# En praktisk och enkel checklista för Internet-of-Things

Version: 1.0
Publiceringsdatum: 2015-12-07

## Förord

Syftet med denna praktiska och lite enklare introduktion för att hjälpa beslutsfattare att förstå risker och hot vid införande av Internet-of-Things. Målgruppen är främst slutanvändarorganisationer. Introduktionen innehåller en del av de säkerhetsfrågor som behöver ställas och redas ut. En mer utförlig och avancerad checklista runt molnsäkerhet [1] finns för övrigt att tillgå på CSA Swedish Chapters hemsida[1]. I övrigt så har CSA globalt en utförlig skrift[2] om vad som kan vara bra att tänka på vid införande av Internet-of-Things.
Vår rekommendation presenteras i kapitel 4 i punktform. Rekommendationen kan vara bra för organisationers ledningsgrupper och styrelser att titta igenom då beslutet och ansvaret för den förändring av t ex IT-policy samt säkerhetsinformation som måste delges anställda vilar på ledningsgrupp och styrelse.
Om du som läsare har idéer till förbättringar av skriften så tag gärna kontakt med kontaktpersonen för den senaste versionen av dokumentet.

## Versionshistoria

| Version | Skribenter | Publicerad |
|---|---|---|
| 1.0 första versionen | **Projektledare/Editor**: Ove Bristrand<br>**Skribenter**: John Lindström (LTU), Ulf Berglund, och Nada Kapidzic Cicovic.<br>**Kontaktperson**: ove.bristrand@netintegrate.se | 2015-12-07 |

**Innehållsförteckning**



## Ordlista och förkortningar

| | |
|---|---|
| IaaS | Infrastructure as a Service |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |
| SECaaS | Security as a Service |
| XaaS | X as a service – används för att benämna “något” eller “allting” som en tjänst |
| Säkerhet | När termen säkerhet eller informationssäkerhet används, så inbegriper den säkerhet för IT, informationssystem och information |
| SMTP | Protokoll som gör att en nätverksansluten enhet kan sända/ta emot e-post via en SMTP-server. |

## Before you read this document…please read:

This document has been written for use mainly within Sweden, and although most of the aspects discussed are of a general nature, readers should have this fact in mind while reading.
These guidelines should not be construed as technical or legal advice on any specific facts or circumstances. The content is not exhaustive and is intended for limited general informational purposes only. The authors make no representations as to accuracy, completeness, actuality, suitability, or validity of any information and will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis with no warranties, and confers no rights. Readers should consult appropriate technical, accounting or legal consultants concerning any specific question or the relevance of the subjects discussed herein to particular factual circumstances.

[1] https://chapters.cloudsecurityalliance.org/sweden/research/
[2]https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

# 1. Introduktion

Internet-of-Things (IoT), som en del men inte CSA väljer att benämna ”Sakernas Internet”, är under både medvetet och framförallt omedvetet införande hos svenska företag och offentliga organisationer. Fördelarna kan vara nog så goda till att införa tekniken, men tyvärr glöms ofta eller negligeras riskerna helt vid införandet. Detta är inte en bra utveckling och kan medföra mer skada än nytta. Därav är syftet med denna text att ge stöd till företag och organisationer före och under införandet av IoT.

IoT är enligt analysföretaget Gartner mer värd affärsmässigt för business-to-business marknaden än för privatmarknaden, även om det skrivs mest om t ex appar till mobiltelefoner som samlas in hälsa, träningsmönster m m. Hos företag och organisationer finns system som länge funnits utan koppling till Internet såsom SCADA samt andra former av automationssystem som styr och reglerar produktionssystem, kylsystem i lager och mataffärer, ventilation och säkerhet i byggnader, trafikledning m m. Nu ansluts vissa av dem till Internet, ofta drivet av ett 24/7 servicetänk, utan att konsekvenserna alltid är klarlagda innan. De enheter och system som ansluts till Internet har antingen inbyggda anslutningar eller så ansluts de via s k gateways. Installationer sker inte alltid med hjälp av IT-personal, och de som ansluter enheter saknar ofta kunskap om IT-säkerhet samt har ej en övergripande förståelse för vad som kan bli konsekvenserna av detta. Detta kan då skapa problem, och syftet med denna skrift är just att medvetandegöra sådana problem så att de till största delen kan undvikas utan större kostnader.

# 2. Kort orientering om risker vid införande av IoT

Det finns överhängande risker vid införande av IoT oavsett omfattning, då de system som ansluts kan orsaka stor skada affärsmässigt och skada organisationens anseende. Nedan finns ett antal risker enkelt beskriva som kan uppkomma i och med anslutning av enheter till Internet, och i kapitel 3 beskriver vi några exempel på införande samt analyserar några uppenbara risker.

För att förstå hur IoT fungerar finns nedan en enkel beskrivning av enheter, programvara, samt anslutningar som kan ingå:

- En ansluten IoT-enhet till Internet kan antingen skicka eller både skicka och ta emot instruktioner och data.
- En ansluten IoT-enhet har nätverksanslutning (kabel eller trådlös) som innehåller program (drivrutin).
- En ansluten IoT-enhet innehåller operativsystem, program och t ex kommunikationsprotokollet TCP/IP.
- En ansluten IoT-enhet samt de program som ingår kan kommunicera med eller utan kryptering.
- En ansluten IoT-enhet kan skyddas av en brandvägg, men tyvärr sker det ofta utan med IoT-enheter.
- En IoT-enhet sänder data till en server eller kan kontrolleras och användas från andra Internetanslutna enheter.
- Vid anslutning till en IoT-enhet kan inloggning krävas, vilket inte alltid sker.
- Vid inloggning kan olika användare ha olika behörigheter.
- Insamling av data från den anslutna IoT-enheten kan ske till en eller flera servrar eller tjänster.
- IoT-enheter kan enkelt anslutas utan kännedom från ledning, ansvariga samt säkerhetschefer.
- Konsumentinriktade IoT-enheter kan anslutas utan kännedom till en organisations nätverk av användare.
- Hela system såsom automationssystem, vilka kan bestå av flertal undersystem och en mängd olika maskiner, sensorer och annan utrustning, kan anslutas. Idag är de hos många organisationer fysiskt separerade eller logiskt avdelade med hjälp av en brandvägg eller liknande.

Relaterat till ovan finns risker. Nedan är ett axplock av sådana:

- Olaga intrång via IoT-enheten, vars svagheter möjliggör intrånget vidare in i nätverket.
- Informationsförlust.
- Förstörelse eller förlorad produktivitet på grund av utredning rörande upptäckt intrång.
- Kostnader för omkonfigurering av alla användares inloggningsuppgifter.
- Kunder väljer att istället använda konkurrent som har bättre säkerhet.
- Förlorad tillgänglighet till viktiga IT-system och infrastruktur.

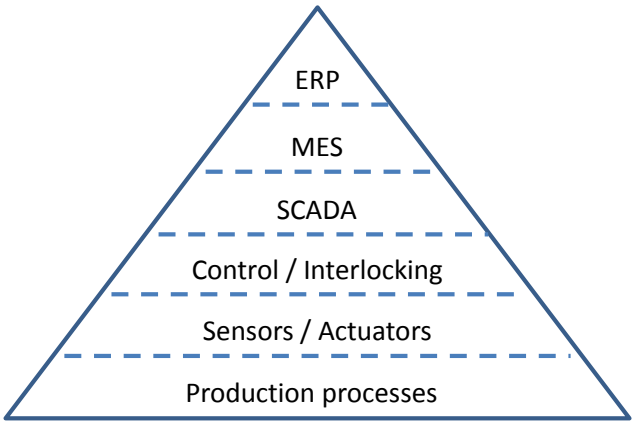
De risker som listats ovan möjliggörs av att det är många länkar med i kedjan som kan orsaka säkerhetsbrister. Det är tyvärr vanligt att många mot Internet exponerade IoT-enheters programvara inte uppdateras, trots att de ofta har enkelt skriven kod. Begränsningen i kapacitet och säkerhet hos de IoT-enheter som används är orsakade av att de dels ska dra lite ström samt vara billiga att producera.

## 3. Exempel på IoT-enheter i nätverk hos organisationer

I organisationers nätverk kan man skilja på separata enheter och hela system (som i sin tur kan innehålla delsystem och mängder av maskiner, utrustning och sensorer m.m.). Att ansluta en IoT-enhet kan öppna för säkerhetshål och intrång. Att exponera t ex en fabriks hela produktionssystem genom att ansluta automationssystemet till Internet kan i värsta fall leda till stopp och förstörelse i produktionssystemet på grund av intrång, virusattacker eller liknande.

Att i ett professionellt sammanhang, och speciellt ute i olika industrier, ansluta enheter till Internet kan istället för IoT snarare kallas industriellt IoT (Industrial IoT).

Nedan finns en översiktlig bild på hur arkitekturen kan se ut vad gäller enheter, information och system i t ex en produktionsmiljö hos ett tillverkande företag eller företag i processindustrin. Högst upp är olika former av informationssystem (ERP – Enterprise Resource Planning) som kan inbegripa det mesta från personalfrågor till beställningar från kunder, följt av produktionsrelaterade system (MES – Manufacturing Execution Systems) som styr och övervakar det som händer på ett fabriksgolv, samt nästa nivå av lägre övervakning och datainsamlingssystem (SCADA – Supervisory Control and Data Acquisition) som samlar in data från de olika undersystem, sensorer, maskiner och annan utrustning som används i produktionsprocessen.




Figur 1 ISA-95 automationspyramiden (baserad på [1, 2])

Ett intrång från de lägre nivåerna i pyramiden som går uppåt, eller åt sidorna, möjliggör då att en inkräktare kan ställa till med en hel del problem samt samla på sig information av olika slag.

### *Olika exempel på industriellt IoT*

Det första exemplet är Internetanslutning av SCADA-system eller liknande, som används för att för kommunicera med underliggande automationssystem (d.v.s. styrning/reglering/övervakning) i bland annat fastighetsbestånd, transportinfrastruktur och annan samhällskritisk infrastruktur.
Organisationen ansluter de enheter som är direkt förberedda för IoT direkt via organisationens interna LAN-nätverk som är anslutet till Internet, och de enheter som inte kan anslutas kopplas till s k gateways för anslutning till nätverket.

Funktionen som organisationens fastighetstekniker vill kunna styra och övervaka är bland annat:

- Kylsystem för datahallar.
- Övervakningskameror vid lastkaj, garage samt ingång till datahallar.
- Kylsystem för samtliga lokaler.
- Fläktar i garaget.
- Öppning/stängning av garagedörr samt dörr vid lastkaj.

Samtliga system ansluts av personal på fastighetsavdelningen till det trådlösa nätverket som organisationen har över hela fastigheten. De flesta system kan styras via den inbyggda webbserver som ingår i enheterna. Dessa enheter får fastighetsavdelningen hjälp med av sin leverantör att istället för anslutning via det trådlösa nätverket så ansluts de via en router med inbyggt 4G-modem. Den brandvägg som finns i routern med 4G konfigureras så att det går att ansluta till de enheter som anslutits till kylsystemet för datahallar samt dörrar i garage och lastkaj från valfri dator på Internet oavsett

plats i världen. För att enkelt testa installationen ändras inte inloggning i webbserver vilket sedan glöms bort och systemet är nu vidöppet. Det krävs inte mycket sökning på Internet för att få fram standardlösenord på anslutna enheter, och i värsta fall har de inget lösenord utan enbart användarnamnet ”admin”.

De risker som här kan uppstå är bl.a. följande:

- Öppning och stängning av garageport samt lastkaj nattetid.
- Stänga av kylsystemet i datahallar eller höja temperaturen till över 40 grader.

Ett annat exempel är olika former av produktionsutrustning, t ex en pappersmaskin på ett pappersbruk eller en masugn på ett stålverk, vilka tidigare varit anslutna till enbart interna nätverk men ej anslutna till Internet. Dessa produktionsutrustningar styrs och regleras normalt av ett processtyrningssystem, som skall hantera driften på ett sätt som skapar så optimal output med så lite onödig styrning, utsläpp/avfall och energiförbrukning som möjligt. Processtyrningssystemet, som ofta finns på MES-nivån, är ihopkopplat med de olika systemen både ovan och nedan för att kunna få in vad som skall produceras och sen utföra det med hjälp av systemen och enheterna på lägre nivåerna. Ett potentiellt intrång här i dessa system, antingen traditionellt genom att hitta svagheter i brandvägg eller via IoT-utrustning som är felaktigt ansluten till Internet och ej korrekt konfigurerad/skyddad. Ett intrång här kan ställa till det ordentligt och leda till skada om produktionsutrustningen, eller dess nära omgivning, kan styras på ett sätt som gör att den eller det som produceras går sönder eller inte blir säljbart. Här kan således skador för stora belopp uppkomma.

## *Olika exempel på ”vanlig” IoT i organisationer*

Ett exempel på vanlig IoT är om en organisations samtliga konferensrum har föråldrade projektorer för anslutning av datorer som kräver dyra serviceavtal. Istället för projektorer införskaffas och installeras Smart-TV för att vara framtidssäkra. Samtliga TV ansluts via det trådlösa nätverket till Internet.

De risker som här kan uppstå är bland annat följande:

- Flera Smart-TV sänder information om vad användaren tittar på, vilka filer som finns på anslutna USB-minnen till leverantörens servrar i USA.
- Vissa Smart-TV kan tillåta installation av appar som i sin tur kan skicka information till leverantören samt till annonsörer.

I vissa Smart-TV kan kamera och mikrofon fjärraktiveras (se artikel i Guardian [3]).

- Ett ytterligare exempel är belysning som kan styras, det finns ett exempel på hur en leverantör av IP-kontrollerade lampor blivit utsatt för attack via ett javascript som laddats ned till dator när användaren besökte en hemsida. Datorn sitter på samma nätverk som belysningen och den trojan som installeras kan då släcka belysningen på kontoret kan styras. Läs artikel i Tripwire[3].

## *Hur säkerhetsmedvetna är organisationers ledningsgrupper kring Internet-of-Things*

Förståelsen för att säkra kommunikationen från ”obemannade” enheter såsom IoT-enheter, som är anslutna internt hos organisationer, är än så länge tämligen obefintlig. De flesta har byggt säkerhet för attacker från Internet med brandväggar och virusskydd. Det påvisas i en rapport som utfördes av företaget Tripwire med 404 IT medarbetare samt 302 chefer i USA och UK under 2014. Rapporten påvisar att chefer har en mycket låg oro över risker med IoT på organisationen medan IT medarbetare hade lite högre oro. Rapporten kan laddas ned och finns sammanfattad på Tripwires hemsida[4].

[3] http://www.tripwire.com/state-of-security/security-awareness/3-internet-of-things-security-nuances-you-may-not-have-considered/

[4] http://www.tripwire.com/company/news/press-release/study-critical-infrastructure-executives-complacent-about-internet-of-things-security/

# 4. Checklista

Att involvera IT-personal samt säkerhetsansvariga vid införande av IOT-enheter är att rekommendera. Rekommenderat är även att personal i organisationen som t ex fastighetstekniker, produktions/underhållsingenjörer med flera får utbildning om vilka risker som kan uppstå, och att alltid vara medvetna om risker vid installation av alla IoT-enheter till nätverket på organisationen. En mer utförlig guide rörande detta finns att tillgå i t ex [4].

Nedan finns ett antal punkter som ledningsgrupper och andra berörda bör gå igenom **innan man ansluter** några enheter till Internet:

- Den viktigaste åtgärden är en revidering av organisationens IT-policy så den täcker IoT-enheter. Det som ska ingå är grunden för nästa steg som inte får negligeras. Eventuellt kan även informationssäkerhetspolicyn behöva uppdateras.
- Utbildning av samtliga anställda behövs för att öka säkerhetsmedvetande om risker samt uppmana till anmälande av alla symptom på säkerhetshot.
- Revidering av organisationen med hänsyn på ansvar och befogenheter vid införande av IoT-enheter.
- Utökad utbildning av IT-personal, utvecklare av interna system, säkerhetsansvariga samt fastighetstekniker och receptionister i säkerhetsmedvetande samt en orientering av risker med IoT.
- Kontinuerlig säkerhetsanalys av samtliga enheters kommunikation, samt även en analys och inventering av anslutningar med routrar som kommunicerar via mobila datanätverk som 4G.
- Vilka delar av organisationen måste/behöver vi exponera mot Internet? Varför och vad får vi ut för affärsnytta av det? Överstiger affärsnyttan riskerna?

