SÄRTRYCK UR STRATEGISK UTBLICK 7

Internet of Things

En IT-säkerhetsmässig mardröm

Daniel Eidenskog och Farzad Kamrani

Internet of Things (IoT) är ett samlingsnamn för produkter som innehåller elektronik med någon form av uppkoppling mot andra system, vanligtvis via internet. Antalet cyberangrepp som involverar IoT-enheter har ökat under senare år, vilket tillsammans med det förändrade omvärldsläget gör att risken är överhängande för större och mer utbredda cyberangrepp där IoT-enheter är centrala. Sveriges totalförsvar bygger i stor utsträckning på motståndskraften i de normala samhällsfunktionerna. Många av dessa har internetanslutna system som till del baseras på IoT-produkter, vilket gör systemen särskilt sårbara samtidigt som samhällskritisk verksamhet utgör en tydlig måltavla för cyberangrepp. För att på sikt minska risken för allvarliga cyberangrepp med störningar i samhällskritisk verksamhet bör Sverige ha en tydlig strategi inom cybersäkerhetsområdet. Sverige bör också ta en aktiv roll i arbetet för ökad cybersäkerhet i kommersiella IoT-produkter.

En tillväxtmarknad med litet säkerhetsfokus

Internet of Things (IoT) utgör en bred marknad där produkter inom en rad olika segment ingår, exempelvis hushållsapparater, fordon, byggnadssystem och industriella maskiner. Tillväxttakten inom IoT-marknaden är hög och flera marknadsanalysföretag förutspår en global ökning från ungefär fem miljarder enheter år 2015 till drygt 75 miljarder enheter år 2025.

Marknadsanalytikerna förutspår att privatpersoner kommer äga en majoritet av dessa IoT-enheter. Privatpersoner utgör ett kundsegment där cybersäkerhet inte är ett viktigt kriterium vare sig vid inköpstillfället eller senare under produktens användning. Istället är nya funktioner och lågt pris ofta drivande faktorer. Det saknas även reglering av cybersäkerhetsaspekter och det är svårt att få tillverkare ansvarsskyldiga för sårbarheter i deras produkter. Tillverkarna har därmed generellt sett små incitament att satsa på cybersäkerhet. Detta leder därför i många fall till produkter med en säkerhetsnivå som ligger långt efter många andra IT-områden.

Även inom IoT-segment som riktar sig mot professionella användare är säkerheten ofta bristfällig. Detta har exempelvis visat sig genom omfattande säkerhetsbrister i professionella nätverksanslutna övervakningskameror. I flera fall har säkerhetsbristerna legat på en nivå som antyder att mjukvaran utvecklats i total avsaknad av grundläggande förståelse för cybersäkerhet.

Givet den stora mängden av IoT-enheter innebär avsaknaden av säkerhetsfokus att cyberangrepp som riktar sig mot eller utnyttjar IoT-produkter riskerar att få stor omfattning. Angreppen kan därmed påverka såväl internetinfrastrukturen som potentiellt samhällsviktiga system och enskilda individer.

Totalförsvaret är beroende av internet

Sveriges totalförsvar bygger på att de normala samhällsfunktionerna kan upprätthålla ett fungerande samhälle även i händelse av kris eller krig, enligt den så kallade ansvarsprincipen. Det gäller både militära och civila funktioner där avbrott och störningar i den egna verksamheten kan påverka hela samhället och dess innevånare. Grundläggande samhällsviktiga sektorer som dricksvattenförsörjning, energiförsörjning, livsmedelsdistribution och kommunikationer är alla beroende av såväl IT-system som industriella styrsystem för sin funktion.

Många system inom kritiska sektorer har anslutningar till internet och bygger åtminstone delvis på IoT-produkter, vilket sätter systemen i riskzonen för cyberangrepp. I det förändrade omvärldsläget är risken överhängande att allt större och mer utbredda angrepp görs mot samhällskritiska funktioner, där angreppen riktas mot IoT-produkter eller där IoT-produkter används som en språngbräda för att förstärka angreppen.

Sveriges omfattande beroende av informationsteknologi innebär att samhället är utsatt för cyberrisker som knappast gick att föreställa sig för bara ett par decennier sedan. Med beroendet av internet som infrastruktur och med vitala samhällsfunktioner i riskzonen för cyberangrepp blir de potentiella konsekvenserna stora vid utbredda angrepp.

För att på sikt minska risken för allvarliga cyberincidenter med efterföljande störningar i kritisk verksamhet bör Sverige

FOI Memo 6172
Godkänd av: Lena Bartholdson

Särtryck ur Strategisk utblick 7
November 2017

arbeta aktivt med cybersäkerheten inom IoT-området:

Sverige bör ha en tydlig strategi med syfte att öka kunskapen och beredskapen inom cybersäkerhetsområdet. En viktig del i en sådan cybersäkerhetsstrategi är att tydliggöra vikten av de system och komponenter som staten inte har kontroll över. Krishanteringens närhetsprincip är lämplig när det gäller att hantera en akut krissituation, men grundproblemet, att det är relativt enkelt att genomföra cyberangrepp oavsett var man befinner sig, går inte att hantera på lokal nivå.

Sverige bör ta en aktiv roll i arbetet för ökad cybersäkerhet i kommersiella produkter, exempelvis inom EU-samarbetet. Cybersäkerhetsfrågor är i grunden globala för alla system med koppling till internet, vilket innebär att arbetet för förbättrad cybersäkerhet måste bedrivas på både nationell och internationell nivå. Cybersäkerhetsläget på den privata marknaden påverkar samhället och måste ingå som en del av statens arbete inom cybersäkerhetsområdet.

Personlig integritet är större än personen

En annan aspekt av IoT-enheternas täta närvaro berör personlig integritet, som i förlängningen även kan påverka nationell säkerhet. Många IoT-enheters syfte är att samla in information om användaren, exempelvis i form av platser som besöks, hälsostatus, träningsvanor eller andra aktiviteter. Informationen förs i regel vidare till tillverkarens molntjänster så att användaren kan nyttja dessa för olika ändamål, samtidigt som tillverkaren får tillgång till informationen för sitt bruk.

Ett grundläggande problem är att IoT kan introducera många nya risker för den personliga integriteten, oftast i snabbare takt än rättsliga mekanismer och sociala normer kan anpassa sig. I en värld där allt fler saker är anslutna till internet sänks kostnaderna för insamling, lagring, bearbetning och delning av data dramatiskt. Integritetsriskerna sträcker sig från vardagliga och enkla problem såsom överbeskyddande föräldrars övervakning av sina barn och alltför påträngande marknadsföring till mer allvarliga fall där regeringar och statliga aktörer begränsar medborgarnas frihet eller utför angrepp mot andra länder.

Den rikedom av information som är åtkomlig genom IoT-enheter kombinerat med utökad beräkningskapacitet och effektivare algoritmer skapar stora möjligheter att identifiera, övervaka, avlyssna och spåra individer samt att kartlägga deras beteendemönster. IoT-enheter använder ofta passiva metoder för datainsamling, vilket resulterar i att användarna i regel är mindre medvetna om att de övervakas.

Personer som innehar nyckelbefattningar i samhället riskerar att bli måltavlor för riktade angrepp som bland annat kan nyttja IoT-enheter. Riktade angrepp mot individer sker oftast med hjälp av välinformerad och sofistikerad social manipulation kombinerat med tekniska angrepp. Den brittiska journalisten och människorättsaktivisten Rori Donaghy utsattes för ett sådant riktat angreppsförsök, genom en kombination av social manipulation och skadlig kod. Framgångsrik social manipulation förutsätter att angriparen har goda kunskaper om den som utsätts för attacken, något som kan uppnås genom att samla in information från flera olika källor. Genom att angripa IoT-enheter och få tillgång till den stora mängd data som dessa potentiellt har så ökar möjligheten för en angripare att genomföra lyckade angrepp mot specifika nyckelpersoner.

Avlyssning har länge varit en välkänd metod för att samla in just den typ av information som beskrivs ovan, men ett hinder har varit svårigheten att placera lämplig avlyssningsutrustning i personernas närhet. Med den snabba tillväxten inom IoT-området sker en dramatisk ökning av antalet enheter som kan användas för avlyssning; enheter som dessutom placeras ut frivilligt av den som kartläggs. Exempel på enheter som kan användas för avlyssning är IP-kameror, datorer, smartphones, smarta klockor, trådlösa headsets och enheter för röststyrning av hem.

Stora mängder sårbarheter och angrepp

Tidigare handlade cyberattacker huvudsakligen om angrepp mot informationssystem, datanät och persondatorer. Med IoT kommer den fysiska världen i form av sensorer, ställdon, kontrollsystem och vardagliga objekt i allt större utsträckning att sammanflätas med internet, vilket möjliggör nya typer av angrepp. IoT-enheternas intåg innebär att en angripare kan ta kontrollen över de fysiska objekten och orsaka fysisk förstörelse eller till och med förlust av liv. Stuxnet-masken som riktade sig mot anrikningsanläggningar i Iran, angreppet mot det ukrainska elnätet 2015 och demonstrationer där forskare tagit total kontroll över en bil genom dess internetanslutning visar att angrepp mot IoT-enheter kan omfatta helt nya dimensioner än de som tidigare har observerats.

Säkerhetsbrister i installerade produkter åtgärdas sällan då det i många fall är en komplex procedur att installera uppdateringar och att detta måste göras manuellt av konsumenten. Dessutom är det vanligt att produkterna

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick

fortfarande används flera år efter att tillverkaren slutat släppa säkerhetsuppdateringar, något som gör det omöjligt för konsumenten att undvika säkerhetsbrister.

Överbelastningsattacker som använder IoT-enheter har ökat i antal under de senaste åren och har åstadkommit några av de kraftigaste störningarna på internet någonsin. I oktober 2016 attackerades en så kallad namnuppslagningsfunktion. Detta resulterade i att ett antal webbplatser var oåtkomliga för de flesta användare under flera timmar. Bland de drabbade webbplatserna fanns de svenska myndighetssidorna krisinformation.se och regeringen.se, men även ett antal kommersiella tjänster och nyhetsplatser såsom Netflix, Spotify, Twitter, BBC, CNN och Fox News. Detta angrepp, likväl som flera andra omfattande överbelastningsattacker, byggde på skadlig kod som infekterat stora mängder IoT-enheter.

