerar din IoT-lösning.

Digitala bedrägerier, intrång i företagsmiljöer och cyberkrigföring. Dagens hotbild gör dataskydd viktigare än någonsin. Trots det finns det fortfarande många som bygger IoT-lösningar utan att reflektera över hur data faktiskt skyddas. Här är säkerhetsaspekterna du bör tänka på när du kopplar upp – från sensor hela vägen till din egen IT-miljö.



Säkerhet från start

Bygg in säkerheten redan i planeringsfasen – inte efter att lösningen är på plats.



Klassificera din data

Kartlägg datans känslighet och verksamhetens risker för att välja rätt säkerhetsnivå.



Skydda hela kedjan

Från sensor och uppkoppling till plattform, IT-miljö och människan – robust säkerhet behöver byggas in i varje lager av IoT-ekosystemet.



Internet of Things (IoT) är inte längre bara en lovande teknik. Miljarder IoT-enheter skapar idag hållbara, innovativa och effektiva lösningar för företag världen över. Samtidigt ökar kraven på säkerhet i takt med att allt fler verksamhetskritiska processer blir uppkopplade.

Många organisationer prioriterar funktionalitet och snabb implementering när nya IoT-lösningar utvecklas. Säkerhetsfrågorna kommer ofta in senare i processen, vilket kan skapa onödiga risker och sårbarheter. IoT-lösningen bör istället ses som en naturlig förlängning av verksamhetens eget nätverk, där datasäkerhet och nätverkssäkerhet är en integrerad del av helheten från start.

IoT-säkerhet är särskilt viktigt i dagens geopolitiska läge. Cyberkriminella orsakar ekonomiska skador, stjäl affärskritisk information, saboterar verksamheter och riktar attacker mot samhällsviktig infrastruktur. Digital säkerhet har därför aldrig varit viktigare.

För att minimera sårbarheter och hantera risker krävs säkerhetslösningar som är anpassade efter verksamhetens behov. Samtidigt behöver lösningarna stödja efterlevnad av gällande regelverk och standarder, såsom GDPR och NIS2. Därför är det viktigt att se säkerheten som en sammanhängande kedja där varje lager bidrar till ett starkare skydd.

Börja med att klassificera och hitta rätt skyddsnivå på din data

IoT används på många olika sätt. Vissa företag har enkla lösningar – som ett fåtal temperatursensorer på kontoret för att optimera inomhusklimatet.
Andra bygger digitala tvillingar av samhällskritisk infrastruktur med miljontals sensorer och dataflöden till och från olika enheter. Säkerhetsbehoven varierar därför kraftigt.

Det första steget är att analysera hur kritisk IoT-lösningen är, hur känslig datan är och vilka system som påverkas av den. Klassificeringen avgör vilken säkerhetsnivå som behövs och vilka skyddsåtgärder som bör implementeras.

För affärs- eller samhällskritisk infrastruktur, som elnät, vattenförsörjning, trafikstyrning och sjukvård, krävs den högsta säkerhetsnivån. Med dedikerade IoT- och fibernät kan enheter kopplas direkt till verksamhetens datacenter utan att passera det publika internet.

Lösningarna bygger på segmentering, kryptering, multifaktorautentisering och **Zero Trust**, som är en säkerhetsstrategi som innebär att ingen användare eller enhet är betrodd som standard, och att åtkomst verifieras kontinuerligt, samtidigt som de stödjer europeiska regelverk och säkerhetskrav.

Starka skydd byggs lager för lager i hela IoT-kedjan

Hoten i det digitala landskapet gör säkerhet viktigare än någonsin. Med en genomtänkt helhetsstrategi kan företag tryggt ta tillvara på IoT:s möjligheter. Det kräver rätt kompetens, robusta enheter, säkra nätverk och plattformar med starka, inbyggda skydd.

Eftersom säkerhet behöver genomsyra hela lösningen är det viktigt att varje del fungerar tillsammans – från människor och processer till uppkoppling, nätverk och plattformar. När alla lager samverkar skapas förutsättningar för säker innovation, hög tillgänglighet och pålitliga dataflöden.

Granska varje del av IoT-kedjan
Läs mer om vad du behöver tänka på när du bygger en IoT-lösning och hur Telia jobbar för att optimera säkerheten i vår IoT-leverans.



De fem grundstenarna i en säker IoT-lösning

Granska varje del av IoT-kedjan och säkerställ att rätt skydd finns på plats, från den första sensorn till färdiga affärsinsikten. Titta närmare på organisationen, enheterna, simkorten, mobilnätet och IoT-plattformen.

Säkerhet börjar med människan

Säkerhet startar alltid med människor, oavsett hur tekniska systemen är. Bristande kunskap, rutiner eller medvetenhet ökar risken för misstag med stora konsekvenser.

Tips för en stark säkerhetskultur:
Uppdatera kompetenser – utbildning är lika viktigt som tekniska uppdateringar. Skapa öppenhet – håll regelbundna säkerhetsmöten där alla kan lyfta frågor och incidenter utan skuld. Gör det enkelt att be om hjälp, det är bättre med en fråga för mycket än ett misstag för mycket.

Så bygger Telia säkerhetskultur:
Hos Telia har vi en bred intern säkerhetskompetens – från juridik och nätverk till applikationer och dataskydd. Genom utbildning och samarbete sprider vi kunskap både internt och till våra kunder.

IoT-enheter och sensorer

IoT-enheter ute i fält är attraktiva mål för attacker. Enheterna är ofta många och geografiskt spridda och kan vara svåra att uppdatera och sakna avancerade säkerhetsfunktioner.

Tips för säkra enheter:
Säkerställ att IoT-enheterna följer tekniska standarder, kan uppdateras på distans och har en etablerad livscykelhantering för löpande säkerhets-uppdateringar. Säkra kommunikationen till och från enheten utifrån hur datat är klassat. Samarbeta med tillverkaren och operatör för att förstå hur enheten skyddas mot attacker.

Så säkrar Telia enheterna:
Vi erbjuder verktyg för att övervaka, uppdatera och skydda enheter på distans. Våra experter samarbetar med ledande tillverkare för att säkerställa korrekt konfiguration och säker kommunikation.

Simkort och uppkoppling

IoT-enheter använder simkort (fysiska eller e-sim). Ett borttappat simkort kan ge obehöriga tillgång till interna system.

Tips för god simkorts-säkerhet:
Segmentera nätverket – låt bara enheter kommunicera med definierade system. Ha rutiner för att upptäcka och stoppa misstänkt aktivitet i realtid. Har ni många simkort? Inventera så att inget försvinner.

Så säkrar Telia simkorten:
Våra simkort kan kopplas till specifika enheter och spärras om de flyttas eller används i fel land. De autentiseras mot vårt mobilnät för säker kommunikation.



Mobilnätet

Mobilnätet transporterar IoT-enheters data och utgör därför en central del av säkerhetskedjan. Med ett licensierat mobilnät, som Telias, får man säkerhet inbyggd från början.



Tips för säker datatransport:

- Använd privata eller dedikerade nät – isolera IoT-trafiken från annan mobiltrafik.
- Välj nät från en licensierad operatör – det minskar risken för störningar och intrång.
- Segmentera trafiken och begränsa åtkomst till definierade servrar.
- Övervaka trafiken kontinuerligt och agera automatiskt vid avvikelser.
- Ha en tydlig incidentplan – vem gör vad vid ett angrepp?

Säker trafikhantering:
IoT-enheter kopplas till nätet via simkort som autentiserar mot rätt APN (Access Point Name). Varje APN är sluten, vilket hindrar enheter från att kommunicera direkt med varandra.

Tre transportvägar med olika säkerhetsnivå:

- Internet: för enklare, mindre kritiska lösningar.
- IPsec VPN: krypterad överföring med verifierad avsändare och mottagare.
- DataNet: all data stannar i Telias fibernät och når kundens datacenter utan att passera internet – för högsta tillgänglighet och prestanda.

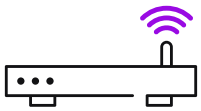
Så säkrar Telia sitt mobilnät:
Telias säkra och robusta nät täcker mer än 99,9 procent av befolkningen och 90 procent av Sveriges yta. Vi har full kontroll över våra nät och är inte beroende av externa aktörer. Våra licensierade nät bygger på GSMA- och 3GPP-standarder och uppfyller samtliga regulatoriska krav. Telias mobilnät stödjer 2G*, 4G (LTE), NB-IoT, LTE-M, 5G NSA och 5G SA

– reserverat för specifika användare och tjänster för maximal tillförlitlighet.

**Planerad nedstängning av 2G-nätet: 2027-12-31*

Avancerad 5G – 5G Standalone (5G SA) – nästa steg i mobilnätsutvecklingen

Till skillnad från tidigare generationer är 5GSA byggt helt på en ny kärnnätverksarkitektur som möjliggör högre säkerhet, ökad tillförlitlighet och mer flexibilitet. Funktioner som end-to-end-kryptering, nätverksisolering och privata nätverk ger verksamheter – särskilt viktigt inom sjukvård, industri och räddningstjänst – full kontroll och skydd på högsta nivå.



IoT-plattform

En IoT-plattform samlar in, lagrar och hanterar data från tusentals enheter och system. Via dashboards får användaren realtidsöverblick via visualiseringar och tabeller samt där data kan analyseras över tid.



Tips för en säker IoT-plattform:
Bygg enligt ett Zero Trust-ramverk – där ingen enhet eller användare får tillgång utan verifiering. Nätverket delas in i zoner med egna säkerhetsregler och segmentering av trafiken begränsar åtkomst. Segmentera användare, roller och kunder för att undvika dataläckor. Automatisera uppdateringar, loggning och övervakning för att minska mänskliga fel.

Så säkrar Telia plattformen:
Telias IoT-plattform har inbyggda säkerhetsfunktioner. Varje kund har ett eget isolerat område (tenant). Data lagras inom EU enligt GDPR. Åtkomst styrs via Telias lösningar för användarhantering (IAM och SSO). Kommunikation via API:er är krypterad, verifierad och spårbar.

Så kopplar du upp säkert i hela IoT-leveransen.

Verksamheten

Utbilda. Engagera.
Gör enkelt att rapportera.

- Öka intern kunskap kontinuerligt = första försvarslinjen
- Verktyg och processer för att hantera incidenter
- Skapa öppen säkerhetskultur med regelbundna säkerhetsmöten



IoT-plattform

Zero Trust. Segmentering.
Övervakning.

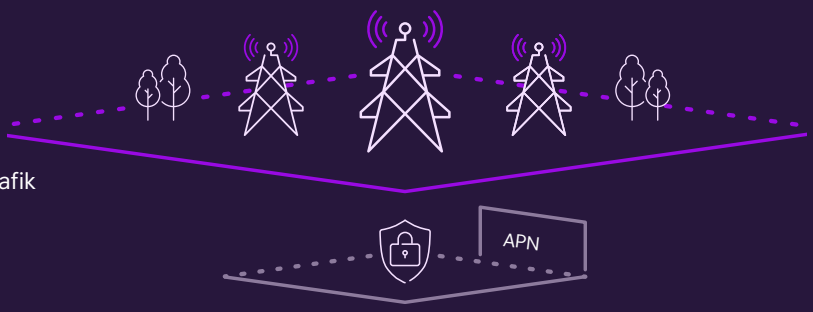
- Ingen åtkomst utan stark autentisering
- Zoner med egna säkerhetsregler
- Automatiska loggar och uppdateringar



Mobilnätet

Isolera IoT-trafik. Använd licensierat nät.
Segmentera.

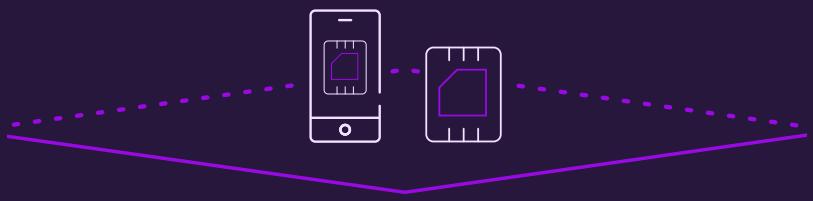
- Använd privata eller dedikerade nät för känslig IoT-trafik
- Segmentera trafiken och begränsa åtkomst
- Övervaka nättrafiken och ha en incidentplan



SIM-kort & uppkoppling

Segmentera. Inventera.
Övervaka aktivitet.

- Segmentera nätverket och begränsa åtkomst
- Övervaka och stoppa misstänkt aktivitet
- Inventera och kontrollera alla simkort



IoT-enheter

Följ standard. Uppdatera.
Skydda kommunikation.

- Välj enheter som kan uppdateras på distans
- Etablera livscykelhantering för löpande säkerhetsuppdateringar
- Skydda kommunikation och data till/från enheten
- Säkerställ att enheten uppfyller relevanta säkerhetskrav
- Samarbeta med tillverkare och opeatör för att optimera säkerheten



Läs mer om Telias IoT-lösningar: telia.se/foretag/iot

Telia