En enkel checklista rörande säkerhet **vid anslutning** av enheter till Internet kan delas in i fem steg:

1. Säker uppstartat av IoT-enheten kan göras/påvisas med hjälp av t ex certifikat som verifierar att endast program som är godkända startas. Det ska minska risken för att spionprogram och andra oönskade program startas i enheten.
2. Sätta korrekt behörighet och åtkomst till IoT-enheten i sig samt vad enheten kan utföra internt i organisationens nätverk. Att det är självklart att byta standardlösenord borde vara självklart samt att begränsa att en IoT-enhet inte ska kunna kommunicera med organisationens servrar.
3. Isolering av IoT-enheter på nätverket är en åtgärd som enkelt kan skapas med dagens smarta switchar i form av VLAN-teknik på samma sätt som organisationer ofta skyddar kritiska servrar från att nås via Internet. Att inte låta alla datorer på organisationen kunna komma åt IoT-enheter som utför uppgifter såsom t ex att öppna och stänga dörren till lastkajen.
4. Brandväggar saknas ofta i IoT-enheter och det uppmanas ibland att öppna brandväggar för att det ska gå att ansluta via Internet till enheterna så att personal med beredskap enkelt ska kunna åtgärda problem hemifrån. Det saknas även program för att kontrollera vad som kommunicerar med en IoT-enhet, och det har vid flera analyser visat sig att IoT-enheter inte bara innehåller en webb-server utan även en öppen e-post server. I början av 2014 skrevs det en del om kylskåp som skickade skräppost, det visade sig att de hade öppna SMTP-servrar som kunde nås av samtliga på Internet för att skicka e-post. Ett skydd av brandväggar hade hindrat det problemet.
5. Uppdateringar av programvara är extremt viktigt, och trots det är det få IoT-enheter som uppdateras kontinuerligt samt att det utförs säkerhetsanalyser i form av penetrationstester.

Sammanfattningsvis kan det sägas att man bör undersöka vilka risker IoT-enheter innebär innan de installeras och börjar användas vare sig i professionella sammanhang eller hemmavid i sitt uppkopplade eller smarta hus. En genomgång och riskbedömning, utifrån hur teknikutvecklingen och kunskaperna om hur intrång genomförs förändras över tid, bör genomföras regelbundet eller vid behov. Behovet uppstår tydligt då särskilda händelser i omvärlden sker såsom intrång hos andra organisationer som använder samma utrustning.

# 5. Källhänvisning

Fler dokument liknande detta kan hittas antingen på CSAs hemsida: https://cloudsecurityalliance.org/ liksom på CSA Swedish Chapters hemsida: https://chapters.cloudsecurityalliance.org/sweden/research/


[1] ISA-95 (2015), ISA-95 automation structure, available at http://www.isa-95.com last – senaste åtkomst 22-Jan-2015.

[2] ProcessIT.EU (2013), ProcessIT.EU Roadmap, available at: http://www.processit.eu/european-roadmap-for-industrial-process-automation - senaste åtkomst 15-Jan-2015.

[3] The Guardian (2015), Samsung smart TVs send unencrypted voice recognition data across internet, tillgängligt hos: http://www.theguardian.com/technology/2015/feb/19/samsung-smart-tvs-send-unencrypted-voice-recognition-data-across-internet - senaste åtkomst 23-Nov-2015

[4] CSA (2015), Security guidance for early adopters of the Internet-of-Things, April 2015, tillgängligt hos: https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf - senaste åtkomst 23-Nov-2015