Myndigheten för samhällsskydd och beredskap

FAKTA

Publ.nr: MSB1248 – juni 2018

AVDELNINGEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

IoT-relaterade risker

Begrepp och kategorisering

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 deras definitioner samt kategoriserar olika risker på en övergripande nivå.

Ordet risk är svårdefinierat och används ofta med olika innebörd. Det är inte ovanligt att till exempel hot och risk blandas ihop. Risk är kombinationen av sannolikheten för att ett givet hot realiseras och därmed uppkommen skadekostnad (konsekvens). För att en risk ska uppstå måste det finnas ett hot och ett sätt på vilket hotet kan realiseras. Hotet kan realiseras via attackvektorer och sårbarheter. För att identifiera hot måste även skyddsvärden vara definierade eftersom det är skyddsvärdet som gör det meningsfullt att diskutera oönskade händelser och deras konsekvenser. För att förstå riskerna relaterade till IoT är det därför relevant att vara bekant med begreppen sårbarheter, attackvektorer, skyddsvärden, hot och risk.

Sårbarheter hos IoT

För IoT som teknologi kan generella egenskaper hos IoT-enheter 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 medför problem med den systemförståelse som krävs för att säkra systemen.

Designförutsättningar: Detta rör konstruktion och funktion. IoT enheter har generellt mycket begränsade resurser vad gäller energi- och beräkningskapacitet. Detta medför att det ofta inte går att på ett bra sätt balansera säkerhetsmekanismer, såsom kryptering, mot enhetens primärsyfte. Ofta beaktas inte ens säkerhet, vilket exempelvis kan medföra brist på förmåga att i

Sårbarhet – Vad i en struktur som är mottagligt för en attack.

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

Skyddsvärden – Det som är värt att skydda i relation till oönskade händelser och konsekvenser. På en övergripande nivå kan elementen i CIA-triaden användas. C står för confidentiality (konfidentialitet), I för integrity (riktighet) och A för availability (tillgänglighet).

Hot – Möjlig och oönskad händelse med negativa konsekvenser.

Risk – Kombinationen av sannolikhet för att ett givet hot realiseras och därmed uppkommen skadekostnad (konsekvens). Det är med avseende på risken som en åtgärd, eller en strategi, kan definieras. Den specifika åtgärden kan sedan sättas in mot sannolikheten för att hotet realiseras eller konsekvensen, beroende på om det är sannolikheten för den oönskade händelsen eller konsekvenserna av den som ska minskas.

efterhand uppdatera och täppa till eventuella säkerhetshål i enhetens mjukvara.

Exponering: Detta rör hur enheter används. IoT-enheter är sårbara för fysisk åtkomst vilket förenklar manipulation. Deras antal skapar möjlighet att otillåtet aggregera information. Det kan antas att lösenordsskydd från både tillverkare och användare kommer hålla 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. Dock kan de grupperas enligt vilken del av IoT de riktas mot: perceptionslagret, överföringslagret, eller applikationslagret. Exempelvis kan störsändning användas mot de första två.

Risker

Risker med IoT kan 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 direkt genom sin användning 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

Åtgärder kan sättas in mot sannolikheten för att hotet realiseras eller konsekvensen av händelsen. Sannolikheten kan minskas genom att arbeta aktivt med kravställning och eget arbete. IoT är dessutom i många fall en språngbräda in mot mer kritiska system snarare än ett mål i sig själv – genom att fortsätta utveckla det ordinarie säkerhetsarbetet kan en organisation systematiskt minska konsekvenserna.

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.

Överföringslager – där utbyte och bearbetning av data mellan perceptionslagret och applikationslagret genomförs. Överföringen av data kan ske genom lokala nätverk och över internet.

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

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

FAKTA-blad om IoT:

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

Kontakta Myndigheten för samhällsskydd och beredskap

651 81 Karlstad

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