Myndigheten för samhällsskydd och beredskap

FAKTA

Publ.nr: MSB1251 – juni 2018

AVDELNINGEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

Säkrare IoT

Rekommendationer till myndigheter

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 säkerhetsmässigt passande sätt, inte minst med hänseende till existerande begräsningar i säkerhet. Vissa åtgärder för förbättrad säkerhet kan myndigheter eller andra offentliga aktörer genomföra. Det finns också åtgärder som lämpligen genomförs i samarbete mellan privata och offentliga aktörer. Nedan beskrivs ett antal sådana tänkbara åtgärder.

En självklar uppgift för myndigheter och andra offentliga aktörer som har ansvar inom området eller är verksamma inom området på annat sätt är att bidra till det medvetandehöjande arbetet. Det medvetandehöjande arbetet bör riktas både till det offentliga Sverige, privat sektor och till privatpersoner för att få ett tydligt genomslag.

Andra möjliga åtgärder är:

- Framtagande av vägledningar, råd och utbildningar inom området. Exempel på frågeställningar som kan belysas är:
  - Kravställning och beställarkompetens avseende IoT-produkter och IoT-beroende tjänster.
  - Säker implementation och arkitektur.
  - Vikten av starka lösenord, flerfaktorsautentisering och god lösenordshantering.
  - Vikten av att IoT-enheter enbart är avsiktligt uppkopplade.
- Verka för att utveckla ordinarie säkerhetsarbete inom samhällsviktig verksamhet i syfte att minska konsekvenserna av en eventuell händelse.
- Medverka till att det finns en aktuell lägesbild innehållandes exempelvis potentiella sårbarheter, vilka som exploateras och vilka som leder till allvarliga konsekvenser.

Internet of Things (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.*

- Inkludera risker med IoT vid övningar.
- Stödja forskning inom området säkerhet och IoT.
- Kontrollera och praktiskt testa säkerheten hos IoT-enheter och tjänster.
- På olika sätt genomföra förebyggande insatser gällande exempelvis lösenordshantering, fysisk exponering och informationsstöld.

För att minska riskerna inom IoT kan myndigheter såsom MSB exempelvis skapa och delta samverkansgrupper i samarbete med privata aktörer för att:

- Utveckla arbetet med hur information om sårbarheter offentliggörs och tillhörande praxis för hantering av dem.
- Möjliggöra informationsdelning.
- Verka för att syfte och metod för enheters uppkoppling är tydligt beskriven och att säkerhetsaspekter är inkluderade redan i designarbetet av nya produkter.
- Arbeta för att säkerhetsaspekter hanteras i standardiseringsarbete.
- Genomföra riskbedömningar över hela försörjningskedjan, inklusive tredjepartsleverantörer.

Det är ofta oklart vem som ansvarar för säkerheten i en viss produkt eller ett visst system. Kostnaden för bristande säkerhet bärs sällan av de som har bäst förutsättningar att höja säkerheten, vilket bidrar till sårbarheter. Möjliga sätt för offentliga aktörer att stärka incitamenten för säkrare IoT-produkter och tjänster kan vara att:

- Verka för att inom ramen för internationella samarbeten införa regler som syftar till att åstadkomma en acceptabel lägstanivå vad gäller säkerhet.
- Verka för att de produkter som säljs i landet eller används inom offentlig verksamhet håller en viss säkerhetsnivå.
- Verka för olika typer av negativa eller positiva ekonomiska incitament såsom skadeståndsansvar, cyberförsäkringar och frivillig certifiering.
- Verka för att statlig reglering och övriga lagar och regler bidrar till att höja säkerheten.

Kontakta Myndigheten för samhällsskydd och beredskap

651 81 Karlstad

Tfn: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se