Myndigheten för samhällsskydd och beredskap

FAKTA

Publ.nr: MSB1252 – juni 2018

AVDELNINGEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

# Så säkrar du ditt IoT

## Råd till systemägare och nyttjare

**För att uppnå bättre IoT-relaterad säkerhet behöver alla parter i en produkts livscykel bedriva ett aktivt arbete. Tillverkare, integratörer och systemutvecklare har ett stort ansvar för att förbättra produkten eller tjänsten och tydliggöra begränsningar avseende säkerhet och funktionalitet. Systemägare och nyttjare måste i sin tur tillse att implementation och användning sker på ett passande sätt, inte minst med hänseende till existerande begränsningar i säkerhet.**

Här ges utförligare exempel på vilka åtgärder en systemägare och nyttjare kan vidta för att minska sina IoT-relaterade risker.

I en attack används IoT oftast mer som medel än som mål. Det vill säga då IoT-produkter och tjänster ofta är en säkerhetsmässigt svag punkt används de som en språngbräda in mot egna eller andras mer kritiska system. Det är alltså ofta inte attacken mot den enskilda IoT-produkten eller tjänsten som renderar de allvarligaste konsekvenserna och är slutmålet för en attack. Det är därför viktigt att fortsätta utveckla det ordinarie säkerhetsarbetet för information och system med högt skyddsvärde, det vill säga för system där otillgänglighet, felaktigheter och förlust eller spridning av känslig information i sin tur medför allvarliga konsekvenser. Det handlar om ett arbete både för att minska sårbarheterna och lindra konsekvenserna.

Stöd i arbetet går att hämta bland annat i *Vägledning till ökad säkerhet i industriella informations- och styrsystem* (www.msb.se/ics) som i många stycken är användbar även för IoT. På www.informationssakerhet.se finns även ett metodstöd för systematiskt informationssäkerhetsarbete. Det finns även mer direkta IoT-relaterade åtgärder som en systemägare eller nyttjare kan vidta för att öka säkerheten.

### Konkreta råd till systemägare och nyttjare

Det inledande rådet är att säkerställa att enheterna uppfyller grundläggande säkerhetskrav, exempelvis via kravställning på leverantör, importör eller distributör. Det handlar till exempel om att kravställa att det finns en livscykelstrategi för systemet.

**Internet of Thing (IoT)**
eller sakernas internet är ett begrepp som används för att beskriva att allt fler föremål, både för privat och industriellt bruk, utrustas med möjligheten att anslutas till internet och andra nätverk. Anslutningen kan ge fördelar och möjliggöra många nya tjänster, men innebär också många utmaningar. Exempelvis har lösningarna ofta låg säkerhet med otillräckligt skydd mot obehörigt användande. Incitamentet att sälja IoT-enheter i stora volymer till relativt låga anskaffningskostnader, tillsammans med begränsad energi- och beräkningskapacitet hämmar också möjligheterna att skapa god säkerhet.

Mer information om säkerhet i IoT, industriella informations- och styrsystem och andra cyberfysiska system finns på: www.msb.se/ics

**Faktablad om IoT:**

- *IoT-relaterade risker – Begrepp och kategorisering.*
- *Så säkrar du ditt IoT – Råd till systemägare och nyttjare*
- *Säkrare IoT – Rekommendationer till myndigheter.*

- Hårdvaran har inbyggda säkerhetsattribut som stödjer t.ex. kryptering och anonymitet.
- Mjukvaran som används underhålls kontinuerligt och att kända säkerhetsbrister har åtgärdats.
- Mjukvaran i en enhet kan säkerhetsuppdateras på ett säkert sätt.
- Enheten är designad med viss tolerans mot avbrott eller fel hos andra enheter.
- Enheterna har ett bra lösenordsskydd, exempelvis genom att produkterna levereras med ett unikt lösenord som kan ändras.
- Säkerhetsaspekten beaktas i utvecklingsprocessens alla steg, inklusive val av plattformar, programspråk och verktyg.

Som systemägare och nyttjare handlar det därtill om att vidta ett antal åtgärder, som till exempel att:

- Installera utrustning på ett säkert sätt. Det kan handla om att minimera risken för fysisk manipulation om den är placerad på en offentligt tillgänglig plats eller att segmentera dina IoT-enheter på ett separat nät för att kunna kontrollera trafiken och tillse att endast godkänd trafik släpps igenom.
- Tillämpa medveten uppkoppling med kunskap om de risker som uppkopplingen medför. Detta innebär exempelvis att:
  - Direkt internetuppkoppling ska inte vara nödvändigt för kritiska funktioner i en IoT-enhet, särskilt inte i industriella sammanhang.
  - Avsikten med olika nätverksanslutningar ska klargöras och kommuniceras med berörda parter.
- Om möjligt installera program som skyddar mot virus och annan skadlig kod.
- Genomföra säkerhetsuppdateringar, övervakning och underhåll.
- Logga och analysera händelser i systemet för att upptäcka intrång.
- Skydda autentiseringsuppgifter och använda starka lösenord.
- Tillämpa ett djupt försvarstänkande, det vill säga att säkerhet implementeras i olika abstraktionslager, ytterst med verktyg på användarnivå för att skydda mot angrepp från exempelvis insiders.
- Uppmärksamma systemanvändare på riskerna med nätfiske (eng. phishing) och social manipulation (eng. social engineering).
- Vara delaktiga i olika plattformar för informationsdelning. Dels för att rapportera sårbarheter, dels för att erhålla aktuell information om hot och sårbarheter från offentliga och privata aktörer.

## Kontakta Myndigheten för samhällsskydd och beredskap

651 81 Karlstad

Tfn: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se