Många angrepp leder till att angriparen får fullständig kontroll över enheten och dess information. I de fall där syftet är mer riktat mot personen eller organisationen som använder IoT-enheten kan användningen vara betydligt mer utstuderad än för exempelvis överbelastningsattacker. Det har exempelvis visats hur enkelt det är att manipulera videoströmmen som levereras av en nätverksansluten övervakningskamera för att dölja en händelse.

Delar av det ukrainska elnätet stängdes ner genom ett omfattande och avancerat IT-angrepp i december 2015. Angreppet byggde nästan uteslutande på sårbarheter i traditionella IT-system men inkluderade även angrepp mot IoT-liknande enheter. Under angreppet byttes mjukvaran ut i vissa komponenter vilket resulterade i att kommunikationen till anläggningarna inte längre fungerade. Detta medförde i sin tur att det krävdes manuella åtgärder på plats för att få igång eldistributionen och att delar av elnätet inte gick att fjärrstyra förrän den drabbade utrustningen hade ersatts.

Förstörande angrepp har även dykt upp på internet genom skadlig kod som riktar sig mot vissa IoT-enheter och gör dessa obrukbara. Det har spekulerats i vem som är det egentliga målet för dessa angrepp. En teori är att de är riktade mot tillverkarna som påverkas negativt av garantiärenden och dålig publicitet till följd av angreppen, där risken att tappa kunder och därmed förlora pengar anses kunna ge ett ökat incitament för säkrare produkter.

Angrepp där målet är att komma åt information i IoT-enheter riktas ofta mot enskilda personer eller organisationer, ofta opportunistiskt eller slumpvis valda, där information kan samlas in eller system tas över för exempelvis utpressningssyften, kartläggning eller övervakning. Uppmärksammade produkttyper är nätverksanslutna övervakningskameror och babymonitorer, som i ökande utsträckning förekommer i privatbostäder. Kända säkerhetsbrister är emellertid inte begränsade till dessa två produktkategorier utan har påvisats i ett brett spektrum av produkter såsom smarta TV-apparater, insulinpumpar, leksaker, vitvaror, industriella diskmaskiner, termostater, bilar och sexleksaker.

Det är synnerligen viktigt att IoT-leverantörer får kännedom om sårbarheter så att dessa kan åtgärdas. Det förekommer att statliga aktörer samlar kunskap om sårbarheter för egen underrättelseverksamhet istället för att rapportera dem till leverantörerna och göra dem allmänt kända, vilket är mycket oroande. Det finns inga garantier att kunskapen inte läcks och skadar allmänheten, något som även har inträffat då en läckt sårbarhet använts i ett utpressningsvirus som nått omfattande spridning.

Styrmedel för cybersäkerhet saknas

I dagsläget saknas det i princip styrmedel för att förbättra cybersäkerheten i civila produkter. Kundernas krav på cybersäkerhetsområdet är än så länge låga, speciellt för konsumentprodukter. Många typer av angrepp, exempelvis överbelastningsattacker, drabbar inte den person som äger utrustningen vilket gör att denne ofta känner liten anledning att bekymra sig om säkerheten i produkterna. Med ökande mediefokus på cyberangrepp och sårbarheter kan mycket väl konsumenternas medvetenhet om effekterna av bristande cybersäkerhet öka och därmed även de krav de ställer på tillverkarna.

Det finns diskussioner på EU-nivå om att införa en märkning, ”Trusted IoT Label”, för IoT-produkter som uppfyller vissa krav. Denna är tänkt att bygga på samma grundtanke som energimärkningen av exempelvis vitvaror, där egenskaperna presenteras på ett tydligt sätt för konsumenterna för att underlätta deras val och styra det mot säkrare produkter.

En annan väg att gå är lagstiftning och regleringar. En möjlighet är att utforma regleringen liknande systemet med obligatorisk CE-märkning av produkter som säljs inom EU. CE-märkningen lägger stort ansvar på tillverkare och importörer av produkter, något som överlag visat sig fungera bra inom exempelvis personsäkerhet hos elektriska produkter, maskiner och skyddsutrustning, även om det

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick

förekommer fusk där produkter CE-märks trots att de inte uppfyller kraven.

Så länge dagens låga incitament för producenterna kvarstår pekar alla tecken på att problematiken med bristande cybersäkerhet inom IoT-området kommer att fortsätta under överskådlig framtid. I och med att antalet installerade IoT-enheter ökar kan det antas att följdverkningarna av osäkra IoT-enheter kommer att växa.

För vidare läsning

Farzad Kamrani, Mikael Wedlin, Ioana Rodhe, *Internet of Things: Security and Privacy Issues*, 2016, FOI-R--4362--SE.

***Strategisk utblick 7* finns att ladda ner från www.foi.se/om-foi/strategisk-utblick**

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick