Faktablad

Avdelningen för cybersäkerhet och säkra kommunikationer
Publ.nr MSB1523 – mars 2020

IoT-relaterade risker, uppdaterad version

Begrepp och kategorisering

Internet of Things (IoT), eller sakernas internet, för med sig stora möjligheter men innebär också risker. Dessa risker behöver tydliggöras för att kunna identifiera relevanta åtgärder. Även begreppsanvändningen behöver ensas. Detta faktablad presenterar ett antal begrepp och definitioner inom ämnet, samt kategoriserar olika risker på en övergripande nivå.

Ordet risk är svårdefinierat och tenderar användas med olika innebörd. Det är inte ovanligt att begreppen hot och risk blandas ihop. Risk är kombinationen av att ett hot kan realiseras utifrån en viss grad av sannolikhet, och därmed leder till en negativ konsekvens. För att en risk ska uppstå måste det finnas ett hot samt att hotet kan uttnyttja en sårbarhet. För att veta skyddsbehovet hos det som ska skyddas måste hoten, sårbarheterna och konsekvenserna identifieras. Det är även viktigt att veta vilka risker som kan accepteras, ex. av ekonomiska skäl. För att förstå riskerna relaterade till IoT är det relevant att vara bekant med begreppen sårbarheter, attackvektorer, skyddsbehov, samt hot och risk.

Sårbarheter hos IoT

För IoT som teknologi kan generella egenskaper som medför potentiella sårbarheter pekas ut. Sårbarheter för IoT kan grupperas enligt följande:

Komplexitet: Antalet IoT-enheter antas komma att öka snabbt, och antalet kommunikationsvägar mellan dessa antas öka ännu snabbare. Vidare kommer antalet tillverkare och antalet varianter av hårdvara, mjukvara och protokoll att växa vilket innebär problem med den systemförståelse som krävs för att säkra systemen.

Designförbättringar: Detta rör konstruktion och funktion. IoT-enheter har generellt mycket begränsade resurser vad gäller energi- och beräkningskapacitet. Detta medför att det

Sårbarhet

Avsaknaden eller brist i en struktur som skulle kunna förhindra eller bidra till att förhindra att en incident inträffar. Alternativt förhindra eller bidra till att mildra konsekvensen av en incident.

Attackvektor

Det sätt på vilket ett angrepp utförs och vilken struktur (teknisk eller samhällelig) som angreppet riktas mot.

Skyddsbehov

Något som är i behov av att skyddas. Det kan vara en process, en verksamhet, information, byggnad, utrustning eller personer. Typ av skydd beror på behovet av konfidentialitet, riktighet och tillgänglighet.

Hot

Möjlig eller oönskad händelse som orsakar eller bidrar till att orsaka att en incident med negativa konsekvenser för organisationen inträffar.

Risk

Definieras som kombinationen av att ett hot kan realiseras med en viss sannolikhet, vilket därmed leder till en negativ konsekvens. Det är med avseende på risken som en åtgärd, eller strategi, definieras och utformas.

Hela studien
IoT relaterade risker och strategier – Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem

Rapportnr: MSB 2017-1554, finns att tillgå via www.msb.se

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap

ofta inte på ett bra sätt går att balansera säkerhetsmekanismer, såsom kryptering, mot enhetens primärsyfte. Ofta beaktas inte säkerhet, vilket exempelvis kan innebära brist på förmåga att i efterhand uppdatera och täppa till eventuella säkerhetshål i enhetens mjukvara.

Exponering: IoT-enheter är sårbara för fysisk åtkomst, vilket förenklar manipulation. Det stora antalet skapar möjlighet att otillåtet inhämta information. Det är vanligt att både tillverkare och användare lösenordsskydd håller en låg nivå, vilket ökar risken för otillbörligt användande och skadlig kod.

Attackvektorer mot IoT

Dessa är i många fall gemensamma med dem för klassisk IT. De kan grupperas enligt vilken del av IoT de riktas mot: perceptionslagret, överföringslagret, eller applikationslagret. Exempelvis kan störsändning användas mot de första två.

Risker

För IoT kan risker grupperas utifrån att de har konsekvenser som äventyrar ett eller flera av skyddsvärdena konfidentialitet, riktighet och tillgänglighet.

- *Konfidentialitet*: IoT-enheter kan användas som språngbräda in i traditionella it-system för att stjäla information. Genom att dessa enheter i många fall är avsedda att inhämta information, genom t.ex. kameror och mikrofoner, möjliggör de inhämtning av individinformation och spionage.
- *Riktighet* där IoT är måltavlan: möjligheten att manipulera enheter medför risk både på individ- och samhällsnivå. Exempelvis om en enskild medicinpump manipuleras eller storskalig manipulation av smarta elnät.
- *Riktighet* där IoT är verktyget: möjligheten att ta över IoT enheter för att skapa exempelvis botnet för DDoS-attacker.
- *Tillgänglighet*: IoT-enheter kan göras obrukbara, exempelvis i utpressningssyfte, eller som en sidoeffekt av att de tas över för andra ändamål, exempelvis som en del i ett botnet.

Åtgärder

Kan sättas in mot sannolikheten att hotet realiseras eller den beräknade konsekvensen av händelsen. Sannolikheten kan minskas genom att arbeta aktivt med kravställning och medvetandehöjande arbete inom organisationen. Genom kontinuerligt utvecklande av organisationens ordinare säkerhetsarbete kan även konsekvenserna minska.

IoT-arkitektur

Perceptionslager – samlar in data om den omgivande miljön med hjälp av bland annat sensorer, kameror, GPS, etc. Här kan också fysisk påverkan av omgivande miljö ske samt samarbete mellan lokala noder.

Applikationslager – bearbetar den mottagna informationen och utfärdar kommandon till de fysiska enheterna.

Överföringslager – där utbyte och bearbetning av data mellan perceptions- och applikationslagret genomförs. Överföring av data kan ske genom lokala nätverk eller över internet.

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

Faktablad om IoT:

Via MSB:s hemsida finns följande faktablad om IoT att tillgå.

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

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap